



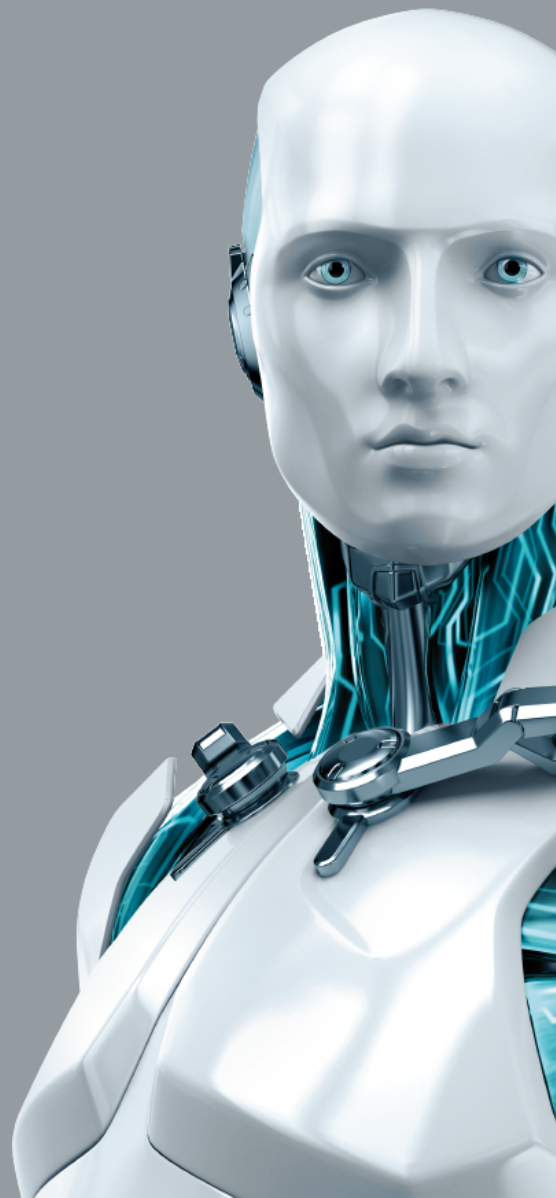
ENDPOINT SECURITY

FOR WINDOWS

Руководство пользователя

Microsoft® Windows® 10/8.1/8/7/Vista

[Щелкните здесь, чтобы загрузить актуальную версию этого документа](#)



ESET ENDPOINT SECURITY 7

© ESET, spol. s r. o., 2018

Программное обеспечение ESET Endpoint Security разработано компанией ESET, spol. s r. o.

Дополнительные сведения см. на веб-сайте www.eset.com.

Все права защищены. Запрещается воспроизведение, сохранение в информационных системах и передача данного документа или любой его части в любой форме и любыми средствами, в том числе электронными, механическими способами, посредством фотокопирования, записи, сканирования, а также любыми другими способами без соответствующего письменного разрешения автора.

ESET, spol. s r. o. оставляет за собой право изменять любые программные продукты, описанные в данной документации, без предварительного уведомления.

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

Версия 15.08.2018

Содержание

1. ESET Endpoint Security 7	8
1.1 Системные требования	8
1.2 Профилактика	9
2. Документация для пользователей, подключенных с помощью ESET Remote Administrator	10
2.1 ESET Remote Administrator Server	11
2.2 Веб-консоль	11
2.3 Прокси-сервер	12
2.4 Агент	12
2.5 RD Sensor	13
3. Использование только продукта ESET Endpoint Security	14
3.1 Установка с помощью средства ESET AV Remover	14
3.1.1 ESET AV Remover	14
3.1.2 Ошибка во время удаления с помощью средства ESET AV Remover	17
3.2 Установка	18
3.2.1 Расширенная установка	20
3.3 Установка продукта с помощью ERA (командная строка)	23
3.4 Активация программы	25
3.5 Сканирование компьютера	26
3.6 Обновление до новой версии	26
3.7 Руководство для начинающих	27
3.7.1 Пользовательский интерфейс	27
3.7.2 Настройка обновлений	30
3.7.3 Настройка зон	32
3.7.4 Инструменты контроля доступа в Интернет	32
3.8 Часто задаваемые вопросы	33
3.8.1 Обновление программы ESET Endpoint Security	33
3.8.2 Активация ESET Endpoint Security	33
3.8.3 Активация нового продукта с использованием текущих учетных данных	34
3.8.4 Удаление вируса с компьютера	34
3.8.5 Разрешение обмена данными определенному приложению	35
3.8.6 Создание задачи в планировщике	36
3.8.7 Планирование задачи сканирования (каждые 24 часа)	36
3.8.8 Подключение ESET Endpoint Security к ESET Remote Administrator	37
3.8.9 Настройка зеркала	37
3.8.10 Как мне обновить свою систему до Windows 10, если у меня установлен продукт ESET Endpoint Security?	37
3.8.11 Использование режима переопределения	38
3.8.12 Активация удаленного мониторинга и управления	40
3.9 Работа с ESET Endpoint Security	42
3.9.1 Компьютер	44
3.9.1.1 Модуль обнаружения	44
3.9.1.1.1 Действия при обнаружении заражения	45
3.9.1.2 Общий локальный кэш	47
3.9.1.3 Защита файловой системы в режиме реального времени	48
3.9.1.3.1 Дополнительные параметры ThreatSense	49

3.9.1.3.2	Уровни очистки	49
3.9.1.3.3	Проверка модуля защиты в режиме реального времени	50
3.9.1.3.4	Момент изменения конфигурации защиты в режиме реального времени	50
3.9.1.3.5	Решение проблем, возникающих при работе защиты файловой системы в режиме реального времени	50
3.9.1.4	Сканирование компьютера	51
3.9.1.4.1	Средство запуска выборочного сканирования	52
3.9.1.4.2	Ход сканирования	54
3.9.1.4.3	Журнал сканирования компьютера	55
3.9.1.5	Контроль устройств	56
3.9.1.5.1	Редактор правил для контроля устройств	56
3.9.1.5.2	Добавление правил контроля устройств	57
3.9.1.6	Съемные носители	59
3.9.1.7	Сканирование в состоянии простоя	60
3.9.1.8	Система предотвращения вторжений на узел	60
3.9.1.8.1	Дополнительные настройки	63
3.9.1.8.2	Интерактивное окно HIPS	64
3.9.1.8.3	Обнаружено потенциальное поведение программы-шантажиста	64
3.9.1.9	Режим презентации	65
3.9.1.10	Сканирование файлов, исполняемых при запуске системы	65
3.9.1.10.1	Автоматическая проверка файлов при запуске системы	66
3.9.1.11	Защита документов	66
3.9.1.12	Исключения	67
3.9.1.13	Параметры ThreatSense	68
3.9.1.13.1	Исключения	73
3.9.2	Сеть	73
3.9.2.1	Файервол	75
3.9.2.1.1	Режим обучения	76
3.9.2.2	Профили файервола	77
3.9.2.2.1	Профили, назначаемые сетевым адаптерам	78
3.9.2.3	Настройка и использование правил	78
3.9.2.3.1	Правила файервола	79
3.9.2.3.2	Работа с правилами	80
3.9.2.4	Доверенная зона	81
3.9.2.5	Настройка зон	81
3.9.2.6	Известные сети	81
3.9.2.6.1	Редактор известных сетей	82
3.9.2.6.2	Аутентификация сети: конфигурация сервера	85
3.9.2.7	Ведение журнала	85
3.9.2.8	Установка соединения: обнаружение	85
3.9.2.9	Решение проблем с помощью персонального файервола ESET	86
3.9.2.9.1	Мастер устранения неполадок	87
3.9.2.9.2	Ведение журнала и создание правил и исключений на основе журнала	87
3.9.2.9.2.1	Создание правил на основе журнала	87
3.9.2.9.3	Создание исключений на основе уведомлений файервола	87
3.9.2.9.4	Расширенное ведение журналов PCAP	88
3.9.2.9.5	Решение проблем с фильтрацией протоколов	88
3.9.3	Интернет и электронная почта	89
3.9.3.1	Фильтрация протоколов	90
3.9.3.1.1	Клиенты Интернета и электронной почты	90
3.9.3.1.2	Исключенные приложения	91
3.9.3.1.3	Исключенные IP-адреса	92
3.9.3.1.4	SSL/TLS	92

Содержание

3.9.3.1.4.1	Шифрованное соединение SSL	93
3.9.3.1.4.2	Список известных сертификатов	94
3.9.3.1.4.3	Список приложений, отфильтрованных с помощью SSL/TLS	94
3.9.3.2	Защита почтового клиента	95
3.9.3.2.1	Почтовые клиенты	95
3.9.3.2.2	Протоколы электронной почты	96
3.9.3.2.3	Предупреждения и уведомления	97
3.9.3.2.4	Защита от спама	98
3.9.3.2.4.1	«Черный» список/«белый» список/список исключений	99
3.9.3.2.4.2	Добавление адресов в «белый» и «черный» списки	100
3.9.3.2.4.3	Пометка сообщений как спама или не спама	100
3.9.3.3	Защита доступа в Интернет	101
3.9.3.3.1	Веб-протоколы	102
3.9.3.3.2	Управление URL-адресами	102
3.9.3.4	Защита от фишинга	103
3.9.4	Контроль доступа в Интернет	105
3.9.4.1	Правила	105
3.9.4.1.1	Добавление правил контроля доступа в Интернет	106
3.9.4.2	Группы категорий	107
3.9.4.3	Группы URL-адресов	108
3.9.5	Обновление программы	108
3.9.5.1	Настройка обновлений	112
3.9.5.1.1	Профили обновления	114
3.9.5.1.2	Откат обновления	114
3.9.5.1.3	Режим обновления	115
3.9.5.1.4	HTTP-сервер	116
3.9.5.1.5	Параметры подключения	116
3.9.5.1.6	Зеркало обновлений	117
3.9.5.1.6.1	Обновление с зеркала	119
3.9.5.1.6.2	Устранение проблем при обновлении с зеркала	121
3.9.5.2	Создание задач обновления	121
3.9.6	Служебные программы	122
3.9.6.1	Файлы журнала	123
3.9.6.1.1	Поиск в журнале	124
3.9.6.2	Настройка прокси-сервера	125
3.9.6.3	Планировщик	125
3.9.6.4	Статистика защиты	127
3.9.6.5	Наблюдение	128
3.9.6.6	ESET SysInspector	129
3.9.6.7	ESET LiveGrid®	129
3.9.6.8	Запущенные процессы	131
3.9.6.9	Сетевые подключения	133
3.9.6.10	Отправка образцов на анализ	134
3.9.6.11	Уведомления по электронной почте	135
3.9.6.12	Карантин	137
3.9.6.13	Microsoft Windows Update	138
3.9.6.14	ESET CMD	138
3.9.7	Интерфейс	139
3.9.7.1	Элементы интерфейса	140
3.9.7.2	Настройка доступа	142
3.9.7.3	Предупреждения и уведомления	143
3.9.7.3.1	Ошибка «Конфликт дополнительных настроек»	144

3.9.7.4	Значок на панели задач	145
3.9.7.5	Контекстное меню	146
3.10	Для опытных пользователей	146
3.10.1	Диспетчер профилей	146
3.10.2	Диагностика	147
3.10.3	Импорт и экспорт параметров	148
3.10.4	Командная строка	149
3.10.5	Сканирование в состоянии простоя	151
3.10.6	ESET SysInspector	151
3.10.6.1	Знакомство с ESET SysInspector	151
3.10.6.1.1	Запуск ESET SysInspector	151
3.10.6.2	Интерфейс пользователя и работа в приложении	152
3.10.6.2.1	Элементы управления программой	152
3.10.6.2.2	Навигация в ESET SysInspector	154
3.10.6.2.2.1	Сочетания клавиш	155
3.10.6.2.3	Сравнение	156
3.10.6.3	Параметры командной строки	157
3.10.6.4	Сценарий обслуживания	158
3.10.6.4.1	Создание сценария обслуживания	158
3.10.6.4.2	Структура сценария обслуживания	159
3.10.6.4.3	Выполнение сценариев обслуживания	161
3.10.6.5	Часто задаваемые вопросы	162
3.10.6.6	ESET SysInspector как часть приложения ESET Endpoint Security	163
3.10.7	Удаленный мониторинг и управление	163
3.10.7.1	Командная строка RMM	164
3.10.7.2	Список команд JSON	166
3.10.7.2.1	получить состояние защиты	166
3.10.7.2.2	получить сведения о приложении	167
3.10.7.2.3	получить сведения о лицензии	170
3.10.7.2.4	получить журналы	170
3.10.7.2.5	получить состояние активации	172
3.10.7.2.6	получить сведения о сканировании	172
3.10.7.2.7	получить конфигурацию	174
3.10.7.2.8	получить состояние обновления	175
3.10.7.2.9	запуск сканирования	176
3.10.7.2.10	запуск активации	177
3.10.7.2.11	запуск деактивации	178
3.10.7.2.12	запуск обновления	178
3.10.7.2.13	настройка конфигурации	179
3.11	Глоссарий	180
3.11.1	Типы угроз	180
3.11.1.1	Вирусы	180
3.11.1.2	Черви	180
3.11.1.3	Троянские программы	181
3.11.1.4	Руткиты	181
3.11.1.5	Рекламные программы	181
3.11.1.6	Шпионские программы	182
3.11.1.7	Упаковщики	182
3.11.1.8	Потенциально опасные приложения	182
3.11.1.9	Потенциально нежелательные приложения	183
3.11.1.10	Ботнет	185

Содержание

3.11.2	Типы удаленных атак	186
3.11.2.1	Атаки червей	186
3.11.2.2	DoS-атаки	186
3.11.2.3	Сканирование портов	186
3.11.2.4	Атака путем подделки записей кэша DNS	186
3.11.3	Электронная почта	187
3.11.3.1	Рекламные объявления	187
3.11.3.2	Мистификации	187
3.11.3.3	Фишинг	188
3.11.3.4	Распознавание мошеннических сообщений	188
3.11.3.4.1	Правила	188
3.11.3.4.2	«Белый» список	189
3.11.3.4.3	«Черный» список	189
3.11.3.4.4	Список исключений	189
3.11.3.4.5	Контроль на стороне сервера	189
3.11.4	Технологии ESET	190
3.11.4.1	Блокировщик эксплойтов	190
3.11.4.2	Расширенный модуль сканирования памяти	190
3.11.4.3	ESET LiveGrid®	190
3.11.4.4	Защита от ботнетов	191
3.11.4.5	Блокировщик эксплойтов Java	191
3.11.4.6	Защита от атак на основе сценариев	191
3.11.4.7	Защита от программ-вымогателей	191
3.11.4.8	Система обнаружения DNA Detections	192
3.11.4.9	Модуль сканирования UEFI	192

1. ESET Endpoint Security 7

ESET Endpoint Security 7 представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Новейшая версия модуля сканирования ThreatSense® в сочетании со специализированными модулями файрвола и защиты от спама обеспечивает скорость и точность, необходимые для безопасности компьютера. Таким образом, продукт представляет собой интеллектуальную систему непрерывной защиты от атак и вредоносных программ, которые могут угрожать безопасности компьютера.

ESET Endpoint Security 7 — это комплексное решение для обеспечения безопасности, являющееся результатом долгих усилий, направленных на достижение оптимального сочетания максимальной степени защиты с минимальным влиянием на производительность компьютера. Современные технологии, основанные на применении искусственного интеллекта, способны превентивно противодействовать заражениям вирусами, шпионскими, троянскими, рекламными программами, червями, руткитами и другими атаками из Интернета без влияния на производительность компьютера и перерывов в работе.

ESET Endpoint Security 7 предназначено в первую очередь для использования на рабочих станциях в средах небольших предприятий. Использование ESET Endpoint Security в сочетании с ESET Remote Administrator в корпоративной среде позволяет с легкостью управлять любым количеством клиентских рабочих станций, применять политики и правила, отслеживать обнаруживаемые угрозы и удаленно конфигурировать клиентов с любого подключенного к сети компьютера.

1.1 Системные требования

Для правильной работы ESET Endpoint Security система должна отвечать перечисленным ниже аппаратным и программным требованиям (настройки программы по умолчанию).

Процессор:

- 32-разрядный (x86) или 64-разрядный (x64) процессор, 1 ГГц и выше.

Операционная система: Microsoft® Windows® 10/8.1/8/7/Vista.

- Операционная система и пакет обновления должны поддерживаться установленной версией продукта ESET.
- Операционная система и другое ПО, установленное на компьютере, должны соответствовать системным требованиям.
- 0,3 ГБ свободной системной памяти (см. примечание 1).
- 1 ГБ свободного места на диске (см. примечание 2).
- Минимальное разрешение дисплея должно составлять 1024 x 768.
- Подключение через Интернет или локальную сеть к источнику обновления продукта (см. примечание 3).

Хотя и существует возможность установить и запустить продукт в системах, которые не соответствуют этим требованиям, рекомендуется сначала провести тестирование возможностей использования на основании требований к производительности.

i ПРИМЕЧАНИЕ.

1. Программа может использовать больше памяти, если на сильно зараженном компьютере память не используется для других задач, а также когда в программу импортируются огромные списки данных (например, «белые» списки URL-адресов).
2. Дисковое пространство, необходимое, чтобы загрузить программу установки, установить программу и хранить копию установочного пакета в данных программы, а также резервные копии обновлений программы, которые нужны для функции отката. Программа может использовать больше дискового пространства при разных настройках (например, когда хранится большее количество резервных копий обновлений, когда хранятся дампы памяти или огромные количества записей журнала) либо на зараженном компьютере (например, вследствие использования функции карантина). Рекомендуется поддерживать достаточное количество свободного дискового пространства, чтобы обеспечить возможность обновления операционной системы и обновления программы ESET.
3. Хотя это и не рекомендуется, программу можно обновить вручную со съемного носителя.

1.2 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 ESET LiveGrid®, тысячи новых уникальных заражений появляются ежедневно. Они созданы для обхода существующих мер безопасности и приносят доход их авторам за счет других пользователей. Специалисты вирусной лаборатории ESET ежедневно анализируют такие угрозы, подготавливают и выпускают обновления для непрерывного улучшения 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 модуль обнаружения обновляется каждый день.

Следуйте основным правилам безопасности

Это наиболее эффективное и полезное правило — 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.

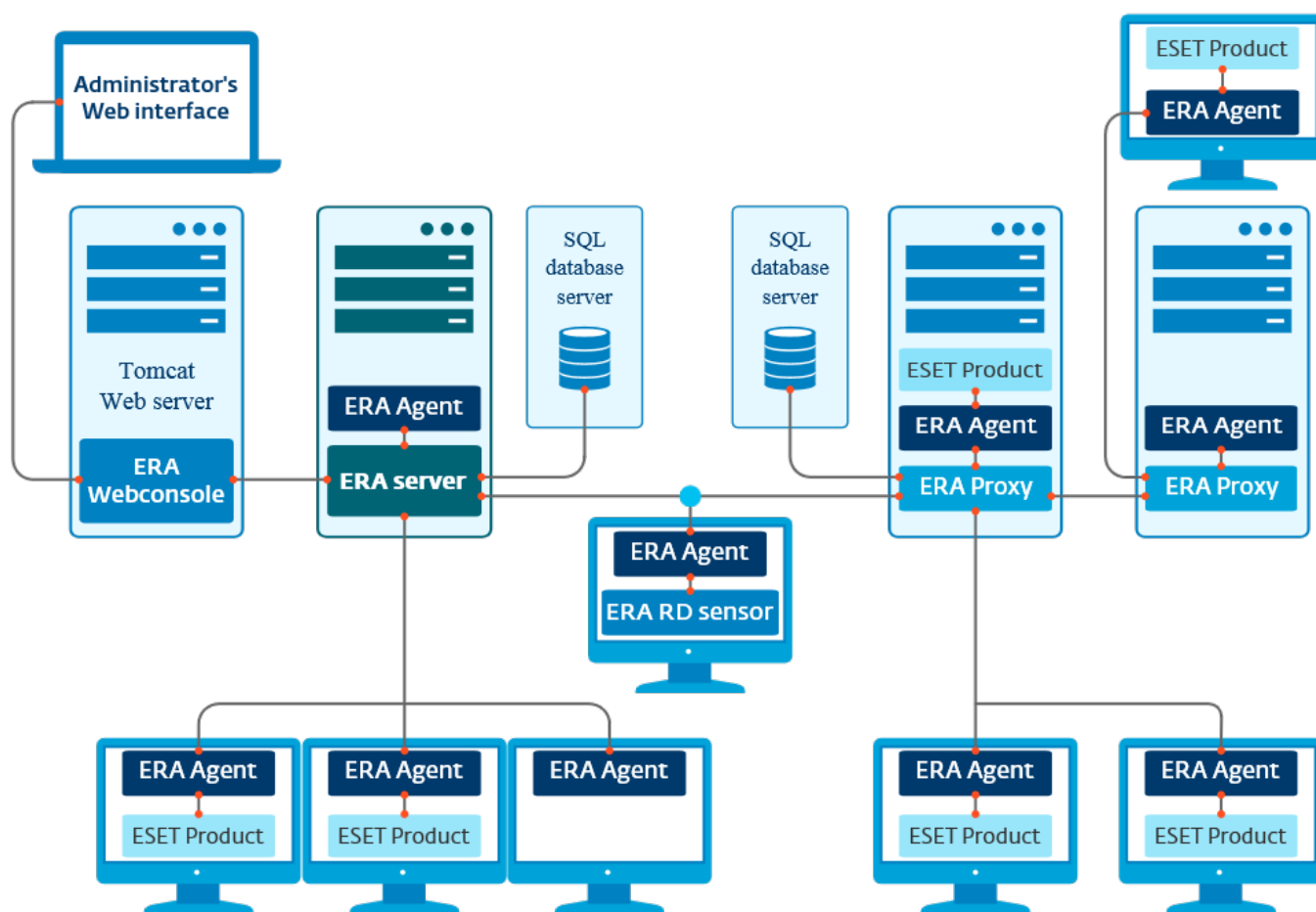
- Не посещайте подозрительные веб-сайты с множеством всплывающих окон и анимированной рекламой.
- Будьте осторожны при установке бесплатных программ, пакетов кодеков и т. п.. Используйте только безопасные программы и посещайте безопасные веб-сайты.
- Будьте осторожны, открывая вложения в сообщения электронной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

2. Документация для пользователей, подключенных с помощью ESET Remote Administrator

ESET Remote Administrator (ERA) — это приложение, позволяющее осуществлять централизованное управление продуктами ESET, установленными в сетевой среде. Система управления задачами ESET Remote Administrator позволяет установить на удаленные компьютеры решения ESET для обеспечения безопасности и быстро реагировать на новые проблемы и угрозы. Приложение ESET Remote Administrator не предоставляет защиту от вредоносного кода, а полагается на то, что на каждом клиенте установлено и используется решение ESET.

В решениях ESET для обеспечения безопасности предусмотрена поддержка сетей, использующих несколько платформ различных типов. В сети могут сосуществовать операционные системы Microsoft, Linux и Mac OS, а также системы, работающие на мобильных устройствах (мобильные телефоны и планшеты).

На рисунке ниже представлен пример архитектуры сети, защищенной решениями ESET для обеспечения безопасности. Этими решениями управляет приложение ERA.



i ПРИМЕЧАНИЕ.

Дополнительные сведения см. в [справке о решении ESET Remote Administrator в Интернете](#).

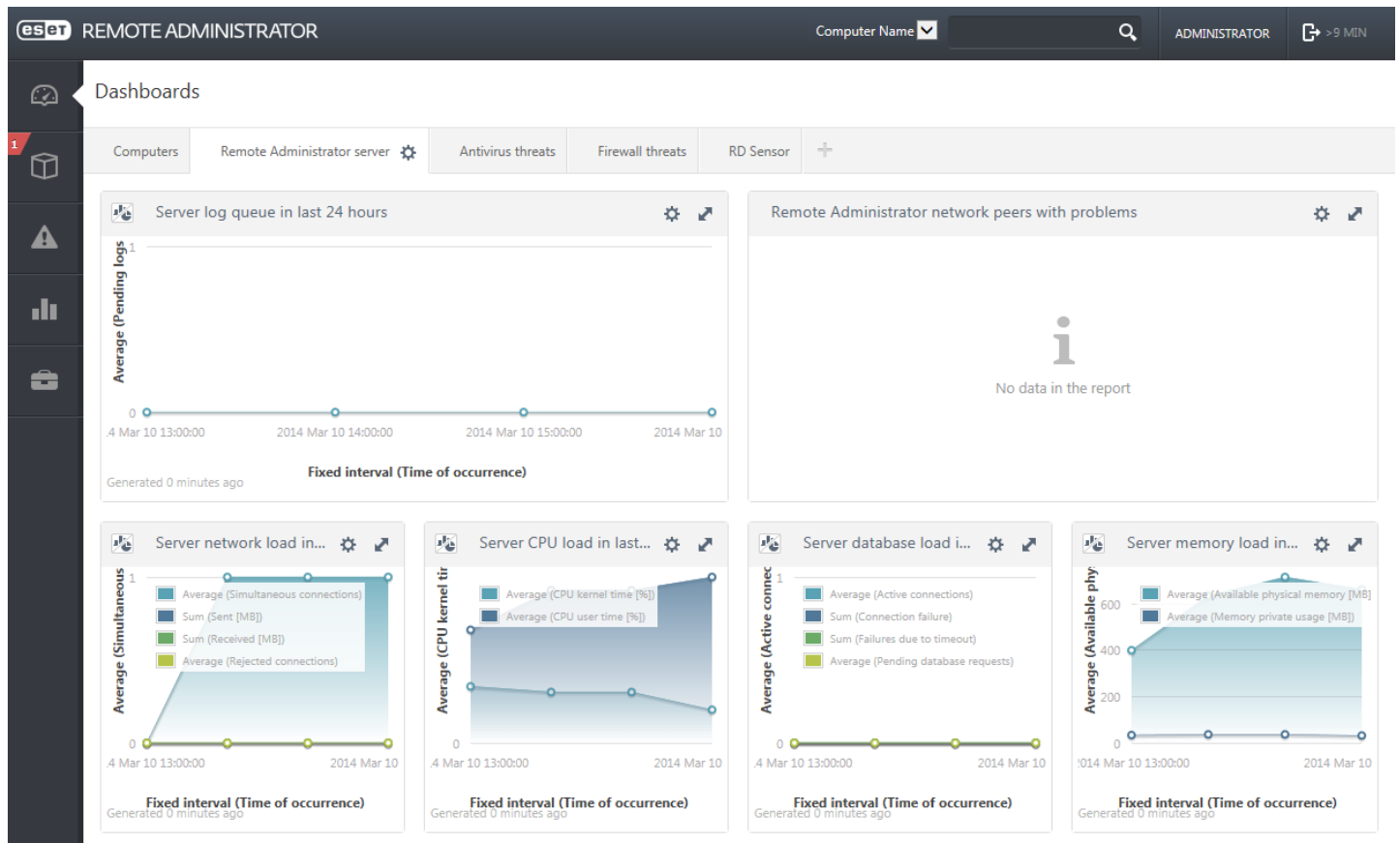
2.1 ESET Remote Administrator Server

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

2.2 Веб-консоль

Веб-консоль ERA — это приложение с веб-интерфейсом, которое отображает данные, полученные с [сервера ERA](#), и позволяет управлять решениями безопасности ESET в вашей сети. Доступ к веб-консоли можно получить с помощью браузера. В ней отображаются общие сведения о статусах клиентов в сети. Кроме того, веб-консоль можно использовать для удаленного развертывания решений ESET на неуправляемых компьютерах. Если разрешить доступ к веб-серверу из Интернета, ESET Remote Administrator можно будет использовать практически в любом месте и на любом устройстве.

Вот так выглядит панель мониторинга веб-консоли.



В верхней части консоли расположено средство **Быстрый поиск**. Из раскрывающегося меню выберите пункт **Имя компьютера**, **Адрес IPv4/IPv6** или **Имя угрозы**, введите поисковую фразу в текстовом поле и щелкните значок лупы или нажмите клавишу **ВВОД**, чтобы выполнить поиск. Вы будете перенаправлены в раздел **Группы**, где будут показаны результаты поиска.

i ПРИМЕЧАНИЕ.

Дополнительные сведения см. в [справке о решении ESET Remote Administrator в Интернете](#).

2.3 Прокси-сервер

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

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

Чтобы обеспечить надлежащую работу прокси-сервера ERA, на главном компьютере, на который вы устанавливаете прокси-сервер ERA, нужно установить агент ESET, а сам компьютер нужно подключить к верхнему уровню сети (к серверу ERA или прокси-серверу ERA верхнего уровня, если такой имеется).

2.4 Агент

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

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

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

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

i ПРИМЕЧАНИЕ.

Прокси-сервер ESET имеет собственного агента, отвечающего за обмен данными с клиентами, другими прокси-серверами и сервером.

2.5 RD Sensor

RD (Rogue Detection) Sensor — это входящий в ESET Remote Administrator инструмент поиска компьютеров в сети. Он позволяет быстро добавлять новые компьютеры в ESET Remote Administrator без необходимости искать и добавлять их вручную. Каждый обнаруженный в сети компьютер отображается в веб-консоли и добавляется в стандартную группу **Все**. После этого вы можете выполнять последующие действия уже с отдельными клиентскими компьютерами.

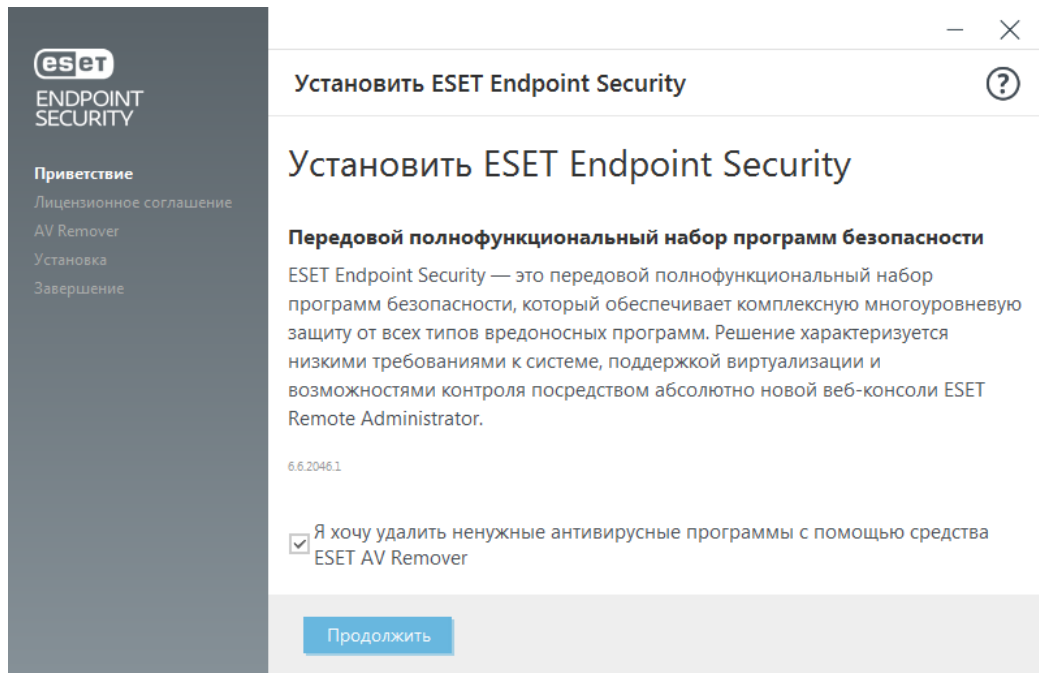
Компонент RD Sensor пассивно прослушивает сеть, обнаруживает находящиеся в ней компьютеры и направляет информацию о них серверу ERA. Затем сервер ERA проверяет, являются ли обнаруженные ПК неизвестными или уже находятся под его управлением.

3. Использование только продукта ESET Endpoint Security

Эта часть руководства предназначена для пользователей, использующих ESET Endpoint Security без ESET Remote Administrator. Доступность тех или иных функций и возможностей ESET Endpoint Security полностью зависит от прав учетной записи пользователя.

3.1 Установка с помощью средства ESET AV Remover

Прежде чем приступить к установке, необходимо удалить все установленные на компьютере приложения для обеспечения безопасности. Установите флажок **Я хочу удалить ненужные антивирусные программы с помощью средства ESET AV Remover**. Средство ESET AV Remover просканирует систему и удалит все [поддерживаемые программы](#). Если вы хотите установить ESET Endpoint Security без использования ESET AV Remover, нажмите кнопку **Продолжить**, не устанавливая этот флажок.



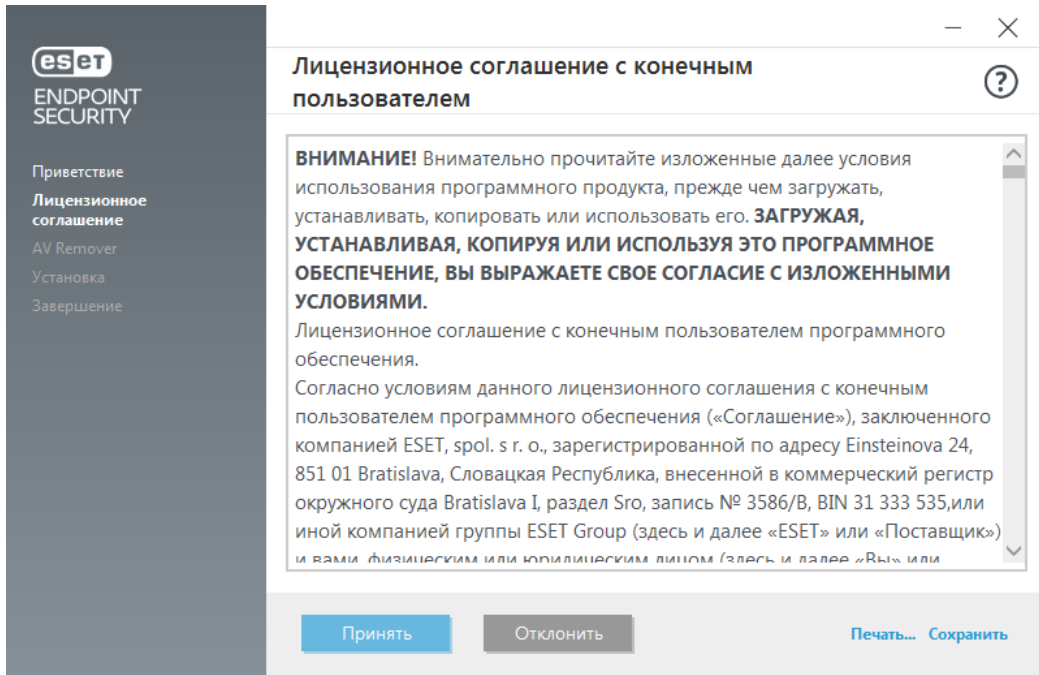
3.1.1 ESET AV Remover

Средство ESET AV Remover поможет удалить практически любую установленную в системе антивирусную программу. Процедура удаления антивирусной программы с помощью средства ESET AV Remover приведена ниже.

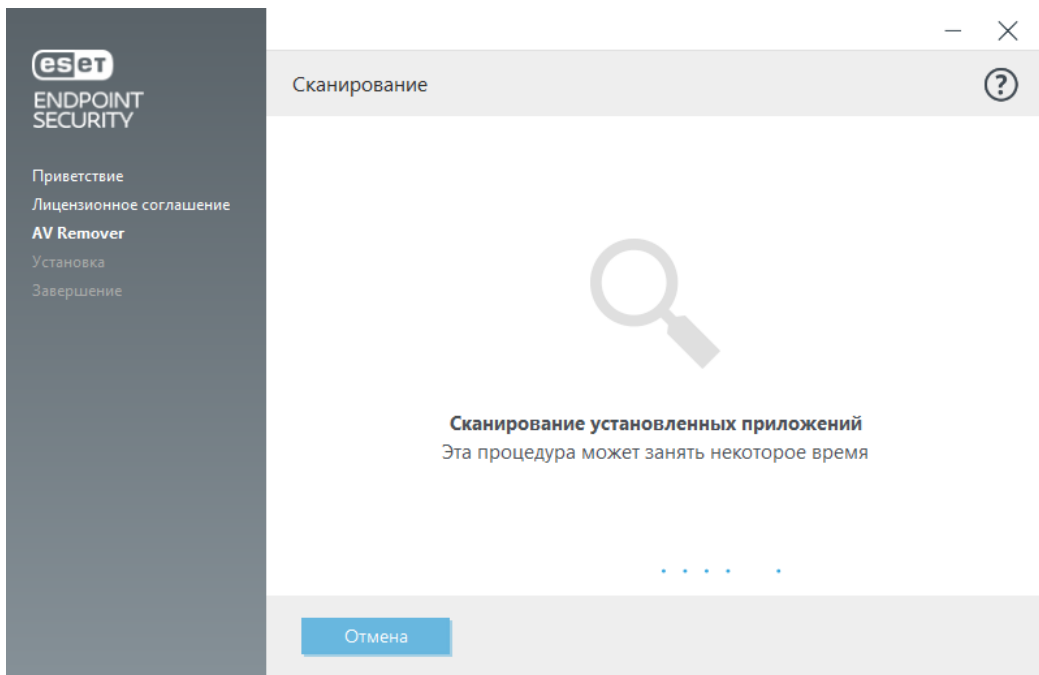
1. Чтобы просмотреть список антивирусных программ, которые можно удалить с помощью ESET AV Remover, ознакомьтесь с соответствующей [статьей базы знаний ESET](#). [Загрузите средство ESET AV Remover](#).



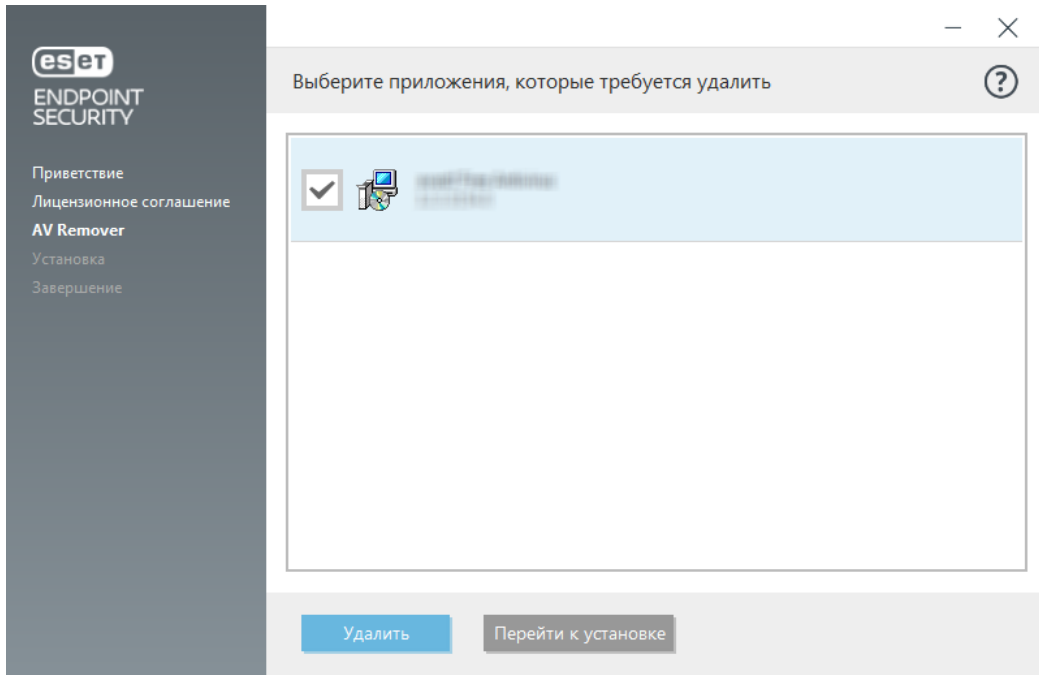
2. Прочтите лицензионное соглашение с конечным пользователем и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с его условиями. Чтобы удалить существующее приложение для обеспечения безопасности с компьютера, нажмите кнопку **Отклонить**.



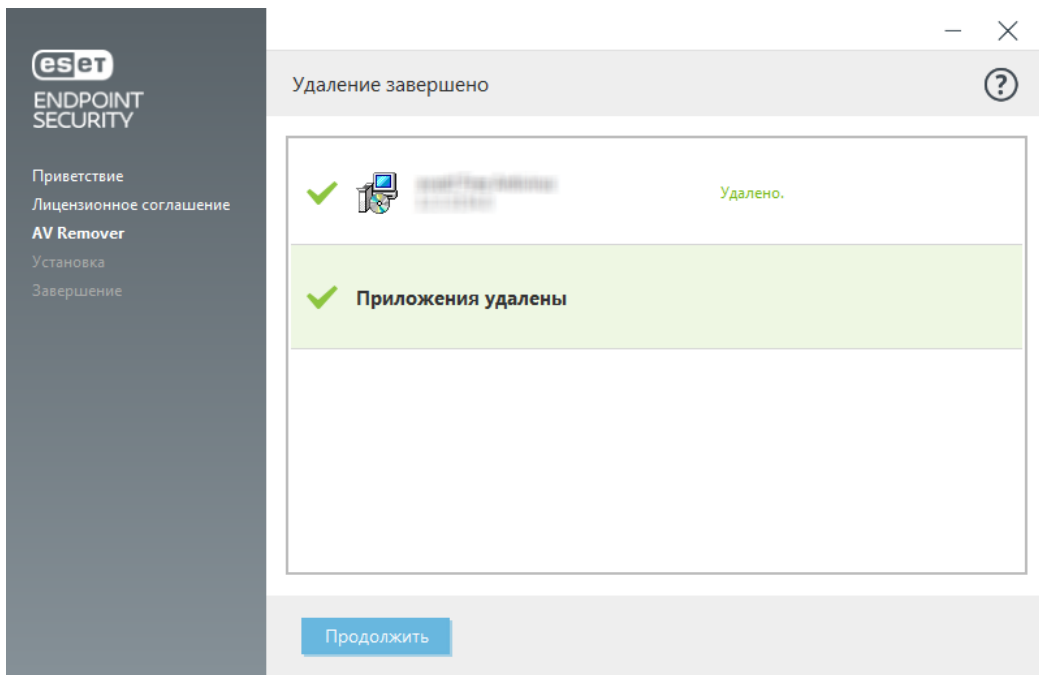
3. Средство ESET AV Remover начнет поиск установленного в системе антивирусного ПО.



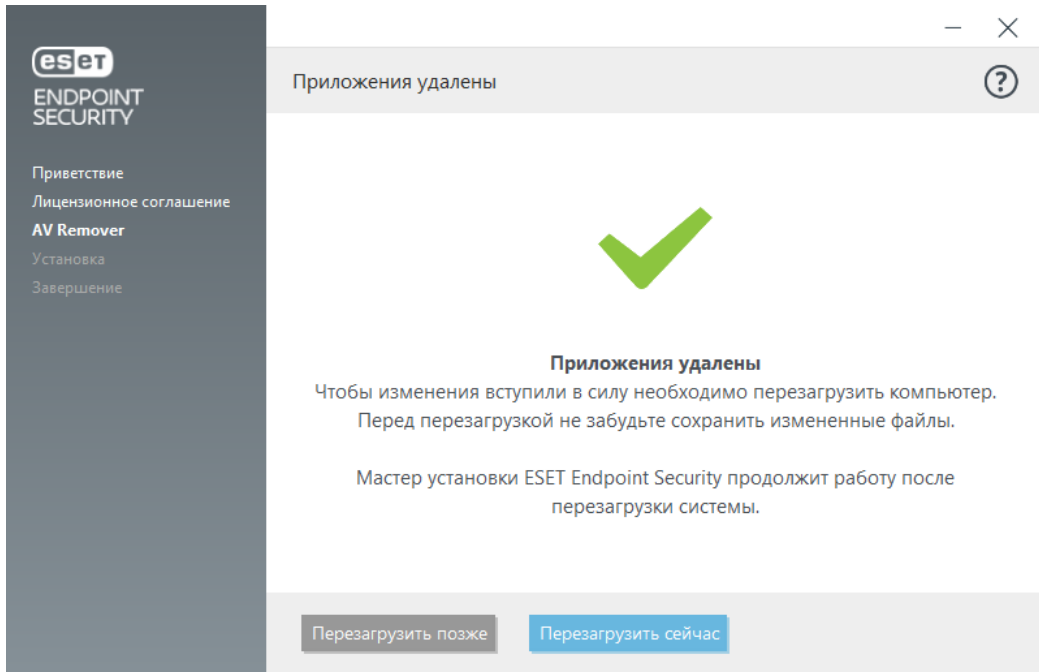
4. Выберите все обнаруженные антивирусные приложения и нажмите кнопку «Удалить». Процедура удаления может занять некоторое время.



5. После завершения удаления нажмите кнопку **Продолжить**.



6. Чтобы изменения вступили в силу, перезагрузите компьютер. Если во время удаления произошла ошибка, см. раздел настоящего руководства [Ошибка во время удаления с помощью средства ESET AV Remover](#).



3.1.2 Ошибка во время удаления с помощью средства ESET AV Remover

Если удалить антивирусную программу с помощью ESET AV Remover не удалось, появится сообщение, что средство ESET AV Remover, возможно, не поддерживает удаляемое приложение. Чтобы узнать, можно ли удалить эту программу, просмотрите список [поддерживаемых продуктов](#) или [программ удаления распространённого антивирусного ПО для Windows](#). Эти списки можно найти в базе знаний ESET.

Если удалить продукт для обеспечения безопасности не удалось или некоторые его компоненты удалены не полностью, появится предложение **Перезагрузить и повторно сканировать**. После перезагрузки появится предупреждение системы контроля учетных записей. Разрешите запуск программы, повторно просканируйте систему и удалите имеющиеся антивирусные приложения.

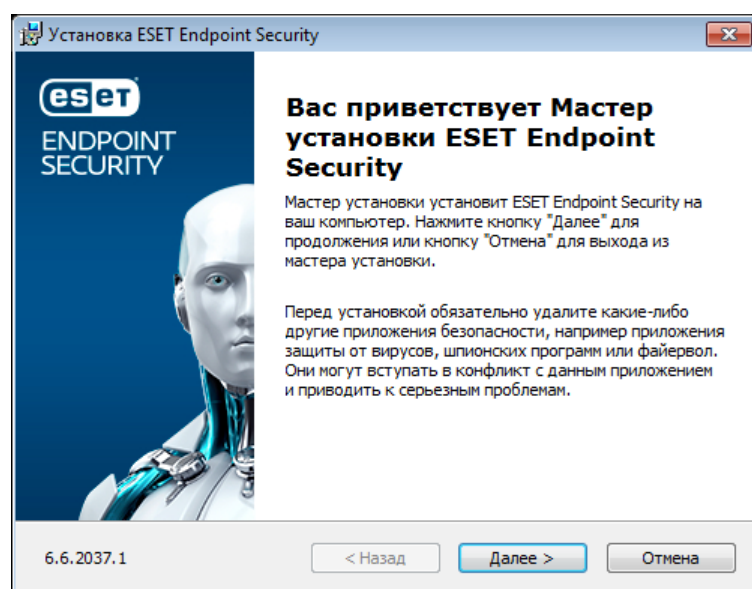
В случае необходимости обратитесь в службу поддержки клиентов ESET, создайте запрос на поддержку и подготовьте файл **AppRemover.log** (он потребуется специалистам ESET). Файл **AppRemover.log** расположен в папке **eset**. Эта папка хранится в расположении **%TEMP%**. Для доступа к нему используйте проводник Windows. Сотрудники службы поддержки клиентов ESET свяжутся с вами, как только появится возможность.

3.2 Установка

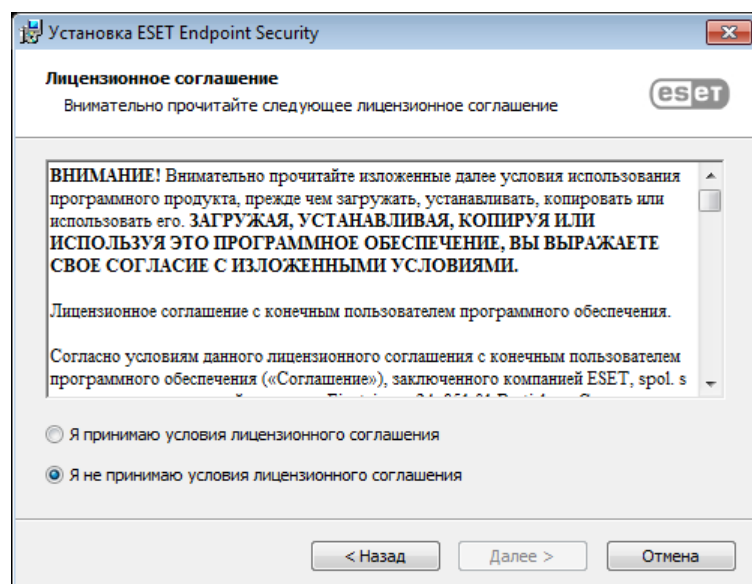
После запуска программы установки мастер установки поможет установить программу.

! ВАЖНО!

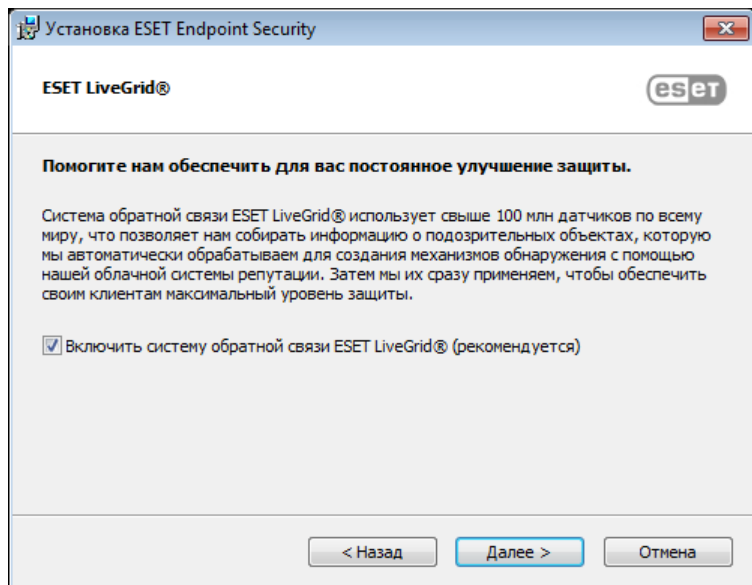
Убедитесь в том, что на компьютере не установлены другие программы защиты от вирусов. Если на одном компьютере установлено два и более решения для защиты от вирусов, между ними может возникнуть конфликт. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера. Список инструментов для удаления популярных антивирусных программ см. в нашей [статье базы знаний](#) (доступна на английском и нескольких других языках).



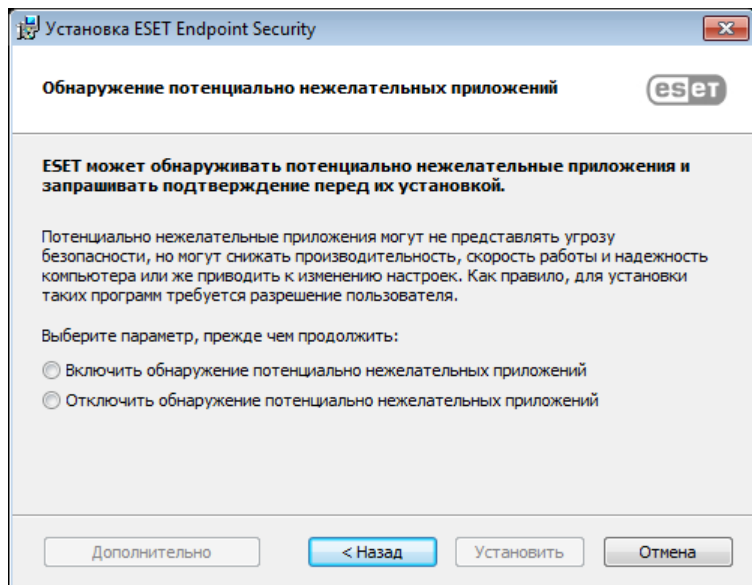
На следующем этапе на экран будет выведено лицензионное соглашение с конечным пользователем. Прочтите его и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с его условиями. Приняв условия, нажмите кнопку **Далее**, чтобы продолжить установку.



После выбора варианта «Я принимаю...» и нажатия кнопки **Далее** на экран будет выведен запрос на включение ESET LiveGrid®. ESET LiveGrid® дает возможность незамедлительно и постоянно информировать компанию ESET о новых заражениях, благодаря чему мы можем защищать своих клиентов более качественно. С помощью этой системы вы можете отправлять новые угрозы в вирусную лабораторию ESET, где они анализируются, обрабатываются и добавляются в модуль обнаружения.



Следующий шаг установки: следует настроить обнаружение потенциально нежелательных приложений, которые — хоть и не обязательно зловредные — могут негативно повлиять на поведение ОС. Дополнительные сведения см. в главе [Потенциально нежелательные приложения](#). Доступ к дополнительным настройкам можно получить, нажав **Дополнительные настройки** (это может понадобиться, например, чтобы указать определенную папку для установки приложения ESET или чтобы включить автоматическое сканирование после установки).



Последний шаг: подтверждение установки. Для этого нужно нажать **Установить**.

3.2.1 Расширенная установка

При расширенной установке можно настроить ряд параметров установки, которые при стандартной установке недоступны.

Когда вы включите обнаружение потенциально нежелательных приложений и нажмете **Дополнительные настройки**, вам будет предложено выбрать расположение для папки установки продукта. По умолчанию программа устанавливается в указанную ниже папку.

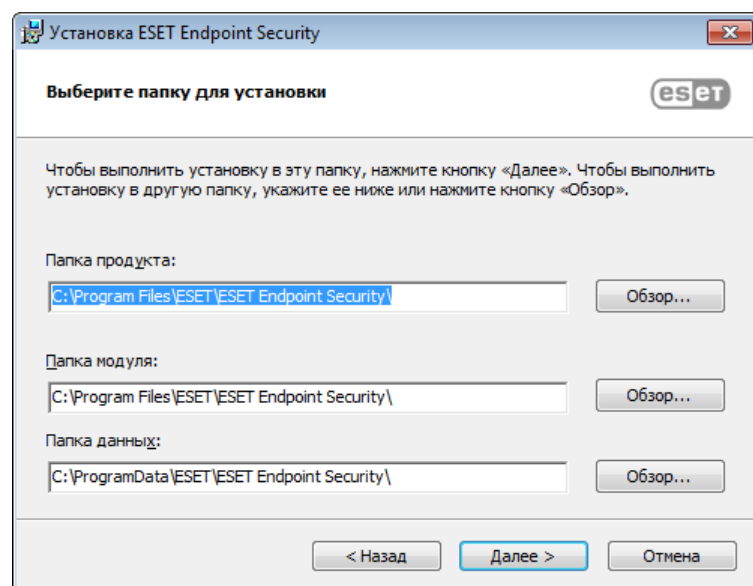
`C:\Program Files\ESET\ESET Endpoint Security\`

Можно указать расположение для модулей и данных программы. По умолчанию они устанавливаются в указанные ниже папки (в том же порядке):

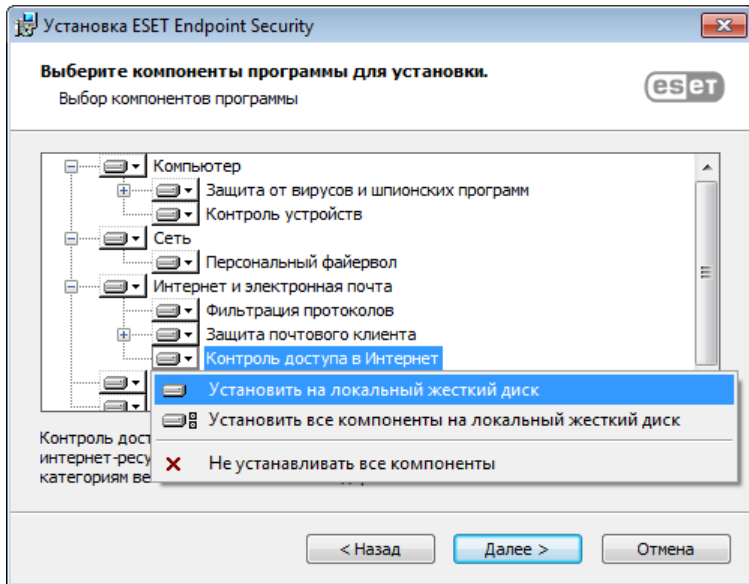
`C:\Program Files\ESET\ESET Endpoint Security\`

`C:\ProgramData\ESET\ESET Endpoint Security\`

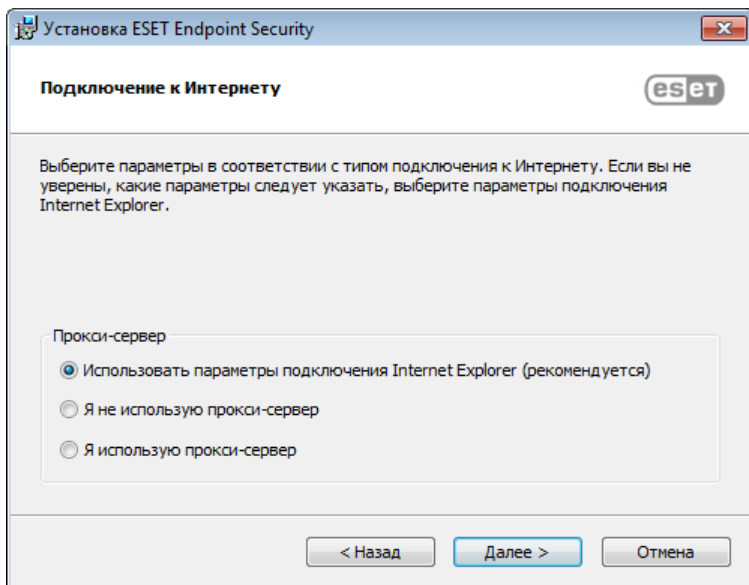
Нажмите кнопку **Обзор...**, чтобы изменить расположения (не рекомендуется).



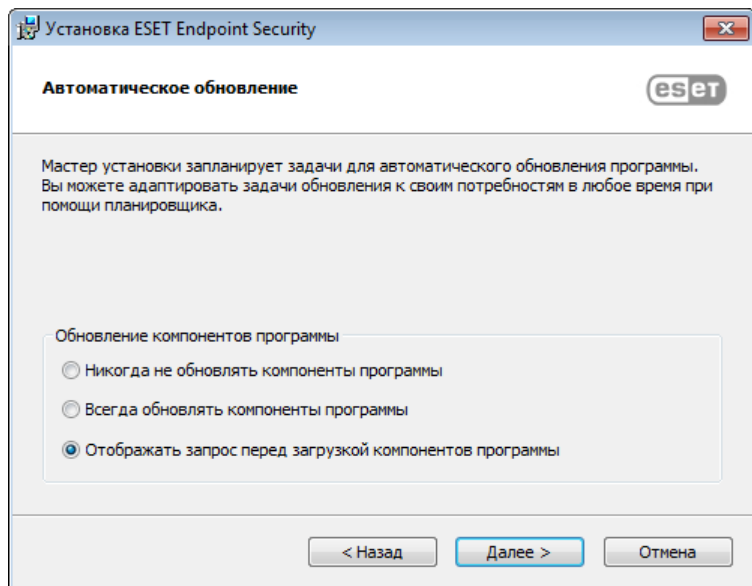
В следующем окне можно выбрать компоненты продукта, которые следует установить. В разделе [Компьютер](#) находятся в том числе такие компоненты: защита файловой системы в режиме реального времени, сканирование компьютера, защита документов и контроль устройств. Обратите внимание, что без первых двух компонентов решение для обеспечения безопасности работать не будет. В разделе [Сеть](#) предлагается установить файрвол, который отслеживает входящий и исходящий трафик и на основе правил работает с отдельными сетевыми подключениями. Файрвол также обеспечивает защиту от атак с удаленных компьютеров. Компоненты раздела [Интернет и электронная почта](#) защищают компьютер, когда вы посещаете веб-сайты и общаетесь с помощью электронной почты. Компонент [Зеркало обновления](#) можно использовать для обновления других компьютеров сети.



Для настройки параметров прокси-сервера выберите вариант **Я использую прокси-сервер** и нажмите кнопку **Далее**. Введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. 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 получения дополнительных сведений см. раздел [Прокси-сервер](#).

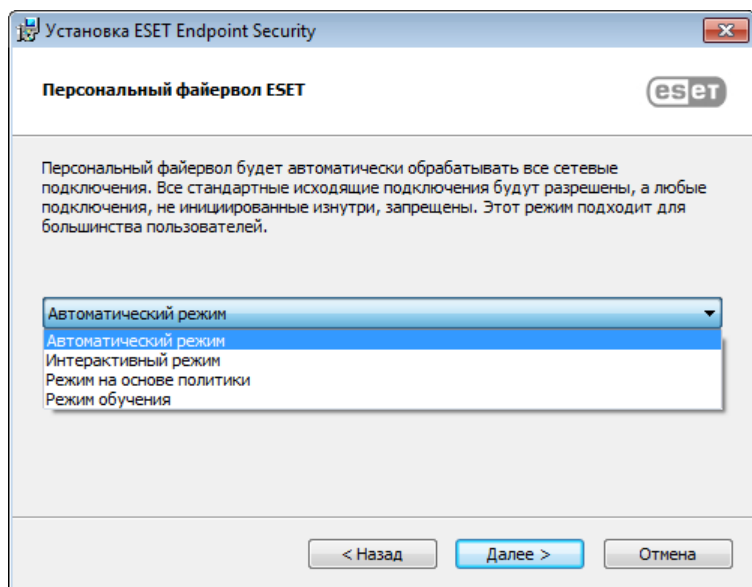


При выборочной установке можно указать, как должно происходить автоматическое обновление системы. Нажмите **Изменить...** для доступа к дополнительным параметрам.

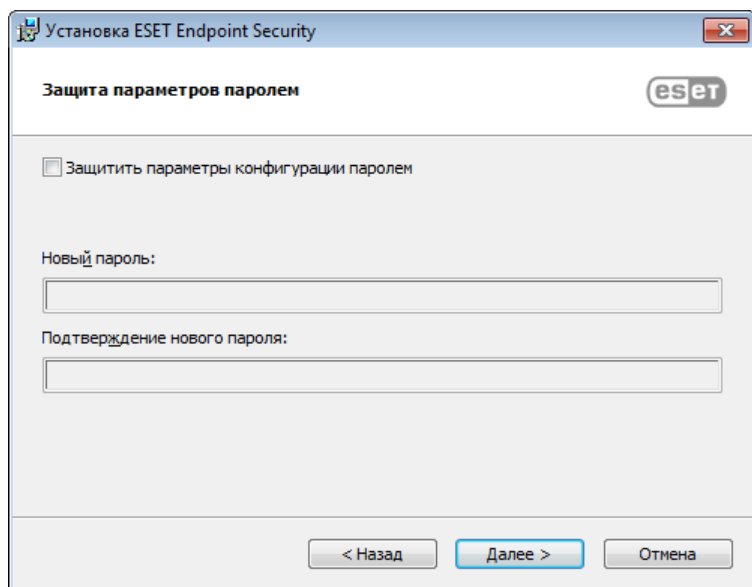


Если нет необходимости обновлять компоненты программы, выберите вариант **Никогда не обновлять компоненты программы**. Выберите параметр **Запросить подтверждение перед загрузкой компонентов программы**, чтобы перед каждой попыткой загрузить компоненты программы отображалось окно подтверждения. Для автоматической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

Далее выберите режим фильтрации для файрвола ESET. В файрволе ESET Endpoint Security есть четыре режима фильтрации. Поведение персонального файрвола зависит от выбранного режима. Кроме того, от выбранного [режима фильтрации](#) зависит степень участия пользователя в процессе.



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



Нажмите кнопку **Установить**, чтобы начать установку.

3.3 Установка продукта с помощью ERA (командная строка)

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

Поддерживаемые параметры:

APPDIR=<путь>

- Путь — действительный путь к каталогу.
- Каталог установки приложения.
- Например: `ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<путь>

- Путь — действительный путь к каталогу.
- Каталог установки данных приложения.

MODULEDIR=<путь>

- Путь — действительный путь к каталогу.
- Каталог установки модуля.

ADDLOCAL=<список>

- Установка компонентов — список необязательных компонентов, которые нужно установить локально.
- Использование с пакетами MSI компании ESET: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Дополнительные сведения о свойстве `ADDLOCAL` см. на странице <http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx>.

Правила

- **Список `ADDLOCAL`** — это разделенный запятыми список имен всех функций, которые нужно установить.
- При выборе функции, которую нужно установить, в список нужно добавить весь путь (указать все родительские функции).
- Чтобы все сделать верно, см. дополнительные правила.

Наличие функции

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

Ниже представлено дерево функций Endpoint 6.1.

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

Дополнительные правила

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

Примеры

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Список свойств CFG_:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0

- 0 — отключено, 1 — включено
- Потенциально нежелательные приложения

CFG_LIVEGRID_ENABLED=1/0

- 0 — отключено, 1 — включено
- LiveGrid

CFG_EPFW_MODE=0/1/2/3

- 0 — автоматически, 1 — интерактивный режим, 2 — политика, 3 — обучение

CFG_PROXY_ENABLED=0/1

- 0 — отключено, 1 — включено

CFG_PROXY_ADDRESS=<IP-адрес>

- IP-адрес прокси-сервера.

CFG_PROXY_PORT=<порт>

- Номер порта прокси-сервера.

CFG_PROXY_USERNAME=<имя пользователя>

- Имя пользователя для проверки подлинности.

CFG_PROXY_PASSWORD=<пароль>

- Пароль для аутентификации.

Установка с помощью SCCM, диалоговое окно отключения активации:

ACTIVATION_DLG_SUPPRESS=1

- 1 — включено (диалоговое окно не отображается).
- 0 — отключено (диалоговое окно отображается).

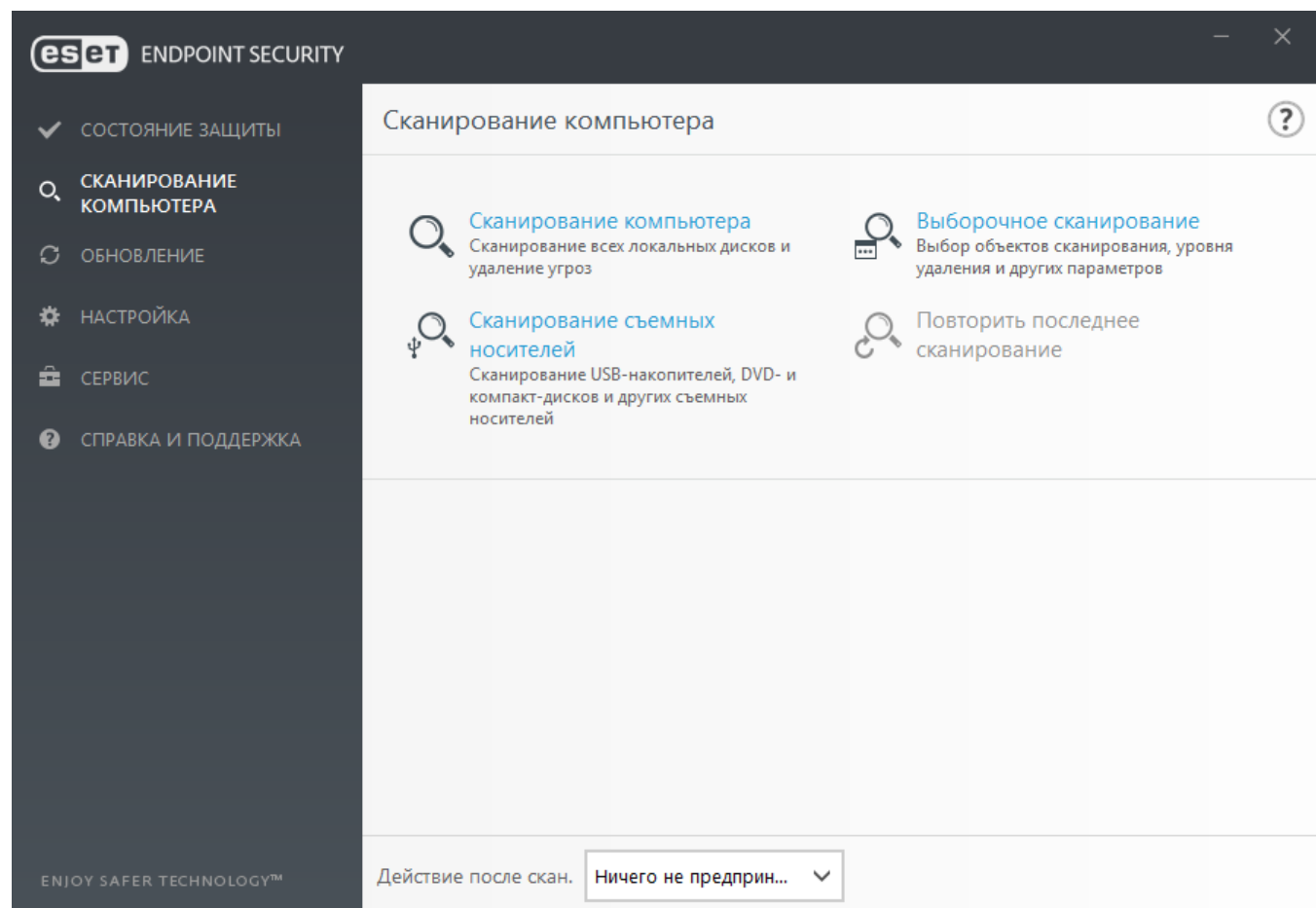
3.4 Активация программы

После завершения установки вам будет предложено активировать установленный продукт.

Выберите доступный метод активации ESET Endpoint Security. См. раздел [Активация ESET Endpoint Security](#) для получения дополнительных сведений.

3.5 Сканирование компьютера

Рекомендуется регулярно сканировать компьютер или [запланировать регулярное сканирование](#), чтобы проверять компьютер на наличие угроз. В главном окне программы выберите пункт **Сканирование компьютера**, а затем — **Сканирование Smart**. Для получения дополнительных сведений о сканировании компьютера см. раздел [Сканирование компьютера](#).



3.6 Обновление до новой версии

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

1. Автоматически путем обновления программы.
Поскольку обновления программы распространяются среди всех пользователей и могут повлиять на некоторые конфигурации компьютеров, 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 путем загрузки и установки новой версии поверх предыдущей.
3. Вручную с автоматическим развертыванием в сетевой среде посредством ESET Remote Administrator.

3.7 Руководство для начинающих

В этом разделе приводятся общие сведения о программном обеспечении ESET Endpoint Security и его основных параметрах.

3.7.1 Пользовательский интерфейс

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

Ниже описаны пункты главного меню.

Состояние защиты: этот пункт предоставляет информацию о состоянии защиты ESET Endpoint Security.

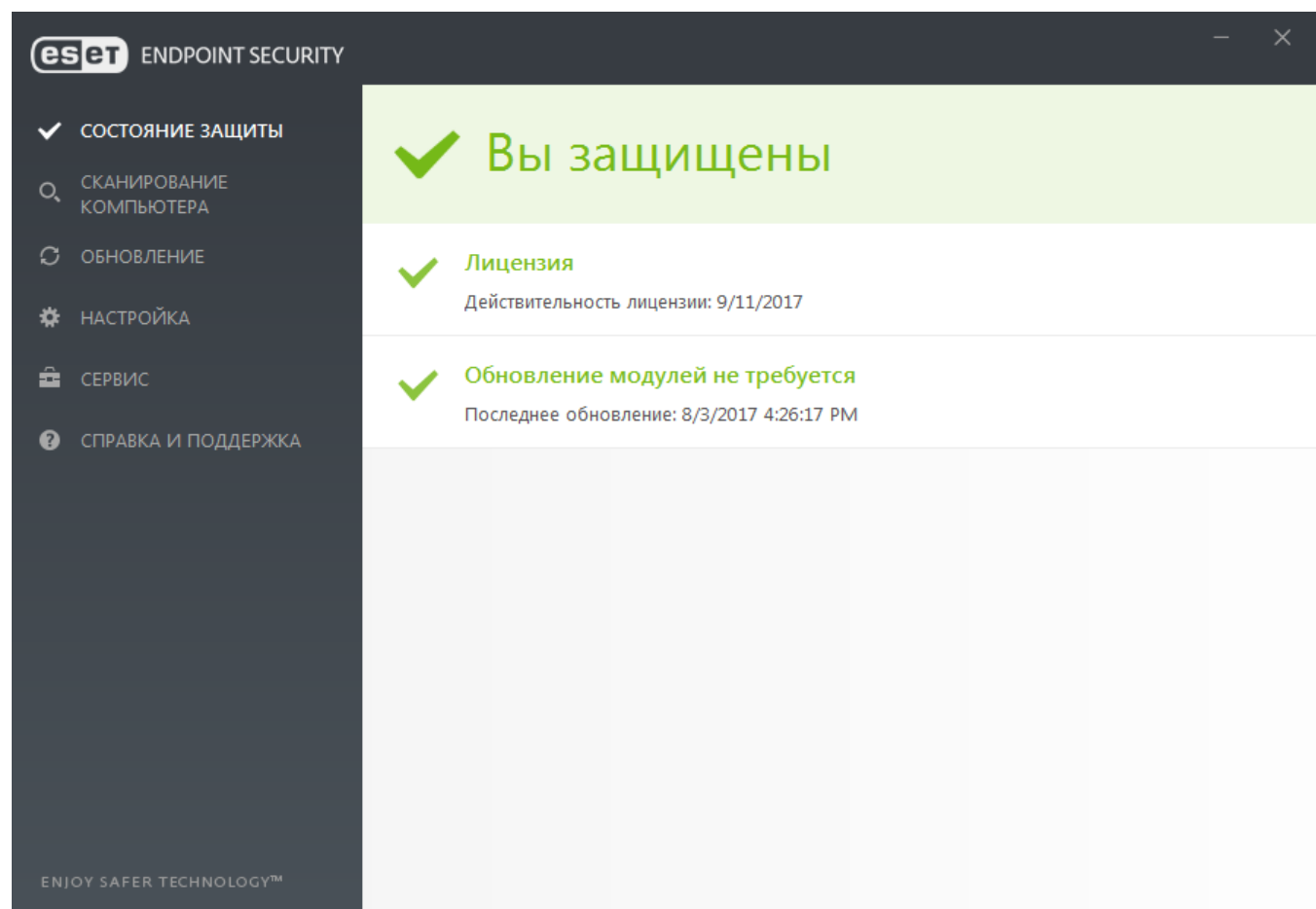
Сканирование компьютера: этот параметр позволяет настроить и запустить сканирование Smart, выборочное сканирование и сканирование съемных носителей. Также можно повторно запустить последнюю операцию сканирования.

Обновление: отображение информации о модуле обнаружения.

Настройка: настройка параметров безопасности компьютера, сети, Интернета и электронной почты.

Служебные программы: доступ к файлам журнала, статистике защиты, программам мониторинга, запущенным процессам, планировщику, карантину, сетевым подключениям, ESET SysInspector и ESET SysRescue для создания компакт-диска аварийного восстановления. Также можно отправить образец на анализ.

Справка и поддержка: доступ к файлам справки, [базе знаний ESET](#) и веб-сайту компании ESET. Также доступны ссылки на форму запроса в службу поддержки клиентов, средства поддержки и информацию об активации продукта.

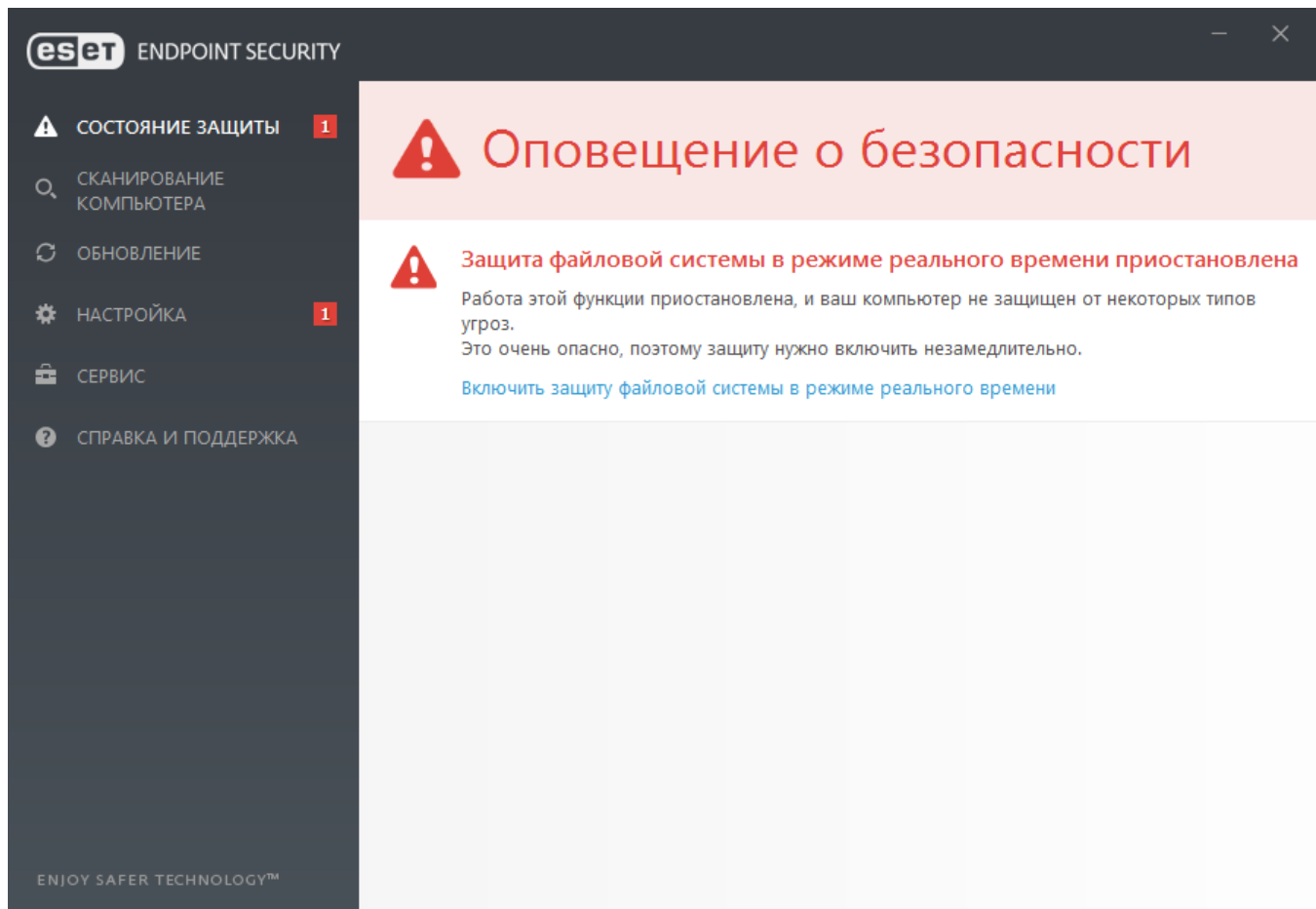


Окно **Состояние защиты** информирует пользователя об уровне безопасности и текущем уровне защиты компьютера. Зеленый значок **Максимальная защита** означает, что обеспечивается максимальная степень защиты.

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

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

Зеленая галочка отображается рядом со всеми программными модулями, которые полноценно функционируют. Красный восклицательный знак или оранжевый значок уведомления отображается, если модуль требует внимания. В верхней части окна выводятся дополнительные сведения о модуле, включая нашу рекомендацию о том, как восстановить полную функциональность. Для того чтобы изменить состояние модуля, выберите в главном меню пункт **Настройка** и щелкните нужный модуль.





Красный восклицательный знак (!) указывает, что максимальная степень защиты компьютера не обеспечивается. Этот тип уведомления может наблюдаться в следующих сценариях:

- **Защита от вирусов и шпионских программ приостановлена:** щелкните **Запустить все модули защиты от вирусов и шпионских программ**, чтобы повторно включить защиту от вирусов и шпионских программ на панели **Состояние защиты** или **Включить защиту от вирусов и шпионских программ** на панели **Настройка** в главном окне программы.
- **Защита от вирусов не работает:** ошибка инициализации модуля сканирования на наличие вирусов. Большинство модулей ESET Endpoint Security не будут функционировать должным образом.
- **Защита от фишинга не работает:** эта функция не работает, так как не активны другие нужные модули программы.
- **Файервол ESET отключен:** об этой проблеме свидетельствует наличие красного значка и уведомления системы безопасности рядом с элементом **Сеть**. Щелкните **Включить режим фильтрации**, чтобы повторно включить защиту сети.
- **Ошибка инициализации файервола:** файервол отключен из-за проблем интеграции с системой. Перезапустите компьютер как можно скорее.
- **Модуль обнаружения устарел:** используется устаревший модуль обнаружения. Обновите его.
- **Продукт не активирован или Срок действия лицензии истек:** об этих проблемах свидетельствует красный значок состояния защиты. С этого момента программа больше не сможет выполнять обновления. Чтобы продлить лицензию, рекомендуется выполнить инструкции в окне предупреждения.
- **Система предотвращения вторжений на узел (HIPS) отключена:** эта проблема указывается, если система HIPS отключена в разделе «Дополнительные настройки». Компьютер не защищен от некоторых типов угроз, и следует немедленно повторно включить защиту, нажав **Включить систему HIPS**.
- **Функция ESET LiveGrid® отключена:** эта проблема указывается, если функция ESET LiveGrid® отключена в разделе «Дополнительные настройки».
- **Регулярные обновления не запланированы:** ESET Endpoint Security не будет проверять наличие важных обновлений и получать их, если не запланировать задачу обновления.
- **Защита Anti-Stealth отключена:** щелкните **Включить защиту Anti-Stealth**, чтобы повторно включить эту функцию.
- **Защита файловой системы в режиме реального времени приостановлена:** защита в режиме реального времени отключена пользователем. Компьютер не защищен от угроз. Нажмите **Включить защиту в режиме реального времени**, чтобы повторно включить эту функцию.



Оранжевый знак «i» указывает на то, что продукт ESET требует вашего внимания в связи с не критичной проблемой. Ниже указаны возможные причины.

- **Защита доступа в Интернет отключена:** щелкните уведомление о защите, чтобы повторно включить защиту доступа в Интернет, а затем щелкните **Включить защиту доступа в Интернет**.
- **Срок действия лицензии скоро закончится:** об этой проблеме свидетельствует появление восклицательного знака на значке состояния защиты. После окончания срока действия лицензии программа больше не сможет выполнять обновления, а значок состояния защиты станет красным.
- **Защита от ботнетов приостановлена:** щелкните **Включить защиту от ботнетов**, чтобы повторно включить эту функцию.
- **Защита от сетевых атак (IDS) приостановлена:** щелкните **Включить защиту от сетевых атак (IDS)**, чтобы повторно включить эту функцию.
- **Защита от спама приостановлена:** щелкните **Включить защиту от спама**, чтобы повторно включить эту функцию.
- **Контроль доступа в Интернет приостановлен:** щелкните **Включить контроль доступа в Интернет**, чтобы повторно включить эту функцию.
- **Действует переопределение политики:** конфигурация, заданная политикой, временно переопределена, возможно, до завершения устранения неполадок. Параметры политики может переопределить только авторизованный пользователь. Дополнительные сведения см. в разделе [Использование режима переопределения](#).
- **Контроль устройств приостановлен:** щелкните **Включить контроль устройств**, чтобы повторно включить эту функцию.

Если предложенные решения не позволяют устранить проблему, выберите пункт **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 клиентов ESET. Ее специалисты оперативно ответят на ваши вопросы и помогут найти решение.

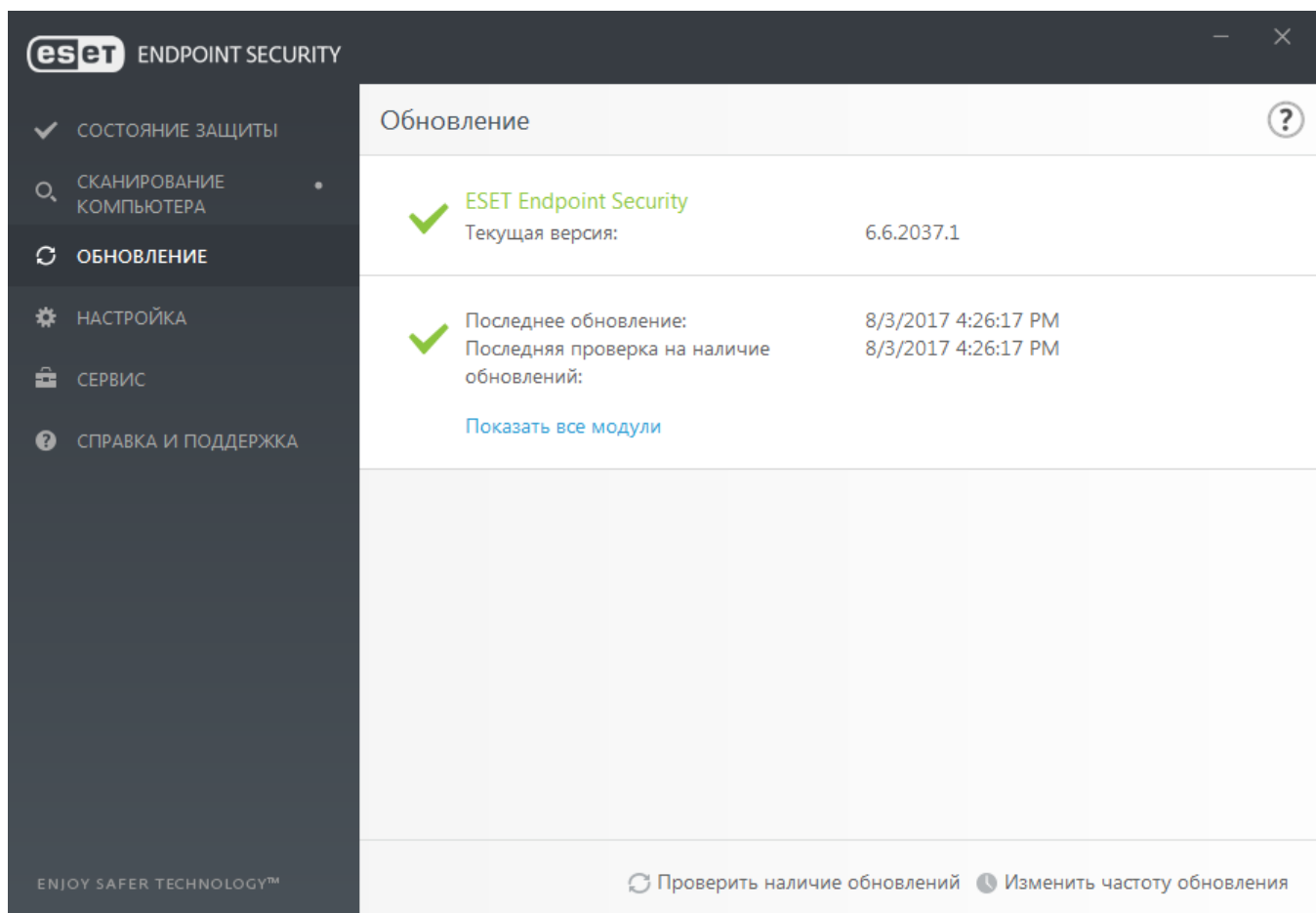
i ПРИМЕЧАНИЕ.

Если состояние относится к функции, заблокированной политикой ERA, ссылка будет неактивна.



3.7.2 Настройка обновлений

Обновление модулей является важной частью обеспечения полной защиты компьютера от вредоносного кода. Уделите особенное внимание изучению конфигурации и работы этого процесса. В главном меню выберите **Обновление > Обновить**, чтобы проверить наличие обновлений модуля.

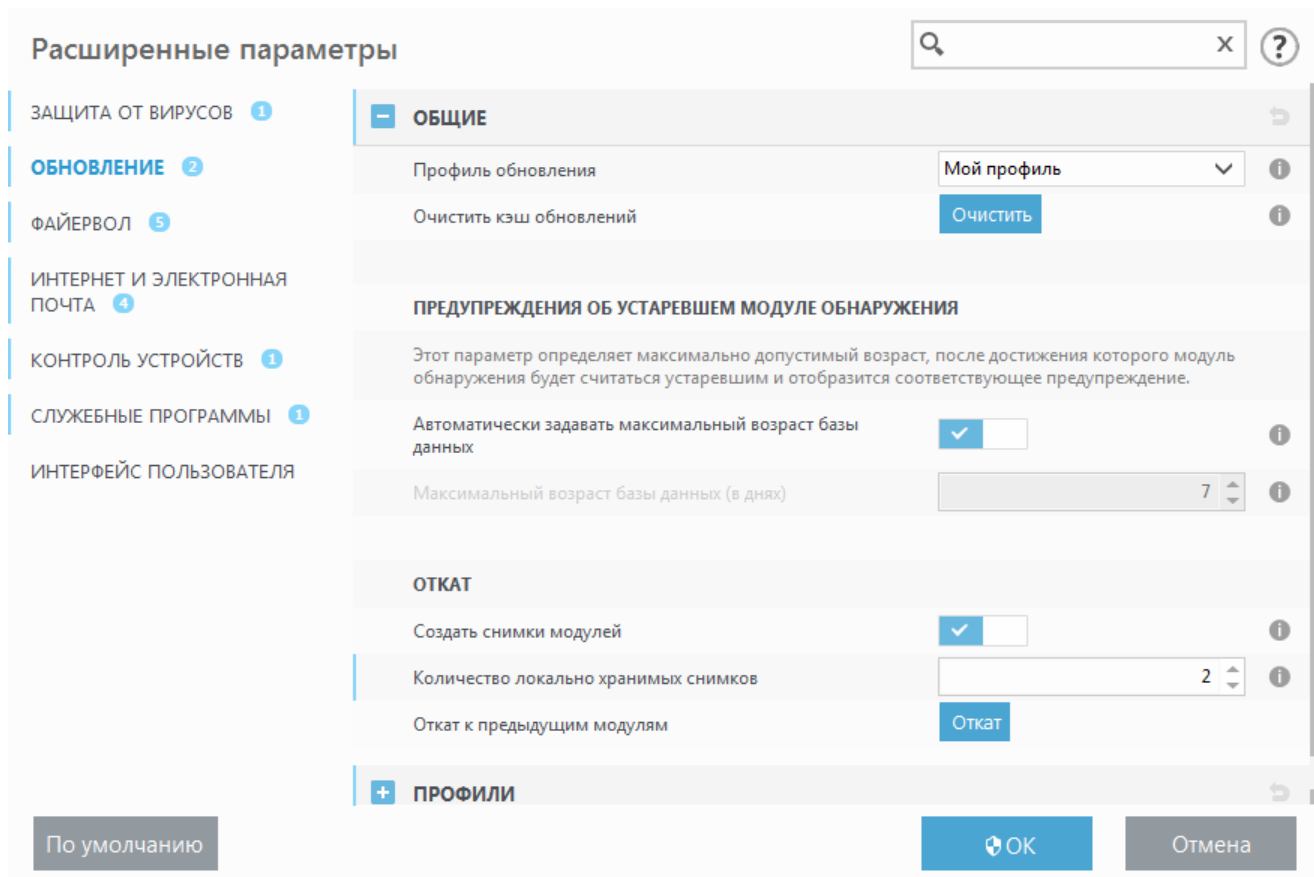
Если **Лицензионный ключ** не был введен, обновление будет невозможно. Взамен вам будет предложено активировать продукт.



The screenshot shows the 'Обновление' (Updates) window in the ESET Endpoint Security interface. The window title is 'eset ENDPOINT SECURITY'. The left sidebar contains navigation options: СОСТОЯНИЕ ЗАЩИТЫ, СКАНИРОВАНИЕ КОМПЬЮТЕРА, ОБНОВЛЕНИЕ (highlighted), НАСТРОЙКА, СЕРВИС, and СПРАВКА И ПОДДЕРЖКА. The main content area shows the update status for 'ESET Endpoint Security' with a green checkmark. It lists the current version as 6.6.2037.1 and shows the last update and check for updates on 8/3/2017 at 4:26:17 PM. A link 'Показать все модули' is visible. At the bottom, there are buttons for 'Проверить наличие обновлений' and 'Изменить частоту обновления'. The footer of the window reads 'ENJOY SAFER TECHNOLOGY™'.

Обновление	
 ESET Endpoint Security	
Текущая версия:	6.6.2037.1
 Последнее обновление:	8/3/2017 4:26:17 PM
Последняя проверка на наличие обновлений:	8/3/2017 4:26:17 PM
Показать все модули	

В окне «Дополнительные настройки» (в главном меню выберите **Настройка > Дополнительные настройки** или нажмите **F5** на клавиатуре) содержатся расширенные параметры обновления. Чтобы настроить расширенные параметры обновления, такие как режим обновления, доступ через прокси-сервер, подключение к локальной сети и настройки создания копий модуля обнаружения, щелкните в дереве дополнительных настроек пункт **Обновление**. При возникновении проблем с обновлением нажмите кнопку **Очистить**, чтобы удалить из кэша временные файлы обновления. По умолчанию в меню **Сервер обновлений** выбран параметр **Автоматический выбор**. При использовании сервера ESET рекомендуется активировать параметр **Выбирать автоматически**. Чтобы отключить отображение уведомлений на панели задач в правом нижнем углу экрана, выберите элемент **Отключить уведомления о завершении обновления**.



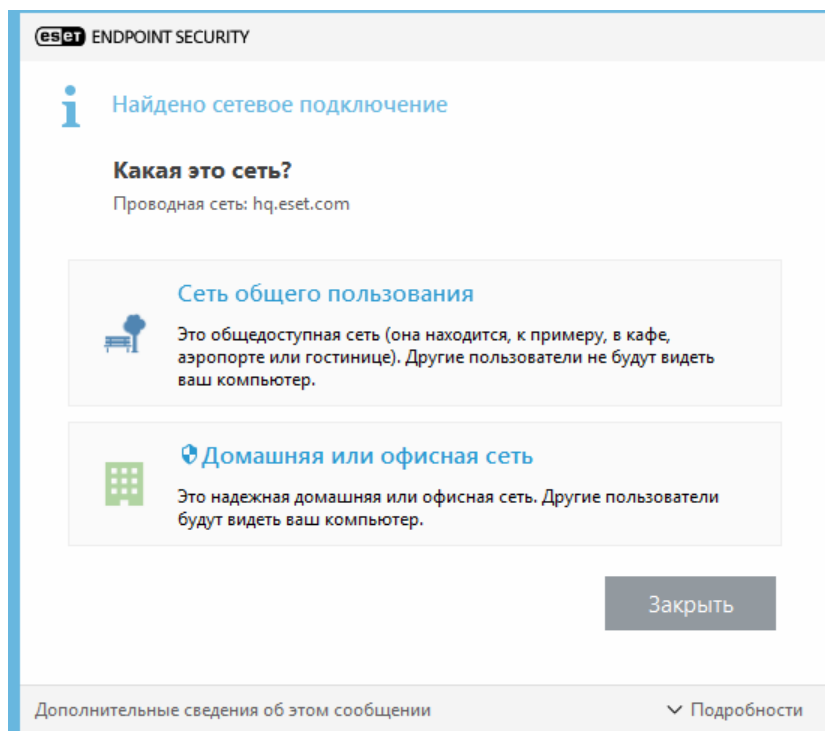
Для того чтобы использовать программу наилучшим образом, необходимо включить ее автоматическое обновление. Это возможно только в случае, если в разделе **Справка и поддержка > Активировать продукт** указан правильный **Лицензионный ключ**.

Вы можете ввести **лицензионный ключ** сразу после установки или в любое другое время. Дополнительные сведения об активации см. в статье [Активация ESET Endpoint Security](#). Учетные данные, полученные вместе с продуктом ESET для обеспечения безопасности, необходимо ввести в окне **Сведения о лицензии**.

3.7.3 Настройка зон

Необходимо настроить доверенные зоны для защиты компьютера в сетевой среде. Настройка доверенной зоны для разрешения общего доступа дает возможность предоставить доступ к компьютеру другим пользователям. Для доступа к настройкам доверенных зон выберите **Дополнительные настройки (F5) > Файервол > Зоны**.

Обнаружение доверенных зон происходит после установки ESET Endpoint Security и при каждом подключении компьютера к новой сети. Таким образом, обычно нет необходимости задавать доверенную зону. По умолчанию при обнаружении новой зоны на экран выводится диалоговое окно, позволяющее настроить уровень защиты для этой зоны.



ВАЖНО!

Неправильная настройка доверенной зоны может повлечь за собой снижение уровня безопасности компьютера.

ПРИМЕЧАНИЕ.

По умолчанию рабочие станции из доверенной зоны получают доступ к файлам и принтерам, для которых открыт общий доступ, для них разрешены входящие соединения RPC, а также доступна служба удаленного рабочего стола.

3.7.4 Инструменты контроля доступа в Интернет

Если вы уже включили контроль доступа в Интернет в ESET Endpoint Security, необходимо также настроить контроль доступа в Интернет для нужных учетных записей пользователя, чтобы обеспечить правильную работу этой функции. Обратитесь к главе [Контроль доступа в Интернет](#) для получения указаний по поводу создания специальных ограничений для клиентских рабочих станций, позволяющих защитить их от потенциально нежелательных материалов.

3.8 Часто задаваемые вопросы

Эта глава содержит ответы на некоторые из наиболее часто задаваемых вопросов и решения проблем пользователей. Щелкните ссылку на тему, которая соответствует вашей проблеме.

[Обновление ESET Endpoint Security](#)

[Активация ESET Endpoint Security](#)

[Активация нового продукта с использованием текущих учетных данных](#)

[Удаление вируса с компьютера](#)

[Разрешение обмена данными определенному приложению](#)

[Создание задачи в планировщике](#)

[Планирование задачи сканирования \(каждые 24 часа\)](#)

[Подключение продукта к ESET Remote Administrator](#)

[Настройка зеркала](#)

Если перечисленные выше разделы справки не дали ответа на ваш вопрос, попробуйте поискать по ключевым словам или фразе, которые описывают проблему, в разделах справки ESET Endpoint Security.

Если с помощью справки не удалось решить проблему или вопрос, посетите [базу знаний ESET](#), в которой есть ответы и решения для самых распространенных ситуаций.

[Удаление троянской программы Sirefef \(ZeroAccess\)?](#)

[Контрольный список для устранения проблем при обновлении с зеркала](#)

[Адреса и порты, которые необходимо открыть в стороннем файрволе для обеспечения полноценной работы продуктов ESET](#)

При необходимости направьте свои вопросы в нашу онлайн-службу технической поддержки. К ссылке на контактную веб-форму можно получить на панели **Справка и поддержка** в главном окне программы.

3.8.1 Обновление программы ESET Endpoint Security


Обновлять ESET Endpoint Security 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](#)).

3.8.2 Активация ESET Endpoint Security

После завершения установки вам будет предложено активировать установленный продукт.

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

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


Для активации ESET Endpoint Security можно воспользоваться любым из перечисленных ниже методов.

- **Лицензионный ключ:** уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.
- **Учетная запись администратора безопасности:** учетная запись, созданная на [портале ESET License Administrator](#) с использованием учетных данных (адрес электронной почты и пароль). Этот метод позволяет централизованно управлять несколькими лицензиями.
- **Офлайн-лицензия:** автоматически созданный файл со сведениями о лицензии, который передается в продукт ESET. Если лицензия позволяет загрузить автономный файл лицензии (.lf), его можно использовать

для автономной активации. Количество офлайн-лицензий будет вычтено из общего количества доступных лицензий. Дополнительные сведения о создании автономного файла см. в [руководстве пользователя ESET License Administrator](#).

Щелкните элемент **Активировать позже**, если компьютер является участником управляемой сети и администратор выполнит удаленную активацию через программу ESET Remote Administrator. Этот параметр можно использовать и в тех случаях, когда нужно активировать клиент позже.

Если у вас есть имя пользователя и пароль, но вы не знаете, как активировать ESET Endpoint Security, щелкните **У меня есть имя пользователя и пароль. Что мне делать?** Отобразится экран ESET License Administrator. Здесь вы сможете преобразовать учетные данные в лицензионный ключ.

Изменить лицензию на продукт можно в любое время. Для этого щелкните **Справка и поддержка > Управление лицензией** в главном окне программы. Отобразится открытый идентификатор лицензии, предназначенный для ее идентификации в службе поддержки ESET. Имя пользователя, под которым зарегистрирован компьютер, можно найти в разделе **О программе** (на панели задач щелкните значок  правой кнопкой мыши).

i ПРИМЕЧАНИЕ.

Приложение ESET Remote Administrator может активировать клиентские компьютеры в автоматическом режиме, используя предоставленные администратором лицензии. Инструкции см. в [руководстве пользователя по ESET Remote Administrator](#).

3.8.3 Активация нового продукта с использованием текущих учетных данных

Если у вас уже есть имя пользователя и пароль и вы желаете получить лицензионный ключ, посетите [портал ESET License Administrator](#). На портале учетные данные можно преобразовать в лицензионный ключ.

3.8.4 Удаление вируса с компьютера

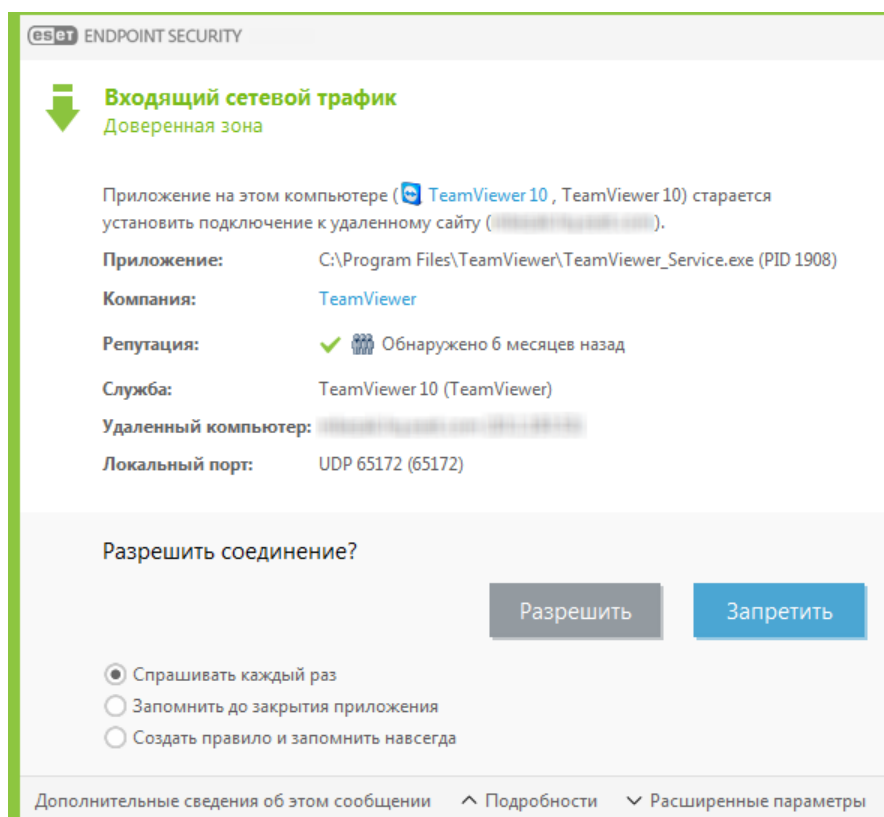
Если компьютер проявляет какие-либо признаки заражения вредоносной программой, например работает медленнее или часто зависает, рекомендуется сделать следующее.

1. В главном окне программы щелкните **Сканирование компьютера**.
2. Нажмите **Сканирование Smart**, 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 элемент **Выборочное сканирование** и укажите объекты, которые следует просканировать на наличие вирусов.

Дополнительные сведения см. в нашей регулярно обновляемой статье [базы знаний ESET](#).

3.8.5 Разрешение обмена данными определенному приложению

Если в интерактивном режиме обнаруживается новое подключение, но соответствующего правила не найдено, пользователь получает запрос, предлагающий разрешить или запретить его. Если нужно, чтобы программа ESET Endpoint Security выполняла одно и то же действие при каждой попытке приложения установить подключение, установите флажок **Запомнить действие (создать правило)**.



Вы можете создать правила файрвола для приложений еще до их обнаружения программой ESET Endpoint Security. Это можно сделать в окне настроек файрвола, последовательно выбрав **Дополнительные настройки > Файрвол > Основная информация > Правила** и нажав кнопку **Изменить**.

Нажмите **Добавить** для добавления правила. На вкладке **Общие** укажите имя, направление и протокол передачи данных для правила. В этом окне можно определить действие, которое нужно выполнить при применении правила.

Введите путь к исполняемому файлу приложения и порт передачи данных на локальном компьютере на вкладке **Локальный компьютер**. Перейдите на вкладку **Удаленный компьютер** и введите удаленный адрес и порт (при необходимости). Новое правило начнет действовать немедленно и сработает сразу, как только данное приложение попытается установить подключение.

3.8.6 Создание задачи в планировщике

Чтобы создать новую задачу, выберите **Служебные программы > Планировщик**, а затем нажмите кнопку **Добавить задачу** или щелкните правой кнопкой мыши и в контекстном меню выберите команду **Добавить...**. 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 при загрузке 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 из них.
- **Сканирование компьютера по требованию:** сканирование файлов и папок на компьютере.
- **Обновление:** планирование задачи обновления путем обновления модулей.

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**).

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 существующих запланированных задач.

3.8.7 Планирование задачи сканирования (каждые 24 часа)

Чтобы запланировать регулярную задачу, откройте главное окно программы и выберите **Служебные программы > Планировщик**. Ниже приведено краткое описание процедуры планирования задачи, которая будет сканировать локальные диски каждые 24 часа.

Для того чтобы запланировать задачу сканирования, выполните следующие действия.

1. В главном окне планировщика нажмите **Добавить**.
2. В раскрывающемся меню выберите **Сканирование компьютера по требованию**.
3. Введите имя задачи и выберите **Многократно**.
4. Укажите, что задача должна выполняться каждые 24 часа.
5. Выберите действие, которое будет выполняться, если по какой-либо причине не удастся выполнить запланированную задачу.
6. Просмотрите сводную информацию о запланированной задаче и нажмите **Готово**.

7. В раскрывающемся меню **Объекты** выберите пункт **Жесткие диски**.

8. Нажмите кнопку **Готово** для применения задачи.

3.8.8 Подключение ESET Endpoint Security к ESET Remote Administrator

Если после установки ESET Endpoint Security на компьютер вы хотите подключиться через ESET Remote Administrator, убедитесь, что на клиентской рабочей станции также установлен агент ERA. Агент ERA — важная составляющая каждого клиентского решения, которое подключается к серверу ERA. Для поиска компьютеров в сети ESET Remote Administrator использует компонент RD Sensor. Каждый компьютер в сети, найденный с помощью компонента RD Sensor, отображается в веб-консоли.

После развертывания агента вы можете удаленно устанавливать на клиентских компьютерах другие решения безопасности ESET. Подробное описание удаленной установки приведено в [руководстве пользователя ESET Remote Administrator](#).

3.8.9 Настройка зеркала

В настройках ESET Endpoint Security можно включить сохранение копий файлов обновления модуля обнаружения и передачу обновлений на другие рабочие станции, на которых работает ESET Endpoint Security или ESET Endpoint Antivirus.

Настройка ESET Endpoint Security для работы в качестве сервера зеркала для передачи обновлений через внутренний HTTP-сервер

Нажмите клавишу **F5**, чтобы получить доступ к дополнительным настройкам, и последовательно щелкните элементы **Обновление > Основные сведения**. Убедитесь, что для **Сервера обновлений** включен параметр **Автоматический выбор**. Выберите **Создать зеркало обновления** и **Передавать файлы обновления через внутренний HTTP-сервер** в **Дополнительные настройки > Обычная > Зеркало**.

Настройка сервера зеркала для передачи обновлений через общую сетевую папку

Создайте общую папку на локальном или сетевом устройстве. Папка должна быть открыта для чтения всеми пользователями решений для обеспечения безопасности ESET и для записи из локальной учетной записи системы. Активируйте элемент **Создать зеркало обновления**. Чтобы получить к нему доступ, последовательно щелкните элементы **Дополнительные настройки > Основные сведения > Зеркало**. Найдите и откройте созданную общую папку.

ПРИМЕЧАНИЕ

Если через внутренний HTTP-сервер обновления выполнять не нужно, снимите флажок **Передавать файлы обновления с помощью внутреннего сервера HTTP**.

3.8.10 Как мне обновить свою систему до Windows 10, если у меня установлен продукт ESET Endpoint Security?

ВНИМАНИЕ!

Прежде чем выполнять обновление до Windows 10, настоятельно рекомендуется обновить продукт ESET до последней версии, а затем загрузить последнюю версию модуля обнаружения. Во время обновления до Windows 10 это обеспечит максимальную защиту, а также сохранение настроек программы и сведений о лицензии.

Версия 6.x и более поздние версии:

Чтобы подготовиться к обновлению до Windows 10, загрузите и установите последнюю версию продукта, щелкнув соответствующую ссылку ниже.

[Загрузить ESET Endpoint Security 6 \(32-разрядная версия\)](#) [Загрузить ESET Endpoint Antivirus 6 \(32-разрядная версия\)](#)

[Загрузить ESET Endpoint Security 6 \(64-разрядная версия\)](#) [Загрузить ESET Endpoint Antivirus 6 \(64-разрядная версия\)](#)

Версия 5.x и более ранние версии:

Чтобы подготовиться к обновлению до Windows 10, загрузите и установите последнюю версию продукта, щелкнув соответствующую ссылку ниже.

[Загрузить ESET Endpoint Security 5 \(32-разрядная версия\)](#) [Загрузить ESET Endpoint Antivirus 5 \(32-разрядная версия\)](#)

[Загрузить ESET Endpoint Security 5 \(64-разрядная версия\)](#) [Загрузить ESET Endpoint Antivirus 5 \(64-разрядная версия\)](#)

Версии на других языках:

Если вы ищете версию продукта ESET для конечных точек на другом языке, [посетите нашу страницу загрузок](#).

ПРИМЕЧАНИЕ.

[Дополнительные сведения о совместимости продуктов ESET с Windows 10.](#)

3.8.11 Использование режима переопределения





Пользователи, на компьютерах которых установлены продукты ESET Endpoint (версии 6.5 и выше) для Windows, могут воспользоваться функцией переопределения. Режим переопределения позволяет пользователям на уровне клиентского компьютера изменять настройки установленного продукта ESET, даже если поверх этих настроек применена та или иная политика. Режим переопределения можно включить для определенных пользователей AD или же защитить паролем. Эта функция не может быть включена более четырех часов подряд.

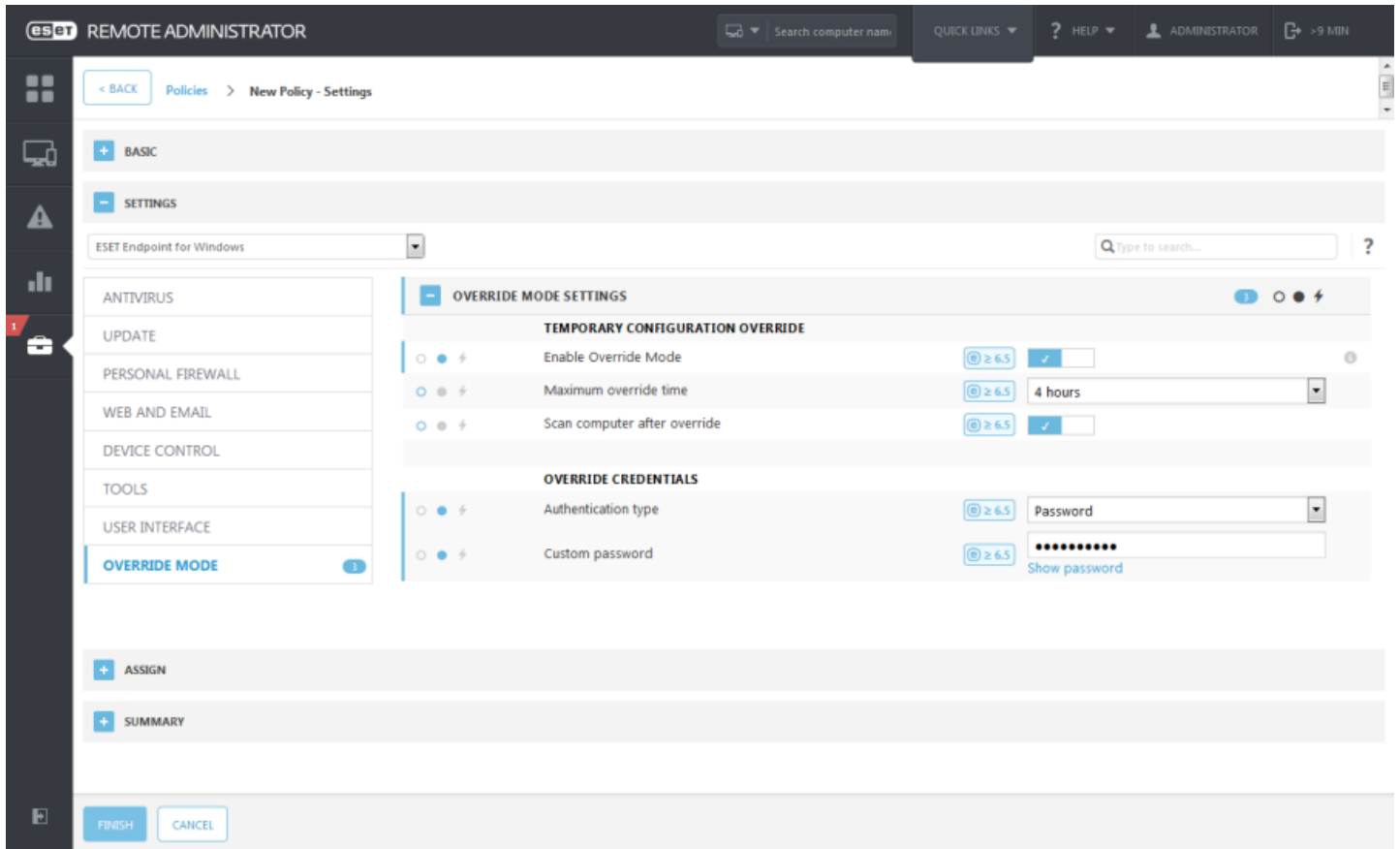
ВНИМАНИЕ!

Режим переопределения нельзя остановить из веб-консоли ERA после того, как он был включен.

Переопределение отключается только по истечении времени переопределения или же после отключения на самом клиенте.

Чтобы задать **режим переопределения**, выполните следующие действия:

1. Перейдите в меню **Администратор > Политики > Создать политику**.
2. В разделе  **Основная информация** введите **имя** и **описание** этой политики.
3. В разделе  **Параметры** выберите **ESET Endpoint для Windows**.
4. Нажмите **Режим переопределения** и настройте правила этого режима.
5. В разделе  **Назначить** выберите компьютер или группу компьютеров, к которым будет применена данная политика.
6. Проверьте настройки в режиме  **Сводка** и нажмите кнопку **Готово**, чтобы применить политику.



После того как к агенту ERA применена политика переопределения ERA Server, в дополнительных настройках (на конечной точке клиента) появится кнопка «Переопределение политики».

1. Щелкните **Переопределение политики**.
2. Укажите время и нажмите кнопку **Применить**.
3. Предоставьте приложению ESET повышенные права.
4. Введите пароль, определенный политикой. Если в политике указан пользователь Active Directory, пароль не нужен.
5. Предоставьте приложению ESET повышенные права.
6. Теперь режим переопределения включен.
7. Чтобы завершить процедуру, нажмите кнопку **Завершить переопределение**.

✓ ПОДСКАЗКА

Если у *Ивана* наблюдается проблема с параметрами конечной точки, блокирующими какую-либо важную функцию или доступ к Интернету на его компьютере, администратор может разрешить *Ивану* переопределить существующую политику конечной точки и настроить параметры вручную на своем компьютере. Впоследствии новые параметры могут быть запрошены системой ERA, чтобы администратор мог создать на их основе новую политику.

Для этого выполните следующие действия:

1. Перейдите в меню **Администратор > Политики > Создать политику**.
2. Заполните поля **Имя** и **Описание**. В разделе **Параметры** выберите **ESET Endpoint для Windows**.
3. Нажмите **Режим переопределения**, включите режим переопределения на один час и выберите пользователя AD *Иван*.
4. Назначьте политику *компьютеру Ивана* и нажмите кнопку **Готово**, чтобы сохранить политику.
5. *Иван* должен включить **режим переопределения** на своей конечной точке ESET и изменить параметры вручную на своем компьютере.
6. В веб-консоли ERA перейдите в раздел **Компьютеры**, выберите *Компьютер Ивана* и нажмите **Показать подробности**.
7. В разделе **Конфигурация** нажмите **Запросить конфигурацию**, чтобы запланировать клиентскую задачу для получения конфигурации от клиента как можно скорее.
8. Вскоре появится новая конфигурация. Щелкните продукт, параметры которого необходимо сохранить, а затем нажмите **Открыть конфигурацию**.
9. Можно просмотреть параметры, а затем нажать кнопку **Преобразовать в политику**.
10. Заполните поля **Имя** и **Описание**.
11. В разделе **Параметры** при необходимости можно изменить параметры.
12. В разделе **Назначить** можно назначить данную политику *компьютеру Ивана* (или другим).
13. Нажмите кнопку **Готово**, чтобы сохранить параметры.
14. Не забудьте удалить политику переопределения после того, как необходимость в ней исчезнет.

3.8.12 Активация удаленного мониторинга и управления

Удаленный мониторинг и управление (RMM) — это процесс контроля систем программного обеспечения (например, на настольных компьютерах, серверах и мобильных устройствах) с помощью локально установленного агента, к которому может получать доступ поставщик службы управления.

Расширенные параметры

ЗАЩИТА ОТ ВИРУСОВ 1

ОБНОВЛЕНИЕ 4

ФАЙЕРВОЛ 5

ИНТЕРНЕТ И ЭЛЕКТРОННАЯ ПОЧТА 4

КОНТРОЛЬ УСТРОЙСТВ 2

СЛУЖБНЫЕ ПРОГРАММЫ 2

Файлы журналов

Прокси-сервер

Уведомления по электронной почте 3

Режим презентации

Диагностика

ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

По умолчанию

OK

Отмена

Расширенные параметры

ESET LIVEGRID®

ЦЕНТР ОБНОВЛЕНИЯ MICROSOFT WINDOWS®

ЗАЩИТА ДОСТУПА К СЕТИ MICROSOFT

ESET CMD

ESET RMM

Включить RMM

Режим работы: Только безопасные операции

Метод авторизации: Путь приложения

Пути приложений: Изменить

Компонент ESET RMM по умолчанию отключен. Чтобы включить его, нажмите клавишу **F5**, чтобы открыть раздел «Дополнительные настройки», щелкните **Службные программы**, разверните пункт **ESET RMM** и активируйте параметр **Включить RMM**.

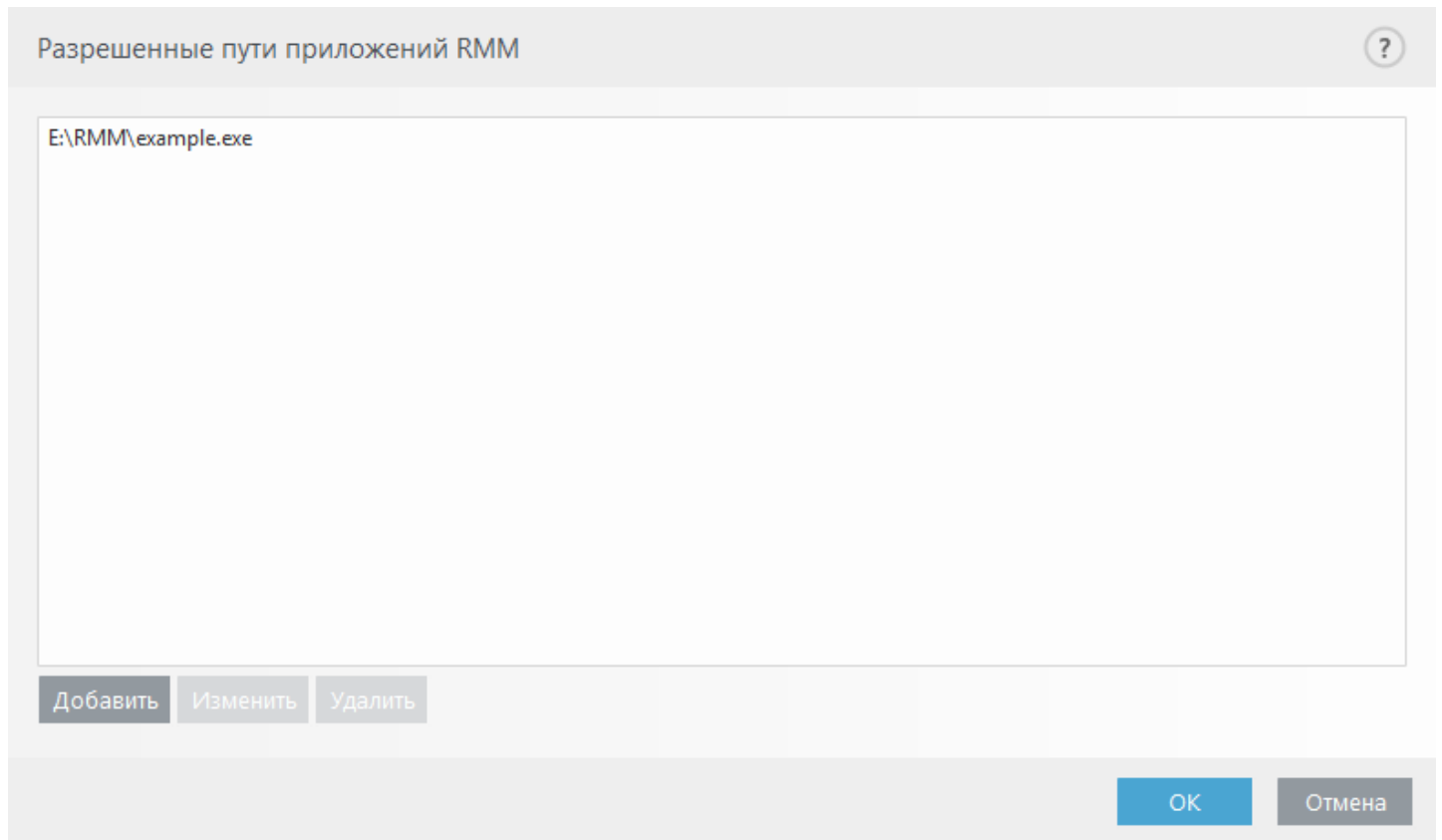
Режим работы: выберите режим работы RMM в раскрывающемся меню. Доступны два варианта: **Только безопасные операции** и **Все операции**.

Метод авторизации: настройте метод авторизации RMM. Чтобы использовать авторизацию, выберите в раскрывающемся меню **Путь к приложению**. Или выберите пункт **Нет**.

⚠ ВНИМАНИЕ!

Компонент RMM должен всегда использовать авторизацию, чтобы вредоносное ПО не могло отключать или обходить защиту ESET Endpoint.

Пути к приложениям: если вы выбрали метод авторизации **Путь к приложению**, щелкните **Изменить**, чтобы открыть окно настройки **Разрешенные пути приложений RMM**.



Добавить: создание разрешенного пути к приложению RMM. Введите путь или нажмите кнопку ..., чтобы выбрать исполняемый файл.

Изменить: изменение существующего разрешенного пути. Если расположение исполняемого файла изменилось, используйте команду **Изменить**.

Удалить: удаление существующего разрешенного пути.

Установка ESET Endpoint Security, используемая по умолчанию, содержит файл `ermm.exe` в каталоге приложения конечной точки (путь по умолчанию — `c:\Program Files\ESET\ESET Security`). Файл `ermm.exe` обменивается данными с подключаемым модулем RMM, который в свою очередь обменивается данными с агентом RMM, подключенным к серверу RMM.

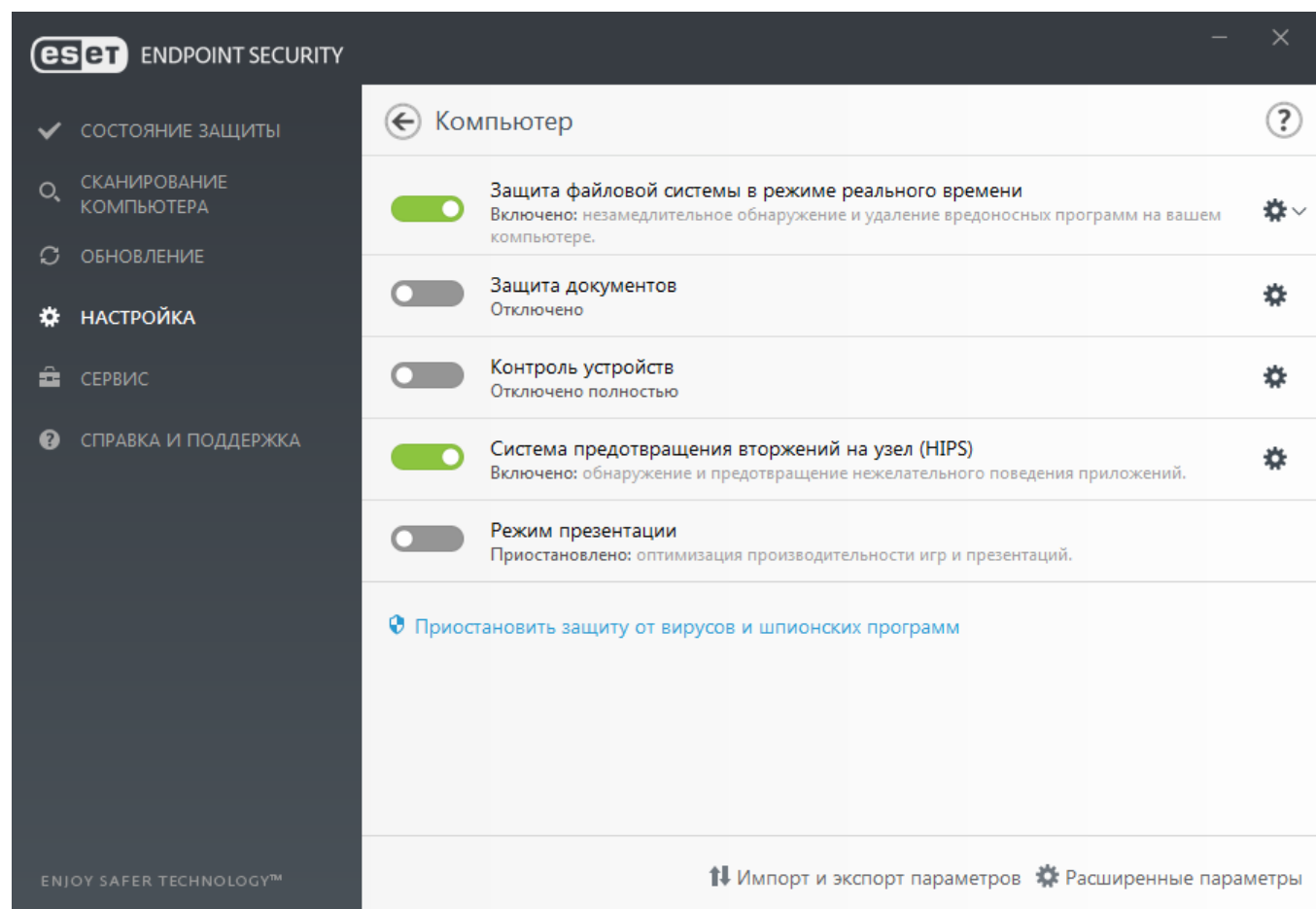
- `ermm.exe` — это разработанная компанией ESET программа командной строки, которая позволяет управлять продуктами для конечных точек и обмениваться данными с любым подключаемым модулем RMM.
- Подключаемый модуль RMM — это стороннее приложение, работающее локально в системе Endpoint Windows. Он предназначен для обмена данными с определенным агентом RMM (например, только Kaseya) и с исполняемым файлом `ermm.exe`.
- Агент RMM — это стороннее приложение (например, от компании Kaseya), работающее локально в системе Endpoint Windows. Агент обменивается данными с подключаемым модулем RMM и сервером RMM.
- Сервер RMM работает как служба на стороннем сервере. Поддерживаются системы RMM от Kaseya, Labtech, Autotask, Max Focus и Solarwinds N-able.

3.9 Работа с ESET Endpoint Security

Параметры ESET Endpoint Security дают пользователю возможность настраивать уровень защиты для компьютера, Интернета, электронной почты и сети.

i ПРИМЕЧАНИЕ.

При создании политики из веб-консоли ESET Remote Administrator можно выбрать флаг для каждого параметра. Параметры с флагом «Принудительно применить» имеют приоритет и не могут быть переопределены последующей политикой (даже если в ней установлен этот флажок). Это гарантирует, что данный параметр не будет изменен (например, пользователем или последующими политиками в ходе объединения). Дополнительные сведения см. в [справке о флагах в ERA в Интернете](#).



Меню **Настройка** содержит следующие разделы.

- **Компьютер**
- **Сеть**
- **Интернет и электронная почта**


В настройках защиты **Компьютер** можно включать и отключать следующие компоненты:


- **Защита файловой системы в реальном времени:** при открытии, создании или исполнении файлов они сканируются на наличие вредоносного кода.
- **Защита документов:** функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, такие как элементы Microsoft ActiveX.
- **HIPS:** система предотвращения вторжений на узел ([HIPS](#)) отслеживает события, происходящие в операционной системе, и реагирует на них в соответствии с настраиваемым набором правил.
- **Режим презентации:** функция для пользователей, которым необходимо отсутствие перерывов при использовании программного обеспечения и отвлекающих внимание всплывающих окон, а также требуется свести к минимуму потребление ресурсов процессора. После включения [Режима презентации](#) на экран будет выведено предупреждение (о потенциальной угрозе безопасности), а для оформления главного окна будет применен оранжевый цвет.
- **Защита Anti-Stealth:** обеспечивает обнаружение опасных программ, например [руткитов](#), способных скрывать свое присутствие от операционной системы. Это значит, что такие программы невозможно обнаружить с помощью обычных методов проверки.


Раздел **Сеть** позволяет включать и отключать **файрвол, защиту от сетевых атак и защиту от ботнетов.**

В настройках защиты **Интернет и электронная почта** можно включать и отключать следующие компоненты:

- **Контроль доступа в Интернет:** блокирование веб-страниц, которые могут содержать потенциально нежелательные материалы. Кроме того, системные администраторы могут задавать параметры доступа для 27 предварительно заданных категорий веб-сайтов.
- **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 спама:** сканируются нежелательные сообщения или спам.
- **Защита от фишинга:** защита от попыток получения паролей, банковских данных и прочей конфиденциальной информации незаконными веб-сайтами, выдающими себя за законные.


Чтобы временно отключить отдельный модуль, щелкните зеленый переключатель  возле нужного модуля. Обратите внимание, что при этом будет ослаблена защита вашего компьютера.

Чтобы возобновить защиту отключенного компонента безопасности, щелкните красный переключатель  — и компонент снова будет включен.

При применении политики ERA будет отображаться значок блокировки  рядом с определенным компонентом. Политика, примененная решением ESET Remote Administrator, может быть переопределена локально после проверки подлинности пользователя, вошедшего в систему (например, администратора).
Дополнительные сведения см. в [справке о решении ESET Remote Administrator в Интернете](#).

i ПРИМЕЧАНИЕ.

Все средства защиты, отключенные таким способом, будут повторно включены после перезагрузки компьютера.


Чтобы открыть подробные настройки компонента безопасности, щелкните значок шестеренки  возле соответствующего компонента.

В нижней части окна настройки есть дополнительные параметры. Чтобы загрузить параметры настройки из файла конфигурации в формате XML или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией **Импорт и экспорт параметров**. Для получения дополнительных сведений см. раздел [Импорт и экспорт параметров](#).

Чтобы открыть дополнительные параметры, щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**.

3.9.1 Компьютер

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

Щелкните значок шестеренки  рядом с элементом **Защита файловой системы в режиме реального времени**, затем щелкните **Изменить исключения**, после чего откроется окно настроек [Исключения](#), в котором можно исключить файлы и папки из сканирования.

i ПРИМЕЧАНИЕ.

Информация о состоянии защиты документа может быть недоступной, пока не будет активирована в меню **Дополнительные настройки (F5) > Защита от вирусов > Защита документов**. После активации перезагрузите компьютер. Для этого в области «Настройки» перейдите к разделу «Компьютер» и выберите в меню «Контроль устройств» команду **Перезапустить**. Или же перейдите к области состояний «Защита» и нажмите кнопку **Перезапустить компьютер**.

Приостановить защиту от вирусов и шпионских программ: при каждом временном отключении защиты от вирусов и шпионских программ можно, воспользовавшись раскрывающимся меню, выбрать период времени, на протяжении которого будет отключен выбранный компонент. После этого следует нажать кнопку **Применить**, чтобы отключить компонент безопасности. Чтобы вновь активировать защиту, нажмите кнопку **Включить защиту от вирусов и шпионских программ**.

Настройка сканирования компьютера...: настройка параметров сканирования компьютера (сканирования, запускаемого вручную).

3.9.1.1 Модуль обнаружения

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

Для настройки параметров модуля защиты от вирусов щелкните элемент **Дополнительные настройки** или нажмите клавишу **F5**.

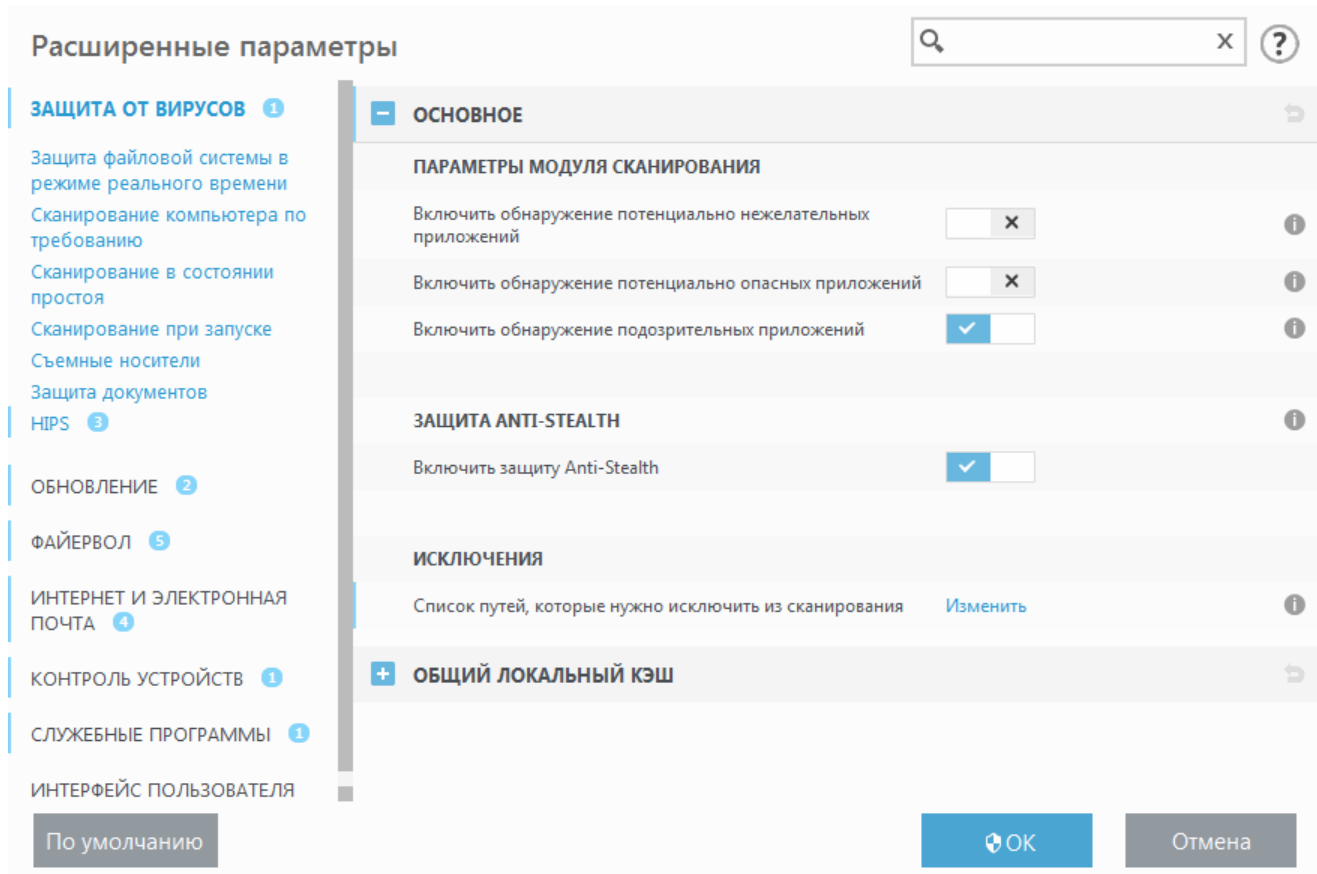
Параметры модуля сканирования для всех модулей защиты (защиты файловой системы в реальном времени, защиты доступа в Интернет и т. д.) позволяют включать и отключать обнаружение приведенных ниже элементов.

- **Потенциально нежелательные приложения** не всегда являются вредоносными, однако могут негативно повлиять на производительность компьютера.
Дополнительную информацию о приложениях этого типа см. в [глоссарии](#).
- **Потенциально опасные приложения:** это определение относится к законному коммерческому программному обеспечению, которое может быть использовано для причинения вреда. К потенциально опасным приложениям относятся средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, регистрирующие каждое нажатие пользователем клавиш на клавиатуре). По умолчанию этот параметр отключен.
Дополнительную информацию о приложениях этого типа см. в [глоссарии](#).
- **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 проверки.

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](#).

Включить расширенное сканирование с помощью AMSI: инструмент Microsoft Antimalware Scan Interface, позволяющий разработчикам приложений создавать новые средства защиты от вредоносного ПО (только Windows 10).



3.9.1.1.1 Действия при обнаружении заражения

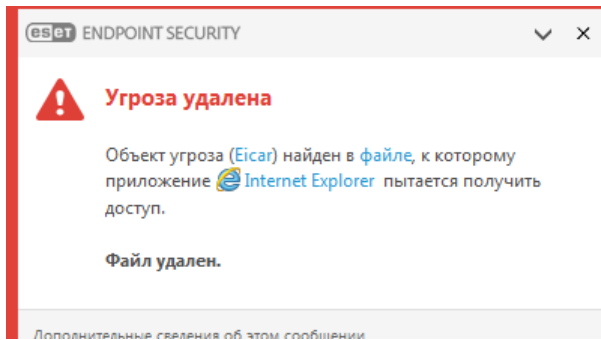
Заражения могут попасть на компьютер из различных источников, таких как веб-сайты, общие папки, электронная почта или съемные носители (накопители USB, внешние диски, компакт- или DVD-диски, дискеты и т. д.).

Стандартное поведение

Обычно ESET Endpoint Security обнаруживает заражения с помощью перечисленных ниже модулей.

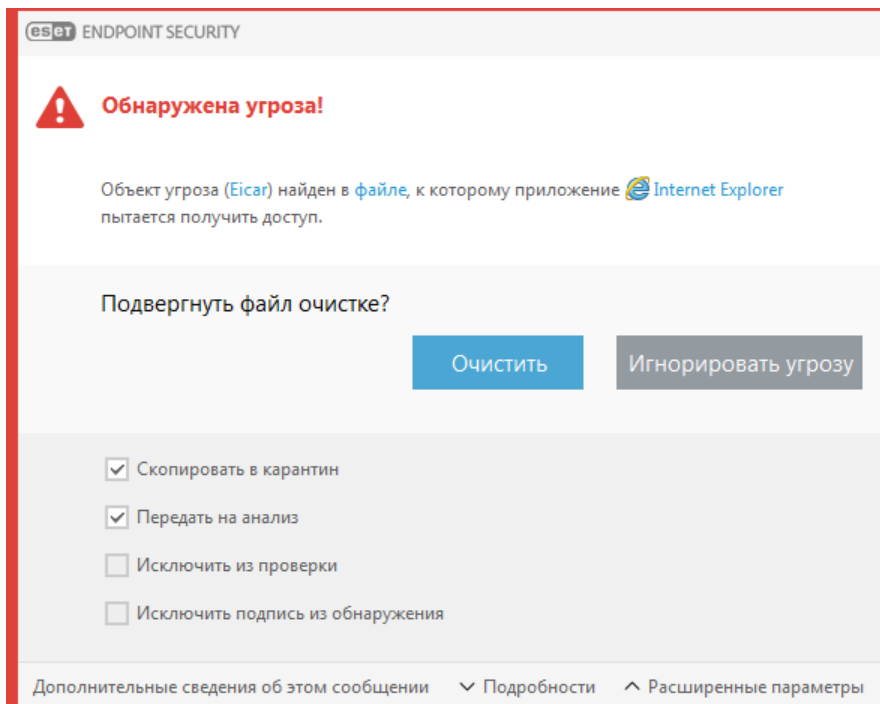
- Защита файловой системы в режиме реального времени
- Защита доступа в Интернет
- Защита почтового клиента
- Сканирование компьютера по требованию

Каждый модуль использует стандартный уровень очистки и пытается очистить файл, поместить его в [карантин](#) или прервать подключение. 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 какие-либо зараженные файлы при сканировании компьютера не были очищены (или был выбран [уровень очистки Без очистки](#)), на экран будет выведено окно предупреждения, в котором пользователю предлагается выбрать действие для таких файлов.

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 Endpoint Security и выберите команду «Сканирование компьютера».
- Выберите вариант **Сканирование Smart** (дополнительную информацию см. в разделе [Сканирование компьютера](#)).
- После окончания сканирования проверьте в журнале количество просканированных, зараженных и очищенных файлов.

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

3.9.1.2 Общий локальный кэш

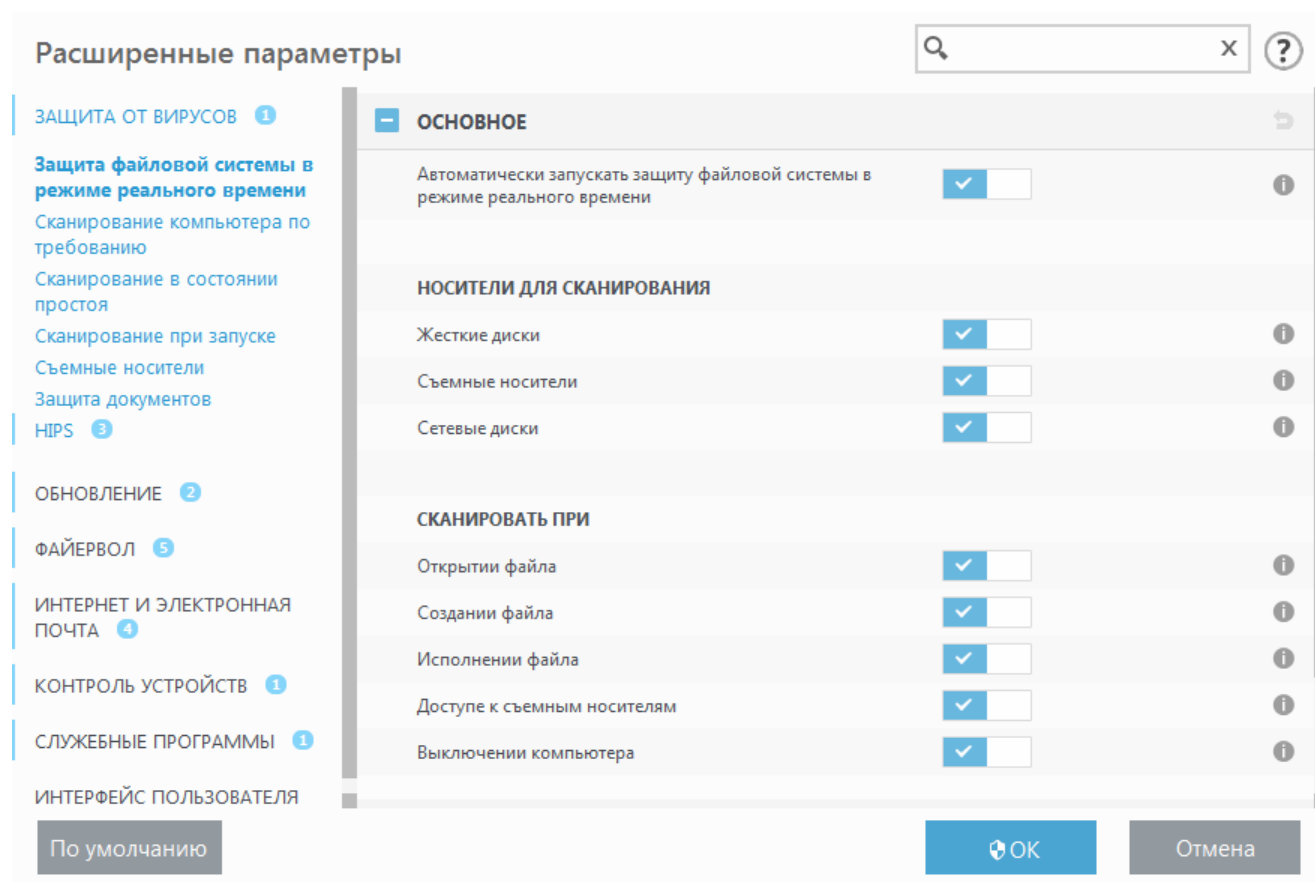
Общий локальный кэш повышает производительность в виртуализированных средах, запрещая повторяющееся сканирование в сети. Благодаря этому каждый файл сканируется только один раз, а затем сохраняется в общем кэше. Включите элемент **Параметры кэширования**, чтобы сохранять данные о сканировании файлов и папок в сети в локальный кэш. При следующем сканировании продукт ESET Endpoint Security будет искать сканируемые файлы в кэше. Если файлы совпадают, они будут исключены из сканирования.

При настройке **сервера кэширования** нужно работать с указанными ниже элементами.

- **Имя хоста:** имя или IP-адрес компьютера, на котором расположен кэш.
- **Порт:** номер порта, используемого для передачи данных (тот же, что указан для общего локального кэша).
- **Пароль:** укажите пароль общего локального кэша ESET, если необходимо.

3.9.1.3 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. Все файлы сканируются на наличие вредоносного кода во время их открытия, создания или запуска. 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 **Расширенные параметры** и в разделе **Защита файловой системы в реальном времени > Основная информация** снять флажок **Включить защиту файловой системы в реальном времени**.

Носители для сканирования

По умолчанию все типы носителей сканируются на наличие возможных угроз.

Жесткие диски — контролируются все жесткие диски системы.

Съемные носители — контролируются компакт-/DVD-диски, USB-устройства хранения, Bluetooth-устройства и т. п.

Сетевые диски — сканируются все подключенные сетевые диски.

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

Сканировать при

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

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

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.

Чтобы снизить влияние на производительность компьютера при использовании защиты в режиме реального времени, повторное сканирование файлов, которые уже были просканированы, не выполняется (если файлы не были изменены). Файлы повторно сканируются сразу после каждого обновления модуля обнаружения. Управление этим режимом осуществляется с помощью параметра **Оптимизация Smart**. Если **оптимизация Smart** отключена, все файлы сканируются каждый раз при получении доступа к ним. Для изменения этого параметра нажмите **F5**, чтобы открыть окно «Дополнительные настройки», и перейдите к разделу **Модуль обнаружения > Защита файловой системы в режиме реального времени**. Последовательно щелкните элементы **Параметры ThreatSense > Другое** и снимите или установите флажок **Включить оптимизацию Smart**.

3.9.1.3.1 Дополнительные параметры ThreatSense

Дополнительные параметры модуля ThreatSense для новых и измененных файлов — вероятность заражения вновь созданных или измененных файлов выше по сравнению с аналогичным показателем для существующих файлов. Именно поэтому программа проверяет эти файлы с дополнительными параметрами сканирования. Вместе с обычными методами сканирования, основанными на сигнатурах, применяется расширенная эвристика, что делает возможным обнаружение новых угроз еще до выпуска обновлений модуля обнаружения. В дополнение ко вновь созданным файлам выполняется также сканирование самораспаковывающихся файлов (.sfx) и упаковщиков (исполняемых файлов с внутренним сжатием). По умолчанию проверяются архивы с глубиной вложенности до 10 независимо от их фактического размера. Для изменения параметров сканирования архивов снимите флажок **Параметры сканирования архива по умолчанию**.

Дополнительную информацию об **упаковщиках, самораспаковывающихся архивах и расширенном эвристическом анализе** см. в разделе о [настройках параметров модуля ThreatSense](#).

Дополнительные параметры модуля ThreatSense для исполняемых файлов: по умолчанию [расширенная эвристика](#) при исполнении файлов не применяется. Если этот параметр включен, настоятельно рекомендуется включить [оптимизацию Smart](#) и ESET LiveGrid®, чтобы уменьшить воздействие на производительность системы.

3.9.1.3.2 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.

Обычная 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. Исключения составляют только системные файлы. Если очистка невозможна, на экран выводится окно предупреждения, в котором

пользователю предлагается выполнить определенное действие.

⚠ ВНИМАНИЕ!

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.

3.9.1.3.3 Проверка модуля защиты в режиме реального времени


Чтобы убедиться, что защита в режиме реального времени работает и обнаруживает вирусы, используйте проверочный файл [eicar.com](http://www.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>.

i ПРИМЕЧАНИЕ.

Перед проверкой защиты в режиме реального времени необходимо отключить [файрвол](#). Если файрвол включен, он обнаружит данный файл и предотвратит его загрузку. Обязательно повторно включите файрвол сразу же после проверки защиты файловой системы в режиме реального времени.

3.9.1.3.4 Момент изменения конфигурации защиты в режиме реального времени

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

После установки ESET Endpoint Security все параметры оптимизированы для максимальной защиты системы. Для восстановления параметров по умолчанию щелкните  возле каждой вкладки в окне (**Расширенные параметры > Модуль обнаружения > Защита файловой системы в режиме реального времени**).

3.9.1.3.5 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 перейдите в раздел **Настройка** и в главном окне программы нажмите **Защита файловой системы в режиме реального времени**.

Если защита в режиме реального времени не запускается при загрузке операционной системы, обычно это связано с тем, что не установлен флажок **Автоматически запускать защиту файловой системы в режиме реального времени**. Чтобы включить этот параметр, перейдите в раздел **Дополнительные настройки (F5)** и последовательно щелкните элементы **Модуль обнаружения > Защита файловой системы в режиме реального времени > Основные сведения**. Установите флажок **Автоматически запускать защиту файловой системы в режиме реального времени**.

Защита в режиме реального времени не обнаруживает и не очищает заражения

Убедитесь в том, что на компьютере не установлены другие программы защиты от вирусов. При одновременной работе двух систем защиты от вирусов могут возникнуть конфликты. Перед установкой ESET рекомендуется удалить с компьютера все прочие программы защиты от вирусов.

Защита файловой системы в режиме реального времени не запускается

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

3.9.1.4 Сканирование компьютера

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

Доступно два типа **сканирования компьютера**. **Сканирование Smart** позволяет быстро просканировать систему без необходимости дополнительной настройки параметров сканирования. **Выборочное сканирование** позволяет выбрать predetermined профиль сканирования и указать объекты, которые нужно просканировать.

См. главу [Ход сканирования](#) для получения дополнительных сведений о процессе сканирования.

Сканировать компьютер

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

Выборочное сканирование

Выборочное сканирование является оптимальным решением в том случае, когда нужно 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.

Для выбора объектов сканирования щелкните **Сканирование компьютера > Выборочное сканирование** и выберите один из вариантов из раскрывающегося меню **Объекты сканирования** или конкретные объекты сканирования в древовидной структуре. Объекты сканирования также можно задать, указав пути к папкам и файлам, которые нужно сканировать. Если нужно только выполнить сканирование системы без дополнительных действий по очистке, выберите параметр **Сканировать без очистки**. При выполнении сканирования можно выбрать один из трех уровней очистки, последовательно щелкнув элементы **Настройка > Параметры ThreatSense > Очистка**.

Пользователям, не имеющим достаточного опыта работы с антивирусными программами, не рекомендуется выполнять выборочное сканирование.

Кроме того, можно использовать функцию **сканирования с использованием перетаскивания**, чтобы вручную сканировать файлы или папки: для этого наведите указатель мыши на нужный файл или папку, щелкните и, удерживая нажатой клавишу мыши, переместите выделенный элемент в отмеченную область, после чего отпустите кнопку мыши. После этого приложение будет переведено в фоновый режим.

Сканирование съемных носителей

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

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

В раскрывающемся списке **Действие после сканирования** можно выбрать действие (бездействие, выключение или перезагрузка), которое нужно выполнить после сканирования.

Выключить после сканирования: разрешает запланированное завершение работы после окончания сканирования компьютера по требованию. На экран будет выведено диалоговое окно подтверждения, которое будет активно в течение 60 секунд. Нажмите кнопку **Отмена**, если нужно отменить завершение работы.

i ПРИМЕЧАНИЕ.

Рекомендуется запускать сканирование компьютера не реже одного раза в месяц. Можно настроить сканирование как [запланированную задачу](#) в меню **Сервис > Планировщик**.

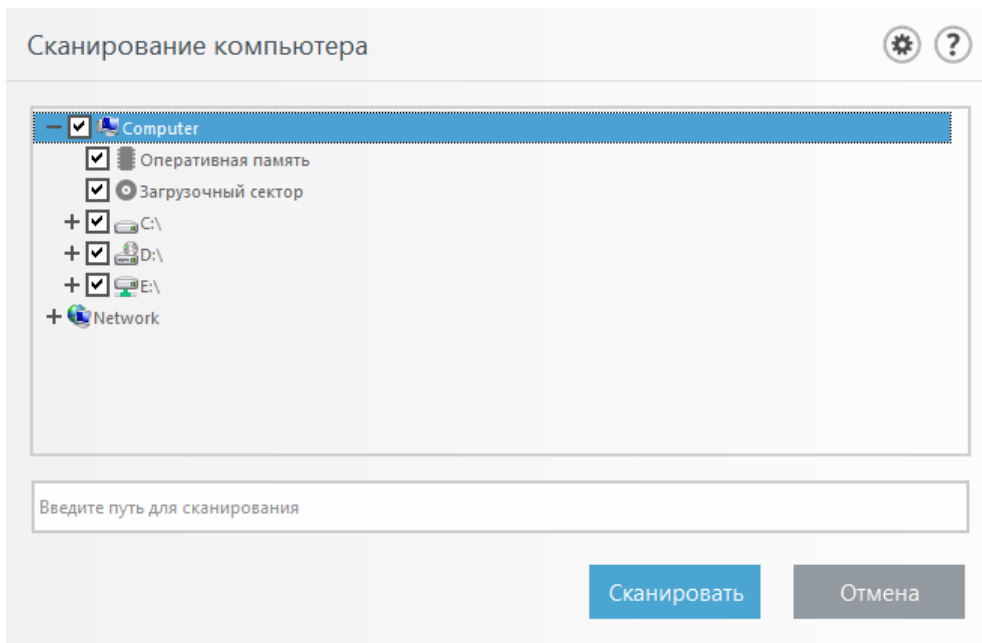
3.9.1.4.1 Средство запуска выборочного сканирования

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

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

- **По параметрам профиля:** выбираются объекты, указанные в выбранном профиле сканирования.
- **Сменные носители:** выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
- **Жесткие диски:** выбираются все жесткие диски системы.
- **Сетевые диски:** выбираются все подключенные сетевые диски.
- **Ничего не выбирать:** выбор объектов отменяется.

Чтобы быстро перейти к какому-либо объекту сканирования или добавить папку или файл, введите имя целевой папки в пустое 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 **Ничего не выбирать**.



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

Если выбран параметр **Пропустить исключения**, файлы с расширениями, которые ранее были исключены из сканирования, будут просканированы.

В раскрывающемся меню **Профиль сканирования** можно выбрать профиль, который будет использоваться для сканирования выбранных объектов. По умолчанию используется профиль **Сканирование Smart**. Существует еще два предварительно заданных профиля сканирования — **Тщательное сканирование** и **Сканирование через контекстное меню**. В этих профилях сканирования используются другие [параметры ThreatSense](#). Чтобы ознакомиться с доступными параметрами, последовательно выберите **Дополнительные настройки > Модуль обнаружения > Сканирование на наличие вредоносных программ > Сканирование по требованию > Параметры ThreatSense.**

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

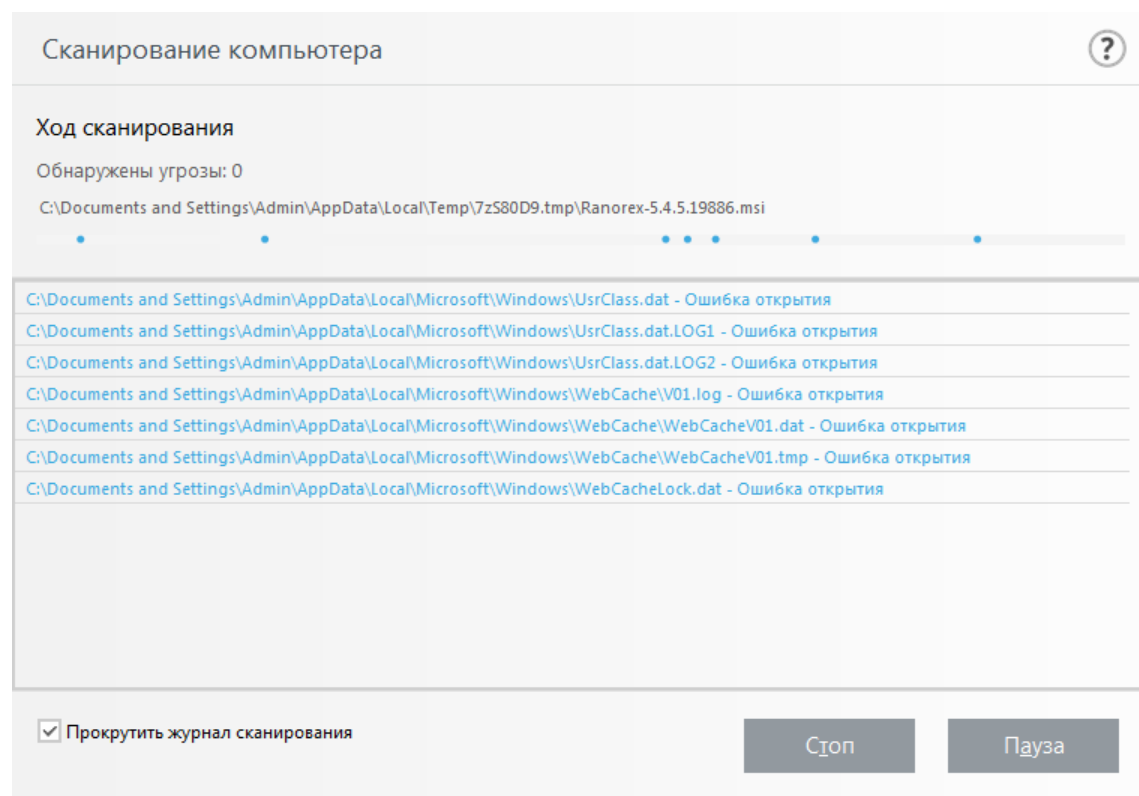
Кнопка **Сканировать с правами администратора** позволяет выполнять сканирование под учетной записью администратора. Воспользуйтесь этой функцией, если текущая учетная запись пользователя не имеет достаточных прав на доступ к файлам, которые следует сканировать. Обратите внимание, что данная кнопка недоступна,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

i ПРИМЕЧАНИЕ.

Журнал сканирования можно просмотреть по завершении сканирования, нажав кнопку [Показать журналы](#).

3.9.1.4.2 Ход сканирования

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



i ПРИМЕЧАНИЕ.

Нормально, что некоторые файлы, такие как защищенные паролем файлы или файлы, используемые исключительно операционной системой (обычно *pagefile.sys* и некоторые файлы журналов), не могут сканироваться.

Ход сканирования: индикатор выполнения показывает состояние уже просканированных объектов по сравнению с оставшимися. Состояние выполнения сканирования формируется на основе общего количества объектов, включенных в сканирование.

Объект: имя объекта, который сканируется в настоящий момент, и его расположение.

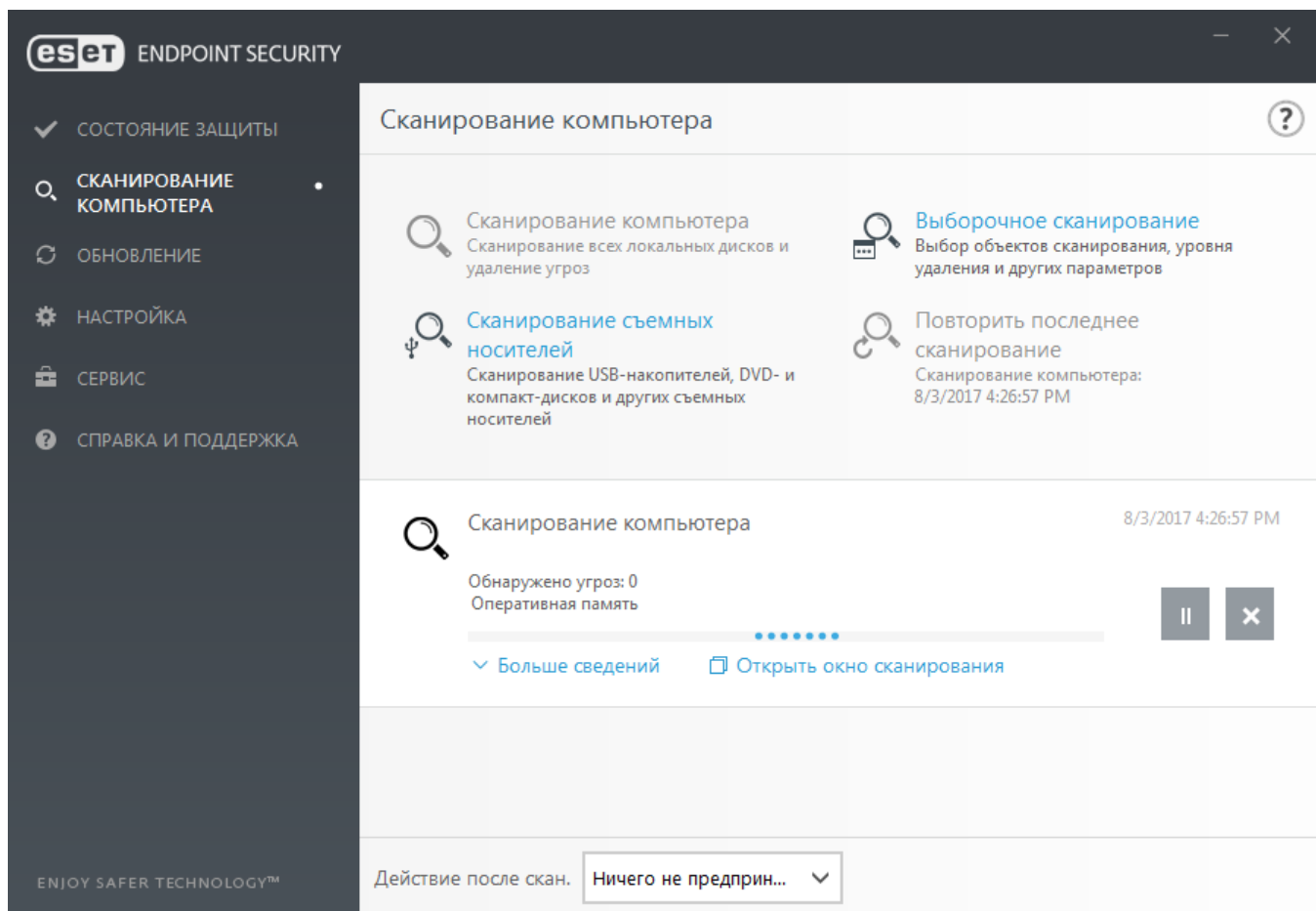
Обнаружены угрозы: общее число угроз, обнаруженных при сканировании.

Пауза: приостановка сканирования.

Возобновить: эта возможность становится доступна после приостановки сканирования. Нажмите **Возобновить**, чтобы возобновить сканирование.

Остановить: прекращение сканирования.

Прокрутить журнал сканирования: если этот параметр активирован, журнал сканирования будет прокручиваться автоматически при добавлении новых записей, чтобы отображались самые свежие элементы.



3.9.1.4.3 Журнал сканирования компьютера

В журнале сканирования компьютера содержатся общие сведения о сканировании, например такие:

- Версия модуля обнаружения
- дата и время сканирования;
- просканированные диски, папки и файлы;
- число просканированных объектов;
- число обнаруженных угроз;
- время завершения;
- общее время сканирования.

3.9.1.5 Контроль устройств

ESET Endpoint Security обеспечивает автоматическое управление устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). Данный модуль позволяет блокировать или 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 содержанием.

Поддерживаемые внешние устройства:

- Дисковый накопитель (жесткий диск, съемный USB-диск)
- Компакт-/DVD-диск
- USB-принтеры
- 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 Endpoint Security 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 использовать [редактор правил](#).

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

3.9.1.5.1 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.

Имя	Включено	Тип	Описание	Действие	Пользователи	Серьезность
Block USB for User	<input checked="" type="checkbox"/>	Дисковый накоп...	Производитель ...	Блокировать	Все	Всегда
Rule	<input checked="" type="checkbox"/>	Устройство Blue...		Чтение и запись	Все	Всегда


Некоторые устройства можно разрешить или заблокировать на основании сведений об их пользователе, группе пользователя или в соответствии с несколькими дополнительными параметрами, которые задаются в конфигурации правил. В списке правил для каждого правила отображается описание, включающее название и тип внешнего устройства, действие, выполняемое после его подключения к компьютеру, а также серьезность для журнала.

Для управления правилом используйте кнопки **Добавить** или **Изменить**. Снимите флажок **Включено** возле правила, чтобы отключить его до тех пор, пока оно не понадобится снова. Чтобы удалить одно или несколько правил, выделите их и выберите команду **Удалить**.

Чтобы создать правило с использованием заранее заданных параметров из другого правила, нажмите кнопку **Копировать**.

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

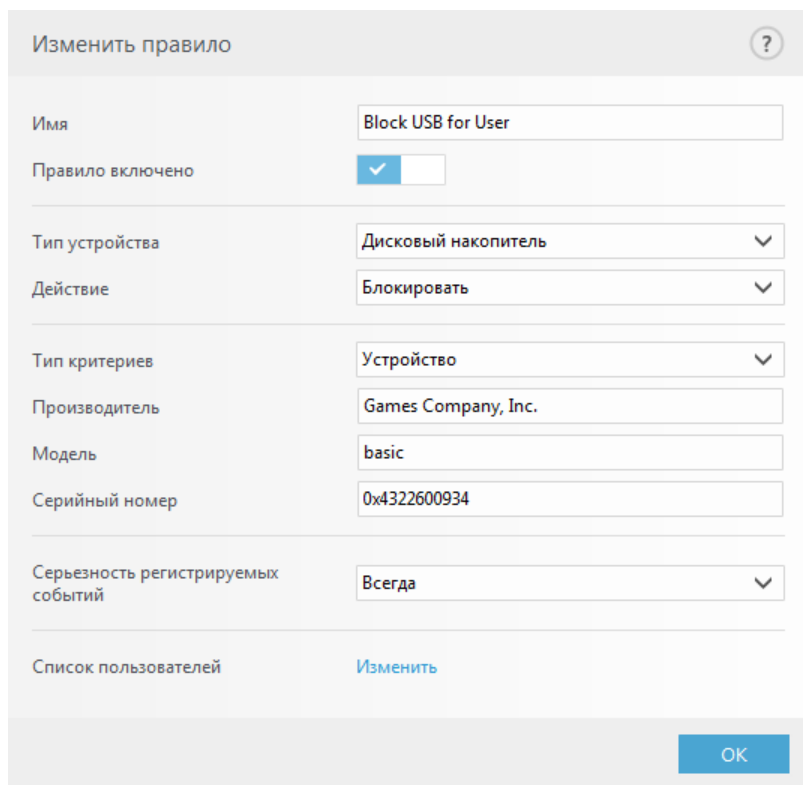
Правила приведены в порядке их приоритета: имеющие более высокий приоритет правила располагаются ближе к началу списка. Для перемещения отдельных правил или групп правил используйте кнопки

 **В начало/Вверх/Вниз/В конец.**

В журнал контроля устройств записываются все случаи, когда срабатывает функция контроля устройств. Записи журнала можно просмотреть в главном окне программы ESET Endpoint Security в разделе **Служебные программы** > [Файлы журнала](#).

3.9.1.5.2 Добавление правил контроля устройств

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



Имя	Block USB for User
Правило включено	<input checked="" type="checkbox"/>
Тип устройства	Дисковый накопитель
Действие	Блокировать
Тип критериев	Устройство
Производитель	Games Company, Inc.
Модель	basic
Серийный номер	0x4322600934
Серьезность регистрируемых событий	Всегда
Список пользователей	Изменить

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.

Применять во время: позволяет применять созданное правило в определенное время. В раскрывающемся меню выберите созданный временной интервал. Чтобы получить дополнительные сведения, щелкните здесь.

Тип устройства

В раскрывающемся меню 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.

i ПРИМЕЧАНИЕ.

Функция списка пользователей недоступна для модемов. Правило применяется ко всем пользователям, а текущий список пользователей удаляется.

Действие

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

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

Обратите внимание, что полный список действий (прав) доступен не для всех типов устройств. Если устройство относится к типу хранилищ, будут доступны все четыре действия. Если устройство не предназначено для хранения данных, доступны будут только три действия. Например, право **Только чтение** неприменимо к Bluetooth-устройствам, поэтому доступ к ним можно только разрешить, заблокировать или разрешить с предупреждением.

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** — имя 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.

i 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

- **Всегда** — записываются все события.
- **Диагностика** — регистрируется информация, необходимая для тщательной настройки программы.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждение**: информация обо всех критических ошибках и предупреждениях записывается и отправляется на сервер ERA Server.
- **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.

i ПРИМЕЧАНИЕ.

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

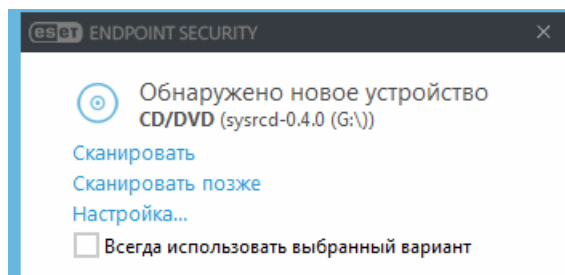
3.9.1.6 Съёмные носители

ESET Endpoint Security обеспечивает автоматическое сканирование съёмных 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 съёмных носителей с нежелательным содержанием.

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

- **Не сканировать:** действия не будут выполняться, а окно **Обнаружено новое устройство** будет закрыто.
- **Автоматическое сканирование устройств:** выполняется сканирование подключенного съёмного носителя по требованию.
- **Показать параметры сканирования:** переход в раздел, где настраиваются действия со съёмными носителями.

Когда вставляется съёмный носитель, отображается следующее диалоговое окно:



Сканировать сейчас: запуск сканирования съёмного носителя.

Сканировать позже: сканирование съёмного носителя будет отложено.

Настройка: вызов дополнительных настроек.

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

Кроме того, в ESET Endpoint Security есть модуль контроля устройств, дающий возможность задавать правила использования внешних устройств на указанном компьютере. Дополнительные сведения об этом модуле см. в разделе [Контроль устройств](#).

3.9.1.7 Сканирование в состоянии простоя

Вы можете разрешить сканирование в состоянии простоя, выбрав **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, щелкнув переключатель **Сканировать даже в случае работы компьютера от аккумулятора** в разделе «Дополнительные настройки».

В дополнительных настройках выберите параметр **Включить ведение журналов**, чтобы результаты сканирования компьютера регистрировались в разделе [Файлы журналов](#) (в главном окне программы перейдите в **Служебные программы > Файлы журналов** и выберите **Сканирование компьютера** в раскрывающемся меню **Журнал**).

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

- выключенный экран или заставка;
- блокировка компьютера;
- выход пользователя.

Выберите [Настройка параметров модуля ThreatSense](#) для изменения параметров сканирования (например, методов обнаружения) для сканирования в состоянии простоя.

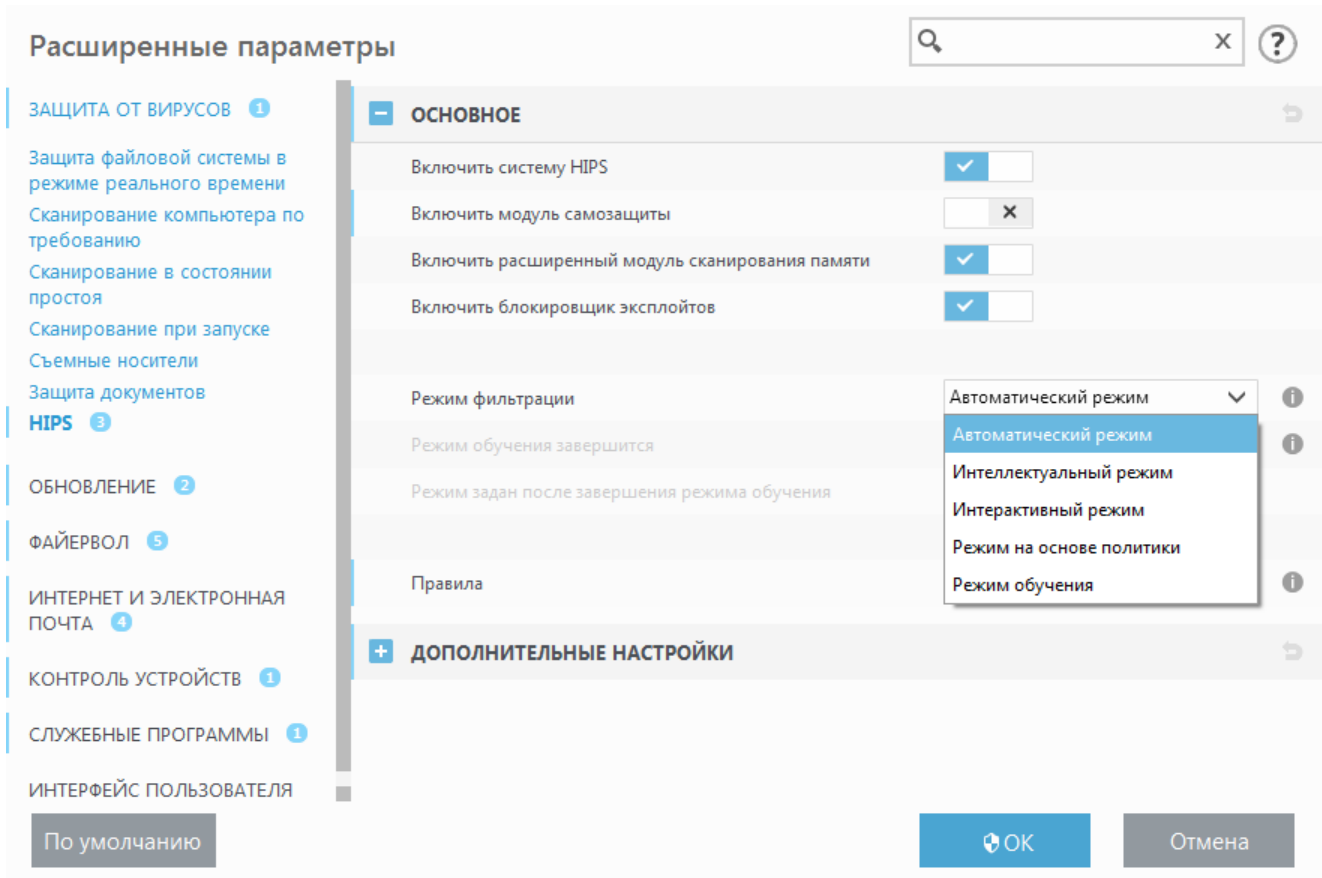
3.9.1.8 Система предотвращения вторжений на узел

ВНИМАНИЕ!

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 файрволом; 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 Endpoint Security, в разделе **Установка > Компьютер**.



В ESET Endpoint Security используется встроенная в систему HIPS технология **самозащиты**, которая не позволяет вредоносным программам повредить или отключить защиту от вирусов и шпионских программ. Модуль самозащиты обеспечивает защиту самых важных процессов системы и программы ESET, разделов реестра и файлов от вмешательства.

Расширенный модуль сканирования памяти работает в сочетании с блокировщиком эксплойтов для усиления защиты от вредоносных программ, которые могут избегать обнаружения продуктами для защиты от вредоносных программ за счет использования умышленного запутывания или шифрования. 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](#).

Защита от программ-шантажистов: это еще один уровень защиты, функционирующий как компонент системы HIPS. Для работы модуля защиты от программ-шантажистов необходимо, чтобы система репутации LiveGrid® была включена. Дополнительную информацию об этом типе защиты см. [здесь](#).

Доступны четыре режима фильтрации.

Автоматический режим: включены все операции за исключением тех, которые заблокированы предварительно заданными правилами, защищающими компьютер.

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

Интерактивный режим: пользователь будет получать запросы на подтверждение операций.

Режим на основе политики: операции блокируются.

Режим обучения: операции включены, и после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в редакторе правил, но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. При выборе режима обучения в раскрывающемся меню режимов фильтрации HIPS становится доступным параметр **Режим обучения завершится**. Выберите длительность для

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

Режим задан после завершения режима обучения: определите режим фильтрации, который будет восстановлен файрволом программы ESET Endpoint Security по завершении периода использования режима обучения.

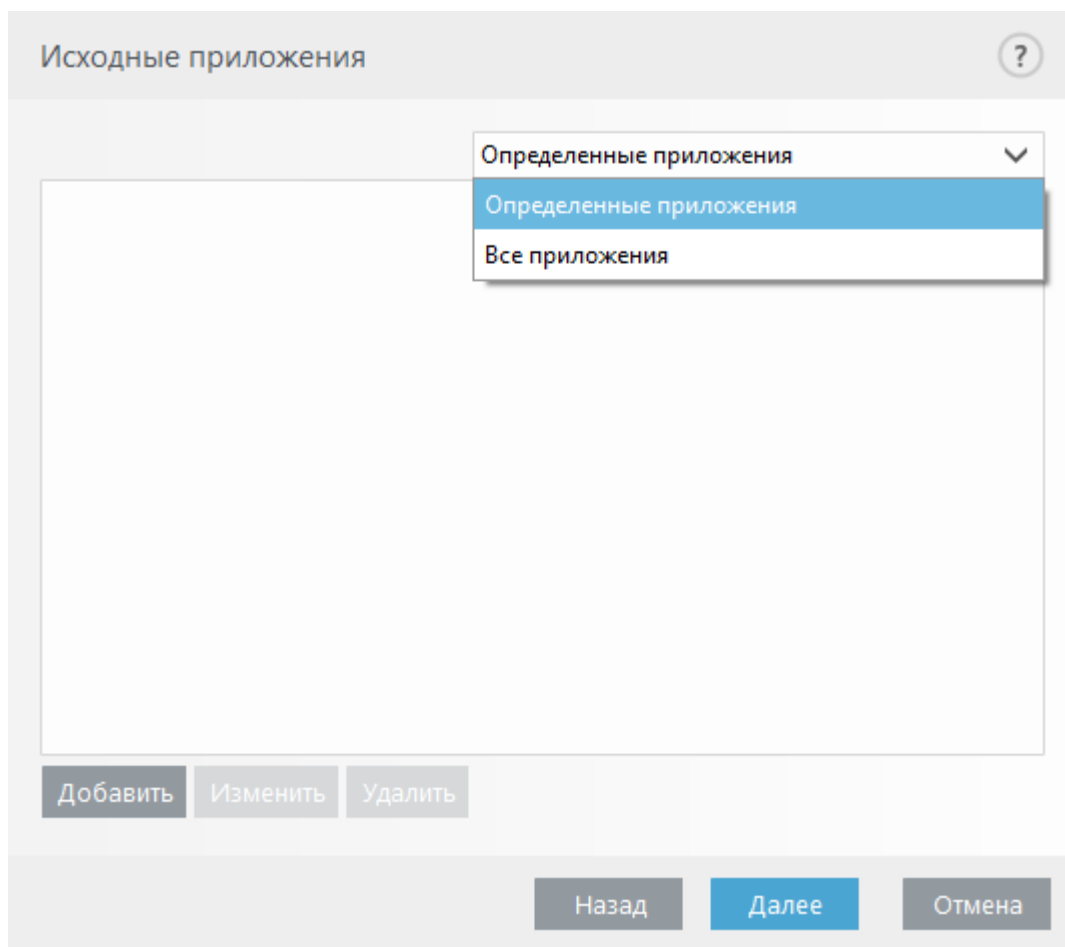
Система HIPS отслеживает события в операционной системе и реагирует на них соответствующим образом на основе правил, которые аналогичны правилам файрвола. Нажмите кнопку **Настроить**, чтобы открыть окно управления правилами системы HIPS. Здесь можно выбирать, создавать, изменять и удалять правила.

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

Параметры правил HIPS ?

Имя правила	<input type="text" value="Example"/>
Действие	<input type="text" value="Разрешить"/>
Операции влияния	
Файлы	<input type="checkbox"/>
Приложения	<input checked="" type="checkbox"/>
Записи реестра	<input type="checkbox"/>
Включено	<input checked="" type="checkbox"/>
Серьезность регистрируемых событий	<input type="text" value="Нет"/>
Уведомить пользователя	<input checked="" type="checkbox"/>

1. Присвойте правилу имя и выберите **Блокировать** в раскрывающемся меню **Действие**.
2. В разделе **Операции влияния** выберите хотя бы одну операцию для запуска.
3. Выберите пункт **Серьезность регистрируемых событий** в раскрывающемся меню. Записи с уровнем детализации Предупреждение могут собираться средством Remote Administrator.
4. Активируйте переключатель **Уведомить пользователя**, чтобы уведомление отображалось при каждом применении правила. Щелкните **Далее**.



5. 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. Щелкните **Далее**.
6. В следующем окне установите ползунок рядом с вариантом **Изменить состояние другого приложения** и щелкните **Далее**. (все операции описаны в справке продукта, которую можно открыть, нажав клавишу F1)..
7. Выберите в раскрывающемся списке вариант **Определенные приложения** и **добавьте** одно или несколько приложений, которые нужно защитить.
8. Нажмите кнопку **Готово**, чтобы сохранить новое правило.

3.9.1.8.1 Дополнительные настройки

Перечисленные далее параметры полезны для отладки и анализа поведения приложения.

Драйверы, загрузка которых разрешена всегда: загрузка выбранных драйверов разрешена всегда, независимо от настроенного режима фильтрации, если они не заблокированы в явном виде правилом пользователя.

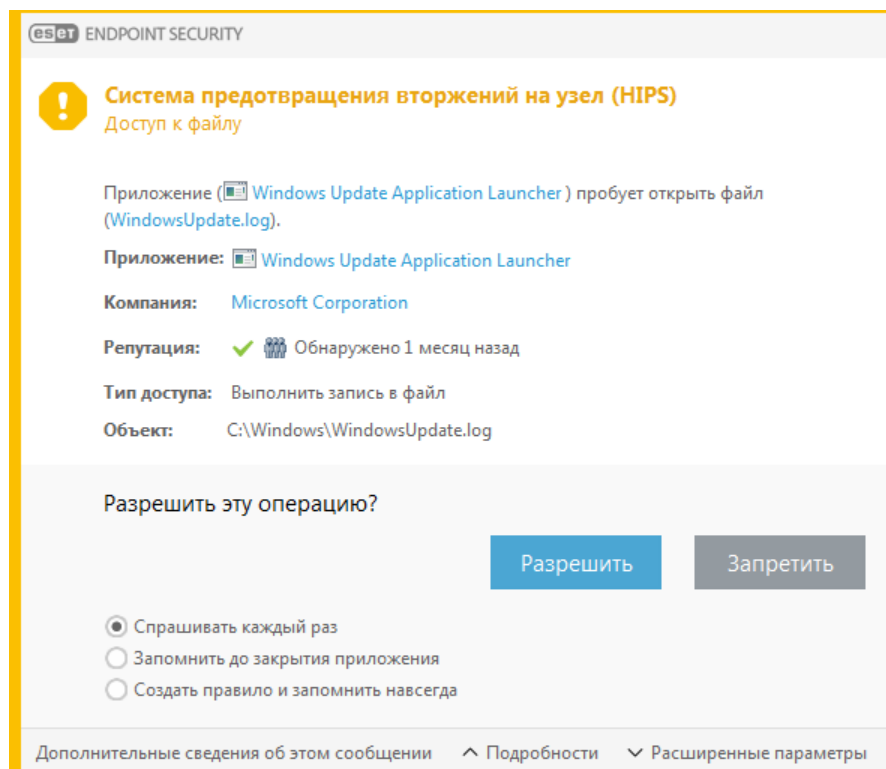
Регистрировать все заблокированные операции: все заблокированные операции будут записываться в журнал HIPS.

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

Обновленную версию этой страницы справочной системы см. в [статье базы знаний ESET](#).

3.9.1.8.2 Интерактивное окно HIPS

Если для правила по умолчанию установлено действие **Запрашивать**, то при каждом запуске правила будет отображаться диалоговое окно. Для операции также можно выбрать другие 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.

Выбор параметра **Временно запомнить это действие для данного процесса** приводит к использованию действия (**Разрешить/Запретить**) до тех пор, пока не будут изменены правила или режимы фильтрации, не будет обновлен модуль системы HIPS или не будет выполнена перезагрузка компьютера. После выполнения любого из этих трех действий временные правила удаляются.

3.9.1.8.3 Обнаружено потенциальное поведение программы-шантажиста

При обнаружении потенциального поведения, характерного для программы-шантажиста, отображается диалоговое окно. В нем можно **запретить** или **разрешить** операцию.



Данное диалоговое окно позволяет **отправить файл на анализ** или **исключить из проверки**. Нажмите кнопку **Сведения**, чтобы просмотреть конкретные параметры обнаружения.

! ВАЖНО!

Для правильной работы модуля защиты от программ-шантажистов система ESET Live Grid должна быть включена.

3.9.1.9 Режим презентации

Режим презентации — это функция для тех, кто стремится избежать перерывов в работе программного обеспечения и появления отвлекающих от дел всплывающих окон, а также желает свести к минимуму нагрузку на процессор. Его также можно использовать во время проведения презентаций, которые нельзя прерывать деятельностью модуля защиты от вирусов. Он блокирует появление всплывающих окон и выполнение запланированных задач. Защита системы по-прежнему работает в фоновом режиме, но не требует какого-либо вмешательства со стороны пользователя.

Выберите **Настройки > Компьютер** и затем щелкните переключатель напротив **Режима презентации** для его ручного включения. В окне **Дополнительные настройки (F5)** выберите **Служебные программы > Режим презентации** и затем щелкните переключатель **Автоматически включать режим презентации при выполнении приложений в полноэкранном режиме**, чтобы при запуске приложений в полноэкранном режиме продукт ESET Endpoint Security автоматически переходил в режим презентации. Включая режим презентации вы подвергаете систему угрозе, поэтому значок состояния защиты на панели задач станет оранжевым, чтобы тем самым предупредить вас. Данное предупреждение также отобразится в главном окне программы: в нем вы увидите надпись **Режим презентации включен** оранжевого цвета.

Если установить флажок **Автоматически включать режим презентации при работе приложений в полноэкранном режиме**, режим презентации будет включаться при запуске любого приложения в полноэкранном режиме и автоматически выключаться после выхода из этого приложения. Это особенно удобно для включения режима презентации непосредственно при запуске игры, полноэкранного приложения или презентации.

Вы также можете выбрать **Автоматически отключать режим презентации через** для указания времени в минутах, через которое режим презентации будет автоматически отключен.

i ПРИМЕЧАНИЕ.

Если файрвол работает в интерактивном режиме и включен режим презентации, возможны проблемы при подключении к Интернету. Это может представлять сложности, если запускается игра, в которой используется подключение к Интернету. Обычно пользователю предлагается подтвердить нужное действие (если не задано никаких правил или исключений для подключения), но в режиме презентации взаимодействие с пользователем невозможно. В качестве решения можно задать правило подключения для каждого приложения, которое может конфликтовать с таким поведением, или использовать другой [Режим фильтрации](#) в файрволе. Также следует помнить о том, что при включенном режиме презентации может быть заблокирован переход на веб-страницу или использование приложения, которые могут представлять угрозу для безопасности, но при этом на экран не будет выведено никакого пояснения или предупреждения, поскольку взаимодействие с пользователем отключено.

3.9.1.10 Сканирование файлов, исполняемых при запуске системы

При загрузке компьютера и обновлении модулей по умолчанию 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 при запуске системы**. Чтобы изменить эти параметры, выберите **Служебные программы > Планировщик**, нажмите кнопку **Автоматическая проверка файлов при запуске системы**, а затем — кнопку **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](#).

3.9.1.10.1 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 **Объекты сканирования** 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, которые запускаются перед входом пользователя:** содержит файлы из таких папок, которые можно открыть без входа пользователя в систему (в том числе большинство элементов, исполняемых при запуске системы: службы, объекты модуля поддержки браузера, уведомления Winlogon, задания в планировщике Windows, известные библиотеки DLL и т. д.).
- **Файлы, 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.
- **Самый низкий:** минимальная нагрузка на систему.
- **Более низкий:** низкая нагрузка на систему.
- **Средний:** средняя нагрузка на систему.

3.9.1.11 Защита документов

Функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, такие как элементы Microsoft ActiveX. Функция защиты документов обеспечивает безопасность в дополнение к функции защиты файловой системы в 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).

3.9.1.12 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. Случаи, в которых может понадобиться исключить объекты, включают сканирование больших баз данных, которые замедляет работу или программ, конфликтующих с процессом сканирования (например, программное обеспечение для резервного копирования).

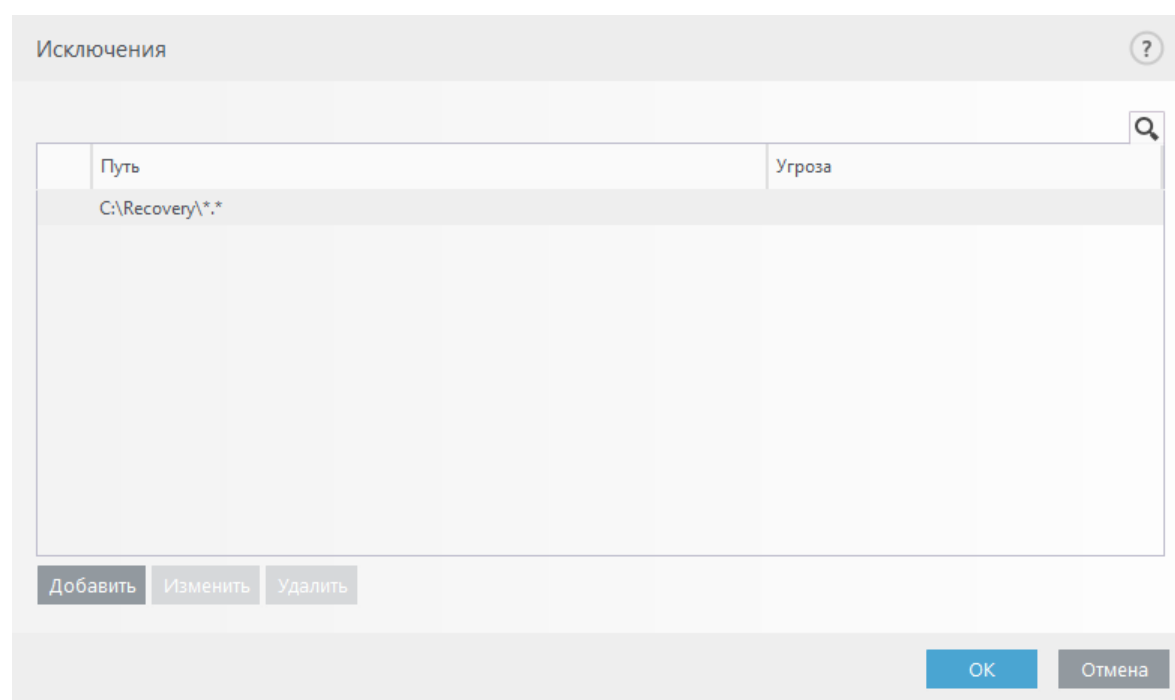
Для исключения объекта из сканирования выполните следующие действия.

1. Нажмите **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

- Чтобы исключить все файлы в папке, укажите путь к папке и используйте 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 число символов (и символы могут меняться), причем известна только первая буква имени (например, D), используйте следующий формат: D?????.exe. Вопросительные знаки замещают отсутствующие (неизвестные) символы.



i 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, это значит, что файл сканируется на наличие всех угроз, кроме этой. Если этот файл позже окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит. Этот тип исключений можно использовать только для определенных типов заражений. Создать такое исключение можно либо в окне предупреждения об угрозе, в котором сообщается о заражении (последовательно щелкните элементы **Показать расширенные параметры** > **Исключить из**

обнаружения), либо в разделе **Сервис > Карантин**, щелкнув правой кнопкой мыши файл на карантине и выбрав в контекстном меню пункт **Восстановить и исключить из обнаружения**.

Элементы управления

Добавить: команда, исключающая объекты из сканирования.

Изменить: изменение выделенных записей.

Удалить: удаление выделенных записей.

3.9.1.13 Параметры ThreatSense

ThreatSense — это технология, состоящая из множества сложных методов обнаружения угроз. Эта технология является упреждающей, т. е. она защищает от новой угрозы уже в начале ее распространения. При этом используется сочетание анализа и моделирования кода, обобщенных сигнатур и сигнатур вирусов, которые совместно значительно повышают уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что делает эффективность и количество обнаруживаемых угроз максимальными. Технология ThreatSense также успешно уничтожает руткиты.

Для модуля ThreatSense 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 **Настройка параметров модуля ThreatSense** в окне дополнительных настроек 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.

Параметры ThreatSense 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: сканирование на наличие угроз, которые атакуют оперативную память системы.

Загрузочные секторы/UEFI: сканирует загрузочные секторы и UEFI на наличие руткитов, буткитов и других вредоносных программ. Чтобы получить дополнительные сведения, щелкните [здесь](#).

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

Архивы: программа поддерживает такие расширения, как 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: архивы (файлы с расширением SFX), которым для распаковки не нужны специальные программы.

Программы сжатия исполняемых файлов: в отличие от стандартных типов архивов, программы сжатия исполняемых файлов после запуска распаковываются в 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 вредоносной активности программ с помощью специального алгоритма. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей версии модуля обновления. Недостатком же является вероятность (очень небольшая) ложных тревог.

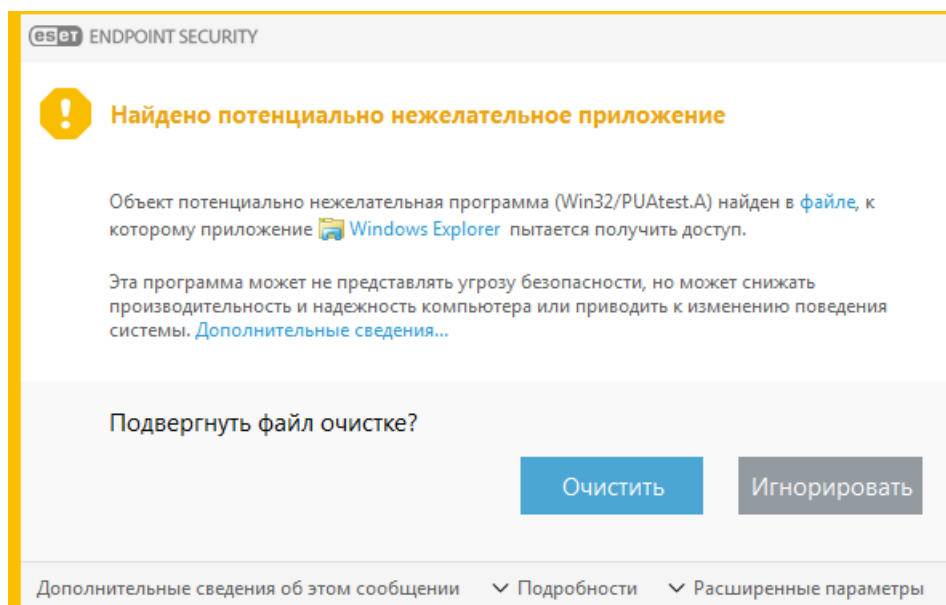
Расширенный эвристический анализ/сигнатуры распределенных сетевых атак: для расширенного эвристического анализа используется уникальный эвристический алгоритм компании ESET, который оптимизирован для обнаружения компьютерных червей и троянских программ и написан на высокоуровневых языках программирования. Использование расширенной эвристики значительным образом увеличивает возможности продуктов ESET по обнаружению угроз. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает наличие новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).

Потенциально нежелательное приложение содержит рекламу, устанавливает панели инструментов или выполняет другие неясные функции. В некоторых ситуациях может показаться, что преимущества такого 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

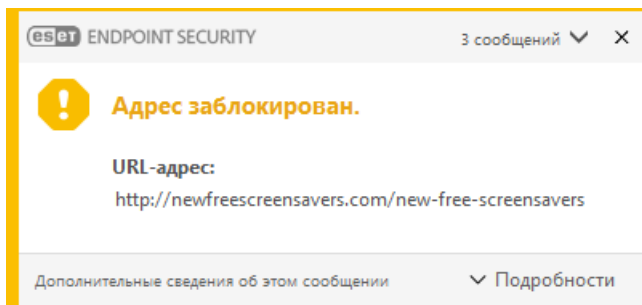
Когда обнаруживается потенциально нежелательное приложение, вы можете самостоятельно решить, какое действие нужно выполнить.

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



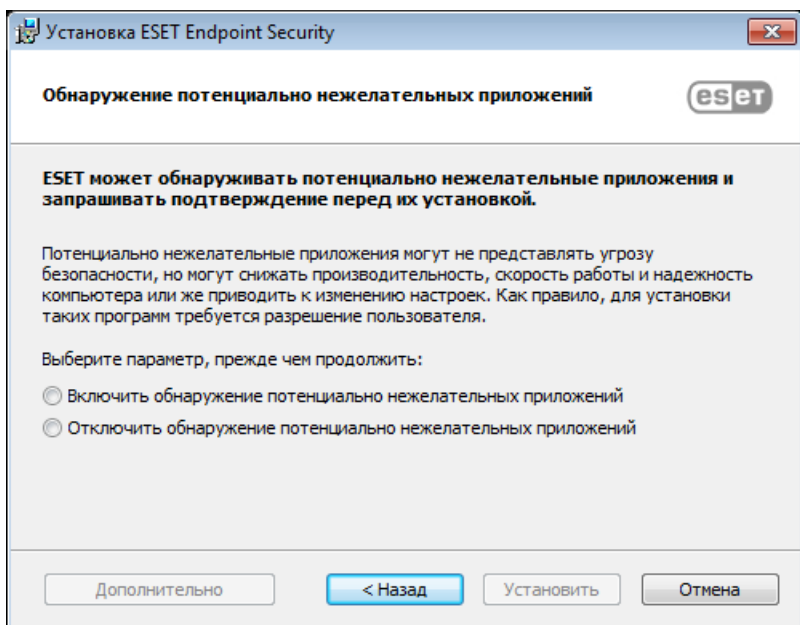
Если обнаружено потенциально нежелательное приложение и его невозможно очистить, в правом нижнем углу экрана отобразится окно уведомлений **Адрес заблокирован**. Дополнительные сведения об этом событии можно получить, последовательно щелкнув в главном меню элементы **Сервис > Файлы журнала >**

Отфильтрованные веб-сайты.



Потенциально нежелательные приложения — параметры

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

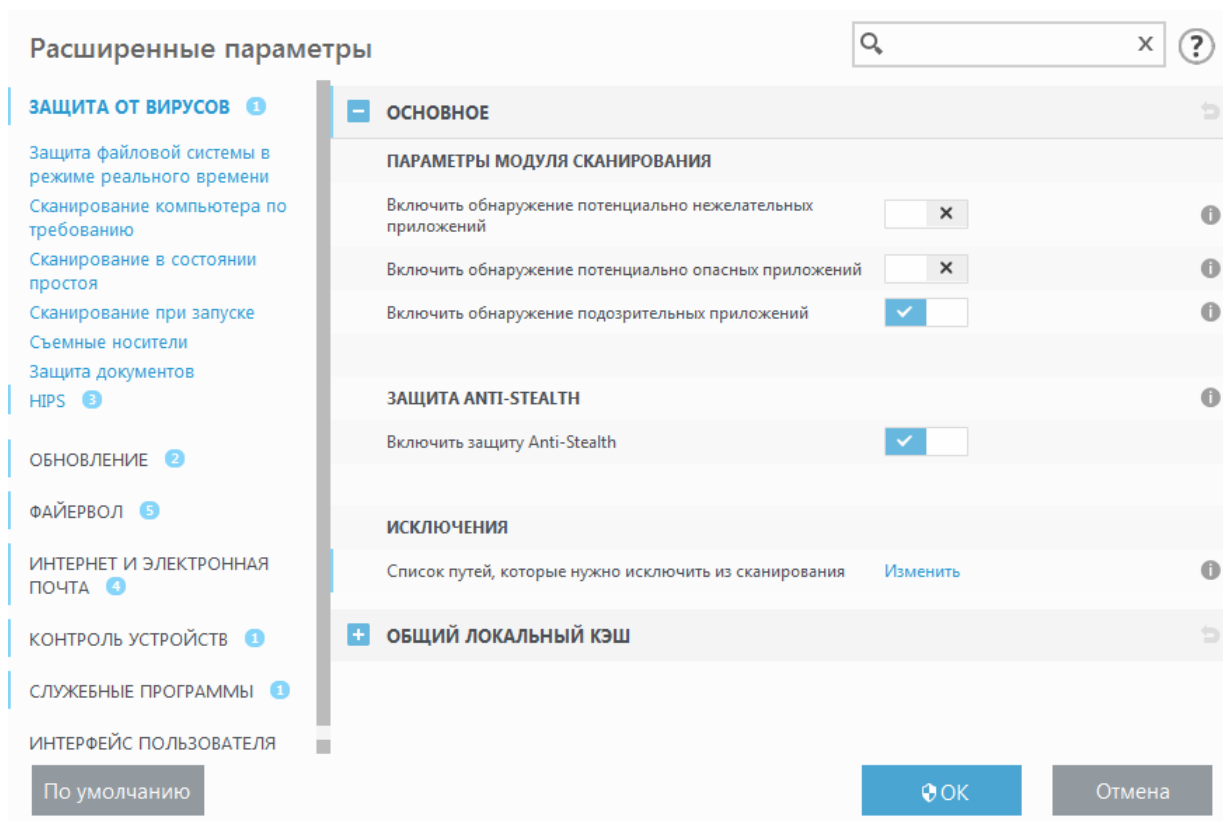


⚠ ВНИМАНИЕ!

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 нижеприведенным инструкциям.

1. Откройте программу ESET. [Как открыть мой продукт ESET?](#)
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 **OK**.



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 рекламой, которые изменяют домашнюю страницу браузера или параметры поиска. При этом файлообменные ресурсы часто не уведомляют производителя программного обеспечения или пользователей 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 этой страницы справочной системы см. в этой [статье базы знаний ESET](#).

Для получения дополнительных сведений щелкните [здесь](#).

Потенциально опасное ПО: к [такому ПО](#) относится нормальное коммерческое программное обеспечение, такое как служебные программы удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, записывающие каждое нажатие клавиши на клавиатуре). По умолчанию этот параметр отключен.

Очистка

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

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

Обычная очистка: программа пытается автоматически очистить или удалить зараженный файл на основе предварительно 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.

ВНИМАНИЕ!

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.

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 модуля ThreatSense также доступны представленные ниже параметры раздела **Другое**.

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

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

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

Включить оптимизацию Smart: 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 интеллектуальная оптимизация отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы сохранить исходное значение времени доступа к сканируемым файлам, а не обновлять их (например, для использования с системами резервного копирования данных).

Ограничения

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

Параметры объектов

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*.

Максимальная продолжительность сканирования объекта (с): определяет максимальное значение времени сканирования объекта. Если пользователь укажет здесь собственное значение, модуль защиты от вирусов прекратит сканирование объекта по истечении указанного времени вне зависимости от того, было ли сканирование завершено. Значение по умолчанию: *не ограничено*.

Настройки сканирования архивов

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

Максимальный размер файла в архиве: этот параметр позволяет задать максимальный размер файлов в архиве (при их извлечении), которые должны сканироваться. Значение по умолчанию: *не ограничено*.

i ПРИМЕЧАНИЕ.

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

3.9.1.13.1 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.

По умолчанию сканируются все файлы. 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 определенных расширений. Чтобы добавить в список новое расширение, щелкните **Добавить**, введите в пустое поле расширение и нажмите кнопку **ОК**. Выбрав **Введите несколько значений**, вы можете добавлять несколько расширений файлов, разделенных переводом строки, запятыми или точками с запятой. Если разрешен ввод нескольких значений, расширения будут отображаться в виде списка. Чтобы удалить расширение из списка, выберите его и нажмите кнопку **Удалить**. Для изменения выбранного расширения щелкните **Изменить**.


Возможно использование следующих специальных символов: ? (вопросительный знак). Звездочка вопросительный знак — любой отдельный символ.

i ПРИМЕЧАНИЕ.

Чтобы расширение (тип файла) отображалось для всех файлов в операционной системе Windows, снимите флажок **Скрывать расширения для зарегистрированных типов файлов**, выбрав **Панель управления > Свойства папки > Вид**.

3.9.2 Сеть

Файервол управляет всем входящим и исходящим сетевым трафиком компьютера. Процесс основан на разрешении или запрете отдельных сетевых соединений в соответствии с правилами фильтрации. Персональный файервол обеспечивает защиту от атак со стороны удаленных компьютеров и блокирует некоторые потенциально опасные службы. Файервол также обеспечивает возможности IDS/IPS посредством контроля содержимого разрешенного сетевого трафика и блокировки трафика, который определен как потенциально опасный. ESET Endpoint Security проинформирует вас при попытке подключения к незащищенной беспроводной сети или сети со слабой защитой.

Настройки **файервола** доступны в области **Настройка** в разделе **Сеть**. Здесь можно настроить режим фильтрации для файервола ESET. Также можно получить доступ к дополнительным настройкам, щелкнув значок шестеренки  > **Настройка** рядом с элементом **Файервол** или нажав клавишу **F5**, которая вызывает меню **Дополнительные настройки**.

Защита от сетевых атак (IDS): анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который расценивается как опасный, блокируется. Защиту от сетевых атак можно на некоторое время отключить. Для этого щелкните элемент

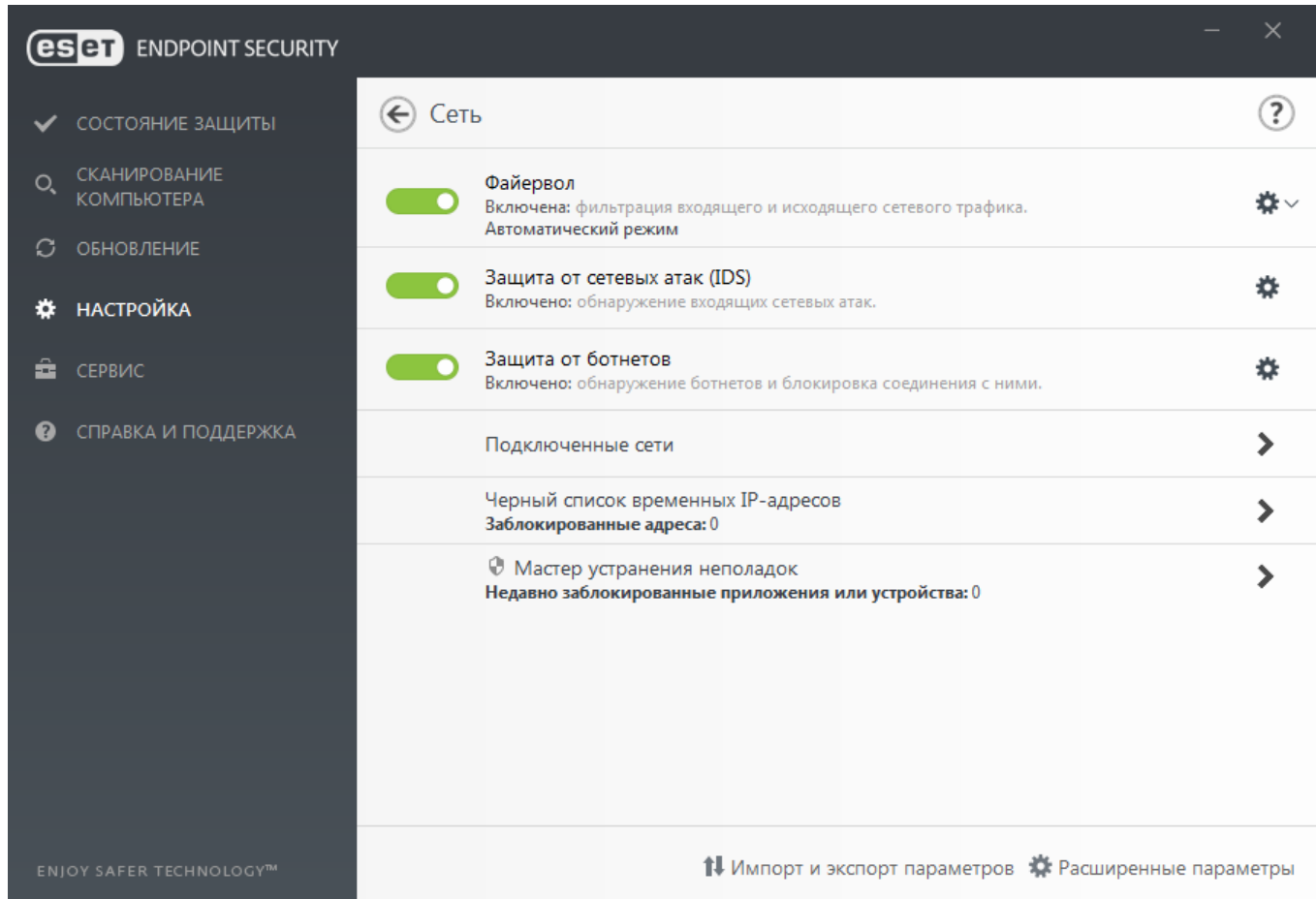
Защита от ботнетов: быстро и точно определяет вредоносные программы в системе. Защиту от ботнетов можно на некоторое время отключить. Для этого щелкните элемент

Подключенные сети: отображение сетей, к которым подключены сетевые адаптеры. При нажатии значка шестеренки появляется возможность выбрать тип защиты сети, к которой выполнено подключение посредством сетевого адаптера.

Сетевые адаптеры: отображение всех сетевых адаптеров, а также назначенных им профилей файервола и доверенных зон. Для получения дополнительных сведений см. раздел Сетевые адаптеры.

Черный список временных IP-адресов: отображение списка IP-адресов, которые были обнаружены как источники атак и добавлены в «черный» список для блокировки соединений в течение определенного периода времени. Чтобы получить дополнительную информацию, щелкните этот параметр и нажмите клавишу F1.

Мастер устранения неполадок: помогает устранять проблемы с подключением, вызванные файерволом ESET. Для получения дополнительных сведений см. раздел [Мастер устранения неполадок](#).



Щелкните значок шестеренки  рядом с элементом **Файервол**, чтобы открыть следующие настройки.

Настроить...: открытие окна «Файервол» в меню дополнительных настроек, в котором можно определить, каким образом файервол будет обрабатывать сетевые подключения.

Блокировать весь трафик: все входящие и исходящие соединения будут блокироваться файерволом. Используйте этот параметр только в особых случаях, когда возникает опасная критическая ситуация, требующая немедленного отключения от сети. Если для фильтрации сетевого трафика выбрано состояние **Блокировать весь трафик**, щелкните **Остановить блокировку всего трафика**, чтобы восстановить нормальную работу файервола.

Приостановить работу файервола (разрешить весь трафик): действие, обратное действию параметра блокирования всего сетевого трафика. В этом режиме файервол отключает все функции фильтрации и разрешает все входящие и исходящие соединения. Щелкните **Включить файервол**, чтобы повторно включить файервол, когда для фильтрации сетевого трафика выбран этот режим.

Автоматический режим (если включен другой режим фильтрации): воспользуйтесь этой командой, чтобы перевести фильтрацию в автоматический режим (с учетом правил, определяемых пользователем).

Интерактивный режим (если включен другой режим фильтрации): воспользуйтесь этой командой, чтобы перевести фильтрацию в интерактивный режим.

3.9.2.1 Файервол

Файервол управляет всем входящим и исходящим сетевым трафиком компьютера. Процесс основан на запрете или разрешении отдельных сетевых соединений в соответствии с определенными правилами. Файервол обеспечивает защиту от атак с удаленных компьютеров и позволяет блокировать некоторые службы. Он также предоставляет защиту от вирусов для протоколов HTTP, POP3 и IMAP. Функционально модуль является очень важным элементом системы безопасности компьютера.

Включить защиту от сетевых атак (IDS). Анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который расценивается как опасный, блокируется.

Включить защиту от ботнетов. Обнаружение и блокирование подключений к вредоносным серверам командования и управления. В основе функции лежит распознавание стандартных шаблонов, с помощью которых зараженный ботом компьютер пытается подключиться к опасным серверам.

В файерволе ESET Endpoint Security есть четыре режима фильтрации. Параметры режимов фильтрации доступны в разделе **Дополнительные настройки (F5)**, если щелкнуть меню **Файервол**. Поведение персонального файервола зависит от режима фильтрации. Кроме того, от выбранного режима фильтрации зависит степень участия пользователя в процессе.

Доступны четыре режима фильтрации.

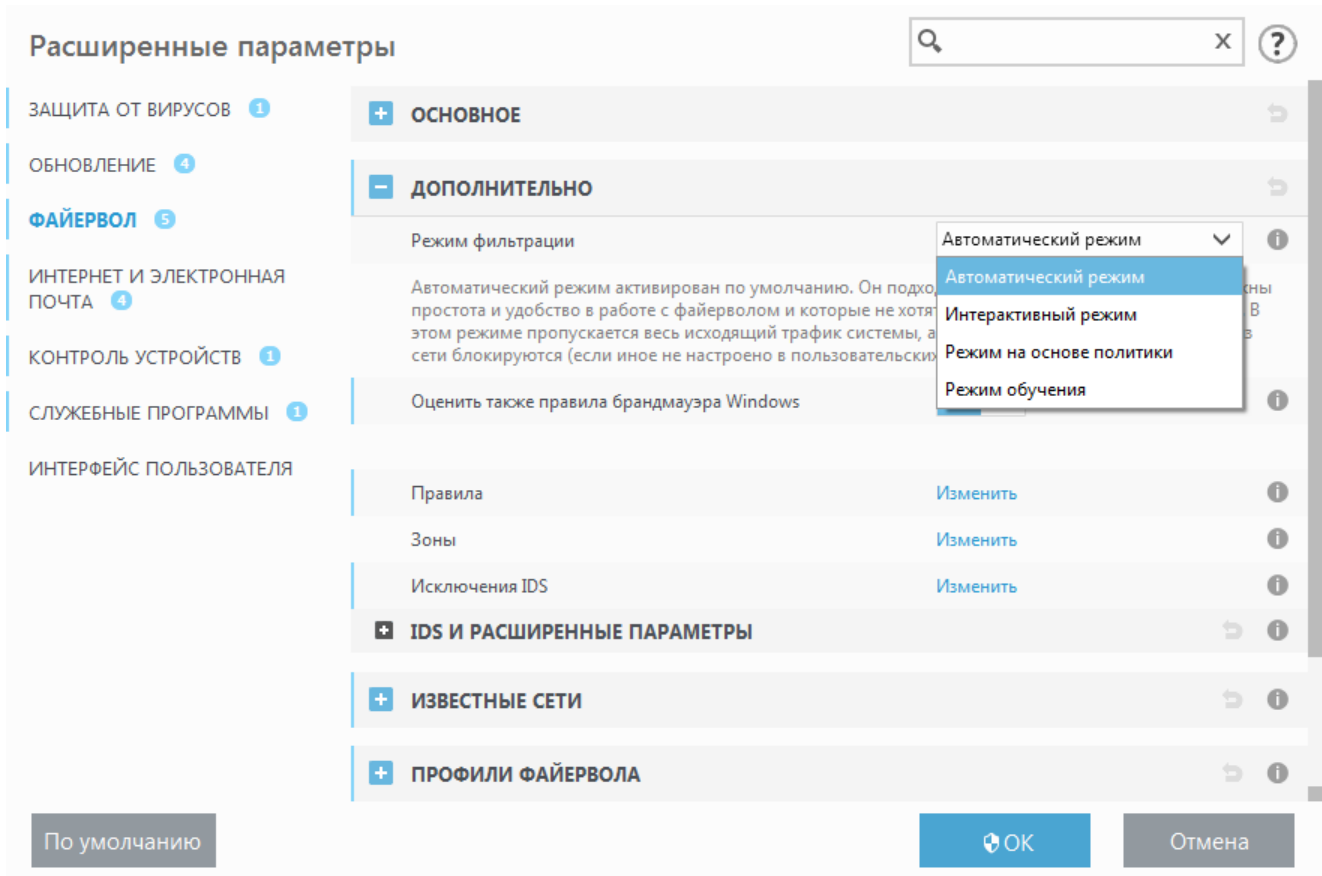
Автоматический режим: режим по умолчанию. Этот режим подходит для пользователей, которым нравится простота и удобство в использовании персонального файервола, а также то, что нет необходимости создавать правила. В режиме по умолчанию можно создавать пользовательские правила, однако это не необходимо. Автоматический режим разрешает весь исходящий трафик для системы и блокирует большую часть входящего трафика (кроме трафика из доверенной зоны в соответствии с разделами IDS и расширенные параметры/Разрешенные службы и входящего трафика в ответ на недавние исходящие соединения к тому же удаленному сайту).

Интерактивный режим: позволяет создать собственную конфигурацию файервола. Если обнаружено соединение, на которое не распространяется ни одно из существующих правил, на экран выводится диалоговое окно с уведомлением о неизвестном подключении. В этом диалоговом окне можно разрешить или запретить соединение, а также на основе этого решения создать правило для применения в будущем. Если принимается решение о создании нового правила, в соответствии с этим правилом все будущие соединения этого типа будут разрешены или запрещены.

Режим на основе политики: блокирует все соединения, которые не удовлетворяют ни одному из ранее определенных разрешающих правил. Этот режим предназначен для опытных пользователей, которые могут создавать правила, разрешающие только нужные и безопасные соединения. Все прочие неуказанные соединения будут блокироваться файерволом.

Режим обучения: автоматическое создание и сохранение правил. Этот режим удобен для первоначальной настройки файервола. Участие пользователя не требуется, потому что ESET Endpoint Security сохраняет правила согласно предварительно настроенным параметрам. Режим обучения является небезопасным, поэтому рекомендуется использовать его только до момента создания правил для всех необходимых соединений.

[Профили](#) можно использовать для настройки поведения файервола ESET Endpoint Security, указывая разные наборы правил для разных ситуаций.



Оценить также правила брандмауэра Windows: если этот параметр включен, то в автоматическом режиме разрешен входящий трафик, разрешенный брандмауэром Windows и не заблокированный правилами файрвола ESET Endpoint Security.

Правила: здесь можно добавлять правила и определять принцип обработки сетевого трафика файрволом.

Зоны: здесь можно создавать зоны, состоящие из нескольких IP-адресов.

IDS и расширенные параметры: здесь можно настроить расширенные параметры фильтрации и функциональность системы IDS (используется для обнаружения некоторых типов атак и эксплойтов).

Исключения IDS: здесь можно добавлять исключения IDS и настраивать способы реагирования на вредоносные действия.

3.9.2.1.1 Режим обучения

В режиме обучения правила для каждого соединения, установленного системой, создаются и сохраняются автоматически. Участие пользователя не требуется, потому что ESET Endpoint Security сохраняет правила согласно предварительно настроенным параметрам.

Использование этого режима может представлять риск для системы, и его рекомендуется использовать только для первоначальной настройки файрвола.

Для отображения настроек режима обучения активируйте его в разделе **Дополнительные настройки (F5) > Файрвол > Настройки режима обучения**. В этом разделе представлены следующие параметры.

⚠ ВНИМАНИЕ!

В режиме обучения файрвол не фильтрует соединения. Разрешены все исходящие и входящие соединения. В этом режиме компьютер защищен файрволом не полностью.

Режим задан после завершения режима обучения: определите режим фильтрации, который будет восстановлен файерволом программы ESET Endpoint Security по завершении периода использования режима обучения. См. дополнительные сведения о [режимах фильтрации](#).

Тип соединения: настройка отдельных параметров создания правил для каждого типа соединений. Существует четыре типа соединений.

- **Входящий трафик из доверенной зоны:** примером входящего соединения в доверенной зоне является удаленный компьютер, находящийся в пределах доверенной зоны, который пытается установить соединение с приложением, запущенным на локальном компьютере.
- **Исходящий трафик в доверенную зону:** приложение на локальном компьютере пытается установить соединение с другим компьютером в пределах локальной сети или сети в доверенной зоне.
- **Входящий интернет-трафик:** удаленный компьютер пытается установить соединение с приложением, запущенным на компьютере.
- **Исходящий интернет-трафик:** приложение на локальном компьютере пытается установить соединение с другим компьютером.

В каждом разделе определяются параметры, которые будут добавляться к новым правилам.

Добавить локальный порт: включает номер локального порта сетевого соединения. Для исходящих соединений обычно создаются случайные номера, поэтому данный параметр рекомендуется включать только для входящих соединений.

Добавить приложение: включает имя локального приложения. Данный параметр предназначен для использования в будущих правилах на уровне приложений (правилах, определяющих соединения для всего приложения). Например, можно разрешить соединения только для веб-браузера или почтового клиента.

Добавить удаленный порт: включает номер удаленного порта сетевого соединения. Например, можно разрешить или запретить подключение определенной службы, связанной со стандартным номером порта (HTTP — 80, POP3 — 110 и т. д.).

Добавить удаленный IP-адрес или удаленную доверенную зону: удаленный IP-адрес или удаленная зона могут использоваться в качестве параметра новых правил, регулирующих все соединения между локальной системой и соответствующим удаленным адресом или зоной. Этот параметр используется при определении действия для конкретного компьютера или группы сетевых компьютеров.

Максимальное количество разных правил для одного приложения: если приложение подключается к разным IP-адресам через разные порты, файервол в режиме обучения создаст для этого приложения соответствующее количество правил. Данный параметр позволяет ограничить число правил, которые могут быть созданы для одного приложения.

3.9.2.2 Профили файервола

Профили позволяют контролировать поведение файервола ESET Endpoint Security. При создании или изменении правила файервола его можно назначить отдельному профилю или применить ко всем профилям. При выборе определенного профиля действуют только глобальные правила (правила без указания профиля) и правила, назначенные этому профилю. Вы можете создать несколько профилей с разными правилами для сетевых адаптеров или сетей, которые позволят легко менять поведение файервола.

Рядом со **списком профилей** щелкните **Изменить**. Откроется окно **Профили файервола**, в котором можно изменять профили.

Сетевой адаптер можно настроить на использование профиля, сконфигурированного для конкретной сети, когда он подключен к этой сети. Кроме того, можно указать конкретный профиль, который будет использоваться для определенной сети, для чего следует выбрать элементы **Дополнительные настройки (F5) > Файервол > Известные сети**. Выберите сеть из списка **Известные сети** и щелкните **Изменить**, чтобы назначить профиль файервола для конкретной сети из раскрывающегося меню **Профиль файервола**. С сетями, для которых не был назначен профиль, будет использоваться профиль адаптера по умолчанию. Если адаптер не настроен на использование профиля сети, будет использоваться его профиль по умолчанию вне зависимости

от того, к какой сети он подключен. Если в настройках сети или адаптера не указан профиль, применяется глобальный профиль по умолчанию. Для назначения профиля сетевого адаптера, выберите сетевой адаптер и щелкните **Изменить** рядом с списком **Профили, назначаемые сетевым адаптерам**, выберите профиль из раскрывающегося меню **Профиль файрвола по умолчанию** и затем нажмите **Сохранить**.

При переключении профилей файрвола в правом нижнем углу рядом с системными часами появляется соответствующее уведомление.

3.9.2.2.1 Профили, назначаемые сетевым адаптерам

Переключая профили, можно быстро изменять поведение файрвола. Для определенных профилей могут быть установлены и применяться пользовательские правила. Записи для всех сетевых адаптеров компьютера автоматически добавляются в список **Сетевые адаптеры**.

Столбцы

Имя: имя сетевого адаптера.

Профиль файрвола по умолчанию: профиль по умолчанию используется, когда вы подключаетесь к сети, для которой отсутствует настроенный профиль или отключено использование сетевого профиля сетевым адаптером.

Предпочитаемый профиль сети: если параметр **Предпочитаемый профиль сети** включен, сетевой адаптер будет использовать профиль файрвола, назначенный для подключенной сети, когда это возможно.

Элементы управления

Добавить: добавление нового сетевого адаптера.

Изменить: изменение существующего сетевого адаптера.

Удалить: выберите сетевой адаптер и щелкните **Удалить**, чтобы удалить выбранный адаптер из списка.

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

3.9.2.3 Настройка и использование правил


Правило содержит набор параметров и условий, которые позволяют проверять все сетевые соединения и выполнять необходимые действия в соответствии с этими условиями. С помощью правил файрвола можно задать действия, которые выполняются при установке сетевых соединений различных типов. Чтобы настроить правило фильтрации, откройте окно **Дополнительные настройки (F5) > Файрвол > Основная информация**. Некоторые предопределенные правила связаны с флажками из **разрешенных служб** (IDS и расширенные функции) и не могут быть отключены напрямую, вместо этого для их отключения необходимо отключить связанные с ними флажки.

В отличие от предыдущей версии ESET Endpoint Security, правила обрабатываются сверху вниз. Действие, определяемое первым соответствующим правилом, используется для каждого обрабатываемого сетевого соединения. Это важное изменение в поведении по сравнению с предыдущей версией, где приоритет определялся автоматическим и был выше у более специфических правил, чем у более общих.

Подключения можно разделить на входящие и исходящие. Входящие подключения инициируются удаленным компьютером, который пытается подключиться к локальной системе. При исходящем соединении, наоборот, локальный компьютер пытается подключиться к удаленному.

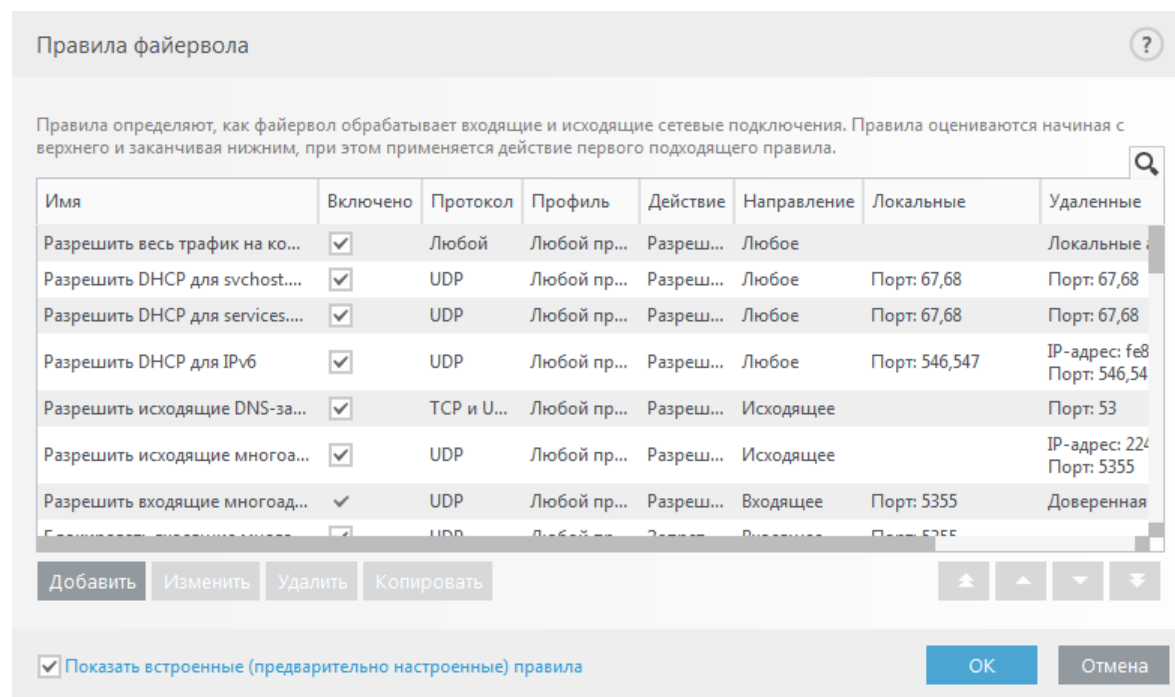
При возникновении неизвестного соединения пользователь должен разрешить или запретить его. Нежелательные, небезопасные или неизвестные соединения несут угрозу безопасности для компьютера. При установлении такого соединения рекомендуется обратить особое внимание на удаленный компьютер и приложение, которые пытаются установить это соединение с компьютером. Многие типы заражений пытаются получить и отправить личные данные или загрузить другие злонамеренные приложения на компьютер. Файрвол дает пользователю возможность обнаружить и разорвать такие подключения.

3.9.2.3.1 Правила файервола

На вкладке **Дополнительно** рядом с элементом **Правила** нажмите кнопку **Изменить**, чтобы открыть окно **Правила файервола**, в котором представлен список всех правил. С помощью команд **Добавить**, **Изменить** и **Удалить** можно добавлять, настраивать и удалять правила. Изменить уровень приоритета правила можно с помощью кнопок  **В начало/Вверх/Вниз/В конец**.

ПОДСКАЗКА.

Щелкните значок, чтобы искать правила по имени, протоколу или порту.



Правила определяют, как файервол обрабатывает входящие и исходящие сетевые подключения. Правила оцениваются начиная с верхнего и заканчивая нижним, при этом применяется действие первого подходящего правила.

Имя	Включено	Протокол	Профиль	Действие	Направление	Локальные	Удаленные
Разрешить весь трафик на ко...	<input checked="" type="checkbox"/>	Любой	Любой пр...	Разреш...	Любое		Локальные
Разрешить DHCP для svchost...	<input checked="" type="checkbox"/>	UDP	Любой пр...	Разреш...	Любое	Порт: 67,68	Порт: 67,68
Разрешить DHCP для services...	<input checked="" type="checkbox"/>	UDP	Любой пр...	Разреш...	Любое	Порт: 67,68	Порт: 67,68
Разрешить DHCP для IPv6	<input checked="" type="checkbox"/>	UDP	Любой пр...	Разреш...	Любое	Порт: 546,547	IP-адрес: fe8 Порт: 546,54
Разрешить исходящие DNS-за...	<input checked="" type="checkbox"/>	TCP и U...	Любой пр...	Разреш...	Исходящее		Порт: 53
Разрешить исходящие многоа...	<input checked="" type="checkbox"/>	UDP	Любой пр...	Разреш...	Исходящее		IP-адрес: 224 Порт: 5355
Разрешить входящие многоа...	<input checked="" type="checkbox"/>	UDP	Любой пр...	Разреш...	Входящее	Порт: 5355	Доверенная
Блокировать входящие много...	<input checked="" type="checkbox"/>	UDP	Любой пр...	Запрет	Входящее	Порт: 5355	

Добавить | Изменить | Удалить | Копировать

Показать встроенные (предварительно настроенные) правила

OK | Отмена

Столбцы

Имя: имя правила.

Включено: сведения о том, включено ли правило. Чтобы активировать правило, установите соответствующий флажок.

Протокол: сведения о протоколе, для которого используется указанное правило.

Профиль: сведения о профиле файервола, для которого используется указанное правило.

Действие: сведения о состоянии подключения (блокировать/разрешать/спрашивать).

Направление: направление соединения (входящее/исходящее/оба).

Локальный: IP-адрес и порт локального компьютера.

Удаленный: IP-адрес и порт удаленного компьютера.

Приложение: приложение, к которому применяется правило.

Элементы управления

Добавить: создание правила.

Изменить: изменение существующего правила.

Удалить: удаление существующего правила.

Копировать: создание копии выбранного правила.

Показать встроенные (предварительно настроенные) правила: предварительно настроенные правила для ESET Endpoint Security, с помощью которых можно разрешать или блокировать определенные соединения. Эти правила можно отключить, но не удалить.



В начало/Вверх/Вниз/В конец: настройка приоритетности правил (правила последовательно выполняются сверху вниз).

3.9.2.3.2 Работа с правилами

После каждого изменения отслеживаемых параметров необходимо обновить правила. Если после внесения изменений правило не может отвечать требованиям и указанное действие не может выполняться, в подключении может быть отказано. Это может привести к проблемам в работе приложения, для которого создавалось правило. Примером может быть изменение сетевого адреса или номера порта удаленного компьютера.

Верхняя часть диалогового окна содержит три вкладки.

- **Общие:** выбор имени правила, направления подключения, действия (**Разрешить, Запретить, Запросить**), протокола и профиля, к которому будет применяться правило.
- **Локальный:** приводится информация о локальном компьютере, участвующем в подключении, с указанием номера локального порта или диапазона портов и имени приложения, которое установило подключение. Позволяет также с помощью кнопки **Добавить** добавлять сюда предварительно заданную или созданную зону с диапазоном IP-адресов.
- **Удаленный:** на этой вкладке приводится информация об удаленном порте (диапазоне портов). Также здесь можно указать список удаленных IP-адресов или зон для конкретного правила. Позволяет также с помощью кнопки **Добавить** добавлять сюда предварительно заданную или созданную зону с диапазоном IP-адресов.

При создании нового правила необходимо ввести его имя в поле **Имя**. Направление подключения, к которому применяется правило, выбирается в раскрывающемся списке **Направление**, а действие, которое должно выполняться, когда подключение удовлетворяет параметрам правила, — в раскрывающемся списке **Действие**.

Протокол: протокол передачи данных, используемый для правила. Выберите в раскрывающемся списке протокол, который нужно использовать для определенного правила.

Тип/код ICMP. Определяемое числом сообщение ICMP (например, 0 означает ответ проверки связи).

По умолчанию все правила активированы для всех профилей. Если необходимо, в раскрывающемся списке **Профили** можно выбрать собственный профиль файрвола.

Если включить параметр **Журнал**, действия, связанные с этим правилом, будут записываться в журнал.

Уведомить пользователя: вывод сообщения в случае применения правила.

i ПРИМЕЧАНИЕ.

Журналы со статусом **Предупреждение** могут собираться ESET Remote Administrator.

Ниже приведен пример создания правила, разрешающего веб-браузеру доступ к сети. В данном примере необходимо настроить следующие параметры.

- На вкладке **Общие** включите исходящие подключения по протоколам TCP и UDP.
- Добавьте процесс браузера (для браузера Internet Explorer — iexplore.exe) на вкладке **Локальный**.
- На вкладке **Удаленный** включите порт 80, если следует разрешить стандартные действия, связанные с посещением веб-страниц.

i ПРИМЕЧАНИЕ.

Обратите внимание, что возможности изменения предварительно заданных правил ограничены.

3.9.2.4 Доверенная зона

Доверенная зона — это группа сетевых адресов, из которых файервол разрешает определенный объем входящего трафика при настройках по умолчанию. Настройки таких функций, как обмен файлами и удаленный рабочий стол в доверенной зоне, можно задать в разделе IDS и расширенные параметры.

Состав доверенной зоны может постоянно меняться и быть разным для каждого сетевого адаптера, в зависимости от того, к какой сети в данный момент подключен компьютер. Адреса, входящие в доверенную зону в редакторе зон, всегда являются доверенными. Если сетевой адаптер подключен к известной сети, **Дополнительные доверенные адреса**, указанные для этой сети, добавляются в доверенную зону адаптера. Если сеть определена как домашняя или рабочая, все подключенные к ней напрямую подсети автоматически считаются доверенными. Доверенную зону каждого сетевого адаптера можно просмотреть, последовательно выбрав элементы **Сеть > Сетевые адаптеры** в окне **Настройки**.

i ПРИМЕЧАНИЕ.

Доверенные зоны, работающие с отдельными интерфейсами, не поддерживаются в операционной системе Windows XP. В этих операционных системах у всех адаптеров есть только одна доверенная зона, что можно также увидеть на странице сетевых адаптеров.

3.9.2.5 Настройка зон

Зоны — это группы IP-адресов. Ими удобно пользоваться, когда один и тот же набор адресов необходимо использовать в нескольких правилах. Зоны можно настроить в меню **Дополнительные настройки > Файервол > Основная информация**. Для этого рядом с элементом **Зоны** нужно нажать кнопку **Изменить**. Чтобы добавить новую зону, нажмите кнопку **Добавить**, в поле **Имя** введите имя зоны, в поле **Описание** — описание, а затем в поле **Адрес удаленного компьютера (IPv4, IPv6, диапазон, маска)** укажите IP-адрес удаленного компьютера.

В окне настроек **Зоны файервола** можно указать имя зоны, ее описание и список сетевых адресов (см. также [Редактор известных сетей](#)).

3.9.2.6 Известные сети

Если вы часто подсоединяете компьютер к сетям общего пользования или сетям, отличным от обычной рабочей сети, мы рекомендуем вам проверять надежность новых сетей, к которым выполняется подключение. После определения сетей ESET Endpoint Security может определять доверенные (домашние или рабочие) сети, используя различные параметры сети, заданные в конфигурации **Сетевая идентификация**. Портативные компьютеры часто входят в сети с IP-адресами, похожими на адрес доверенной сети. В таких случаях ESET Endpoint Security может отнести неизвестную сеть к доверенным (домашним или рабочим). Во избежание этого мы рекомендуем использовать **сетевую аутентификацию**.

Когда сетевой адаптер подключается к сети или происходит изменение его параметров сетевой конфигурации, ESET Endpoint Security будет проверять наличие новой сети в списке известных сетей. Если **Сетевая идентификация** и **Сетевая аутентификация** (опционально) совпадают, сеть будет помечена как подключенная к интерфейсу адаптера. Если сеть не найдена среди известных, конфигурация сетевой идентификации создает новое сетевое подключение, на основании которого определяется эта сеть при следующем подключении к ней. По умолчанию для нового сетевого подключения используется тип защиты **Публичная сеть**. В диалоговом окне **Обнаружено новое сетевое подключение** вам будет предложено выбрать тип защиты: **Публичная сеть**, **Домашняя/рабочая сеть** либо **Использовать параметр Windows**. Если сетевой адаптер подключен к известной сети, помеченной как **Домашняя/рабочая сеть**, то локальные подсети адаптера будут добавлены в доверенную зону.

Тип защиты новых сетей. Выберите один из следующих параметров: **Использовать параметр Windows**, **Спросить пользователя** либо **Отметить как общедоступ..** Этот параметр будет использоваться для новых сетей по умолчанию.

i ПРИМЕЧАНИЕ.

Когда выбрана установка **Использовать параметр Windows**, диалоговое окно не отображается и сеть, к которой вы подключены, автоматически помечается согласно вашим настройкам ОС Windows. В результате

для новых сетей будут доступны некоторые функции (например, обмен файлами и удаленный рабочий стол).

Настройку новых сетей можно осуществить вручную из окна [Редактора известных сетей](#).

3.9.2.6.1 Редактор известных сетей

Настройку известных сетей вручную можно выполнить, выбрав **Дополнительные настройки > Файервол > Известные сети** и щелкнув **Изменить**.

Столбцы

Имя: имя известной сети.

Тип защиты: этот элемент отображается, если для сети выбрана установка **Публичная сеть, Домашняя/рабочая сеть** либо **Использовать параметр Windows**.

Профиль файервола: выберите профиль из раскрывающегося меню **Показывать правила, используемые в этом профиле**, чтобы отобразить используемые в нем правила фильтрации.

Профиль обновления: позволяет применить созданный профиль обновления при подключении к данной сети.

Элементы управления

Добавить: используется для создания новой известной сети.

Изменить: используется для изменения существующей известной сети.

Удалить: выберите сеть и щелкните **Удалить**, чтобы удалить ее из списка известных сетей.



Вверх/Поднять/Опустить/Вниз : позволяет настроить уровень приоритета известных сетей (оценка сетей осуществляется сверху вниз).

Параметры конфигурации сети разделены на следующее вкладки:

Сеть

Здесь можно определить **имя сети** и выбрать для нее **тип защиты** («Сеть общего пользования», «Домашняя/рабочая сеть» либо «Использовать параметр Windows»). Используйте раскрывающееся меню **Профиль файервола** для выбора профиля сети. Если для сети выбран тип защиты **Домашняя/рабочая сеть**, все подключенные к ней напрямую подсети автоматически считаются доверенными. Например, если сетевой адаптер подключен к такой сети с IP-адресом 192.168.1.5 и маской подсети 255.255.255.0, подсеть 192.168.1.0/24 будет добавлена в доверенную зону адаптера. Если у адаптера имеется больше адресов или подсетей, все они будут считаться доверенными вне зависимости от конфигурации **Сетевой идентификации** известной сети.

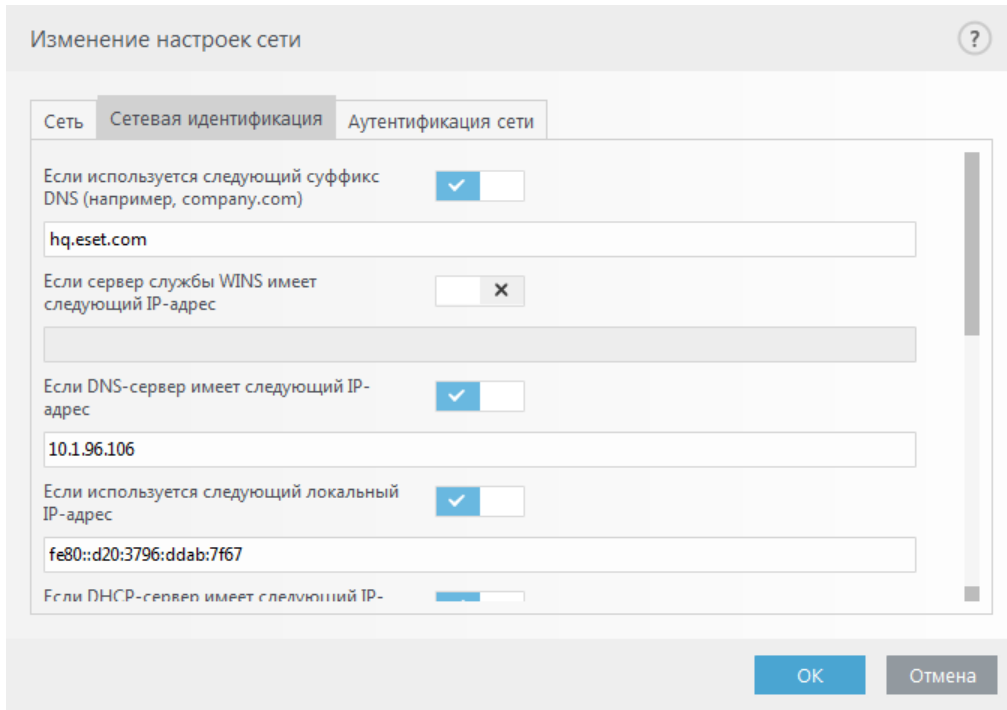
Кроме этого, адреса, добавленные в **Дополнительные доверенные адреса**, всегда включаются в доверенную зону адаптеров, подсоединенных к сети (вне зависимости от типа защиты такой сети).

Для того чтобы сеть была отмечена как подключенная, необходимо выполнение указанных ниже условий.

- Сетевая идентификация: все введенные параметры должны отвечать параметрам активного подключения.
- Аутентификация сети: если выбран сервер аутентификации, должна быть выполнена успешная аутентификация с помощью сервера аутентификации ESET.
- Ограничения сети (только Windows XP): должны соблюдаться все глобальные ограничения.

Сетевая идентификация

Аутентификация выполняется на основе параметров адаптера локальной сети. Происходит сравнение всех установленных параметров с фактическими параметрами активного сетевого подключения. Разрешено использование адресов IPv4 и IPv6.



Аутентификация сети

В рамках аутентификации сети выполняется поиск определенного сервера в сети, а для аутентификации сервера используется асимметричное шифрование (RSA). Имя аутентифицируемой сети должно совпадать с именем сети, указанным в настройках сервера аутентификации. Имя вводится с учетом регистра. Укажите имя сервера, его прослушивающий порт и открытый ключ, соответствующий закрытому ключу сервера (см. раздел [Аутентификация сети: конфигурация сервера](#)). Имя сервера можно ввести в виде IP-адреса, имени DNS или NetBios. После имени сервера можно указать путь к файлу ключа на сервере (например, имя_сервера_/_каталог1/каталог2/аутентификация). На случай недоступности сервера можно указать дополнительные серверы через точку с запятой.

[Загрузите сервер аутентификации ESET.](#)

Открытым ключом может быть файл одного из указанных ниже типов.

- Зашифрованный открытый ключ в формате PEM (.pem). Этот ключ можно создать с помощью приложения ESET Authentication Server (см. раздел [Аутентификация сети: конфигурация сервера](#)).
- Зашифрованный открытый ключ.
- Сертификат открытого ключа (.crt).

Изменение настроек сети ?

Сеть Сетевая идентификация **Аутентификация сети**

Имя сервера или IP-адрес	<input type="text" value="10.1.1.24"/>
Порт сервера	<input type="text" value="80"/>
Открытый ключ (кодировка base64)	<input type="text"/>

Чтобы проверить настройки, нажмите кнопку **Проверить**. Если аутентификация прошла успешно, на экране появится сообщение *Аутентификация сервера завершена*. Если аутентификация не настроена должным образом, на экране появится одно из указанных ниже сообщений об ошибке.

Сбой аутентификации сервера. Недопустимая или несовпадающая подпись.

Подпись сервера не отвечает введенному открытому ключу.

Сбой аутентификации сервера. Имя сети не совпадает.

Настроенное имя сервера не соответствует зоне сервера аутентификации. Проверьте оба имени и убедитесь, что они одинаковы.

Сбой аутентификации сервера. Нет ответа от сервера, или получен недопустимый ответ.

Ответ отсутствует, если сервер не работает или недоступен. Недопустимый ответ может быть получен в случае, если запущен другой HTTP-сервер с указанным адресом.

Указан недействительный открытый ключ.

Проверьте, не поврежден ли файл открытого ключа.

Ограничения сети (только для Windows XP)

В современных операционных системах (Windows Vista и более новые) каждый сетевой адаптер имеет собственную доверенную зону и активный профиль файервола. К сожалению, в Windows XP такая структура не поддерживается, поэтому все сетевые адаптеры всегда имеют одну и ту же доверенную зону и профиль активного файервола. Это представляет потенциальный риск для безопасности компьютера, одновременно подключенного к нескольким сетям. В таких случаях трафик из ненадежной сети может оцениваться с использованием доверенной зоны и профиля файервола для другой подключенной сети. Для снижения рисков для безопасности вы можете соблюдать следующие ограничения, позволяющие избежать глобального применения конфигурации одной из сетей во время подключения другой (потенциально ненадежной).

В Windows XP параметры подключенных сетей (доверенная зона и профиль файервола) применяются глобально, кроме случаев, когда как минимум одно из указанных ниже ограничений включено и не выполняется.

- a. Активно только одно подключение.
- b. Беспроводное соединение не установлено.
- c. Нет установленных небезопасных беспроводных подключений.

3.9.2.6.2 Аутентификация сети: конфигурация сервера

Аутентификацию сети можно выполнить с помощью любого подключенного к ней компьютера или сервера. Для этого на компьютер или сервер, который всегда доступен для аутентификации, когда клиент пытается подключиться к сети, нужно установить приложение ESET Authentication Server. Файл установки приложения ESET Authentication Server можно загрузить с веб-сайта ESET.

После установки приложения ESET Authentication Server откроется диалоговое окно (приложение можно запустить, последовательно щелкнув элементы **Пуск > Программы > ESET > ESET Authentication Server**).

Чтобы настроить сервер аутентификации, введите имя сети аутентификации, прослушивающий порт сервера (по умолчанию 80) и место, в котором будут храниться открытый и закрытый ключи. Далее создайте открытый и закрытый ключи, которые будут использоваться при аутентификации. Закрытый ключ должен использоваться на сервере, а открытый — импортироваться на сторону клиента, что можно сделать в разделе аутентификации сети при настройке сети в файрволе.

3.9.2.7 Ведение журнала

Файрвол ESET Endpoint Security сохраняет данные обо всех важных событиях в файле журнала, который можно открыть с помощью главного меню. Выберите **Служебные программы > Файлы журнала**, а затем **Файрвол** в раскрывающемся меню **Журнал**. Чтобы включить ведение журнала в файрволе, последовательно щелкните элементы **Дополнительные настройки > Служебные программы > Файлы журнала** и для минимальной степени детализации журнала выберите значение **Диагностика**. Все отклоненные соединения будут записываться в журнал.

Файлы журнала могут использоваться для обнаружения ошибок и вторжений на компьютер. Журналы файрвола ESET содержат следующие сведения:

- **Время:** дата и время события.
- **Событие:** имя события.
- **Источник:** сетевой адрес источника.
- **Объект:** сетевой адрес целевого объекта.
- **Протокол:** сетевой протокол передачи данных.
- **Имя правила или червя:** применяемое правило или имя червя, если указано.
- **Приложение:** задействованное приложение.
- **Пользователь:** имя пользователя, который находился в системе при обнаружении заражения.

Тщательный анализ информации значительно облегчает процесс оптимизации безопасности компьютера. Многие факторы являются признаками потенциальных угроз и позволяют пользователю свести их влияние к минимуму. Индикаторы потенциальных угроз могут быть следующими: слишком частые соединения от неизвестных компьютеров, множественные попытки установить соединение, сетевая активность неизвестных приложений или использование неизвестных номеров портов.

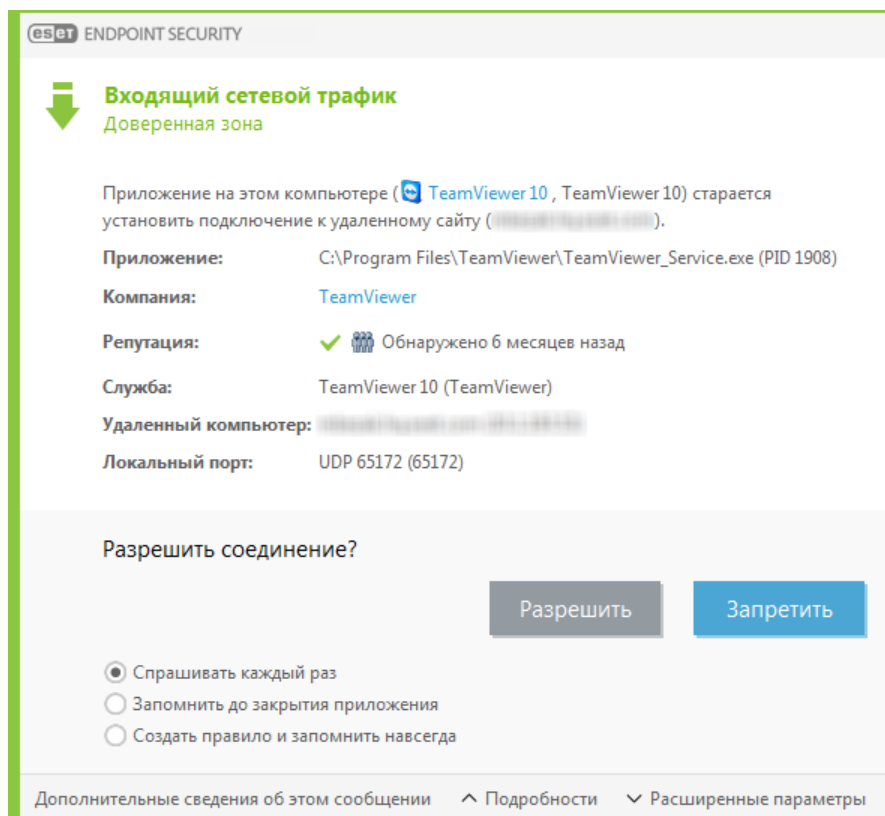
3.9.2.8 Установка соединения: обнаружение

Файрвол обнаруживает каждое из новых сетевых соединений. Активный режим персонального файрвола определяет, какие действия должны выполняться для нового правила. Если активирован **автоматический режим** или **режим на основе политики**, файрвол выполнит предварительно заданные действия без вмешательства пользователя.

В интерактивном режиме выводится информационное окно с уведомлением об обнаружении нового сетевого соединения. В окне приводится дополнительная информация о соединении. Пользователь может разрешить или запретить (заблокировать) соединение. Если соединения одного типа возникают регулярно, и их приходится разрешать вручную, рекомендуется создать для них правило. Для этого выберите функцию **Запомнить действие (создать правило)** и сохраните новое правило для файрвола. Если персональный файрвол обнаружит такое соединение в будущем, он применит это правило.

Выбор параметра **Временно запомнить действие для процесса** приводит к использованию действия (**Разрешить/Запретить**) до перезапуска приложения, изменения правил или режимов фильтрации,

обновления модуля фаервола или перезагрузки компьютера. После выполнения любого из этих действий временные правила удаляются.



Будьте внимательны при создании новых правил и разрешайте только те соединения, в безопасности которых вы уверены. Если разрешить все соединения, фаервол не сможет обеспечивать защиту. Ниже перечислены наиболее важные параметры соединений.

- **Удаленный компьютер:** разрешать соединения только с доверенными и известными адресами.
- **Локальное приложение:** не рекомендуется разрешать соединения с неизвестными приложениями и процессами.
- **Номер порта:** подключение через стандартные порты (например, порт номер 80 для просмотра веб-страниц) в обычных условиях следует разрешить.

Компьютерные вирусы для размножения часто используют соединения с Интернетом или скрытые соединения, через которые происходит заражение других компьютеров. Если правила настроены правильно, фаервол является эффективным средством противодействия разнообразным атакам с применением вредоносного кода.

3.9.2.9 Решение проблем с помощью персонального фаервола ESET

Если ESET Endpoint Security не удается подключиться к сети, есть несколько способов узнать, обусловлены ли они работой фаервола ESET. Кроме того, с помощью фаервола ESET можно создать новые правила или исключения для решения проблем с подключением.

Для решения проблем с фаерволом ESET см. следующие темы:

- [Мастер устранения неполадок](#)
- [Ведение журнала и создание правил и исключений на основе журнала](#)
- [Создание исключений на основе уведомлений фаервола](#)
- [Расширенное ведение журналов PCAP](#)
- [Решение проблем с фильтрацией протоколов](#)

3.9.2.9.1 Мастер устранения неполадок

Мастер устранения неполадок автоматически отслеживает все заблокированные соединения и помогает устранять неполадки для исправления проблем с файерволом в работе определенных приложений и устройств. После этого мастер предложит новый набор правил, который вам нужно будет подтвердить. **Мастер устранения неполадок** можно найти в главном меню, последовательно выбрав **Настройки > Сеть**.

3.9.2.9.2 Ведение журнала и создание правил и исключений на основе журнала

По умолчанию файервол ESET не вносит в журнал все блокируемые соединения. Если нужно просмотреть, что заблокировано файерволом, включите ведение журнала в разделе **Устранение неполадок** в меню **Дополнительные настройки**, последовательно выбрав **Файервол > IDS и расширенные параметры**. Если в журнале есть элемент, который файерволу не следует блокировать, можно создать правило или исключение IDS, щелкнув этот элемент правой кнопкой мыши и выбрав **Не блокировать подобные события в будущем**. Обратите внимание, что журнал всех заблокированных соединений может содержать тысячи элементов, поэтому найти конкретный элемент может быть трудно. После решения проблемы ведение журнала можно выключить.

Для получения дополнительных сведений о журнале см. раздел [Файлы журнала](#).

i ПРИМЕЧАНИЕ.

Используйте журнал, чтобы узнать, в каком порядке файервол блокировал те или иные соединения. Кроме того, правила, созданные на основе журнала, будут выполнять нужные вам действия.

3.9.2.9.2.1 Создание правил на основе журнала

В новой версии ESET Endpoint Security можно создавать правила на основе журнала. В главном меню последовательно выберите **Служебные программы > Файлы журнала**. В раскрывающемся меню выберите пункт **Файервол**, щелкните нужную запись журнала правой кнопкой мыши и в контекстном меню выберите пункт **Не блокировать подобные события в будущем**. Новое правило отобразится в окне уведомлений.

Чтобы можно было создавать правила на основе журнала, ESET Endpoint Security следует настроить следующим образом:

- установите минимальную степень детализации журнала **Диагностика**, последовательно выбрав **Дополнительные настройки (F5) > Служебные программы > Файлы журнала**;
- установите флажок **Показывать уведомление при обнаружении атаки, использующей бреши в системе безопасности** в меню **Дополнительные настройки (F5) > Файервол > IDS и расширенные параметры > Обнаружение вторжений**.

3.9.2.9.3 Создание исключений на основе уведомлений файервола

Когда файервол ESET обнаруживает вредоносную сетевую деятельность, отображается окно уведомлений с описанием этого события. Уведомление содержит ссылку, перейдя по которой можно получить дополнительные сведения о событии и создать исключение для этого события (если нужно).

i ПРИМЕЧАНИЕ.

Если сетевое приложение или устройство не соблюдает сетевые стандарты надлежащим образом, возможно, начнут регулярно появляться уведомления IDS файервола. Исключение можно создать непосредственно на основе уведомления. Благодаря этому файервол ESET не будет обнаруживать это приложение или устройство.

3.9.2.9.4 Расширенное ведение журналов PCAP

Эта функция предназначена для предоставления более комплексных файлов журнала службе поддержки клиентов ESET. Используйте эту функцию только по запросу службы поддержки клиентов ESET, поскольку она может создать очень большой файл журнала и замедлить работу компьютера.

1. Перейдите в раздел **Дополнительные настройки > Службные программы > Диагностика** и включите параметр **Включить расширенное ведение журнала фильтрации протоколов**.
2. Попробуйте воспроизвести текущую проблему.
3. Отключите расширенное ведение журнала PCAP.
4. Файл журнала PCAP можно найти в папке, где создаются дампы памяти для диагностики.

- Microsoft Windows Vista или более новая версия

C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

- Microsoft Windows XP

C:\Documents and Settings\All Users\...

3.9.2.9.5 Решение проблем с фильтрацией протоколов

Если возникают проблемы с браузером или почтовым клиентом, сначала следует определить, нормально ли работает фильтрация протоколов. Для этого временно отключите фильтрацию протоколов приложений в дополнительных настройках (обязательно включите его после решения проблемы, иначе браузер и почтовый клиент останутся без защиты). Если после отключения неполадка исчезает, см. ниже список типичных проблем и способов их решения.

Проблемы с обновлением или безопасностью подключения

У приложения проблемы с обновлением или защищенностью канала связи.

- Если включена фильтрация протоколов SSL, попробуйте временно ее отключить. Если помогло, значит, можно продолжать использовать фильтрацию SSL и выполнять обновления. Для этого нужно исключить проблемное соединение.
Переведите фильтрацию протоколов SSL в интерактивный режим. Запустите обновление еще раз. Должно появиться диалоговое окно с уведомлением о зашифрованном сетевом трафике. Приложение должно быть аналогичным тому, с которым возникли проблемы, а сертификат должен исходить из сервера, с которого выполняются обновления. Затем запомните действия для сертификата и нажмите кнопку «Пропустить». Если не отобразятся соответствующие диалоговые окна, переключитесь обратно в автоматический режим фильтрации. Проблема должна быть решена.
- Если приложение не является браузером или почтовым клиентом, его можно полностью исключить из фильтрации протоколов (исключение браузера или почтового клиента оставило бы вас незащищенным). Любое приложение, в отношении которого выполнялась в прошлом фильтрация соединений, должно быть в списке, предоставляемом при добавлении исключений. Поэтому не должно возникнуть необходимости добавлять исключения вручную.

Проблема с доступом к устройству в сети

Если не удастся использовать какие-либо функции устройства в сети (например, не удастся открыть веб-страницу с фотографиями веб-камеры или воспроизвести видео на домашнем мультимедийном проигрывателе), добавьте IPv4- и IPv6-адреса в список исключенных адресов.

Проблемы с определенным веб-сайтом

Исключить определенные веб-сайты из фильтрации протоколов можно с помощью управления URL-адресами. Например, если не удается получить доступ к странице <https://www.gmail.com/intl/en/mail/help/about.html>, попробуйте добавить *gmail.com* в список исключенных адресов.

Ошибка «Все еще работают некоторые приложения, которые могут импортировать корневой сертификат»

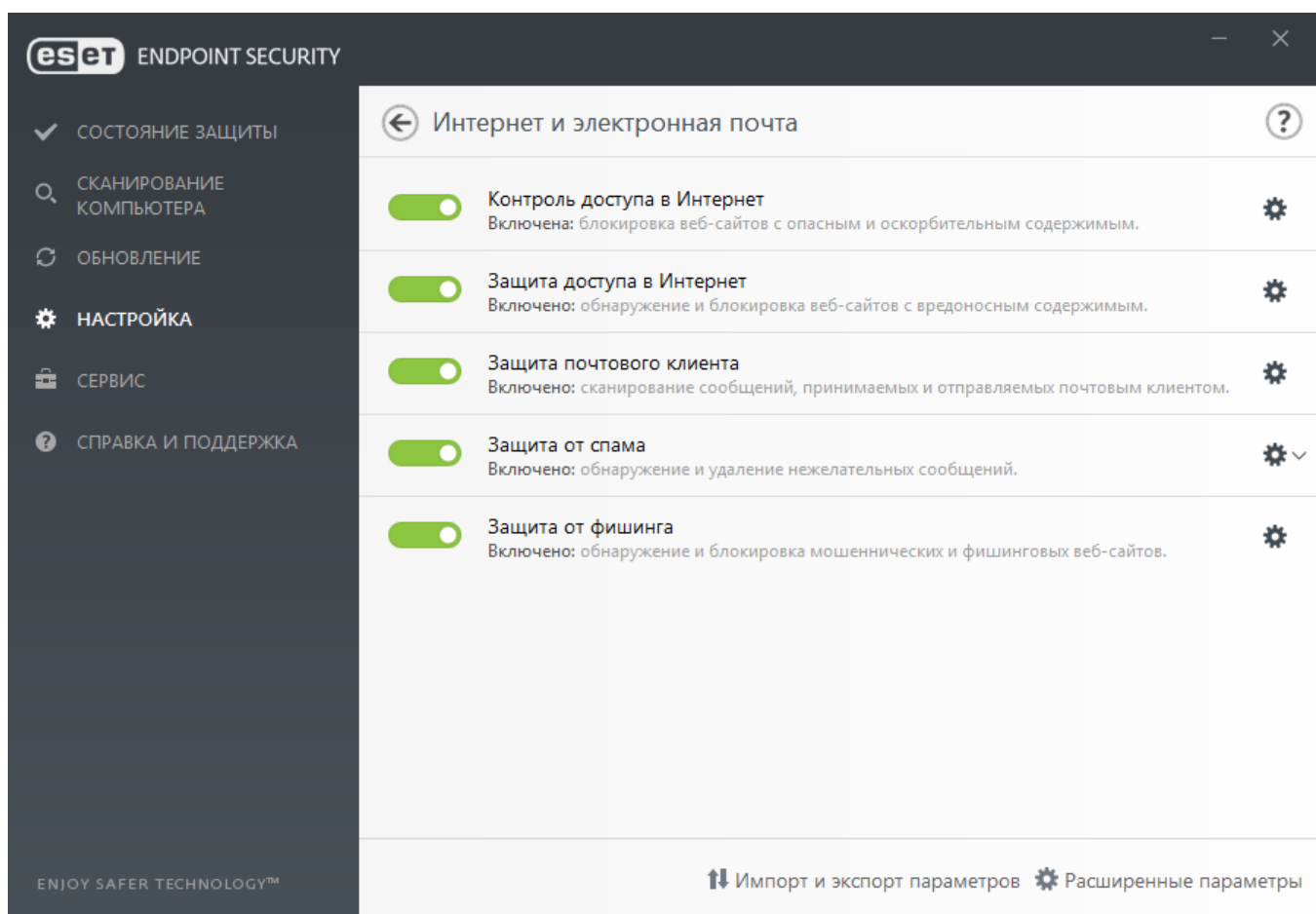
При включении фильтрации протоколов SSL программа ESET Endpoint Security выполняет фильтрацию протокола SSL так, что установленные программы доверяют ее действиям (происходит импорт сертификата в их хранилище сертификатов). Для некоторых приложений это невозможно, если они запущены. Например, для браузеров Firefox и Opera. Закройте эти приложения (для этого рекомендуется открыть диспетчер задач и удалить записи firefox.exe и opera.exe на вкладке «Процессы»), а затем нажмите кнопку «Повторить».

Ошибка: недоверенный издатель или недопустимая подпись

Скорее всего, это значит, что при вышеописанном импорте произошла ошибка. Сначала закройте все упомянутые приложения. Затем выключите фильтрацию протоколов SSL и включите ее обратно. Будет выполнена повторная попытка импорта.

3.9.3 Интернет и электронная почта

Конфигурацию защиты доступа в Интернет и электронной почты можно найти, выбрав **Настройка > Интернет и электронная почта**. В этом окне предоставляется доступ к дополнительным параметрам программы.



Модуль **контроля доступа в Интернет** позволяет настраивать параметры, которые дают администраторам возможность использовать автоматизированные средства для защиты своих компьютеров и задавать ограничения, связанные с посещением веб-страниц. Цель заключается в предотвращении доступа к страницам, содержимое которых является неприемлемым или вредоносным. Для получения дополнительных сведений см. раздел [Контроль доступа в Интернет](#).

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

Защита почтового клиента обеспечивает контроль обмена данными по протоколам POP3 и IMAP. С помощью подключаемого модуля для почтового клиента программа ESET Endpoint Security позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, IMAP, HTTP, MAPI).


Функция **защиты от спама** отфильтровывает нежелательные сообщения, поступающие по электронной почте.

Если щелкнуть значок шестеренки  рядом с элементом **Защита от спама**, доступны следующие возможности:

Настроить...: переход к расширенным настройкам защиты почтового клиента от спама.

«Белый» список пользователя / «черный» список пользователя / список исключений пользователя: переход к диалоговому окну, в котором можно добавить, изменить и удалить адреса электронной почты, считающиеся безопасными или опасными. В соответствии с указанными здесь правилами, электронные письма с этих адресов не будут сканироваться или будут считаться спамом. Щелкните элемент **Список исключений пользователя**, чтобы открыть диалоговое окно, в котором можно добавить, изменить и удалить адреса электронной почты, которые могут быть подделаны и использованы для отправки спама. Сообщения электронной почты, полученные с адресов, присутствующих в списке исключений, всегда будут сканироваться на предмет наличия спама.

Защита от фишинга представляет собой еще один уровень безопасности, который обеспечивает улучшенную защиту от незаконных веб-сайтов, пытающихся получить пароли и прочую конфиденциальную информацию. Функция защиты от фишинга доступна на панели **Настройка** в разделе **Интернет и электронная почта**. Для получения дополнительных сведений см. раздел [Защита от фишинга](#).

Отключить: отключение защиты доступа в Интернет / электронной почты./защиты от спама для веб-браузеров и почтовых клиентов .

3.9.3.1 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**.

Включить фильтрацию содержимого, передаваемого по протоколам приложений: может использоваться для отключения фильтрации протоколов. Многие компоненты ESET Endpoint Security (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 фильтрации протоколов. Эта функция полезна, если фильтрация протоколов вызывает проблемы совместимости.

Веб-клиенты и почтовые клиенты: (используется только в операционной системе Windows XP) позволяет выбрать приложения, трафик которых будет проходить фильтрацию протоколов вне зависимости от используемого порта.

3.9.3.1.1 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 Endpoint Security основное внимание уделяется обеспечению безопасности веб-браузеров. Каждое приложение, обращающееся к сети, может быть помечено как веб-браузер. Приложения, которые уже использовали протоколы для передачи данных или приложения, находящиеся по выбранному адресу, можно внести в список веб-клиентов и почтовых клиентов.

3.9.3.1.2 Исключенные приложения

Для исключения соединений определенных сетевых приложений из фильтрации протоколов добавьте их в список. Соединения выделенных приложений по протоколам HTTP/POP3/IMAP не будут проверяться на наличие угроз. Рекомендуется использовать этот метод, только если при включенной фильтрации протоколов приложения не функционируют надлежащим образом.

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

Изменить: изменение выбранных в списке записей.

Удалить: удаление выбранных записей из списка.

Исключенные приложения

C:\WINDOWS\SYSTEM32\SVCHOST.EXE
C:\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.30319\MSCORSVW.EXE
C:\WINDOWS\MICROSOFT.NET\FRAMEWORK64\V4.0.30319\MSCORSVW.EXE
C:\Windows\System32\svchost.exe

Добавить Изменить Удалить

ОК Отмена

3.9.3.1.3 Исключенные IP-адреса

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

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

Изменить: изменение выбранных в списке записей.

Удалить: удаление выбранных записей из списка.

Исключенные IP-адреса

10.1.2.3
10.2.1.1-10.2.1.10
192.168.1.0/255.255.255.0
fe80::b434:b801:e878:5975
2001:21:420::/64

Добавить Изменить Удалить

OK Отмена

3.9.3.1.4 SSL/TLS

ESET Endpoint Security 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/TLS: если фильтрация протокола отключена, программа не сканирует обмен данными по протоколу SSL.

Режим фильтрации протоколов SSL/TLS доступен со следующими параметрами.

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

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

Список приложений, отфильтрованных с помощью SSL/TLS: может использоваться для настройки поведения ESET Endpoint Security для заданных приложений.

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

Исключить соединение с доверенными доменами: уровень доверенности домена определяется встроенным «белым» списком.

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

Корневой сертификат

Корневой сертификат: для нормальной работы SSL-подключений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET в список известных корневых сертификатов (издателей). Параметр **Добавить корневой сертификат к известным браузерам** должен быть активирован. Выберите этот параметр, чтобы автоматически добавить корневой сертификат ESET в известные браузеры (например, Opera и Firefox). Для браузеров, использующих системное хранилище сертификатов (например, Internet Explorer), сертификат добавляется автоматически.

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

Срок действия сертификата

Если проверить сертификат с помощью хранилища сертификатов TRCA не удастся: в некоторых случаях сертификат невозможно проверить с помощью хранилища сертификатов доверенных корневых центров сертификации (TRCA). 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 неправильное собственное заверение. В этом случае рекомендуется выбрать **Блокировать соединения, использующие сертификат**.

3.9.3.1.4.1 Шифрованное соединение SSL

Если в системе настроено сканирование протокола SSL, диалоговое окно с запросом на выбор действия будет отображаться в двух случаях.

Во-первых, если веб-сайт использует непроверенный или недействительный сертификат, а продукт ESET Endpoint Security настроен на выдачу запросов в таких случаях (по умолчанию запросы отображаются для непроверенных сертификатов, а для недействительных — нет), появится запрос на **блокирование** или **разрешение** подключения.

Во-вторых, если в качестве **режима фильтрации протокола SSL** выбран **интерактивный режим**, то при подключении к любому веб-сайту будет отображаться запрос на **сканирование** или **игнорирование**. Некоторые приложения проверяют SSL-трафик на предмет изменений и мониторинга. В таких случаях для сохранения работоспособности приложения программа ESET Endpoint Security должна SSL-трафик **игнорировать**.

В каждом из этих случаев пользователь может сохранить в системе выбранное действие. Сохраненные действия хранятся в списке **Список известных сертификатов**.

3.9.3.1.4.2 Список известных сертификатов

Список известных сертификатов позволяет настроить поведение ESET Endpoint Security в отношении конкретных сертификатов SSL, а также настроить запоминание действий пользователя, если в разделе **Режим фильтрации 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**.

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

Столбцы

Имя : имя сертификата.

Издатель сертификата : имя создателя сертификата.

Субъект сертификата : это поле указывает на субъект, которому принадлежит открытый ключ, содержащийся в поле открытого ключа субъекта.

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

Сканировать: в качестве значения параметра **Действие сканирования** выберите **Сканировать** или **Пропустить**, чтобы сканировать или игнорировать обмен данными, защищенный этим сертификатом. Выберите **Автоматически**, чтобы сканировать в автоматическом режиме и запрашивать действия в интерактивном. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

Элементы управления

Добавить: сертификат можно загрузить вручную как файл с расширением *.cer*, *.crt* или *.pem*. Щелкните элемент **Файл**, чтобы передать локальный сертификат, или щелкните **URL-адрес**, чтобы указать расположение сертификата в Интернете.

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

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

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

3.9.3.1.4.3 Список приложений, отфильтрованных с помощью SSL/TLS

Список приложений, отфильтрованных с помощью SSL/TLS может использоваться для настройки поведения ESET Endpoint Security в отношении конкретных приложений, а также запоминания выбранных действий, 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 приложений, отфильтрованных с помощью SSL/TLS**.

Окно **Список приложений, отфильтрованных с помощью SSL/TLS** содержит такие элементы:

Столбцы

Приложение: имя приложения.

Действие сканирования: выберите **Сканировать** или **Пропустить**, чтобы сканировать или игнорировать обмен данными. Чтобы сканировать в автоматическом режиме и запрашивать действия в интерактивном, выберите элемент **Автоматически**. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

Элементы управления

Добавить: добавление отфильтрованных приложений.

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

Удалить: выберите сертификат, который нужно удалить, и щелкните **Удалить**.

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

3.9.3.2 Защита почтового клиента

3.9.3.2.1 Почтовые клиенты

Интеграция ESET Endpoint Security с почтовыми клиентами увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, в ESET Endpoint Security можно настроить интеграцию. Если интеграция активирована, панель инструментов ESET Endpoint Security вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты (панель инструментов для последних версий Почты Windows Live не вставляется).

Параметры интеграции доступны в разделе **Настройка > Дополнительные настройки > Интернет и электронная почта > Защита почтового клиента > Почтовые клиенты**.

Интеграция с почтовым клиентом

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

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

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

Сканируемая электронная почта

Включить защиту электронной почты с помощью подключаемых модулей клиента. Даже если защита электронной почты с помощью почтового клиента отключена, проверка почтового клиента с использованием фильтрации протоколов все равно будет работать.

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 — в этом случае программа будет выявлять зараженные вложения, но не будет выполнять никаких действий с сообщениями электронной почты.

Удалить сообщение — программа будет уведомлять пользователя о заражениях и удалять сообщения.

Переместить сообщение в папку «Удаленные» — зараженные сообщения будут автоматически перемещаться в папку «Удаленные».

Переместить сообщение в папку — зараженные сообщения будут автоматически перемещаться в указанную папку.

Папка — выбор папки, в которую будут перемещаться обнаруженные зараженные сообщения электронной почты.

Повторить сканирование после обновления — включение или отключение повторного сканирования после обновления модуля обнаружения.

Принять результаты сканирования из других модулей — если установлен этот флажок, модуль защиты электронной почты будет принимать результаты сканирования от других модулей защиты (сканирование каталогов POP3, IMAP).

i ПРИМЕЧАНИЕ.

Рекомендуем включить параметры **Включить защиту электронной почты с помощью подключаемых модулей клиента** и **Включить защиту электронной почты с помощью фильтрации протоколов** («Дополнительные настройки» (F5) > «Интернет и электронная почта» > «Защита почтового клиента» > «Протоколы электронной почты»).

3.9.3.2.2 Протоколы электронной почты

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

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

Включить защиту протоколов электронной почты: позволяет включить проверку 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**. Все порты также сканируются для приложений, отмеченных как [веб-клиенты и почтовые клиенты](#).

ESET Endpoint Security также поддерживает сканирование протоколов IMAPS и POP3S, которые для передачи информации между сервером и клиентом используют зашифрованный канал. ESET Endpoint Security проверяет соединения, использующие методы шифрования SSL и TLS. Программа будет выполнять сканирование только трафика на **портах, используемых протоколом IMAPS/POP3S**, вне зависимости от версии операционной системы.

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

The screenshot shows the 'Расширенные параметры' (Advanced Parameters) window. On the left is a navigation pane with categories: ЗАЩИТА ОТ ВИРУСОВ (1), ОБНОВЛЕНИЕ (4), ФАЙЕРВОЛ (5), ИНТЕРНЕТ И ЭЛЕКТРОННАЯ ПОЧТА (4), **Защита почтового клиента (4)**, Защита доступа в Интернет, Защита от фишинга, Контроль доступа в Интернет (2), КОНТРОЛЬ УСТРОЙСТВ (1), СЛУЖЕБНЫЕ ПРОГРАММЫ (1), and ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ. The main area is titled 'ПОЧТОВЫЕ КЛИЕНТЫ' and contains the following settings:

- ПРОТОКОЛЫ ЭЛЕКТРОННОЙ ПОЧТЫ:** Включить защиту электронной почты с помощью фильтрации протоколов (checked).
- НАСТРОЙКА МОДУЛЯ СКаниРОВАНИЯ IMAP:** Включить проверку протокола IMAP (checked).
- НАСТРОЙКА МОДУЛЯ СКаниРОВАНИЯ IMAPS:** Включить проверку протокола IMAPS (checked); Порты, используемые протоколом IMAPS: 585, 993.
- НАСТРОЙКА МОДУЛЯ СКаниРОВАНИЯ POP3:** Включить проверку протокола POP3 (checked).

At the bottom, there are buttons: 'По умолчанию', 'OK', and 'Отмена'.

3.9.3.2.3 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 Endpoint Security позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP). При проверке входящих сообщений программа использует все современные методы сканирования, обеспечиваемые модулем сканирования ThreatSense. Это позволяет обнаруживать вредоносные программы даже до того, как данные о них попадают в модуль обнаружения. Сканирование соединений по протоколам POP3 и IMAP не зависит от используемого почтового клиента.

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

Настройка параметров модуля ThreatSense: расширенная настройка модуля сканирования для защиты от вирусов, которая позволяет настраивать объекты сканирования, методы обнаружения и т. д. Нажмите для вывода на экран окна подробной 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.
- **Только к зараженным сообщениям:** будут отмечены только сообщения, содержащие злонамеренные программы (по умолчанию).
- **Ко всем сканируемым сообщениям:** программа будет добавлять уведомления ко всем сканируемым сообщениям электронной почты.

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

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

3.9.3.2.4 Защита от спама

Нежелательные сообщения, также называемые спамом, являются одной из самых серьезных проблем современных телекоммуникационных технологий. Доля спама в общем объеме передаваемых по электронной почте сообщений составляет около 80 %. Защита от спама ограждает от этой проблемы. Используя несколько принципов защиты электронной почты, модуль защиты от спама обеспечивает превосходную фильтрацию и не пропускает в папку входящих сообщений нежелательную почту.

The screenshot shows the 'Advanced Parameters' (Расширенные параметры) window with a search bar at the top right. The left sidebar lists various security categories, with 'Client Mail Protection' (Защита почтового клиента) selected. The main area displays the following settings:

Parameter	Value	Info
Автоматически запускать модуль защиты почтового клиента от спама	<input checked="" type="checkbox"/>	
Разрешить расширенный поиск спама	<input type="checkbox"/>	?
ОБРАБОТКА СООБЩЕНИЙ		
Добавить текст к теме сообщения	<input checked="" type="checkbox"/>	?
Текст	<input type="text" value="[SPAM]"/>	?
Перемещать сообщения в папку для спама	<input checked="" type="checkbox"/>	?
Использовать папку	<input type="checkbox"/>	?
Папка	<input type="text"/>	
Отмечать сообщения со спамом как прочитанные	<input type="checkbox"/>	?
Отмечать повторно классифицированные сообщения как прочитанные	<input checked="" type="checkbox"/>	?
Записывание в журнал оценки нежелательности	<input type="text" value="Нет"/>	?

At the bottom, there are three buttons: 'По умолчанию' (Default), 'OK', and 'Отмена' (Cancel).

Одним из важнейших принципов обнаружения спама является его распознавание на основе предварительно определенных списков доверенных («белый» список) и нежелательных («черный» список) адресов. Все адреса, найденные в адресной книге почтового клиента, автоматически попадают в «белый» список, а остальные адреса должны быть помечены пользователем как безопасные.

Основным методом, используемым для обнаружения спама, является сканирование свойств сообщения. Полученные сообщения сканируются на основные критерии защиты от спама (определения сообщения, статистические эвристики, алгоритмы распознавания и другие уникальные методы). Результатом работы этих методов является значение индекса, по которому можно с высокой степенью достоверности определить, является ли сообщение спамом.

Автоматически запускать модуль защиты почтового клиента от нежелательной почты: если этот флажок установлен, защита от спама будет автоматически активироваться при загрузке компьютера.

Разрешить расширенный поиск спама: периодически будут загружаться дополнительные данные, которые повышают эффективность защиты от спама.

Защита от спама в ESET Endpoint Security позволяет задать другие параметры для работы со списками рассылки. Доступны следующие параметры.

Обработка сообщений

Добавить текст к теме сообщения: позволяет добавлять настраиваемую строку префикса в поле темы сообщений, которые классифицированы как спам. Строка по умолчанию — [SPAM].

Перемещать сообщения в папку для спама: если этот флажок установлен, сообщения со спамом будут перемещаться в стандартную папку для нежелательной почты, а сообщения, повторно классифицированные

как не спам, — в папку со входящей почтой. Если щелкнуть сообщение правой кнопкой мыши и выбрать в контекстном меню пункт ESET Endpoint Security, появится возможность выбрать один из нескольких вариантов действий.

Использовать эту папку: этот параметр позволяет перемещать спам в папку, указанную пользователем.

Отмечать сообщения со спамом как прочитанные: установите этот флажок, чтобы автоматически помечать нежелательные сообщения как прочитанные. Это помогает сосредоточиться на «чистых» сообщениях.

Отмечать повторно классифицированные сообщения как непрочитанные: сообщения, первоначально классифицированные как спам, а затем помеченные как «чистые», будут отображаться как непрочитанные.

Регистрация оценки нежелательности : модуль защиты от спама ESET Endpoint Security присваивает оценку нежелательности каждому просканированному сообщению. Данное сообщение будет записано в [журнал защиты от спама](#) (ESET Endpoint Security > Служебные программы > Файлы журнала > Защита от спама).

- **Нет:** оценка, полученная в результате сканирования на предмет спама, не вносится в журнал.
- **Реклассифицировано и помечено как спам:** если выбран этот параметр, оценки нежелательности всех сообщений, помеченных как спам, будут записываться в журнал.
- **Все:** в журнал будут записываться все сообщения вместе с оценкой нежелательности.

i ПРИМЕЧАНИЕ.


Если в папке нежелательной почты выбрать сообщение и выбрать команду **Классифицировать выбранные сообщения как НЕ спам**, выбранное сообщение переместится в папку входящей почты. Если в папке входящих сообщений выбрать сообщение, которые вы считаете нежелательным, и выбрать команду **Классифицировать выбранные сообщения как НЕ спам**, выбранное сообщение переместится в папку спама. Это же действие можно выполнить сразу с несколькими выбранными сообщениями.

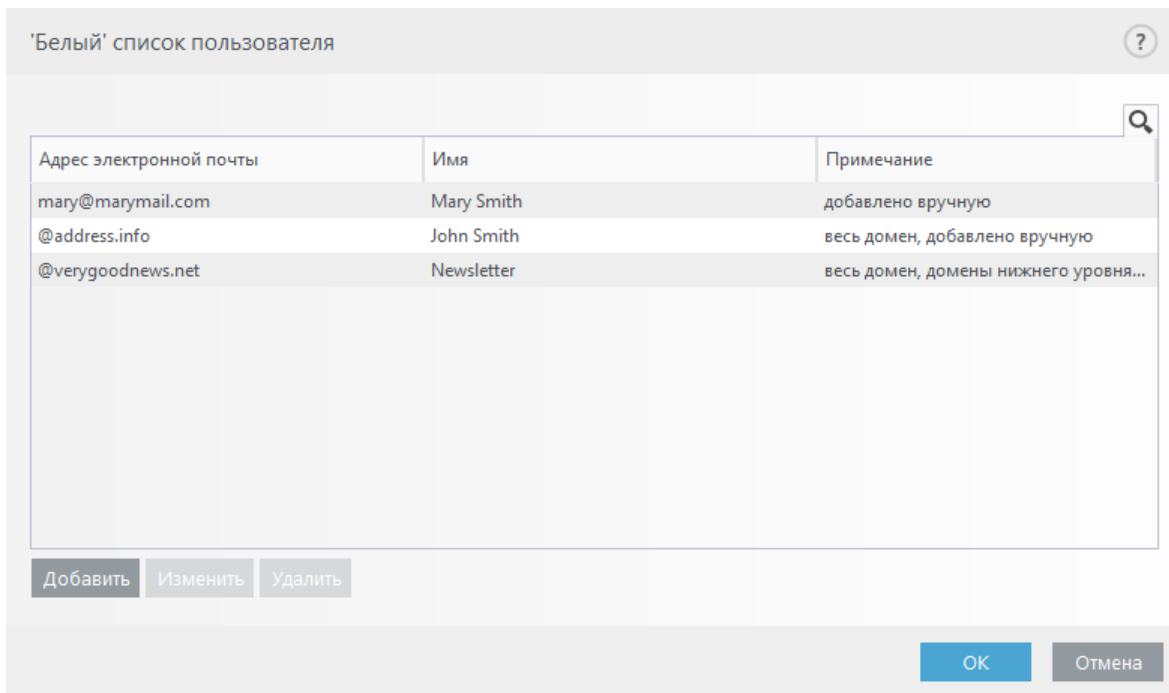
i ПРИМЕЧАНИЕ.

ESET Endpoint Security обеспечивает защиту от спама в таких почтовых приложениях: Microsoft Outlook, Outlook Express, Почта Windows и Почта Windows Live.

3.9.3.2.4.1 «Черный» список/«белый» список/список исключений

Чтобы обеспечить защиту от нежелательных сообщений, ESET Endpoint Security позволяет распределять адреса электронной почты по специальным спискам. [«Белый» список](#) содержит адреса электронной почты, которые считаются безопасными. Сообщения от пользователей, адреса которых находятся в «белом» списке, всегда видны в папке входящих сообщений. В [«Черном» списке](#) содержатся адреса электронной почты, классифицированные как отправители спама. Все сообщения от отправителей из данного списка будут помечены соответствующим образом. Список исключений содержит адреса электронной почты, сообщения с которых всегда проверяются на наличие спама. Этот список также может содержать адреса из нежелательных сообщений, которые изначально не были распознаны как спам.

Все списки можно редактировать в главном окне программы ESET Endpoint Security в области **Дополнительные настройки > Интернет и электронная почта > Защита почтового клиента > Адресные книги модуля защиты от спама** при помощи кнопок «Добавить», «Редактировать» и «Удалить» в диалоговом окне каждого списка или в области **Настройка > Интернет и электронная почта**, щелкнув значок шестеренки  рядом с элементом **Защита от спама**.



По умолчанию программа ESET Endpoint Security добавляет все адреса из адресных книг поддерживаемых почтовых клиентов в «белый» список. «Черный» список по умолчанию пуст. В [списке исключений](#) по умолчанию содержатся только собственные адреса электронной почты пользователя.

3.9.3.2.4.2 Добавление адресов в «белый» и «черный» списки

Адреса электронной почты, принадлежащие лицам, с которыми пользователь часто общается, можно добавить в «белый» список, чтобы отправляемые с этих адресов сообщения никогда не классифицировались как спам. Известные адреса отправителей спама можно добавить в «черный» список, чтобы отправляемые с них сообщения всегда классифицировались как спам. Для добавления нового адреса в «белый» или «черный» список щелкните сообщение правой кнопкой мыши и выберите **ESET Endpoint Security > Добавить в «белый» список** или **Добавить в «черный» список** или нажмите кнопку **Доверенный адрес** или **Адрес отправителя спама** в панели инструментов защиты от спама ESET Endpoint Security в почтовом клиенте.

Точно такой же процесс применяется к адресам отправителей спама. Если адрес электронной почты содержится в «черном» списке, каждое сообщение электронной почты, отправленное с этого адреса, будет классифицировано как спам.

3.9.3.2.4.3 Пометка сообщений как спама или не спама

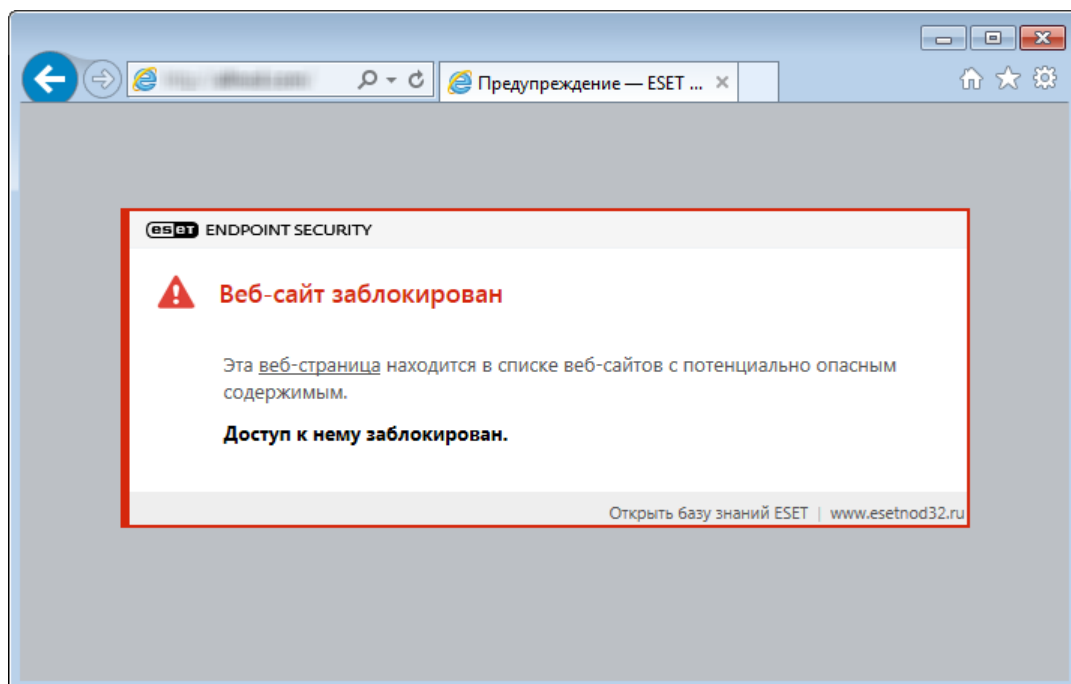
Любое сообщение, просматриваемое в почтовом клиенте, может быть помечено как спам. Для этого нужно щелкнуть его правой кнопкой мыши и нажать **ESET Endpoint Security > Классифицировать выбранные сообщения как спам** или нажать **Спам** в панели инструментов защиты от спама ESET Endpoint Security, которая расположена в верхней части окна почтового клиента.

При классификации сообщение автоматически помещается в папку спама, но адрес отправителя не вносится в «Черный» список. Сходным образом происходит классификация сообщений как нормальных. Для этого следует щелкнуть **ESET Endpoint Security > Классифицировать выбранные сообщения как НЕ спам** или щелкнуть **Не спам** на панели инструментов защиты от спама ESET Endpoint Security, которая расположена в верхней части окна почтового клиента. Если сообщения из папки **нежелательной почты** классифицируются как не спам, они перемещаются в папку **Входящие**. Если сообщение помечено как не спам, адрес отправителя автоматически вносится в «Белый» список.

3.9.3.3 Защита доступа в Интернет

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

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



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

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

- **Веб-протоколы** — возможность настройки отслеживания в стандартных протоколах, которые используются в большинстве веб-браузеров.
- **Управление URL-адресами** — здесь можно задавать HTTP-адреса, которые следует блокировать, разрешать или исключать из проверки.
- **Настройка параметров модуля ThreatSense** — 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.

3.9.3.3.1 Веб-протоколы

По умолчанию ESET Endpoint Security настроен на отслеживание протокола HTTP, используемого большинством интернет-браузеров.

В Windows Vista и более поздних версиях, HTTP-трафик отслеживается для всех портов и приложений. В Windows XP можно изменить **порты, используемые протоколом HTTP**. Для этого последовательно выберите элементы **Дополнительные настройки (F5) > Интернет и электронная почта > Защита доступа в интернет > Веб-протоколы > Настройка модуля сканирования HTTP**. HTTP-трафик всех приложений отслеживается на указанных портах и все порты для приложений помечены как [Клиенты Интернета и электронной почты](#).

ESET Endpoint Security также поддерживает проверку протокола HTTPS. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. ESET Endpoint Security проверяет соединения, использующие методы шифрования SSL и TLS. Программа сканирует только те порты, которые указаны в списке **Порты, используемые протоколом HTTPS**, вне зависимости от версии операционной системы.

По умолчанию сканирование зашифрованных соединений отключено. Для включения сканирования зашифрованных соединений перейдите к элементу [SSL/TLS](#) в разделе «Дополнительные настройки», выберите элементы **Интернет и электронная почта > SSL/TLS**, а затем щелкните элемент **Включить фильтрацию протоколов SSL/TLS**.

3.9.3.3.2 Управление URL-адресами

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

Посещение веб-сайтов, добавленных в **список заблокированных адресов** невозможно, кроме случаев, когда их адреса также добавлены в **список разрешенных адресов**. Веб-сайты из **списка адресов, для которых отключена проверка**, загружаются без проверки на вредоносный код.

Если кроме HTTP-сайтов вы также хотите фильтровать веб-сайты, использующие протокол HTTPS, выберите [Включить фильтрацию протокола SSL](#). В противном случае в список будут добавлены только посещенные вами домены HTTPS-сайтов, а не полный URL-адрес.

Во всех списках можно использовать символы шаблона «*» (звездочка) и «?» (вопросительный знак). Звездочка означает любое количество символов, а вопросительный знак — только один символ. Работать с содержимым списка исключенных адресов следует особенно аккуратно, так как он должен содержать только доверенные и безопасные адреса. Точно так же нужно убедиться в том, что символы 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**.

Если вы хотите заблокировать все HTTP-адреса, кроме адресов, включенных в активный **список разрешенных адресов**, добавьте символ звездочки (*) в активный **список заблокированных адресов**.

Список адресов ?

Имя списка	Типы адресов	Описание списка
Список разрешенных адресов	Разрешено	
Список заблокированных адресов	Заблокировано	
Список адресов, для которых отключена п...	Исключены из проверки	

Добавить Изменить Удалить

Добавьте в список заблокированных адресов подстановочный знак (*), чтобы блокировать все URL-адреса, кроме адресов, включенных в список разрешенных.

OK
Отмена

Добавить: создание нового списка в дополнение к предварительно заданным. 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 существующих списков. Используйте этот пункт для добавления или удаления адресов из списков.

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

3.9.3.4 Защита от фишинга

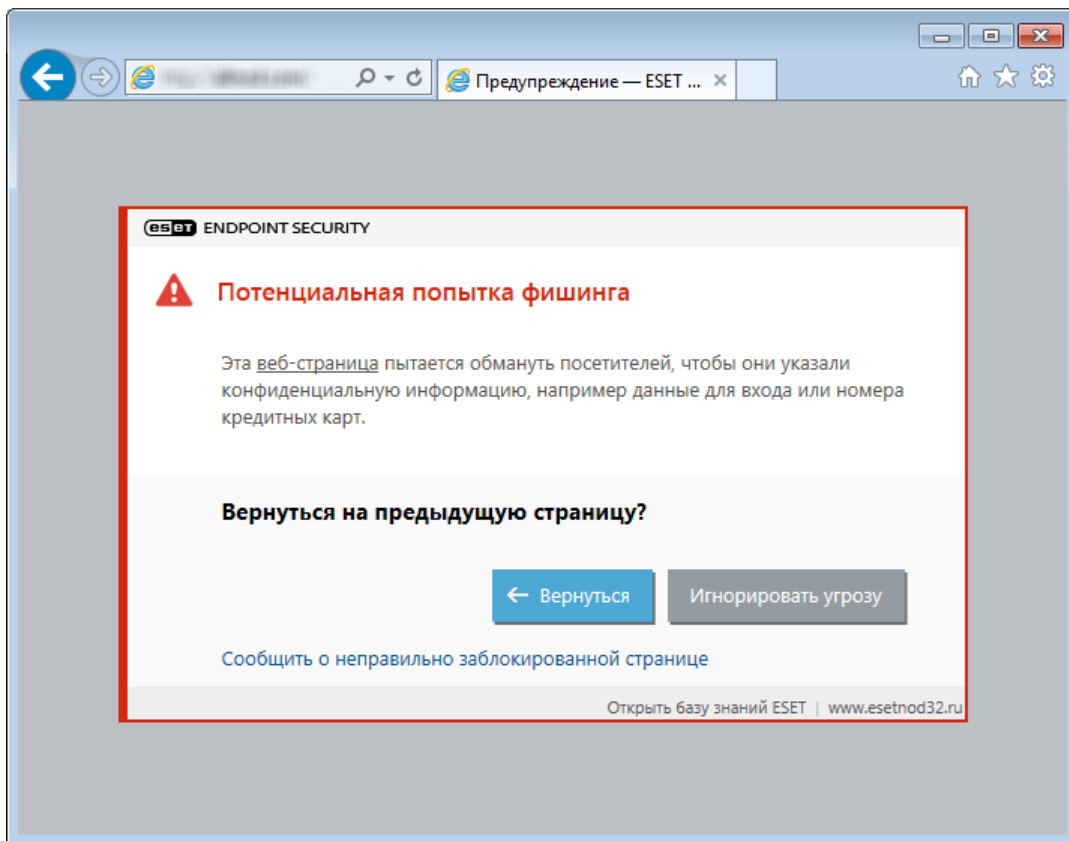
Термин «фишинг» обозначает преступную деятельность, в рамках которой используется социальная инженерия (манипулирование пользователями, направленное на получение конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов,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

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

Дополнительные сведения о защите от фишинга в программе ESET Endpoint Security см. в [статье нашей базы знаний](#).

Доступ к фишинговому веб-сайту

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



i 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.

i 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.).

3.9.4 Контроль доступа в Интернет

В разделе «Контроль доступа в Интернет» можно настроить параметры, которые защитят вашу компанию от опасности юридических исков. Функция контроля доступа в Интернет может управлять доступом к веб-сайтам, которые нарушают права на интеллектуальную собственность. Цель заключается в предотвращении доступа сотрудников к страницам с неприемлемым или опасным содержанием, а также к ресурсам, посещение которых может отрицательно сказаться на эффективности работы.

Функция контроля доступа в Интернет позволяет блокировать веб-страницы, которые могут содержать потенциально нежелательные материалы. Кроме того, работодатели или системные администраторы могут запрещать доступ к более чем 27 предварительно заданным категориям веб-сайтов, включая более 140 подкатегорий.

Контроль доступа в Интернет по умолчанию находится в выключенном состоянии. Чтобы активировать контроль доступа в Интернет, нажмите клавишу F5 и выберите **Дополнительные настройки**, а затем разверните пункты **Интернет и электронная почта > Контроль доступа в Интернет**. Выберите параметр **Интегрировать в систему**, чтобы активировать функцию контроля доступа в Интернет в ESET Endpoint Security. Нажмите кнопку **Изменить** рядом с элементом **Правила**, чтобы открыть окно [Редактор правил для контроля доступа в Интернет](#).

Поля **Сообщение о блокировке веб-страницы** и **Заблокированный графический объект веб-страницы** позволяют с легкостью настроить сообщение, которое отображается при блокировке веб-сайта.

✓ ПОДСКАЗКА

Сообщение о блокировке веб-страницы может выглядеть так: *Веб-страница заблокирована, так как ее содержимое является неприличным или опасным. Дополнительные сведения можно получить у системного администратора.* В сообщение можно добавить веб-адрес или сетевой путь к изображению, например <http://test.com/test.jpg>. Размер изображения должен быть равен 90 x 30. Другой размер изображения будет автоматически преобразован под это требование.

✓ ПОДСКАЗКА

Информацию о том, как заблокировать все веб-страницы и оставить доступными только некоторые, можно получить [здесь](#).

3.9.4.1 Правила

В окне **Правила** отображаются существующие правила на основе URL-адресов и категорий.

Включено	Имя	Тип	URL-адрес/категория	Пользователи	Права доступа	Серьезность
<input checked="" type="checkbox"/>	Block page	Действие на осн...	www.blockedpage.o...	Все	Блокировать	Всегда
<input checked="" type="checkbox"/>	Allow this page	Действие на осн...	www.allowedpage.c...	Все	Разрешить	Всегда
<input checked="" type="checkbox"/>	Group all harmf...	Действие на осн...	Группа 1	Все	Блокировать	Всегда

В списке правил представлен ряд их описаний, например имена, тип блокирования, действие, выполняемое при срабатывании правила контроля доступа в Интернет, 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**. Чтобы выделить несколько правил и удалить все выбранные правила, щелкните их, удерживая нажатой клавишу **CTRL**. Флажок **Включено** позволяет включить или отключить правило. Это может быть полезно, если вы не хотите полностью удалять правило, поскольку оно может понадобиться позднее.

Правила сортируются по приоритету: правила с самым высоким приоритетом располагаются сверху. Оценка правил на основании URL-адреса имеет более высокий приоритет, чем оценка на основании категории. Например, если правило, основанное на URL-адресе, находится в списке правил под правилом, основанном на категории, оно все равно имеет более высокий приоритет и его оценка будет выполняться первой.

3.9.4.1.1 Добавление правил контроля доступа в Интернет

В окне «Правила контроля доступа в Интернет» можно вручную создавать и изменять правила фильтрации для контроля доступа в Интернет.

Изменить правило

Имя: Block page

Включено:

Тип: Действие на основе URL-адреса

Права доступа: Блокировать

URL-адрес: www.blockedpage.org

[Использовать группу URL-адресов](#)

Серьезность регистрируемых событий: Всегда

Список пользователей: [Изменить](#)

OK

Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить это правило, щелкните переключатель **Включено**. Это может быть полезно в том случае, если вы не хотите безвозвратно удалять правило.

Тип действия

- **Действие на основе URL-адреса.** Если правила управляют доступом к определенному веб-сайту, укажите адрес веб-сайта в поле **URL-адрес**.
- **Действие на основе категории.** Активировав эту функцию, выберите в раскрывающемся меню категорию действия.

Такие специальные символы, как * (звездочка) и ? (знак вопроса) нельзя использовать в списке URL-адресов. При создании группы URL-адресов, в которую входит веб-сайт с несколькими доменами верхнего уровня, каждый домен нужно добавлять отдельно. Если в группу добавить домен, все содержимое этого домена и всех его поддоменов (например, *sub.examplepage.com*) будет разрешено или заблокировано в зависимости от выбранного действия на основе URL-адреса.

Права доступа

- **Разрешить:** доступ к URL-адресу или категории будет открыт.
- **Предупредить:** будет показано предупреждение об URL-адресе или категории.
- **Блокировать:** URL-адрес или категория будет блокироваться.

Применять во время: позволяет применять созданное правило в определенное время. В раскрывающемся меню выберите созданный временной интервал. Чтобы получить дополнительные сведения о **временных интервалах**, щелкните здесь.

URL-адрес или **Использовать группу URL-адресов.** Если будет обнаружена указанная URL-ссылка или группа ссылок, доступ будет разрешен, заблокирован или будет показано предупреждение.

Серьезность регистрируемых событий

- **Всегда:** создает файлы журнала для всех случаев передачи данных через Интернет.
- **Диагностика:** регистрируется информация, необходимая для тщательной настройки программы.
- **Информация** — в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждение:** записывается информация обо всех критических ошибках и предупреждениях.
- **Нет:** журналы не будут создаваться.

i ПРИМЕЧАНИЕ.

Уровень серьезности регистрируемых событий можно настроить для каждого списка. Журналы со статусом **Предупреждение** могут собираться ESET Remote Administrator.

Список пользователей

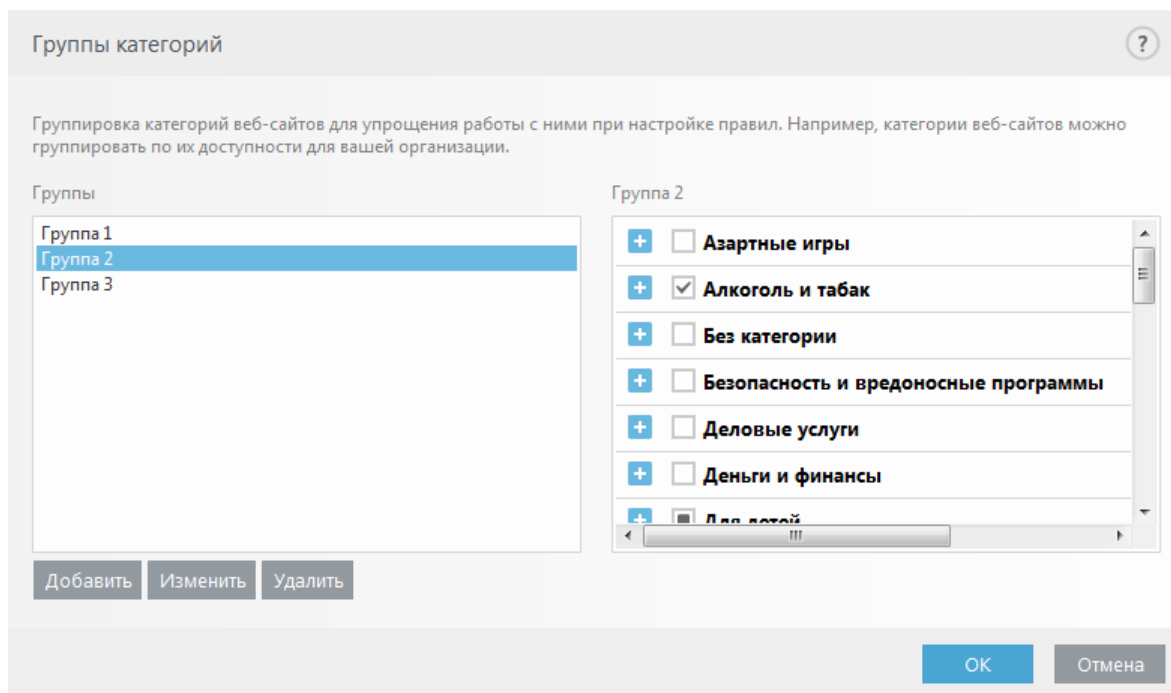
- **Добавить** — открытие диалогового окна **Выбор пользователей или групп**, в котором можно выбрать необходимых пользователей. Если не указан ни один пользователь, правило будет применяться ко всем пользователям.
- **Удалить** — выбранный пользователь удаляется из фильтра.

3.9.4.2 Группы категорий

Окно «Группы категорий» разделено на две части. В правой представлен список категорий и подкатегорий. Выбор категории в списке «Категория» позволяет просмотреть соответствующие подкатегории.

Каждая группа содержит подкатегории, связанные с содержимым для взрослых или неприемлемыми материалами. Открыв окно «Группы категорий» и щелкнув первую группу, можно добавлять в список приемлемых групп или удалять из него те или иные категории и подкатегории (например, «Насилие» или «Оружие»). Веб-страницы с неприемлемыми материалами могут блокироваться или пользователи могут информироваться после создания правила с предварительно заданными действиями.

Поставьте флажок для добавления или удаления подкатегории отдельной группы.



Ниже приведены некоторые примеры групп, о которых пользователям может быть неизвестно.

Разное: обычно частные (локальные) IP-адреса, например адреса в интрасети, такие как 192.168.0.0/16 и другие. Веб-сайт, на котором отображается код ошибки 403 или 404, также попадает в эту категорию.

Не разрешенное: эта категория включает веб-страницы, которые не разрешены из-за возникновения ошибки при подключении к модулю базы данных контроля доступа в Интернет.

Без категории: неизвестные веб-страницы, которых еще нет в базе данных контроля доступа в Интернет.

Прокси-серверы: такие веб-страницы, как анонимайзеры, перенаправители или открытые прокси-серверы, могут использоваться для получения (анонимного) доступа к веб-сайтам, которые обычно запрещены фильтром контроля доступа в Интернет.

Обмен файлами: такие веб-страницы содержат большой объем данных, включая фотографии, видео или электронные книги. Существует опасность, что эти веб-сайты содержат потенциально нежелательные материалы или материалы для взрослых.

i ПРИМЕЧАНИЕ

Подкатегория может относиться только к одной группе. Некоторые подкатегории не включены в заранее заданные группы (например, «Игры»). Чтобы они использовались фильтром контроля доступа в Интернет, добавьте их в нужную группу.

3.9.4.3 Группы URL-адресов

С помощью функции группы URL-адресов можно создать группу ссылок, для которых нужно создать правило (разрешить или заблокировать определенные сайты).

Чтобы создать новую группу URL-адресов, нажмите кнопку **Добавить**. Выберите группу URL-адресов и в правом нижнем углу окна нажмите кнопку **Добавить**, чтобы добавить в список новые ссылки. Также можно воспользоваться функцией **Импорт из файла**. Она позволяет импортировать файл с URL-адресами (в качестве разделителя используется разрыв строки, например текстовый файл с кодировкой UTF-8). Если для определенной группы URL-адресов нужно настроить какое-то действие, откройте **редактор правил для контроля доступа в Интернет**, выберите в раскрывающемся списке нужную группу URL-адресов, настройте параметры и нажмите кнопку **ОК**.

i ПРИМЕЧАНИЕ.

Блокирование или разрешение конкретной веб-страницы может быть более точным, чем блокирование или разрешение целой категории веб-страниц. Следует быть особенно внимательным при изменении этих параметров и добавлении категории или веб-страницы в список.

3.9.5 Обновление программы

Регулярное обновление ESET Endpoint Security — лучший способ добиться максимального уровня безопасности компьютера. Модуль обновления поддерживает актуальность программы двумя способами: обновляет модуль обнаружения и компоненты системы.

Выбрав пункт **Обновление** в главном окне программы, можно получить информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления. Кроме того, можно щелкнуть ссылку **Показать все модули**, чтобы открыть список установленных модулей и проверить версию и дату последнего обновления модуля.

Вы также можете вручную запустить обновление, для этого щелкните **Проверить наличие обновлений**. Обновление модуля обнаружения и компонентов программы — важнейшая процедура по обеспечению полной защиты компьютера от вредоносного кода. Уделите особое внимание изучению конфигурирования и работы этого процесса. Если в процессе установки не были указаны сведения о лицензии, лицензионный ключ можно указать при обновлении. Чтобы получить доступ к серверам обновлений ESET, щелкните элемент **Активация продукта**.

Если активировать ESET Endpoint Security с помощью автономного файла лицензии (не вводя имя пользователя и пароль) и попробовать выполнить обновление, отобразится красного цвета текст **Произошла ошибка обновления модуля обнаружения**. Он означает, что загружать обновления можно только с зеркала.

i ПРИМЕЧАНИЕ

Лицензионный ключ предоставляет компания ESET после приобретения ESET Endpoint Security.

Обновление	
✓ ESET Endpoint Security	
Текущая версия:	6.6.2037.1
✓ Последнее обновление:	8/3/2017 4:26:17 PM
✓ Последняя проверка на наличие обновлений:	8/3/2017 4:26:17 PM
Показать все модули	

ENJOY SAFER TECHNOLOGY™

Проверить наличие обновлений Изменить частоту обновления

Текущая версия: номер сборки ESET Endpoint Security.

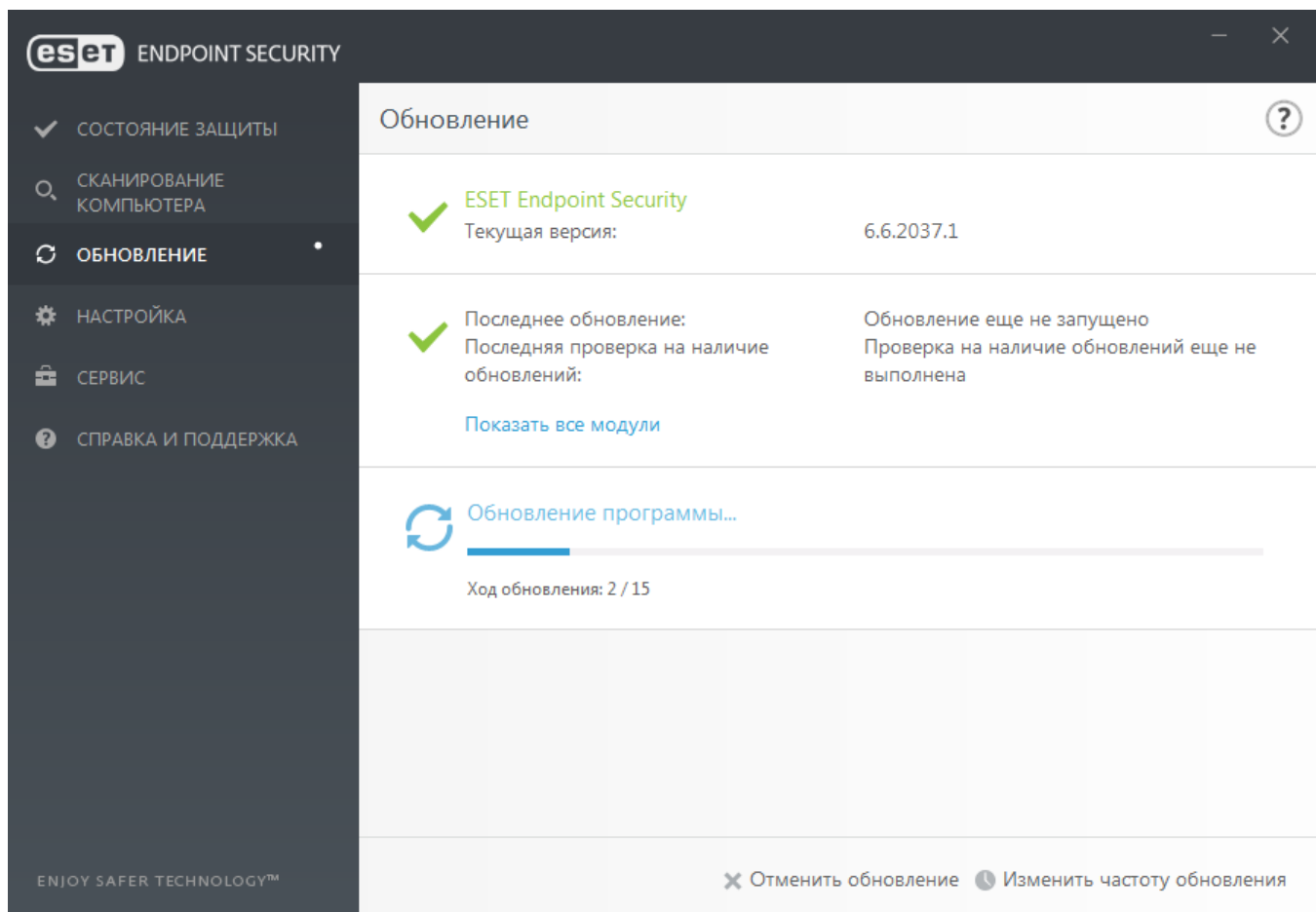
Последнее обновление: дата и время последнего обновления. Следует убедиться, что в этом поле указана недавняя дата, поскольку это значит, что версия модуля обнаружения актуальна.

Последняя проверка на наличие обновлений: дата и время последней попытки обновления модулей.

Показать все модули: щелкните эту ссылку, чтобы открыть список установленных модулей и проверить версию и дату последнего обновления модуля.

Процесс обновления

После нажатия кнопки **Проверить наличие обновлений** начинается процесс загрузки. На экран будут выведены индикатор выполнения загрузки и время до ее окончания. Чтобы прервать обновление, нажмите кнопку **Отменить обновление**.



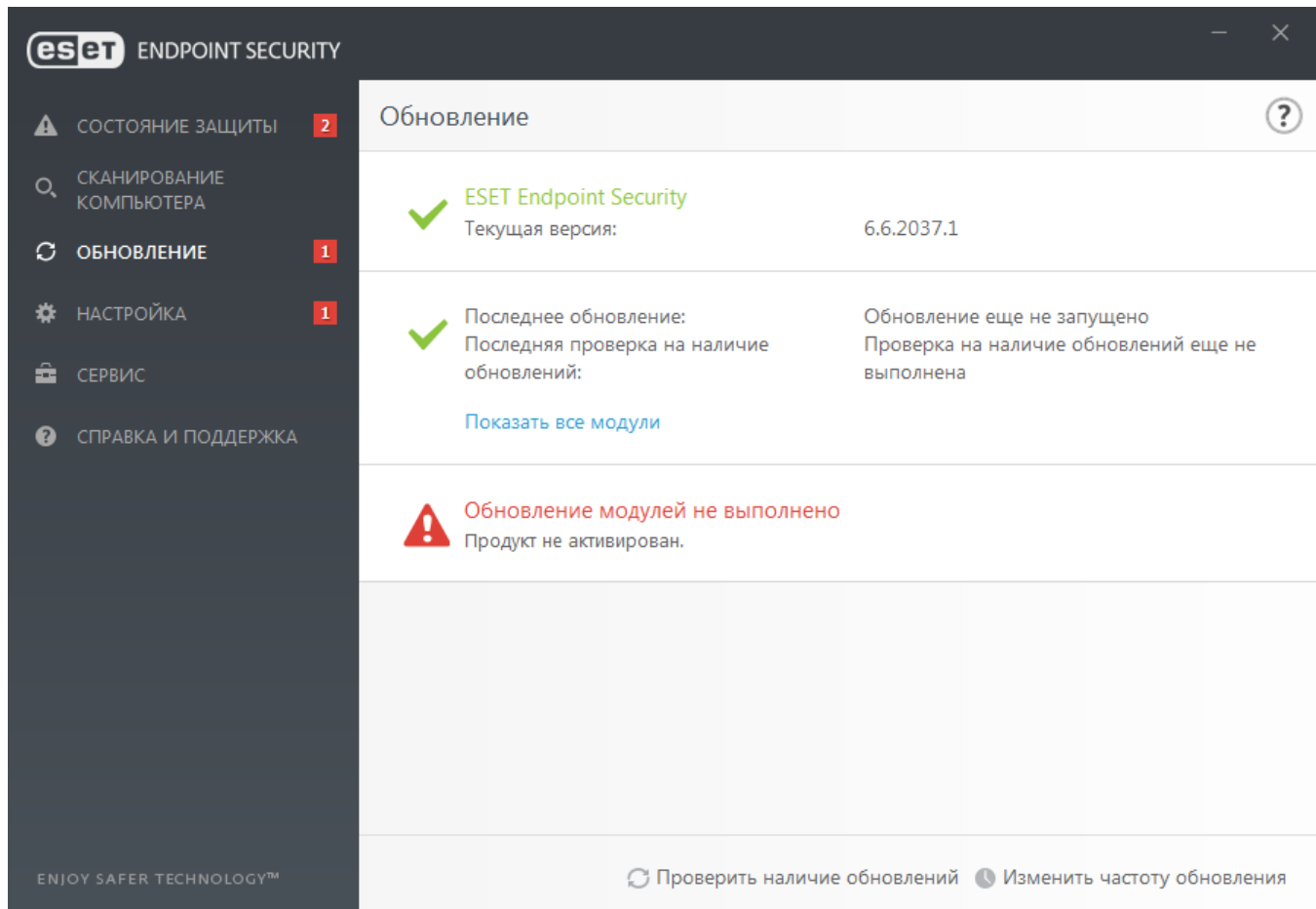
! ВАЖНО!

Как правило, модуль обнаружения обновляется несколько раз в день. Если этого сообщения нет, программа устарела. При этом повышается риск заражения. Необходимо обновить модуль обнаружения как можно скорее.

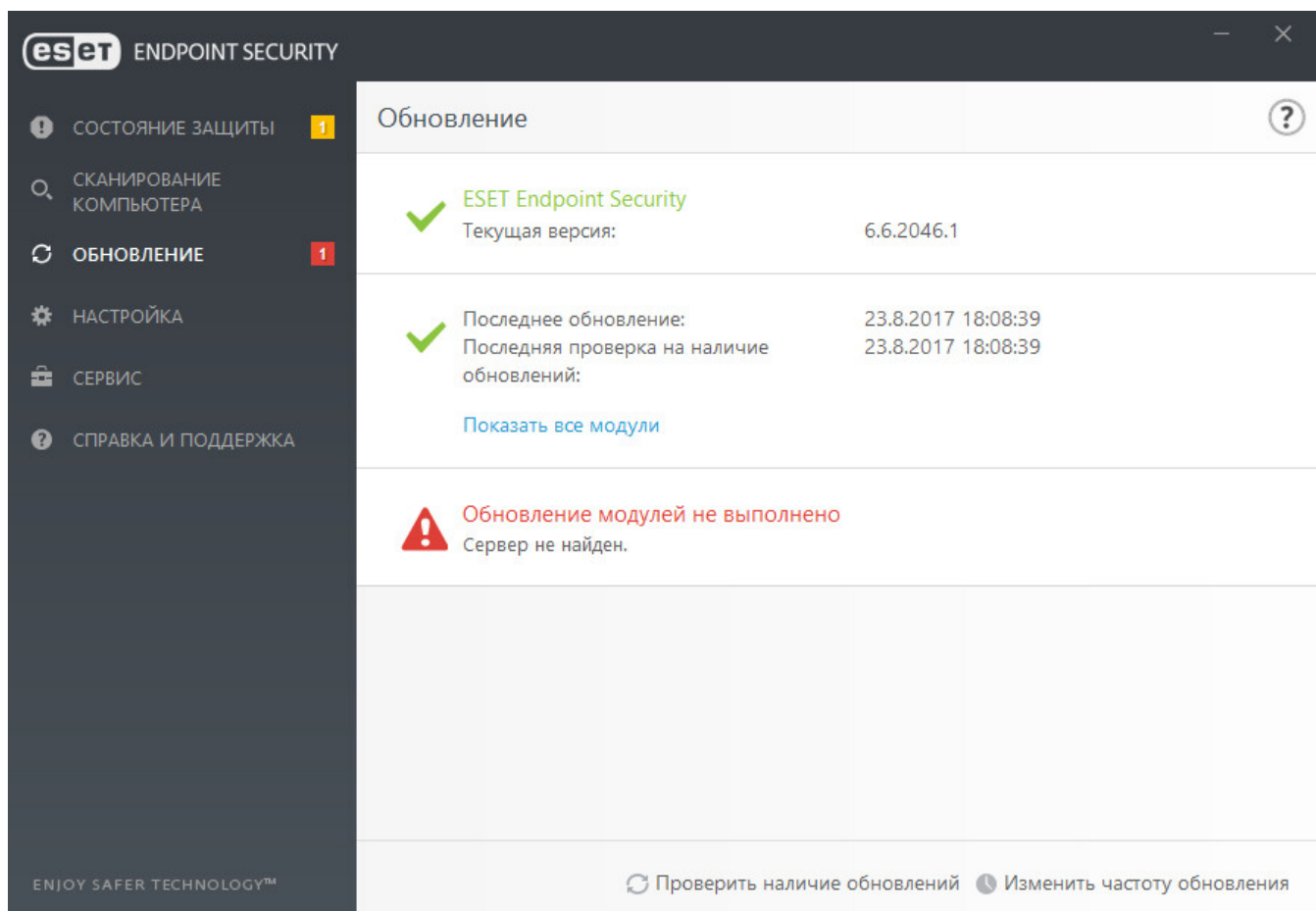
Модуль обнаружения устарел: эта ошибка появляется после нескольких неудачных попыток обновить модуль обнаружения. Рекомендуется проверить параметры обновлений. Наиболее частая причина этой ошибки — неправильно введенные данные для аутентификации или неверно настроенные [параметры подключения](#).

Предыдущее уведомление связано с двумя указанными ниже сообщениями об ошибках при обновлении (**Обновление модуля обнаружения не выполнено**).

1. **Недействительная лицензия:** в разделе параметров обновления введен неправильный лицензионный ключ. Рекомендуется проверить данные аутентификации. В окне «Расширенные параметры» (в главном меню выберите пункт **Настройка**, после чего щелкните **Расширенные параметры** или нажмите клавишу F5) содержатся расширенные параметры обновления. В главном меню последовательно щелкните элементы **Справка и поддержка > Управление лицензией** и введите новый лицензионный ключ.



2. При загрузке файлов обновлений произошла ошибка: 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.



i ПРИМЕЧАНИЕ.

Дополнительные сведения можно найти в этой [статье базы знаний ESET](#).

3.9.5.1 Настройка обновлений

Параметры обновления доступны в дереве **Дополнительные настройки** (F5) в разделе **Обновление**. В этом разделе указывается информация об источниках обновлений, таких как серверы обновлений и данные аутентификации для них.

- Общие

Текущий профиль обновления отображается в раскрывающемся меню **Профиль обновления**. Чтобы создать новый профиль, перейдите на вкладку **Профили** и нажмите кнопку **Изменить** рядом с элементом **Список профилей**, введите собственное **имя профиля** и затем нажмите **Добавить**.

Если во время загрузки обновлений модуля обнаружения возникли проблемы, щелкните **Очистить**, чтобы удалить временные файлы обновлений (очистить кэш).

Предупреждения об устаревшем модуле обнаружения

Автоматически задавать максимальный возраст базы данных: позволяет задать максимальное время (в днях), по истечении которого модуль обнаружения будет считаться устаревшим. Значение по умолчанию — 7.

Откат

Если вы подозреваете, что последнее обновление модуля обнаружения и/или программных модулей повреждено или работает нестабильно, вы можете выполнить откат до предыдущей версии и отключить обновления на установленный период времени. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени.

Программа ESET Endpoint Security создает снимки модуля обнаружения и программных модулей. Эти снимки используются функцией *отката*. Если нужно, чтобы снимки файлов обновлений создавались, оставьте флажок **Создать снимки файлов обновлений** установленным. В поле **Количество локально хранимых снимков** указывается количество хранящихся снимков предыдущих баз данных сигнатур вирусов.

После нажатия кнопки **Откатить (Дополнительные настройки (F5) > Обновление > Общие)** в раскрывающемся меню нужно выбрать промежуток времени, на который будет приостановлено обновление модуля обнаружения и программных модулей.

The screenshot shows the 'Расширенные параметры' (Advanced Parameters) window. On the left is a sidebar with categories: ЗАЩИТА ОТ ВИРУСОВ (1), ОБНОВЛЕНИЕ (2), ФАЙЕРВОЛ (5), ИНТЕРНЕТ И ЭЛЕКТРОННАЯ ПОЧТА (4), КОНТРОЛЬ УСТРОЙСТВ (1), СЛУЖЕБНЫЕ ПРОГРАММЫ (1), and ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ. The main area is titled 'ОБЩИЕ' (General) and contains several settings:

- Профиль обновления**: dropdown menu set to 'Мой профиль'.
- Очистить кэш обновлений**: button labeled 'Очистить'.
- ПРЕДУПРЕЖДЕНИЯ ОБ УСТАРЕВШЕМ МОДУЛЕ ОБНАРУЖЕНИЯ**: section header.
- Этот параметр определяет максимально допустимый возраст, после достижения которого модуль обнаружения будет считаться устаревшим и отобразится соответствующее предупреждение.**: explanatory text.
- Автоматически задавать максимальный возраст базы данных**: checkbox checked.
- Максимальный возраст базы данных (в днях)**: spinner box set to 7.
- ОТКАТ**: section header.
- Создать снимки модулей**: checkbox checked.
- Количество локально хранимых снимков**: spinner box set to 2.
- Откат к предыдущим модулям**: button labeled 'Откат'.

At the bottom, there are buttons for 'По умолчанию' (Default), 'OK', and 'Отмена' (Cancel).

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).

Профили

Чтобы создать профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**. Чтобы изменить созданный профиль, выберите его и нажмите кнопку **Изменить** возле элемента **Список профилей**.

Основные сведения

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. **Тестовое обновление** — это обновление, которое уже прошло полное внутреннее тестирование и в ближайшее время станет доступным всем пользователям. Преимущество тестовых обновлений заключается в том, что у вас появляется возможность использовать новейшие исправления и способы обнаружения. Однако такие обновления иногда могут быть недостаточно стабильны и НЕ ДОЛЖНЫ использоваться на

производственных серверах и рабочих станциях, где требуются максимальные работоспособность и стабильность. Вариант **Отложенное обновление** позволяет загружать обновления со специальных серверов с задержкой в несколько часов (т. е. после того, как обновления будут протестированы в реальных средах и признаны стабильными).

Отключить оповещение об успешном обновлении: отключает уведомления на панели задач 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.

Обновить со съемного носителя: позволяет выполнить обновление со съемного носителя, если он содержит созданное зеркало. Если установлен флажок **Автоматически**, обновление будет выполняться в фоновом режиме. Если диалоговые окна обновления должны отображаться, выберите **Всегда спрашивать**.

По умолчанию в меню **Сервер обновлений** установлен параметр **Выбирать автоматически**. Сервер обновлений — это компьютер, на котором хранятся файлы обновлений. При использовании сервера ESET рекомендуется оставить параметры по умолчанию.

При использовании локального HTTP-сервера, который называется зеркалом, сервер обновлений должен быть указан следующим образом:

`http://имя_компьютера_или_его_IP-адрес:2221.`

Если используется локальный HTTP-сервер с поддержкой SSL, сервер обновлений должен быть указан следующим образом:

`https://имя_компьютера_или_его_IP-адрес:2221.`

Если используется локальная общая папка, сервер обновлений должен быть указан следующим образом:

`\\имя_компьютера_или_его_IP-адрес\общая_папка`

Обновление с зеркала

На серверах обновлений для аутентификации используется **лицензионный ключ**, который создается и отправляется после покупки. При использовании сервера зеркала можно определить, с помощью каких учетных данных клиентам следует выполнять вход на этот сервер перед получением обновлений. По умолчанию проверка не требуется, то есть поля **Имя пользователя** и **Пароль** остаются пустыми.

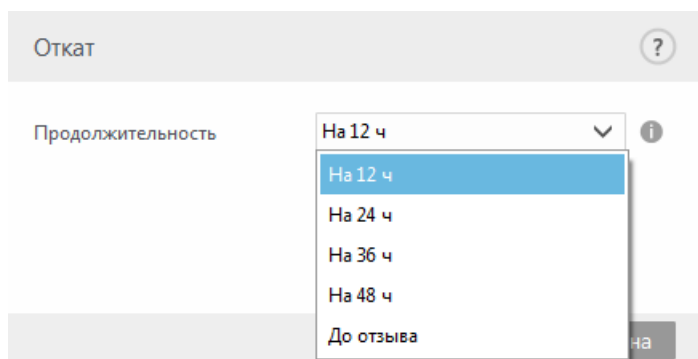
3.9.5.1.1 Профили обновления

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 **Профиль обновления** отображается текущий профиль. По умолчанию для него задано значение **Мой профиль**. Чтобы создать профиль, рядом с элементом **Список профилей** нажмите кнопку **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**.

3.9.5.1.2 Откат обновления

После нажатия кнопки **Откатить** (**Дополнительные настройки** (F5) > **Обновление** > **Профиль**) в раскрывающемся меню нужно выбрать промежуток времени, на который будет приостановлено обновление модуля обнаружения и программных модулей.



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.

Программа возвращается к самой старой версии модуля обнаружения, которая хранится в качестве снимка в файловой системе локального компьютера.

i ПРИМЕЧАНИЕ.

Предположим, последней версии модуля обнаружения присвоен номер 10646. Версии 10645 и 10643 хранятся в качестве снимков модуля обнаружения. Обратите внимание, что версия 10644 недоступна, поскольку, например, компьютер был выключен и более новая версия обновления стала доступна до того, как была загружена версия 10644. Если в поле **Количество локально хранимых снимков** установить значение 2 и нажать кнопку **Откатить**, программа вернется к версии 10643 модуля обнаружения (включая программные модули). Это может занять некоторое время. Чтобы проверить, произведен ли откат до предыдущей версии модуля обнаружения, в главном окне ESET Endpoint Security откройте раздел [Обновление](#).

3.9.5.1.3 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.

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

- **Запросить подтверждение перед загрузкой компонентов программы** — вариант по умолчанию. Пользователю будет предлагаться подтвердить обновление компонентов программы или отказаться от него, когда такое обновление становится доступно.
- **Выполнять обновление компонентов программы, если доступно** — обновления компонентов программы будут загружаться и устанавливаться автоматически. Обратите внимание на то, что может потребоваться перезагрузка компьютера.
- **Никогда не обновлять компоненты программы** — обновление компонентов программы выполняться не будет. Этот вариант подходит для серверной установки, поскольку серверы обычно перезапускаются только при техническом обслуживании.

i ПРИМЕЧАНИЕ.

Наиболее подходящий вариант зависит от конкретной рабочей станции, на которой будут применяться параметры. Необходимо помнить о различиях между рабочими станциями и серверами. Например, автоматический перезапуск сервера после обновления программы может привести к серьезным проблемам.

Включить ручное обновление компонентов программы — по умолчанию отключено. Если этот параметр включен и доступна более новая версия ESET Endpoint Security, можно проверить наличие обновлений на панели **Обновление** и **установить** новую версию.

Если установлен флажок **Запрашивать подтверждение перед загрузкой обновления**, на экран будет выводиться уведомление каждый раз, когда появляется новое обновление.

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

3.9.5.1.4 HTTP-сервер

Порт сервера: по умолчанию порт сервера имеет значение 2221.

Аутентификация: определяется метод аутентификации, используемый для доступа к файлам обновлений. Доступны варианты **Нет**, **Обычная** и **NTLM**. Чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите **Обычная**. Вариант **NTLM** обеспечивает шифрование с использованием безопасного метода. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений. Значение по умолчанию — **Нет**. Этот вариант дает доступ к файлам обновлений без аутентификации.

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

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

3.9.5.1.5 Параметры подключения

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 меню **Подключаться к локальной сети** как один из следующих 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.

Параметры **Имя пользователя** и **Пароль** являются необязательными.

⚠ 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 даже после загрузки обновлений.

3.9.5.1.6 Зеркало обновлений

ESET Endpoint Security дает возможность создавать копии файлов обновлений, которые могут использоваться для обновления других рабочих станций в сети. Использование *зеркала* (копии файлов обновлений в локальной сети) позволяет избежать загрузки одних и тех же обновлений с сервера производителя всеми рабочими станциями. Обновления загружаются на локальный сервер зеркала, а затем распространяются на рабочие станции. Это позволяет избежать перерасхода трафика. Обновление клиентских рабочих станций с зеркала оптимизирует трафик в сети и сокращает объем потребляемого интернет-трафика.

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

Расширенные параметры

ЗАЩИТА ОТ ВИРУСОВ 1

ОБНОВЛЕНИЕ 4

ФАЙЕРВОЛ 5

ИНТЕРНЕТ И ЭЛЕКТРОННАЯ ПОЧТА 4

КОНТРОЛЬ УСТРОЙСТВ 1

СЛУЖЕБНЫЕ ПРОГРАММЫ 1

ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

Создать зеркало обновления

ДОСТУП К ФАЙЛАМ ОБНОВЛЕНИЯ

Передавать файлы обновлений через внутренний HTTP-сервер

Папка для хранения копий файлов:
C:\ProgramData\ESET\ESET Smart Security Premium\mirror [Очистить](#) ⓘ

Имя пользователя ⓘ

Пароль ⓘ

ФАЙЛЫ

Файлы [Изменить](#)

⊞ HTTP-СЕРВЕР ⤴

⊞ ПОДКЛЮЧАТЬСЯ К ЛОКАЛЬНОЙ СЕТИ КАК ⤴

⊞ ОБНОВЛЕНИЕ КОМПОНЕНТОВ ПРОГРАММЫ ⤴

По умолчанию

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

Доступ к файлам обновления

Передавать файлы обновлений через внутренний HTTP-сервер: если этот параметр активирован, файлы обновлений будут доступны по протоколу HTTP без необходимости указывать имя пользователя и пароль.

i ПРИМЕЧАНИЕ.

Для использования HTTP-сервера в Windows XP необходимо установить пакет обновления 2.

Способы доступа к серверу зеркала детально описаны в статье [Обновление с зеркала](#). Есть два основных способа доступа к зеркалу: папка с файлами обновлений может использоваться как общая сетевая папка или клиенты могут получить доступ к зеркалу на HTTP-сервере.

Папка, предназначенная для хранения файлов обновлений для зеркала, указывается в разделе **Папка для хранения копий файлов**. Чтобы выбрать другую папку, щелкните **Очистить** для удаления предварительно заданной папки `C:\ProgramData\ESET\ESET Endpoint Security\mirror`, а затем щелкните **Изменить** для выбора папки на локальном компьютере или общей сетевой папки. Если для указанной папки нужна авторизация, данные аутентификации должны быть указаны в полях **Имя пользователя** и **Пароль**. Если выбранная папка назначения расположена на сетевом диске компьютера под управлением ОС Windows NT/2000/XP, указанные имя пользователя и пароль должны принадлежать пользователю с правами на запись в указанную папку. Имя пользователя и пароль следует вводить в формате *Домен/Пользователь* или *Рабочая_группа/Пользователь*. Не забудьте ввести соответствующие пароли.

Файлы: при настройке зеркала можно указать предпочитаемые языки обновлений. Выбранные языки должны поддерживаться сервером зеркала, который настроил пользователь.

Обновление компонентов программы

Автоматическое обновление компонентов: разрешает установку новых и обновление существующих компонентов. Обновление может выполняться как в автоматическом режиме без вмешательства пользователя, так и с уведомлением. После установки обновления компонентов программы может потребоваться перезагрузка компьютера.

Обновить компоненты сейчас: обновляет компоненты программы до последней версии.

Расширенные параметры

ЗАЩИТА ОТ ВИРУСОВ 1

ОБНОВЛЕНИЕ 4

ФАЙЕРВОЛ 5

ИНТЕРНЕТ И ЭЛЕКТРОННАЯ ПОЧТА 4

КОНТРОЛЬ УСТРОЙСТВ 1

СЛУЖЕБНЫЕ ПРОГРАММЫ 1

ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

ФАЙЛЫ

Файлы [Изменить](#)

HTTP-СЕРВЕР

Порт сервера 2221

Аутентификация Нет

SSL ДЛЯ HTTP-СЕРВЕРА

Файл цепочки сертификатов ...

Тип сертификата PEM

Файл закрытого ключа ...

Тип закрытого ключа Интегрирован

ПОДКЛЮЧАТЬСЯ К ЛОКАЛЬНОЙ СЕТИ КАК

ОБНОВЛЕНИЕ КОМПОНЕНТОВ ПРОГРАММЫ

По умолчанию OK Отмена

3.9.5.1.6.1 Обновление с зеркала

Существует два способа настройки зеркала. Зеркало — это, по сути, репозиторий, с которого клиенты могут загружать файлы обновлений. Папкой с файлами обновлений может выступать общий сетевой ресурс или HTTP-сервер.

Доступ к файлам зеркала с помощью внутреннего HTTP-сервера

Это вариант по умолчанию, выбранный в предварительно заданной конфигурации программы. Для обеспечения доступа к зеркалу с помощью HTTP-сервера перейдите на вкладку **Дополнительные настройки > Обновление > Профили > Зеркало** и выберите элемент **Создать зеркало обновления**.

В разделе **HTTP-сервер** вкладки **Зеркало** можно указать **Порт сервера**, на котором HTTP-сервер будет принимать запросы, а также тип **аутентификации**, используемой HTTP-сервером. По умолчанию порт сервера имеет значение **2221**. С помощью параметра **Аутентификация** определяется метод аутентификации, используемый для доступа к файлам обновлений. Доступны варианты **Нет**, **Обычная** и **NTLM**. Чтобы использовать кодировку base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите **Обычная**. Вариант **NTLM** обеспечивает шифрование с использованием безопасного метода. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений. Значение по умолчанию — **Нет**. Этот вариант дает доступ к файлам обновлений без аутентификации.

ВНИМАНИЕ!

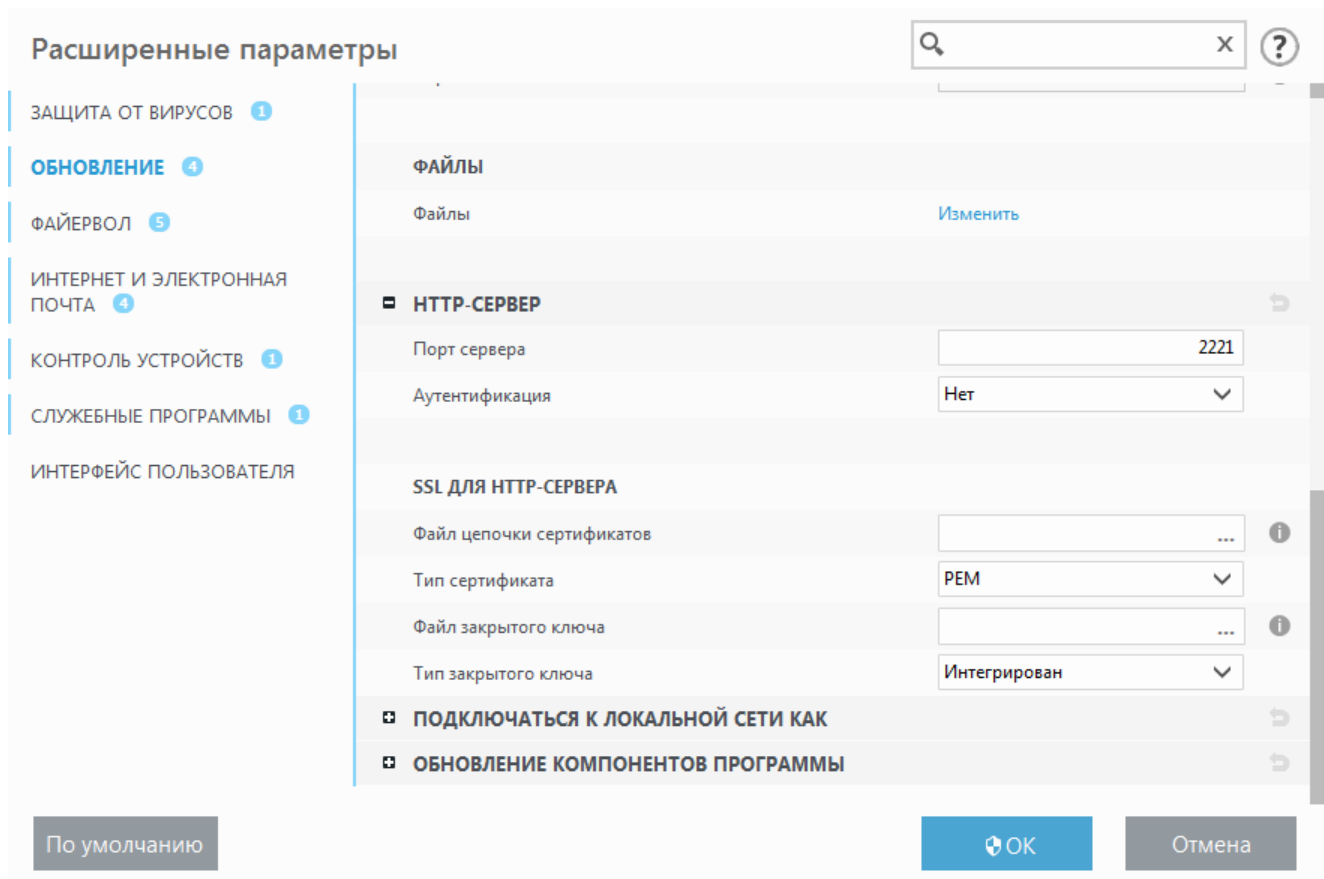
Если планируется организовать доступ к файлам обновлений с помощью HTTP-сервера, папка зеркала должна находиться на том же компьютере, что и экземпляр ESET Endpoint Security, который ее создает.

SSL для HTTP-сервера

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

ПРИМЕЧАНИЕ.

После нескольких неудачных попыток обновить модуль обнаружения с зеркала в главном меню на панели обновления появится ошибка **Неверные имя пользователя и (или) пароль**. Рекомендуем перейти в меню **Дополнительные настройки > Обновление > Профили > Зеркало** и проверить указанные имя пользователя и пароль. Обычно эта ошибка вызвана неправильными аутентификационными данными.



После настройки сервера зеркала вам следует добавить сервер обновлений на клиентские рабочие станции. Для этого выполните следующие действия.

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

Доступ к зеркалу через общие системные папки

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

Далее на вкладке **Дополнительные настройки** > **Обновление** > **Профили** > **Зеркало** необходимо настроить доступ к зеркалу, сняв флажок **Передавать файлы обновлений через внутренний HTTP-сервер**. Этот вариант включен по умолчанию после установки программы.

Если общая папка расположена на другом компьютере в сети, необходимо указать данные аутентификации для доступа к нему. Для этого откройте в ESET Endpoint Security раздел **Дополнительные настройки** (F5) и щелкните **Обновление** > **Профили** > **Подключаться к локальной сети как**. Этот параметр аналогичен используемому для обновления и описан в разделе [Подключение к локальной сети](#).

После окончания настройки зеркала укажите на рабочих станциях адрес нового сервера обновлений в формате `\\UNC\ПУТЬ`.

1. Откройте в ESET Endpoint Security меню **Дополнительные настройки > Обновление > Профили > Обычное**.
2. Снимите флажок **Выбирать автоматически** и добавьте новый сервер в поле **Сервер обновлений**. Для этого используйте формат `\\UNC\ПУТЬ`.

i ПРИМЕЧАНИЕ.

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

Последний раздел контролирует компоненты программы (PCU). По умолчанию после загрузки их можно копировать в локальное зеркало. Если установлен флажок **Обновление компонентов программы**, не нужно нажимать кнопку **Обновить**, т. к. файлы автоматически копируются на локальное зеркало. Дополнительные сведения об обновлении компонентов программы см. в разделе [Режим обновления](#).

3.9.5.1.6.2 Устранение проблем при обновлении с зеркала

В большинстве случаев проблемы при обновлении с сервера зеркала возникают в связи с по крайней мере одной из следующих причин: неверное указание параметров папки зеркала, неверные данные аутентификации для папки зеркала, неверные параметры на рабочих станциях, которые пытаются загружать файлы обновлений с зеркала, а также различные сочетания этих причин. Ниже приведен краткий обзор наиболее часто возникающих проблем при обновлении с зеркала.

Ошибка при подключении ESET Endpoint Security к серверу зеркала: обычно происходит при указании неправильных данных сервера обновлений (сетевого пути к папке зеркала), с которого рабочие станции загружают обновления. Для проверки папки нажмите кнопку **Пуск** в системе Windows, выберите **Выполнить**, введите имя папки и нажмите кнопку **OK**. На экран должно быть выведено содержимое папки.

ESET Endpoint Security запрашивает имя пользователя и пароль: вероятная причина заключается в том, что введены неверные данные аутентификации (имя пользователя и пароль) в разделе обновлений. Имя пользователя и пароль используются для доступа к серверу обновлений, с которого выполняется обновление программы. Убедитесь, что данные аутентификации указаны верно и в правильном формате. Например, *Домен/Имя_пользователя* или *Рабочая_группа/имя_пользователя* в сочетании с соответствующим паролем. Если сервер зеркала доступен всем участникам сети, это не означает, что у любого пользователя есть к нему доступ. Параметр «Все» означает то, что папка доступна всем пользователям домена, а не то, что предоставляется доступ без авторизации. В результате, если папка доступна всем участникам, в настройках обновления все же необходимо указать имя пользователя и пароль для домена.

Ошибка при подключении ESET Endpoint Security к серверу зеркала: подключение к порту, указанному для доступа к HTTP-версии зеркала, блокируется.

3.9.5.2 Создание задач обновления

Обновление можно запустить вручную, нажав **Проверить наличие обновлений** в основном окне, которое появляется после выбора пункта **Обновление** в главном меню.

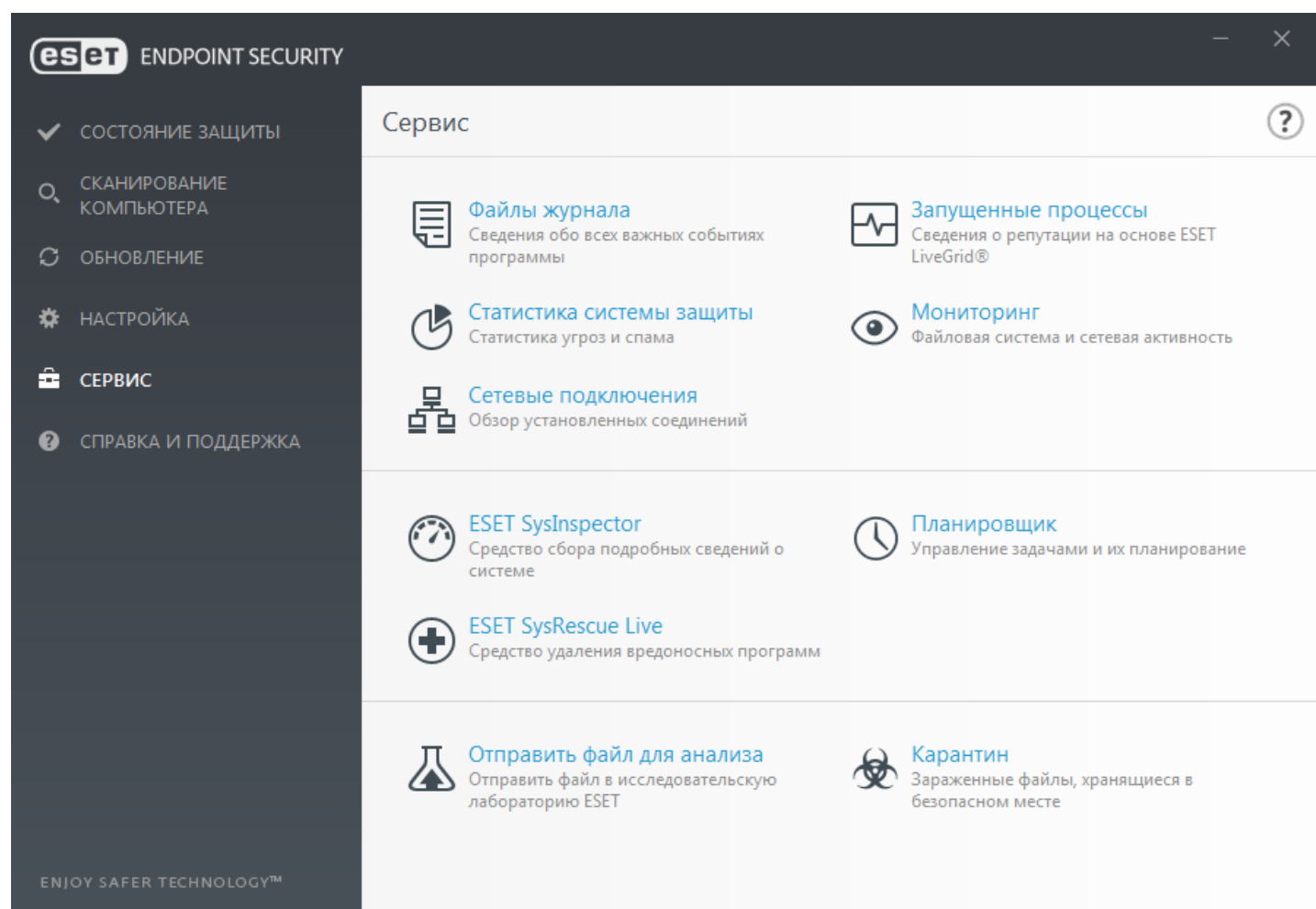
Обновления также можно выполнять как запланированную задачу. Для настройки запланированной задачи перейдите в раздел **Служебные программы > Планировщик**. По умолчанию в ESET Endpoint Security активированы указанные ниже задачи.

- **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](#).

3.9.6 Служебные программы

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



В этом меню представлены следующие служебные программы.

- [Файлы журнала](#)
- [Статистика защиты](#)
- [Наблюдение](#)
- [Запущенные процессы](#) (если использование системы ESET LiveGrid® включено в ESET Endpoint Security)
- [Планировщик](#)
- [Карантин](#)
- [Сетевые подключения](#) (если [файервол](#) включен в ESET Endpoint Security)
- [ESET SysInspector](#)

Отправка образца на анализ: возможность отправить подозрительный файл на анализ в вирусную лабораторию ESET. Диалоговое окно, открывающееся при использовании этой функции, описано в разделе [Отправка образцов на анализ](#).

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

3.9.6.1 Файлы журнала

Файлы журнала содержат информацию о важных программных событиях и предоставляют сводные сведения об обнаруженных угрозах. Журналы являются важнейшим элементом анализа, обнаружения угроз и устранения неполадок. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просматривать текстовые сообщения и журналы можно непосредственно в среде ESET Endpoint Security. Также предусмотрена возможность архивации файлов журнала.

Получить доступ к файлам журнала можно из главного окна программы с помощью команды **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 модулями ESET Endpoint Security. Регистрируется информация о времени обнаружения, название угрозы, место обнаружения, выполненные действия и имя 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 Endpoint Security. Он содержит информацию о событиях и ошибках, которые произошли во время работы программы. Он помогает системным администраторам и пользователям решать проблемы. Зачастую информация, которая содержится в этом журнале, оказывается весьма полезной при решении проблем, возникающих в работе программы.
- **Сканирование компьютера:** в этом окне отображаются результаты всех выполненных операций сканирования. Каждая строка соответствует одной проверке компьютера. Чтобы получить подробную информацию о той или иной операции сканирования, дважды щелкните соответствующую запись.
- **Заблокированные файлы:** сведения о файлах, которые были заблокированы и являются недоступными. В протоколе отображаются сведения о причине и исходном модуле, заблокировавшем файл, а также о приложении и пользователе, которые инициировали исполнение файла.
- **HIPS:** система содержит записи о правилах, помеченных для внесения в журнал. Протокол показывает приложение, которое вызвало операцию, результат (было правило разрешено или запрещено) и имя созданного правила.
- **Файервол:** в журнале файервола отображаются все попытки удаленных атак, которые обнаружил файервол. В нем находится информация обо всех атаках, которые были направлены на компьютер пользователя. В столбце *Событие* отображаются обнаруженные атаки. В столбце *Источник* указываются дополнительные сведения о злоумышленнике. В столбце *Протокол* перечисляются протоколы обмена данными, которые использовались для атаки. Анализ журнала файервола может помочь вовремя обнаружить попытки заражения компьютера, чтобы предотвратить несанкционированный доступ на компьютер. Дополнительные сведения о некоторых сетевых атаках см. в разделе IDS и расширенные функции.
- **Отфильтрованные веб-сайты:** Этот список используется для просмотра списка веб-сайтов, заблокированных при помощи функции [защиты доступа в Интернет](#) или [контроля доступа в Интернет](#). В этих журналах отображается время, URL-адрес, пользователь и приложение, с помощью которого установлено соединение с конкретным веб-сайтом.
- **Защита от спама:** содержит записи, связанные с сообщениями электронной почты, которые были помечены как спам.
- **Контроль доступа в Интернет:** отображение списка заблокированных или разрешенных URL-адресов и сведений об их группировке по категориям. В столбце *Предпринятое действие* указывается, как были применены правила фильтрации.
- **Контроль устройств:** содержит список подключенных к компьютеру съемных носителей и устройств. В файл журнала записываются только устройства с правилом контроля устройств. 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 (сочетание клавиш **CTRL+C**), выделите нужную запись и нажмите кнопку **Копировать**. 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 подробной информации о выбранном журнале.
- **Фильтрация одинаковых записей:** после активации этого фильтра будут показаны только записи одного типа (диагностические записи, 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 обо 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.

3.9.6.1.1 Поиск в журнале

В журналах хранится информация о важных системных событиях. Функция фильтрации журнала позволяет отображать записи о событиях определенного типа.

Введите ключевое слово для поиска в поле **Найти текст**. Если нужно искать это ключевое слово в конкретных столбцах, измените фильтр с помощью раскрывающегося меню **Искать в столбцах**.

Типы записей: выберите один или несколько типов записей журнала в раскрывающемся меню.

- **Диагностика:** в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информация:** в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения:** в журнал вносится информация обо всех критических ошибках и предупреждениях.
- **Ошибки:** в журнал вносится информация об ошибках загрузки файлов и критических ошибках.
- **Критическое:** регистрируются только критические ошибки (ошибки запуска защиты от вирусов, встроенного файрвола и т. п.).

Период времени: задайте период времени, результаты за который нужно вывести на экран.

Искать слова целиком: установите этот флажок, если для получения более точных результатов нужно искать определенные слова целиком.

С учетом регистра: установите этот флажок, если при фильтрации должен учитываться регистр букв.

Искать вверх: сначала отображаются результаты, которые находятся выше в документе.

3.9.6.2 Настройка прокси-сервера

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 ESET Endpoint Security 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 Endpoint Security в целом. Они используются всеми модулями программы, которым требуется подключение к Интернету.

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

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

i ПРИМЕЧАНИЕ.

В настройках **прокси-сервера** имя пользователя и пароль нужно вводить вручную.

Использовать прямое подключение, если прокси-сервер недоступен: если в программе настроено использование прокси-сервера HTTP, а он недоступен, программа будет обходить прокси-сервер и подключаться к серверам ESET напрямую.

Параметры прокси-сервера также можно настроить в области дополнительных настроек обновления (последовательно откройте **Дополнительные настройки > Обновление > Профили > Обновления > Параметры подключения** и в раскрывающемся списке **Режим прокси-сервера** выберите элемент **Подключение через прокси-сервер**). Этот параметр применяется к указанному профилю обновления и рекомендуются для ноутбуков, которые часто получают обновления модуля обнаружения из разных источников. Для получения дополнительных сведений об этих параметрах см. раздел [Дополнительные настройки обновления](#).

3.9.6.3 Планировщик

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

Перейти к планировщику можно из главного окна программы ESET Endpoint Security, 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 модуля обнаружения, сканирование, проверка файлов, исполняемых при запуске системы, и обслуживание журнала. Добавлять и удалять задачи можно непосредственно в главном окне планировщика (нажмите кнопку **Добавить задачу** или **Удалить** в нижней части окна). С помощью контекстного меню окна планировщика можно выполнить следующие действия: отображение подробной информации, 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**
- **Автоматическая проверка файлов при запуске системы** (после входа пользователя в систему)
- **Автоматическая проверка файлов при запуске системы** (после успешного обновления модуля)

Чтобы изменить параметры запланированных задач (как определенных по умолчанию, так и пользовательских), щелкните правой кнопкой мыши нужную задачу и выберите команду **Изменить...** или выберите 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 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 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 из них.
- **Сканирование компьютера по требованию:** сканирование файлов и папок на компьютере.
- **Обновление:** планирование задачи обновления, в рамках которой обновляется модуль обнаружения и программные модули.

4. Активируйте кнопку **Включено** при необходимости активировать задачу (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 указанные дату и время.
- **Многократно:** задача будет выполняться регулярно через указанный промежуток времени.
- **Ежедневно:** задача будет многократно выполняться каждые сутки в указанное время.
- **Еженедельно:** задача будет выполняться в выбранный день недели в указанное время.
- **При определенных условиях:** задача будет выполнена при возникновении указанного события.

5. 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**.

Имя задачи

Автоматическое обновление после входа пользователя в систему

Тип задачи

Обновление

Запуск задачи

После входа пользователя (один раз в час как максимум)

Действие, предпринимаемое в случае, если задача не запустилась в определенное время

В следующее запланированное время

OK

3.9.6.4 Статистика защиты

Для просмотра диаграммы статистических данных, связанных с модулями защиты ESET Endpoint Security, 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.

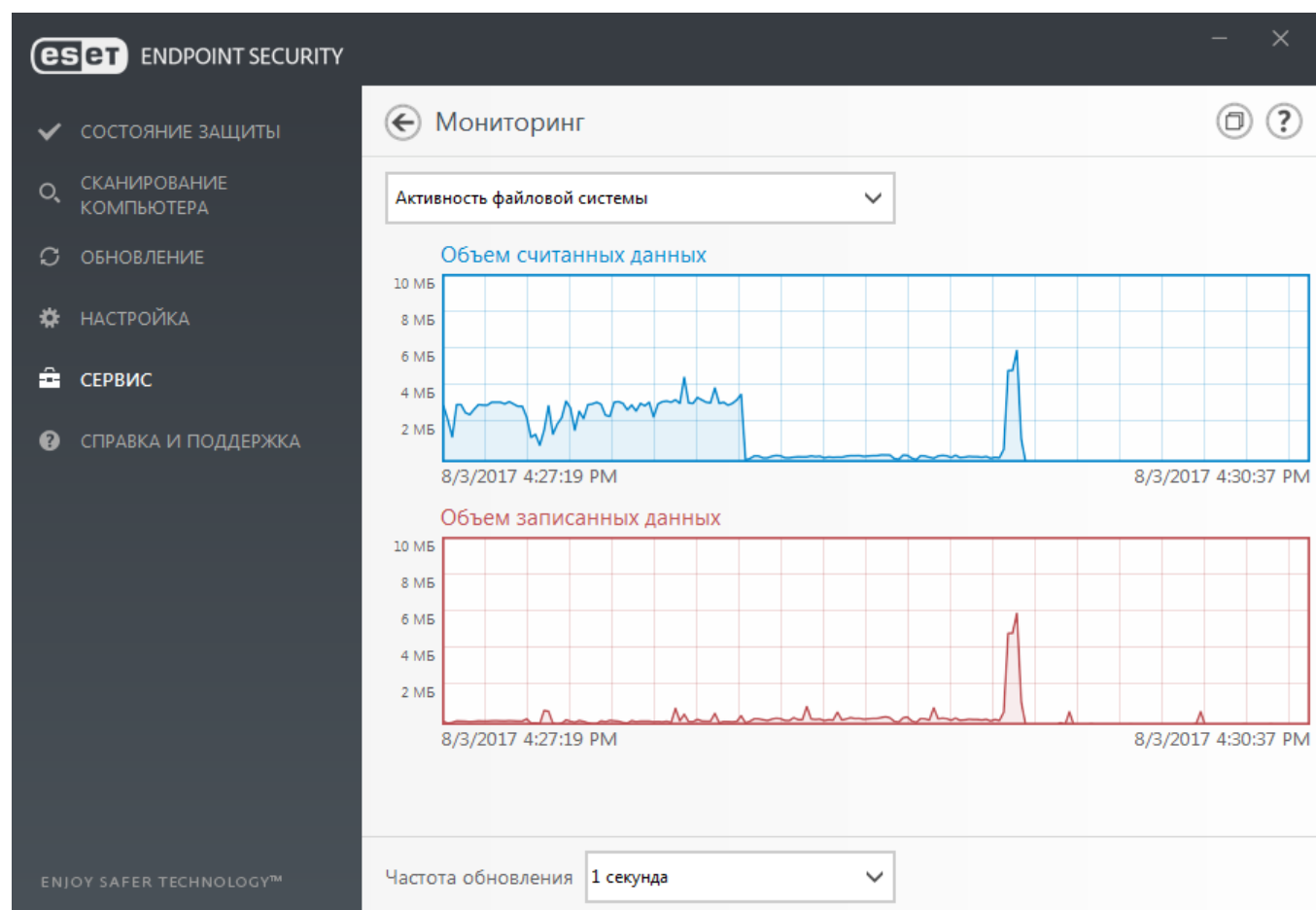
Доступны следующие статистические диаграммы.

- **Защита от вирусов и шпионских программ:** отображение числа 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.
- **Защита почтового клиента от спама:** отображение статистики защиты от спама с момента последнего запуска.

Возле графиков статистики отображается количество просканированных, зараженных, очищенных и чистых объектов. Нажмите кнопку **Сброс**, чтобы очистить данные статистики, или нажмите кнопку **Сбросить все**, чтобы очистить и удалить все существующие данные.

3.9.6.5 Наблюдение

Чтобы просмотреть текущую **активность файловой системы** в графическом виде, выберите **Службные 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:** диаграмма обновляется каждую секунду, временная шкала охватывает последние 10 минут.
- **Шаг: 1 минута (последние 24 часа):** диаграмма обновляется каждую минуту, временная шкала охватывает последние 24 часа.
- **Шаг: 1 час (последний месяц):** диаграмма обновляется каждый час, временная шкала охватывает последний месяц.
- **Шаг: 1 час (выбранный месяц):** диаграмма обновляется каждый час, временная шкала охватывает последние X выбранных месяцев.

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

В раскрывающемся меню можно также выбрать элемент **Сетевая активность**. Вид диаграмм и параметры для режимов **Активность файловой системы** и **Сетевая активность** одинаковы, за исключением того, что для последней отображается объем полученных (синий цвет) и отправленных (красный цвет) данных.

3.9.6.6 ESET SysInspector

[ESET SysInspector](#) — это приложение, которое тщательно проверяет компьютер и собирает подробные сведения о компонентах системы, таких 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 выбраны файлы журнала, в контекстном меню доступны следующие элементы:

- **Показать:** открытие выбранного 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.

3.9.6.7 ESET LiveGrid®

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

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

ESET LiveGrid® собирает о компьютерах пользователей информацию, которая связана с новыми обнаруженными угрозами. Это может быть образец 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 Endpoint Security 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.

Система репутации ESET LiveGrid® использует «белый» и «черный» списки, которые хранятся в облаке. Чтобы открыть настройки ESET LiveGrid®, нажмите клавишу **F5**. В окне дополнительных настроек последовательно щелкните **Службные 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: имя угрозы, дата и время обнаружения, способ обнаружения, связанные метаданные, версия и конфигурация продукта (включая информацию о системе).

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

Установите флажок **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.

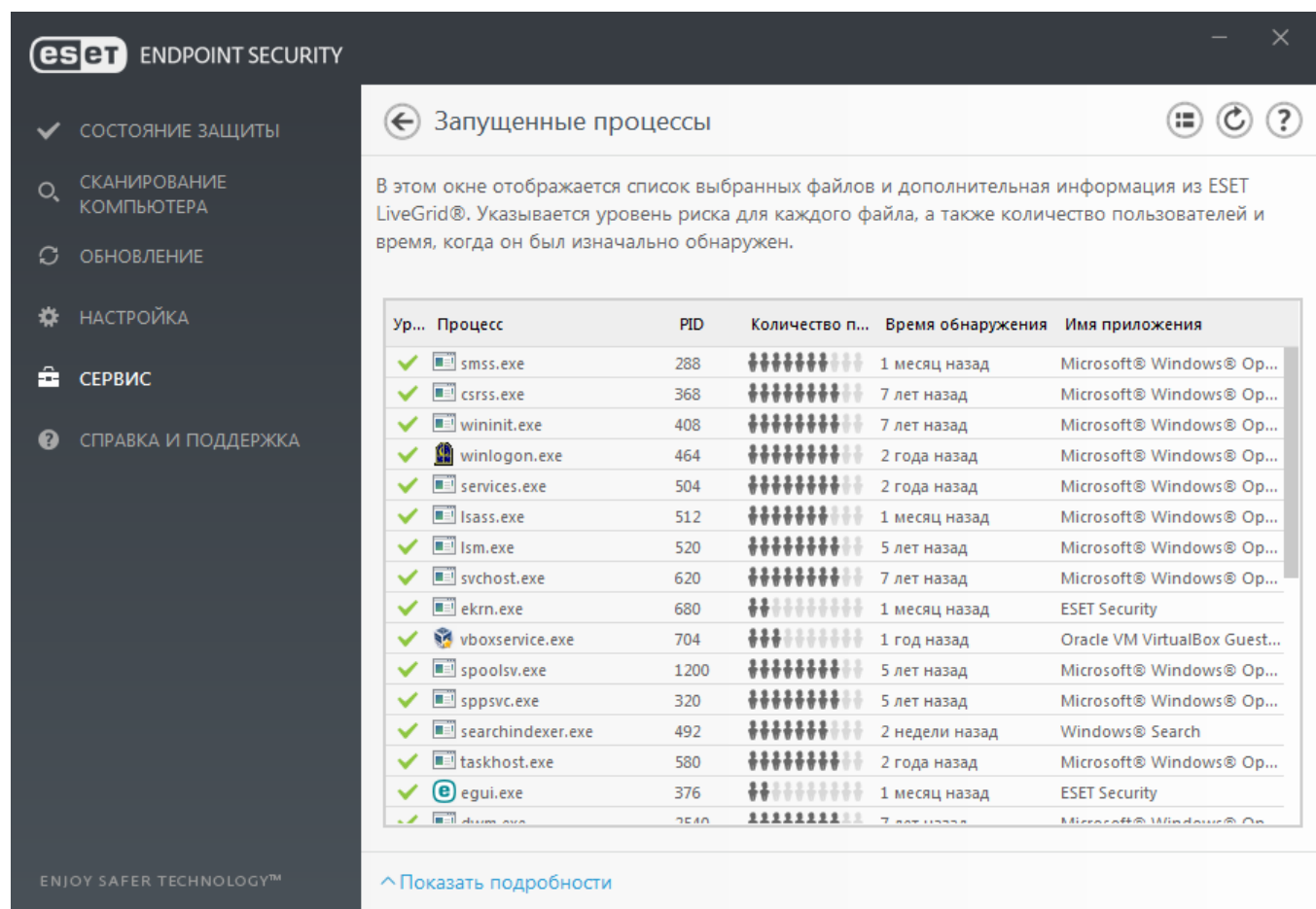
Контактный адрес электронной почты (необязательно) — вместе с подозрительными файлами можно отправить контактный адрес электронной почты, чтобы специалисты ESET могли обратиться к вам, если для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не отправляет ответы пользователям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

Исключение — фильтр исключений позволяет указывать 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.

3.9.6.8 Запущенные процессы

В разделе «Запущенные процессы» отображаются выполняемые на компьютере программы или процессы. Кроме того, эта функция позволяет оперативно и непрерывно уведомлять компанию ESET о новых заражениях. ESET Endpoint Security предоставляет подробные сведения о запущенных процессах для защиты пользователей с помощью технологии [ESET LiveGrid®](#).



Ур...	Процесс	PID	Количество п...	Время обнаружения	Имя приложения
✓	smss.exe	288	☆☆☆☆☆☆☆☆	1 месяц назад	Microsoft® Windows® Op...
✓	csrss.exe	368	☆☆☆☆☆☆☆☆	7 лет назад	Microsoft® Windows® Op...
✓	wininit.exe	408	☆☆☆☆☆☆☆☆	7 лет назад	Microsoft® Windows® Op...
✓	winlogon.exe	464	☆☆☆☆☆☆☆☆	2 года назад	Microsoft® Windows® Op...
✓	services.exe	504	☆☆☆☆☆☆☆☆	2 года назад	Microsoft® Windows® Op...
✓	lsass.exe	512	☆☆☆☆☆☆☆☆	1 месяц назад	Microsoft® Windows® Op...
✓	lsm.exe	520	☆☆☆☆☆☆☆☆	5 лет назад	Microsoft® Windows® Op...
✓	svchost.exe	620	☆☆☆☆☆☆☆☆	7 лет назад	Microsoft® Windows® Op...
✓	ekrn.exe	680	☆☆☆☆☆☆☆☆	1 месяц назад	ESET Security
✓	vboxservice.exe	704	☆☆☆☆☆☆☆☆	1 год назад	Oracle VM VirtualBox Guest...
✓	spoolsv.exe	1200	☆☆☆☆☆☆☆☆	5 лет назад	Microsoft® Windows® Op...
✓	sppsvc.exe	320	☆☆☆☆☆☆☆☆	5 лет назад	Microsoft® Windows® Op...
✓	searchindexer.exe	492	☆☆☆☆☆☆☆☆	2 недели назад	Windows® Search
✓	taskhost.exe	580	☆☆☆☆☆☆☆☆	2 года назад	Microsoft® Windows® Op...
✓	egui.exe	376	☆☆☆☆☆☆☆☆	1 месяц назад	ESET Security
✓

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

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

Идентификатор процесса: идентификатор процессов, запущенных в операционных системах Windows.

i ПРИМЕЧАНИЕ.

Известные приложения, помеченные как **Безопасно (зеленый)**, точно являются безопасными (внесены в «белый» список) и исключаются при сканировании, благодаря чему ускоряется сканирование компьютера по требованию или защита файловой системы в режиме реального времени.

Количество пользователей: количество пользователей данного приложения. Эта информация собирается технологией ESET LiveGrid®.

Время обнаружения: время, прошедшее с момента обнаружения приложения технологией ESET LiveGrid®.

i ПРИМЕЧАНИЕ.

Если для приложения выбран уровень безопасности **Неизвестно (оранжевый)**, оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в безопасности файла, воспользуйтесь функцией [отправки на анализ](#), чтобы отправить файл в вирусную лабораторию ESET. Если файл окажется вредоносным приложением, необходимая для его обнаружения информация будет включена в последующие обновления модуля обнаружения.

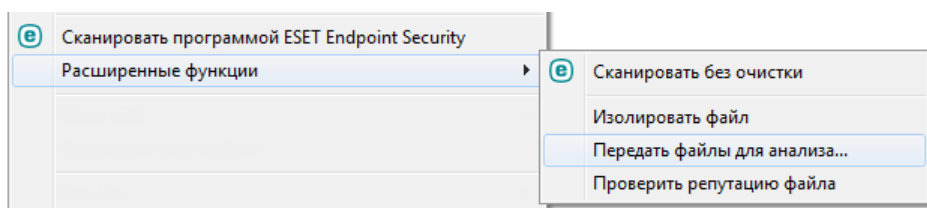
Имя приложения: конкретное имя программы или процесса.

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

- **Путь:** расположение приложения на компьютере.
- **Размер:** размер файла в КБ (килобайтах) или МБ (мегабайтах).
- **Описание:** характеристики файла на основе его описания в операционной системе.
- **Компания:** название поставщика или процесса приложения.
- **Версия:** информация от издателя приложения.
- **Продукт:** имя приложения и/или наименование компании.
- **Дата создания:** дата и время создания приложения.
- **Дата изменения:** дата и время последнего изменения приложения.

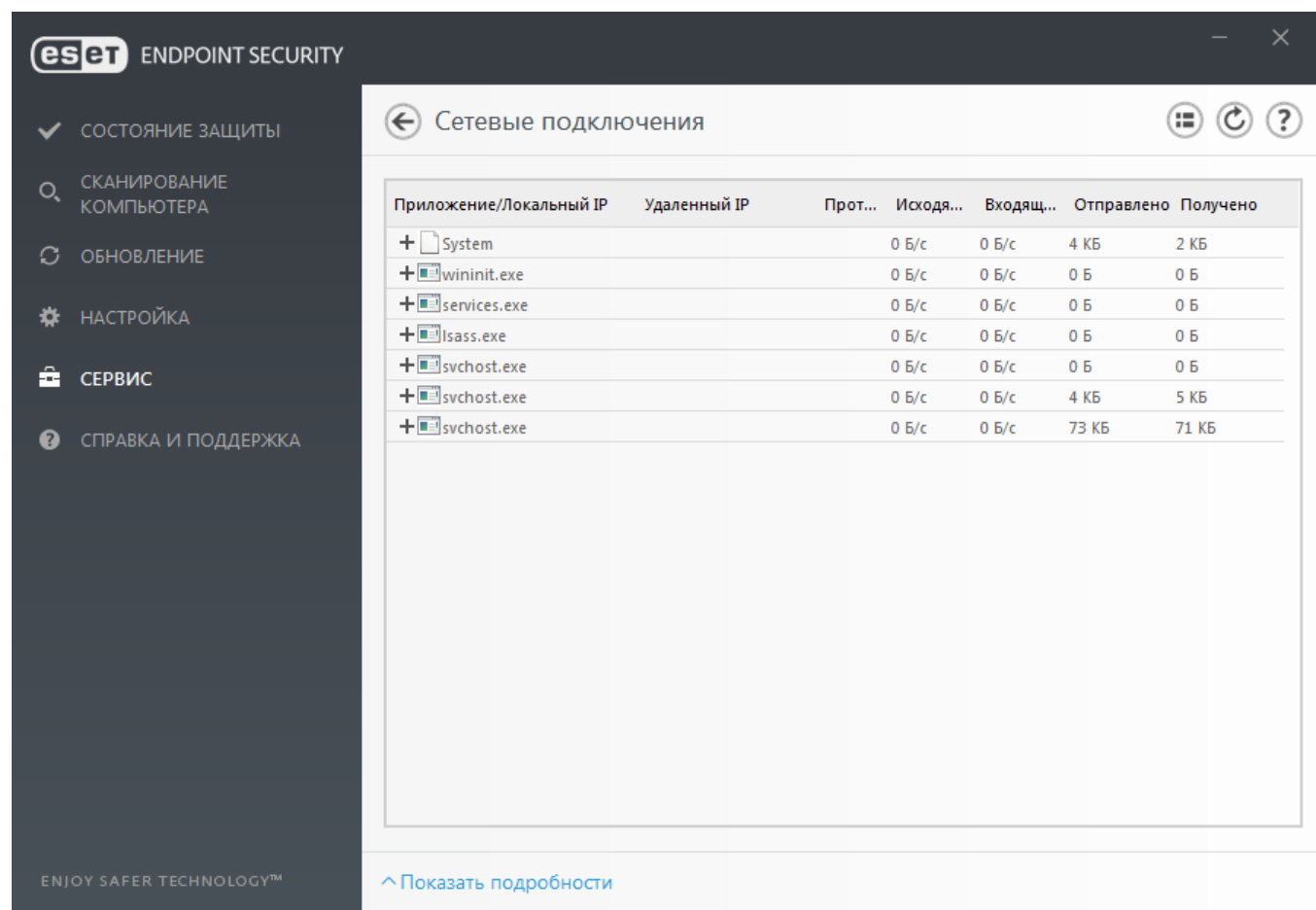
i ПРИМЕЧАНИЕ.

Также вы можете проверить репутацию файлов, которые не являются запущенными программами или процессами. Для этого пометьте нужные файлы, щелкните их правой кнопкой мыши и в [контекстном меню](#) выберите **Расширенные параметры > Проверить репутацию файла с помощью ESET LiveGrid®**.



3.9.6.9 Сетевые подключения

В разделе «Сетевые подключения» отображается список активных и отложенных соединений. Это позволяет управлять всеми приложениями, которые устанавливают исходящие соединения.



Приложение/Локальный IP	Удаленный IP	Прот...	Исходя...	Входящ...	Отправлено	Получено
+ System			0 Б/с	0 Б/с	4 КБ	2 КБ
+ wininit.exe			0 Б/с	0 Б/с	0 Б	0 Б
+ services.exe			0 Б/с	0 Б/с	0 Б	0 Б
+ lsass.exe			0 Б/с	0 Б/с	0 Б	0 Б
+ svchost.exe			0 Б/с	0 Б/с	0 Б	0 Б
+ svchost.exe			0 Б/с	0 Б/с	4 КБ	5 КБ
+ svchost.exe			0 Б/с	0 Б/с	73 КБ	71 КБ

Первая строка содержит имя приложения и его скорость передачи данных. Для просмотра всего списка соединений отдельного приложения, а также более подробной информации нажмите +.

Столбцы

Приложение/Локальный IP-адрес: имя приложения, локальные IP-адреса и порты обмена данными.

Удаленный IP-адрес: IP-адрес и номер порта соответствующего удаленного компьютера.

Протокол: используемый протокол передачи данных.

Исходящая скорость/Входящая скорость: текущая скорость обмена данными в соответствующих направлениях.

Отправлено/Получено: объем переданных данных с начала соединения.

Показать подробности: выберите эту функцию для отображения подробной информации о выбранном подключении.

Выберите приложение или IP-адрес на экране сетевых подключений и щелкните правой кнопкой мыши поле экрана, чтобы открыть контекстное меню со следующей структурой:

Определять имена хостов: все сетевые адреса, если это возможно, отображаются в формате DNS, а не в числовом формате IP-адресов.

Показывать только соединения по TCP: в списке отображаются только подключения по протоколу TCP.

Показывать ожидание соединения: установите этот флажок для отображения только тех подключений, по которым в настоящий момент не происходит обмена данными, но для которых система уже открыла порт и ожидает подключения.

Показывать внутренние соединения: установите этот флажок, чтобы отобразить только те соединения, в которых удаленной стороной является локальный компьютер (так называемые *локальные соединения*).

Щелкните подключение правой кнопкой мыши, чтобы просмотреть дополнительные параметры, среди которых есть следующие.

Запретить обмен данными для соединения: разрывает установленное соединение. Этот параметр доступен, только если щелкнуть активное подключение.

Обновить скорость: выберите периодичность обновления активных подключений.

Обновить сейчас: перезагрузка окна «Сетевые подключения».

Представленные ниже возможности доступны, только если щелкнуть приложение или процесс, а не активное подключение.

Временно запретить сетевое соединение для процесса: запретить текущие соединения для данного приложения. При создании нового соединения фаервол использует predefined правило. Описание параметров см. в разделе [Правила и зоны](#).

Временно разрешить сетевое соединение для процесса: разрешить текущие соединения для данного приложения. При создании нового соединения фаервол использует predefined правило. Описание параметров см. в разделе [Правила и зоны](#).

3.9.6.10 Отправка образцов на анализ

Диалоговое окно отправки образцов позволяет отправить файл или сайт на анализ в ESET. Чтобы открыть это окно, выберите **Служебные программы > Отправить образец на анализ**. При обнаружении на компьютере файла, проявляющего подозрительную активность, или подозрительного сайта в Интернете его можно отправить в вирусную 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).

i ПРИМЕЧАНИЕ.

Прежде чем отправлять образец в компанию ESET, убедитесь в том, что он соответствует одному или нескольким из следующих критериев:

- файл или веб-сайт совсем не обнаруживается;
- файл или веб-сайт ошибочно обнаруживается как угроза.

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

В раскрывающемся меню **Причина отправки образца** выберите наиболее подходящее описание своего сообщения.

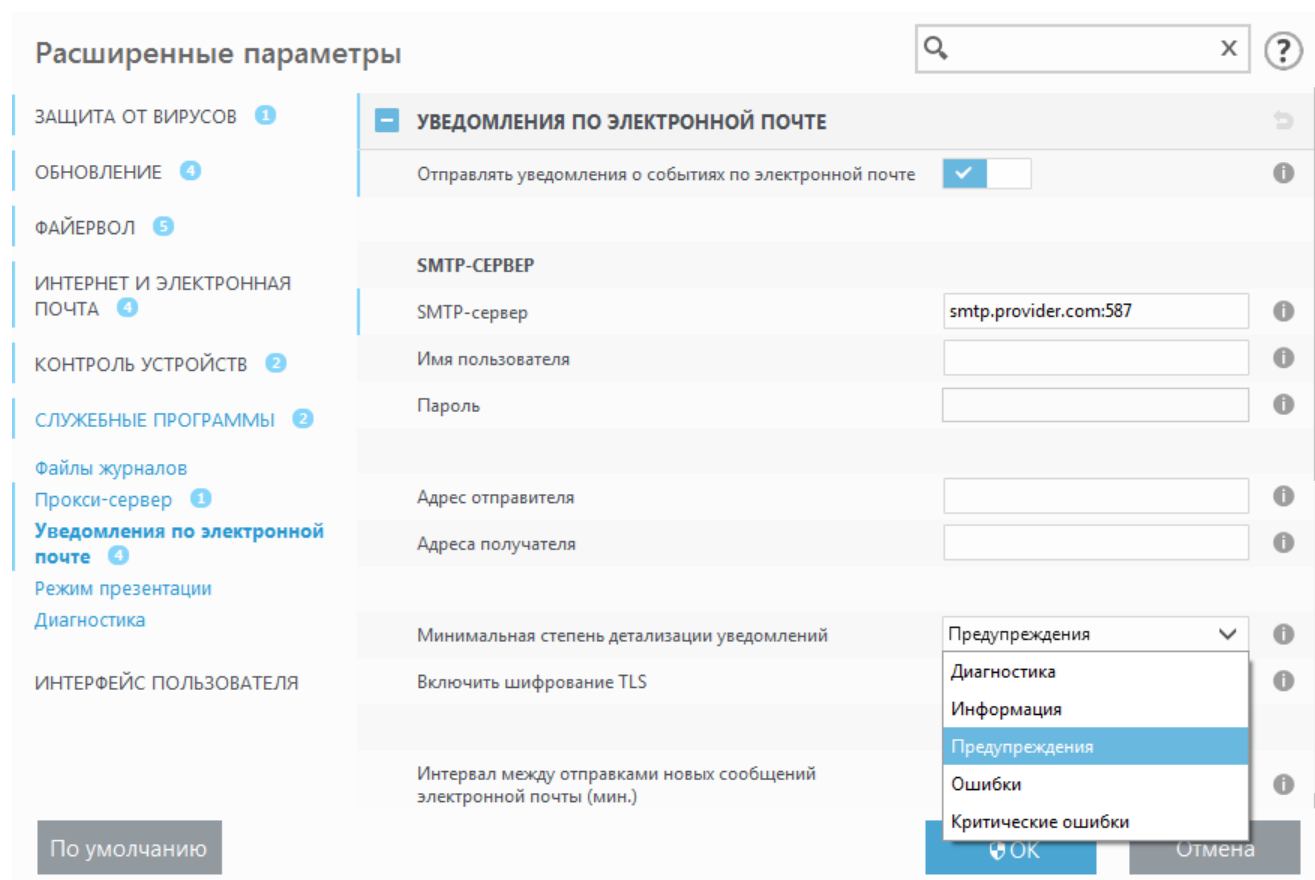
- **Подозрительный файл**
- **Подозрительный сайт** (веб-сайт, зараженный вредоносной программой)
- **Ложно обнаруженный файл** (файл обнаружен как зараженный, хотя не является таковым)
- **Ложно обнаруженный сайт**
- **Другое**

Файл/сайт: путь к отправляемому на анализ файлу или веб-сайту.

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.

3.9.6.11 Уведомления по электронной почте

ESET Endpoint Security 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).

И ПРИМЕЧАНИЕ.

ESET Endpoint Security поддерживает SMTP-серверы, использующие шифрование TLS.

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

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

Адреса получателей: в этом поле указываются адреса получателей, которые будут отображаться в заголовке писем с уведомлением. Для разделения адресов электронной почты используется точка с запятой (;).

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

- **Диагностика:** в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информационные:** записываются информационные сообщения, такие как нестандартные сетевые события, включая сообщения об успешной операции обновления, а также все перечисленные выше записи.
- **Предупреждения:** записываются критические ошибки и предупреждения (например, не удалось выполнить обновление или система Antistalth работает неправильно).
- **Ошибки:** записываются ошибки (не активирована защита документов) и критические ошибки.
- **Критические ошибки:** 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 отправками новых сообщений электронной почты (мин.): время в минутах, через которое по электронной почте будут отправлены 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

Обмен данными между программой и удаленным пользователем или системным администратором осуществляется посредством электронной почты или сообщений в локальной сети (используется служба обмена сообщениями Windows). Формат предупреждений и уведомлений, установленный по умолчанию, будет оптимален в большинстве случаев. В некоторых случаях может понадобиться изменить формат сообщений о событиях.

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

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

Кодировка: преобразовывает кодировку сообщения электронной почты в кодировку ANSI на основе региональных параметров Windows (например, windows-1250), кодировку Unicode (UTF-8), 7-битную кодировку ACSII (например, «á» будет преобразовано в «a», а неизвестные символы — в «?») или кодировку ISO-2022-JP (для японской версии).

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

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

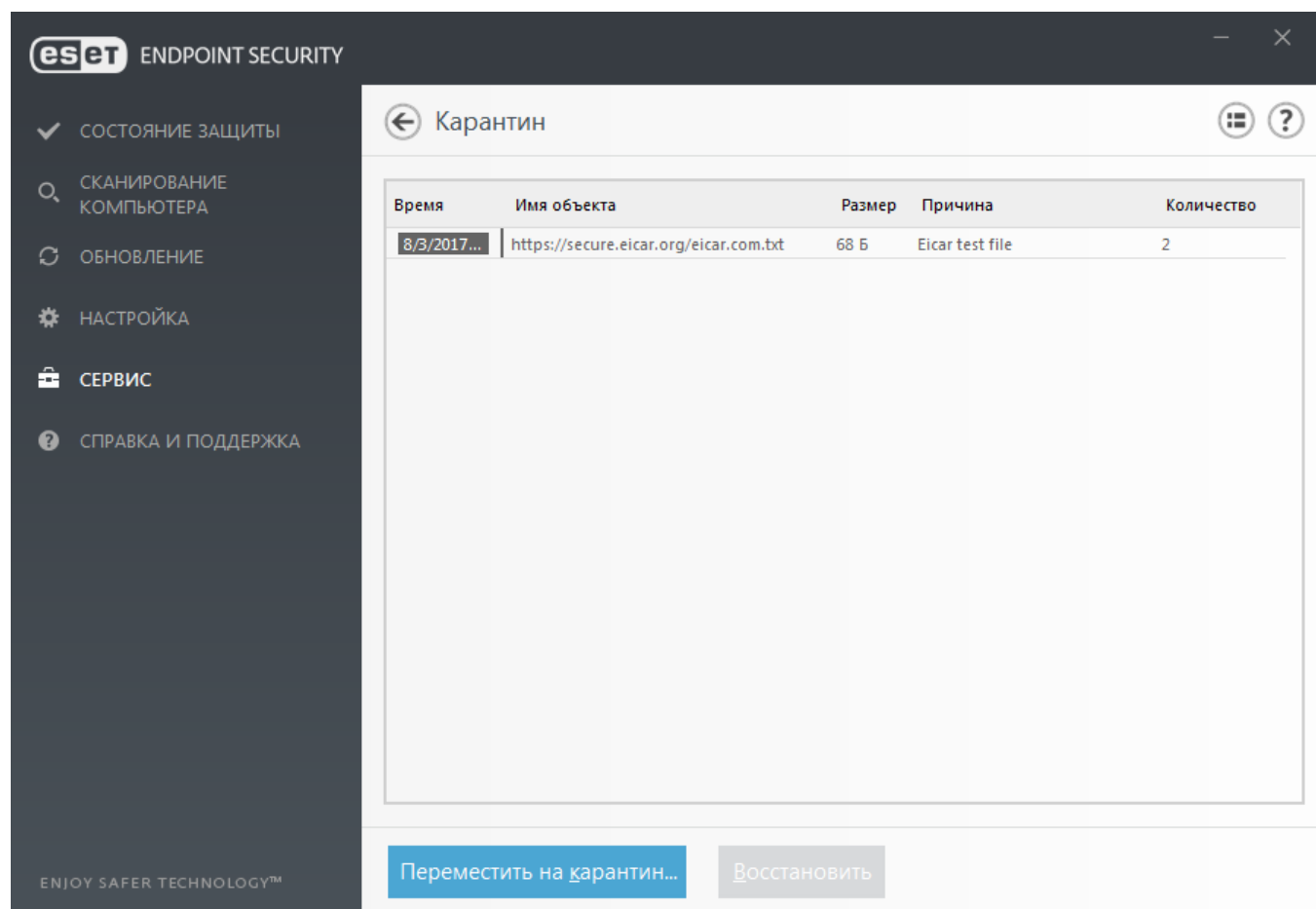
- **%ComputerName%:** имя компьютера, на котором произошло событие.
- **%ProgramName%:** программа, создавшая предупреждение.
- **%TimeStamp%:** дата и время события.
- **%UserName%:** имя пользователя, вошедшего в систему, в которой произошло событие.
- **%InfectedObject%:** имя зараженного файла, сообщения и т. п.
- **%VirusName%:** данные, идентифицирующие заражение.
- **%ErrorDescription%:** описание события, не имеющего отношения к вирусам.
- **%Scanner%:** задействованный модуль.
- **%Action%:** действие, предпринятое в случае заражения.

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

3.9.6.12 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 Endpoint Security к зараженным по ошибке.

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



Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, 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 Endpoint Security автоматически помещает удаленные файлы в карантин (если этот параметр не был отменен пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить в карантин вручную с помощью кнопки **Карантин**. В этом случае исходный файл будет удален из исходного расположения. Для этого также можно воспользоваться контекстным меню, нажав правой кнопкой мыши в окне **Карантин** и выбрав пункт **Карантин**.

Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Чтобы восстановить файл из карантина, щелкните его правой кнопкой мыши в окне карантина и в контекстном меню выберите пункт **Восстановить**. Если файл помечен как [потенциально нежелательное приложение](#), будет также доступен пункт **Восстановить и исключить из сканирования**. Контекстное меню содержит также пункт **Восстановить в**, с помощью которого можно восстановить файл в расположение, отличное от исходного.

Удаление из карантина: щелкните элемент правой кнопкой мыши и выберите команду **Удалить из карантина** или выберите элемент, который нужно удалить, и нажмите клавишу **DELETE** на клавиатуре. Вы также можете выделить и удалить несколько элементов одновременно.

i ПРИМЕЧАНИЕ.

Если программа поместила незараженный файл в карантин по ошибке, [исключите этот файл из процесса сканирования](#) после восстановления и отправьте его в службу поддержки клиентов ESET.

Отправка файла из карантина

Если вы поместили в карантин файл, который программа не смогла определить как опасный, или если файл был ошибочно определен как угроза и помещен в карантин, передайте этот файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **Передать на анализ**.

3.9.6.13 Microsoft Windows Update

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 Endpoint Security уведомляет пользователя об отсутствующих обновлениях в соответствии с выбранным уровнем. Доступны следующие уровни.

- **Без обновлений:** запросы на загрузку обновлений системы не отображаются.
- **Необязательные обновления:** отображаются запросы на загрузку обновлений с низким и более высоким уровнем приоритета.
- **Рекомендуемые обновления:** отображаются запросы на загрузку обновлений с обычным и более высоким уровнем приоритета.
- **Важные обновления:** отображаются запросы на загрузку обновлений, помеченных как важные и с более высоким уровнем приоритета.
- **Критические обновления:** пользователю предлагается загрузить только критические обновления.

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

3.9.6.14 ESET CMD

Эта функция включает расширенные команды escmd. Она дает возможность экспортировать и импортировать параметры с помощью командной строки (escmd.exe). До этого экспорт и импорт параметров был возможен только с использованием [графического интерфейса](#). Конфигурацию ESET Endpoint Security можно экспортировать в файл в формате *XML*.

При включенной функции ESET CMD доступны два метода авторизации:

- **Нет** — без авторизации. Этот метод не рекомендуется, так как он разрешает импорт любой неподписанной конфигурации, что представляет собой потенциальный риск.
- **Пароль для расширенной настройки** — использование защиты паролем. Файл в формате *XML*, из которого импортируется конфигурация, должен быть подписан (см. информацию о подписании файла конфигурации в формате *XML* ниже). При этом методе авторизации в ходе импорта конфигурации пароль проверяется на соответствие паролю, указанному в разделе [Параметры доступа](#). Если настройка доступа не включена, пароль не совпадает или файл конфигурации в формате *XML* не подписан, конфигурация не будет импортирована.

После включения функции ESET CMD можно начать использовать командную строку для экспорта и импорта конфигурации ESET Endpoint Security. Это можно сделать вручную или создать сценарий с целью автоматизации.

! ВАЖНО!

Для использования расширенных команд `ecmd` необходимо выполнять их с правами администратора или же открыть командную строку Windows (`cmd`) в режиме **Запуск от имени администратора**. В противном случае появится сообщение **Error executing command..** Кроме того, во время экспорта конфигурации должна существовать папка назначения.

i ПРИМЕЧАНИЕ.

Расширенные команды `ecmd` можно выполнить только локально. Выполнение клиентской задачи **Выполнение команды** с использованием ERA не работает.

✓ ПРИМЕР

Команда экспорта параметров:

```
ecmd /getcfg c:\config\settings.xml
```

Команда импорта параметров:

```
ecmd /setcfg c:\config\settings.xml
```

Подписание файла конфигурации в формате *XML*:

1. Загрузите средство **XmlSignTool** со [страницы загрузки средств и утилит ESET](#) и извлеките его. Это средство было разработано специально для подписания файлов конфигурации ESET в формате *XML*.
2. Откройте командную строку Windows (`cmd`) в режиме **Запуск от имени администратора**.
3. Перейдите в папку с файлом `XmlSignTool.exe`.
4. Выполните команду для подписания файла конфигурации в формате *XML*. Использование: `XmlSignTool <путь_к_файлу_xml>`
5. Введите пароль [для расширенной настройки](#), а затем введите его еще раз по запросу средства `XmlSignTool`. Теперь файл конфигурации в формате *XML* подписан и его можно импортировать на другом экземпляре ESET Endpoint Security с функцией ESET CMD с помощью метода авторизации «Пароль для расширенной настройки».

⚠ ВНИМАНИЕ!

Включать ESET CMD без авторизации не рекомендуется, поскольку это даст возможность импортировать любую неподписанную конфигурацию. Установите пароль в разделе **Дополнительные настройки > Интерфейс пользователя > Настройка доступа**, чтобы пользователи не вносили неавторизованные изменения.

3.9.7 Интерфейс

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

С помощью служебной программы [Элементы интерфейса](#) можно изменить внешний вид программы и используемые эффекты.

Для обеспечения максимального уровня безопасности программного обеспечения можно предотвратить несанкционированное изменение с помощью инструмента [Настройка доступа](#).

Путем настройки параметров в разделе [Предупреждения и уведомления](#) можно изменить поведение предупреждений об обнаруженных угрозах и системных уведомлениях. Их можно настроить в соответствии со своими потребностями.

Если запретить отображение каких-то уведомлений, они будут отображаться в разделе **Элементы интерфейса > Состояния приложения**. Здесь можно проверить состояние этих уведомлений и настроить запрет на их отображение.

Щелчок по выделенному объекту правой кнопкой мыши открывает [контекстное меню](#). Эта возможность позволяет интегрировать элементы управления ESET Endpoint Security в контекстное меню.

[Режим презентации](#) предназначен для пользователей, которые хотят работать с приложениями, не отвлекаясь на всплывающие окна, запланированные задачи и любые компоненты, которые могут загружать процессор и оперативную память.

3.9.7.1 Элементы интерфейса

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

В разделе **Элементы интерфейса** можно настроить рабочую среду. Щелкните раскрывающееся меню **Режим запуска** и выберите один из следующих режимов запуска графического интерфейса пользователя.

Полный: будет отображаться полный графический интерфейс пользователя.

Минимальный: графический интерфейс не запущен, отображаются только уведомления.

Ручной: уведомления и предупреждения не отображаются.

Скрытый: ни пользовательский интерфейс, ни уведомления и предупреждения не отображаются. Этот режим может пригодиться в ситуациях, в которых нужно экономить ресурсы системы. Он может быть запущен только администратором.

i ПРИМЕЧАНИЕ.

После выбора минимального графического интерфейса и перезагрузки компьютера уведомления будут отображаться, а графический интерфейс — нет. Чтобы из этого режима перейти в режим полного графического интерфейса, запустите интерфейс из меню «Пуск». Для этого последовательно щелкните элементы **Все программы > ESET** и войдите в ESET Endpoint Security от имени администратора. Это также можно сделать в ESET Remote Administrator, применив соответствующую политику.

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

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

Интегрировать с контекстным меню: можно интегрировать элементы управления ESET Endpoint Security в контекстное меню.

Состояния

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

Информация о лицензии

Показать сведения о лицензии: если этот параметр отключен, сведения о лицензии не будут отображаться в окнах **Состояние защиты** и **Справка и поддержка**.

Показывать сообщения и оповещения о лицензии: если этот параметр отключен, уведомления и сообщения будут отображаться только по истечении срока действия лицензии.

i ПРИМЕЧАНИЕ.

Настройки сведений о лицензии применяются, но являются недоступными, если продукт ESET Endpoint Security активирован с помощью лицензии MSP.

Расширенные параметры

 × ?

ЗАЩИТА ОТ ВИРУСОВ 1

ОБНОВЛЕНИЕ 4

ФАЙЕРВОЛ 5

ИНТЕРНЕТ И ЭЛЕКТРОННАЯ
ПОЧТА 4

КОНТРОЛЬ УСТРОЙСТВ 2

СЛУЖЕБНЫЕ ПРОГРАММЫ 2

ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

Настройка

ЭЛЕМЕНТЫ ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ

Режим запуска

Полный ▾

Будет отображаться полный графический интерфейс пользова

Полный

Минимальный

Ручной

Скрытый

Показывать заставку при запуске

Использовать звуки

Интеграция в контекстное меню

СОСТОЯНИЯ

Состояния приложения

[Изменить](#)

СВЕДЕНИЯ О ЛИЦЕНЗИИ

Показать сведения о лицензии

Показывать сообщения и оповещения о лицензии

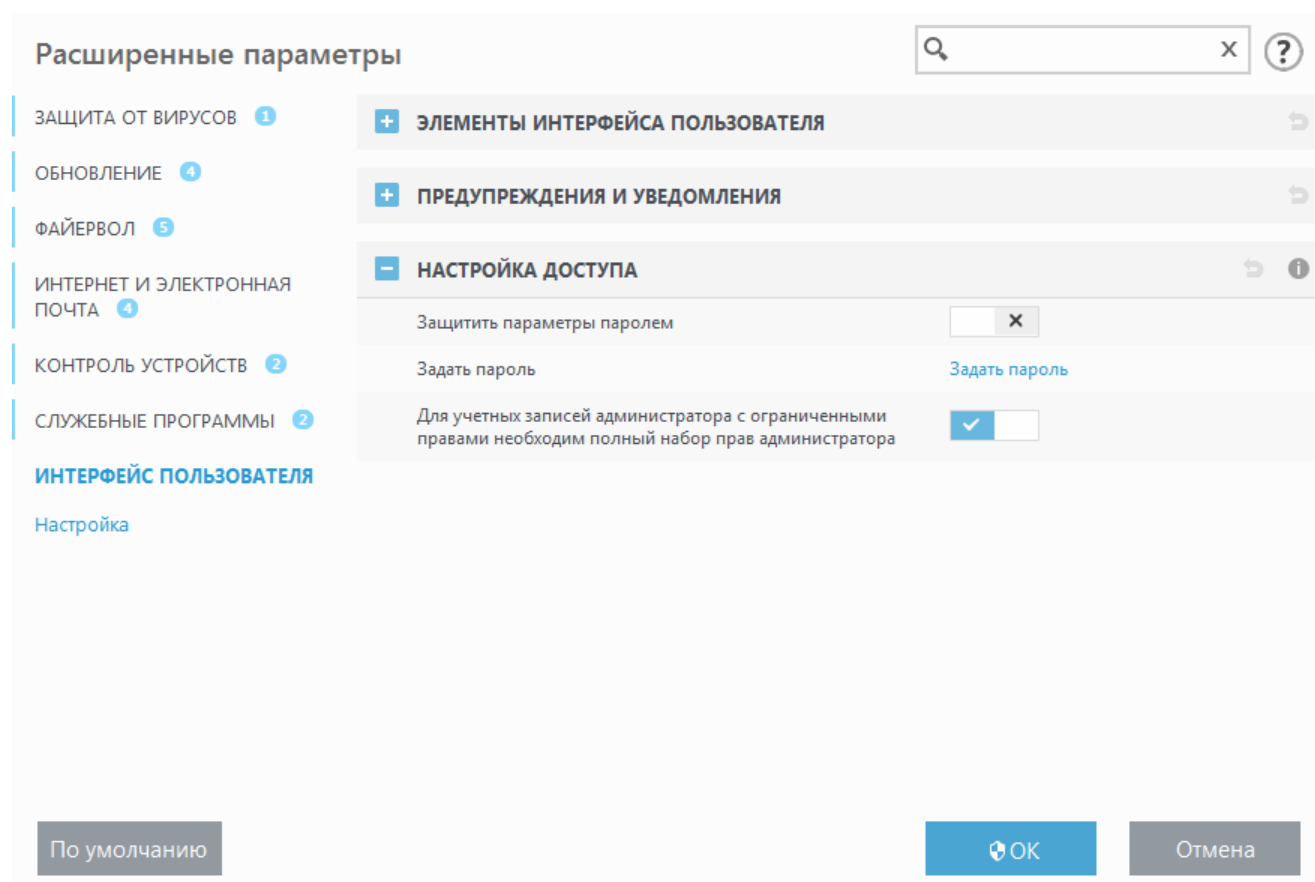
По умолчанию

OK

Отмена

3.9.7.2 Настройка доступа

Для обеспечения максимальной безопасности системы важно правильно настроить ESET Endpoint Security. Неквалифицированное изменение параметров может привести к потере важных данных. Во избежание несанкционированного изменения параметры ESET Endpoint Security можно защитить паролем. Чтобы открыть настройки защиты паролем, последовательно выберите **Интерфейс пользователя > Настройка доступа > Дополнительные настройки (F5)**.



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

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

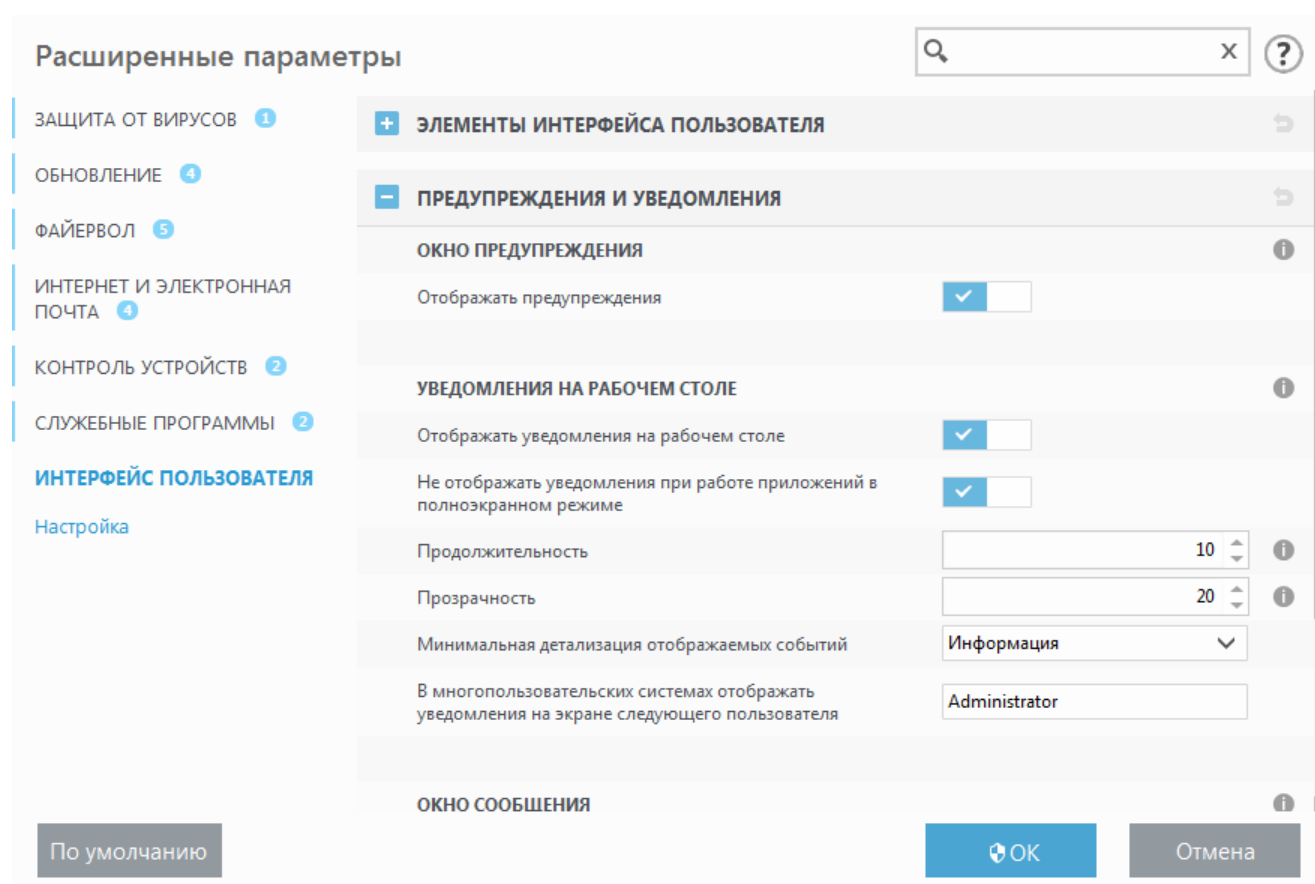
Для учетных записей администратора с ограниченными правами необходим полный набор прав администратора: установите этот флажок, чтобы при изменении определенных параметров системы текущему пользователю (если у него нет прав администратора) предлагалось ввести имя и пароль администратора (как и при контроле учетных записей в Windows Vista). К изменениям относится отключение модулей защиты или файрвола.

Только для Windows XP:

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

3.9.7.3 Предупреждения и уведомления

В разделе **Предупреждения и уведомления** окна **Интерфейс** можно настроить способ обработки предупреждений об угрозах и системных уведомлениях (например, сообщений об успешном выполнении обновлений) для программы ESET Endpoint Security. 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. Такой подход следует использовать только в небольшом количестве особых ситуаций. В большинстве случаев рекомендуется оставить для этого параметра значение по умолчанию (включен).

Уведомления на рабочем столе

Уведомления на рабочем столе и всплывающие подсказки предназначены только для информирования и не требуют действий 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 переключатель **Не отображать уведомления при работе приложений в полноэкранном режиме** в положение «Вкл.», чтобы запретить все неинтерактивные уведомления. Более подробные параметры, такие как время отображения и прозрачность окна уведомлений, можно изменить, выполнив инструкции ниже.

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

- **Диагностика** — в журнал вносится информация, необходимая для тщательной настройки программы, и все перечисленные выше записи.
- **Информация:** в журнал вносятся информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.
- **Предупреждения:** в журнал вносится информация обо всех критических ошибках и предупреждениях.
- **Ошибки:** в журнал вносится информация об ошибках загрузки файлов и критических ошибках.
- **Критические:** регистрируются только критические ошибки (ошибки запуска защиты от вирусов, встроенного файрвола 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, если одновременно может быть подключено несколько пользователей. Обычно это системный или сетевой администратор. Это особенно полезно для серверов терминалов (если все системные уведомления отправляются администратору).

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.


3.9.7.3.1 Ошибка «Конфликт дополнительных настроек»

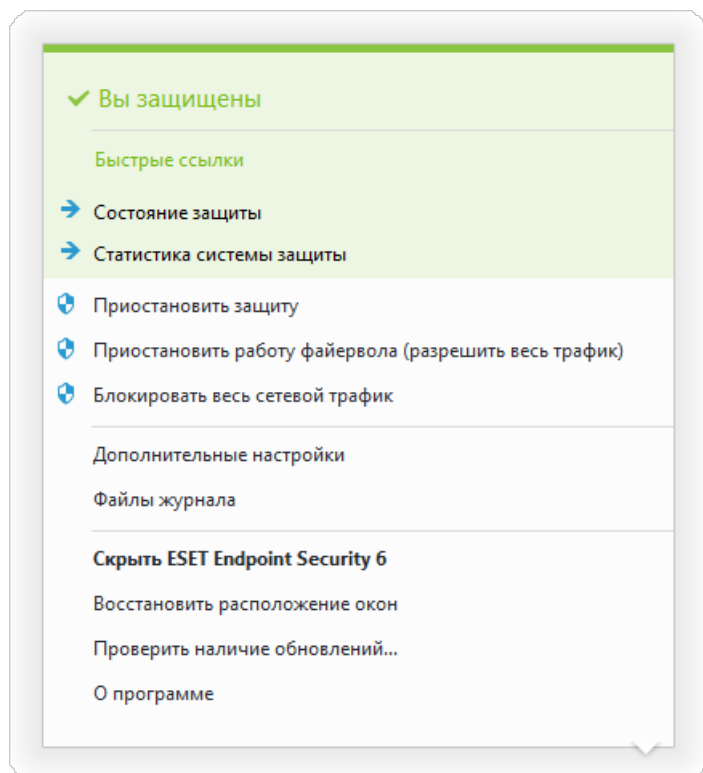
Эта ошибка может возникнуть, если один из компонентов (например, система предотвращения вторжений на узел или файрвол) и пользователь создали правила в интерактивном режиме или режиме обучения одновременно.

ВАЖНО!

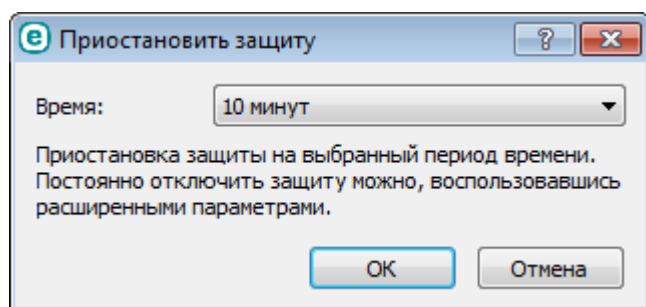
Рекомендуется изменить режим фильтрации на **Автоматический режим** по умолчанию, если вы хотите создавать собственные правила. См. дополнительные сведения о [режиме обучения](#).

3.9.7.4 Значок на панели задач

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



Приостановить защиту: на экран выводится диалоговое окно для подтверждения. В нем можно отключить [защиту от вирусов и шпионских программ](#), которая контролирует обмен файлами и данными через Интернет и электронную почту, предотвращая тем самым атаки на компьютер.



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

Приостановить работу файрвола (разрешить весь трафик): файрвол переводится в неактивное состояние. Для получения дополнительных сведений см. раздел [Сеть](#).

Блокировать весь сетевой трафик: файрвол будет блокировать весь исходящий и входящий обмен данными по сети и через Интернет. Чтобы разблокировать трафик, щелкните **Остановить блокировку всего сетевого трафика**.

Дополнительные настройки: выберите этот параметр, чтобы перейти к дереву **Дополнительные настройки**. Чтобы перейти к дополнительным настройкам, можно также нажать клавишу F5 или использовать меню **Настройка > Дополнительным настройками**.

Файлы журналов: [файлы журналов](#) содержат информацию обо всех важных событиях программы и предоставляют общие сведения об обнаруженных угрозах.

Скрыть ESET Endpoint Security: позволяет скрыть окно ESET Endpoint Security.

Восстановить расположение окон: восстановление размеров окна ESET Endpoint Security и его положения на экране по умолчанию.

Проверить наличие обновлений...: запуск обновления модулей программы для поддержания необходимого уровня защиты от вредоносного кода.

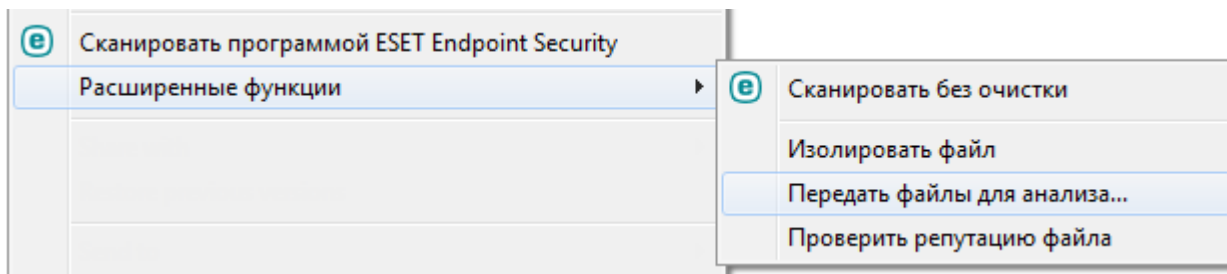
О программе: отображение системной информации, сведений об установленной версии ESET Endpoint Security и модулях программы, а также срока действия лицензии. В нижней части окна представлена информация об операционной системе и системных ресурсах.

3.9.7.5 Контекстное меню

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

Элементы управления ESET Endpoint Security можно интегрировать в контекстное меню. Настройка этих функций выполняется в дереве расширенных параметров, в разделе **Интерфейс > Элементы интерфейса**.

Интегрировать с контекстным меню: возможность интеграции элементов управления ESET Endpoint Security в контекстное меню.



3.10 Для опытных пользователей

3.10.1 Диспетчер профилей

Диспетчер профилей используется в двух разделах ESET Endpoint Security: в разделе **Сканирование компьютера по требованию** и в разделе **Обновление**.

Сканирование компьютера по требованию

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

Для создания профиля откройте окно «Дополнительные настройки» (F5) и щелкните **Защита от вирусов > Сканирование компьютера по требованию**, а затем нажмите кнопку **Изменить** рядом с элементом **Список профилей**. В раскрывающемся меню **Профиль обновления** отображаются существующие профили сканирования. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел [Настройка параметров модуля ThreatSense](#), где описывается каждый параметр, используемый для настройки сканирования.

Пример. Предположим, пользователю требуется создать собственный профиль сканирования. Хотя конфигурация сканирования Smart частично устраивает его, сканировать упаковщики или потенциально опасные приложения не требуется, и нужно применить **тщательную очистку**. Введите имя нового профиля в окне **Диспетчер профилей** и нажмите кнопку **Добавить**. Выберите новый профиль в раскрывающемся меню **Профиль обновления** 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.

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

Список профилей: создание или редактирование профилей обновления.

3.10.2 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 Endpoint Security. Откройте раскрывающееся меню рядом с элементами **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 определить 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 защиты сети: запись всех сетевых данных, проходящих через файервол в формате PCAP. Это помогает разработчикам выявлять и устранять проблемы, связанные с файерволом.

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

Включить расширенное ведение журнала для модуля обновления: запись всех событий, которые происходят во время обновления. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем обновления.

Включить расширенное ведение журнала для контроля доступа в Интернет: запись всех событий, которые происходят в модуле родительского контроля. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем родительского контроля.

Включить расширенное ведение журнала для лицензирования: запись всего обмена данными между программой и сервером лицензий.

Включить расширенное ведение журнала для модуля защиты от спама: запись всех событий, которые происходят в процессе сканирования на наличие спама. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем защиты от спама ESET.

Включить расширенное ведение журнала операционной системы: будут собираться дополнительные сведения об операционной системе, например о запущенных процессах, активности ЦП и работе дисков. Это помогает разработчикам выявлять и исправлять проблемы, связанные с программами ESET в вашей операционной системе.

Файлы журналов хранятся в расположении:

C:\ProgramData\ESET\ESET Security\Diagnostics\ в Windows Vista и более поздних версиях либо по адресу C:\Documents and Settings\All Users\... в более ранних версиях Windows.

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

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

Создать дамп диагностики: нажмите кнопку **Создать**, чтобы создать в **целевом каталоге** файлы дампа диагностики.

3.10.3 Импорт и экспорт параметров

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

Импорт и экспорт файлов конфигурации удобны, если нужно создать резервную копию текущей конфигурации программы ESET Endpoint Security 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 окне программы выберите **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.

i ПРИМЕЧАНИЕ.

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

Импорт и экспорт параметров

Текущая конфигурация может быть сохранена в XML-файле и при необходимости восстановлена позже.

Импортировать параметры

Экспортировать параметры

Полный путь к файлу с именем:

...

Импорт Заккрыть

3.10.4 Командная строка

Модуль защиты от вирусов ESET Endpoint Security может быть запущен из командной строки вручную (с помощью команды `ecls`) или в пакетном режиме (с помощью 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

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

Параметры модуля сканирования

<code>/files</code>	сканировать файлы (по умолчанию)
<code>/no-files</code>	не сканировать файлы
<code>/memory</code>	сканировать память
<code>/boots</code>	сканировать загрузочные секторы
<code>/no-boots</code>	не сканировать загрузочные секторы (по умолчанию)
<code>/arch</code>	сканировать архивы (по умолчанию)
<code>/no-arch</code>	не сканировать архивы
<code>/max-obj-size=РАЗМЕР</code>	сканировать файлы, только если их размер не превышает РАЗМЕР в мегабайтах (по умолчанию 0 = без ограничений)
<code>/max-arch-level=УРОВЕНЬ</code>	максимальная степень вложенности архивов для сканирования
<code>/scan-timeout=ОГРАНИЧЕНИЕ</code>	сканировать архивы не более указанного в ОГРАНИЧЕНИИ количества секунд
<code>/max-arch-size=РАЗМЕР</code>	сканировать файлы в архивах, только если их размер не превышает РАЗМЕР (по умолчанию 0 = без ограничений)
<code>/max-sfx-size=РАЗМЕР</code>	сканировать файлы в самораспаковывающихся архивах, только если их размер не превышает РАЗМЕР в мегабайтах (по умолчанию 0 = без ограничений)
<code>/mail</code>	сканировать файлы электронной почты (по умолчанию)
<code>/no-mail</code>	не сканировать файлы электронной почты
<code>/mailbox</code>	сканировать почтовые ящики (по умолчанию)
<code>/no-mailbox</code>	не сканировать почтовые ящики
<code>/sfx</code>	сканировать самораспаковывающиеся архивы (по умолчанию)
<code>/no-sfx</code>	не сканировать самораспаковывающиеся архивы
<code>/rtp</code>	сканировать упаковщики (по умолчанию)
<code>/no-rtp</code>	не сканировать упаковщики
<code>/unsafe</code>	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)». Приложение ecls.exe попытается автоматически очистить или удалить зараженные файлы.
- «Тщательная». Приложение ecls.exe попытается автоматически очистить или удалить зараженные файлы без вмешательства пользователя (вам не будет предложено подтвердить удаление файлов).
- «Наиболее тщательная». Приложение ecls.exe удалит все файлы независимо от их типа без очистки.
- «Удаление». Приложение ecls.exe удалит все файлы без очистки, но не затронет важные файлы (например, 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

i ПРИМЕЧАНИЕ.

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

3.10.5 Сканирование в состоянии простоя

Настройки сканирования в состоянии простоя можно изменить в меню **Дополнительные настройки > Защита от вирусов > Сканирование в состоянии простоя > Сканирование 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.

3.10.6 ESET SysInspector

3.10.6.1 Знакомство с ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и отображает собранные данные в обобщенном виде. Такая информация, как данные об установленных драйверах и приложениях, сетевых соединениях и важных записях в реестре, позволяет определить причину подозрительного поведения системы, которое могло иметь место, например, вследствие несовместимости программного или аппаратного обеспечения или заражения вредоносными программами.

Доступ к программе ESET SysInspector можно получить двумя способами: воспользовавшись ее интегрированной версией в решениях ESET Security или бесплатно загрузив автономную версию (SysInspector.exe) с веб-сайта ESET. Обе версии работают одинаково и имеют одинаковое управление. Единственная разница состоит в способе управления полученными данными. И автономная, и интегрированная версии дают возможность экспортировать снимки системы в XML-файлы и сохранять их на диске. Однако интегрированная версия позволяет также сохранять снимки системы непосредственно в меню **Служебные программы > ESET SysInspector** (за исключением программы ESET Remote Administrator). Дополнительные сведения см. в разделе [ESET SysInspector как часть приложения ESET Endpoint Security](#).

Подождите некоторое время, пока программа ESET SysInspector сканирует компьютер. Это может занять от 10 секунд до нескольких минут в зависимости от конфигурации оборудования, операционной системы и количества установленных на компьютере приложений.

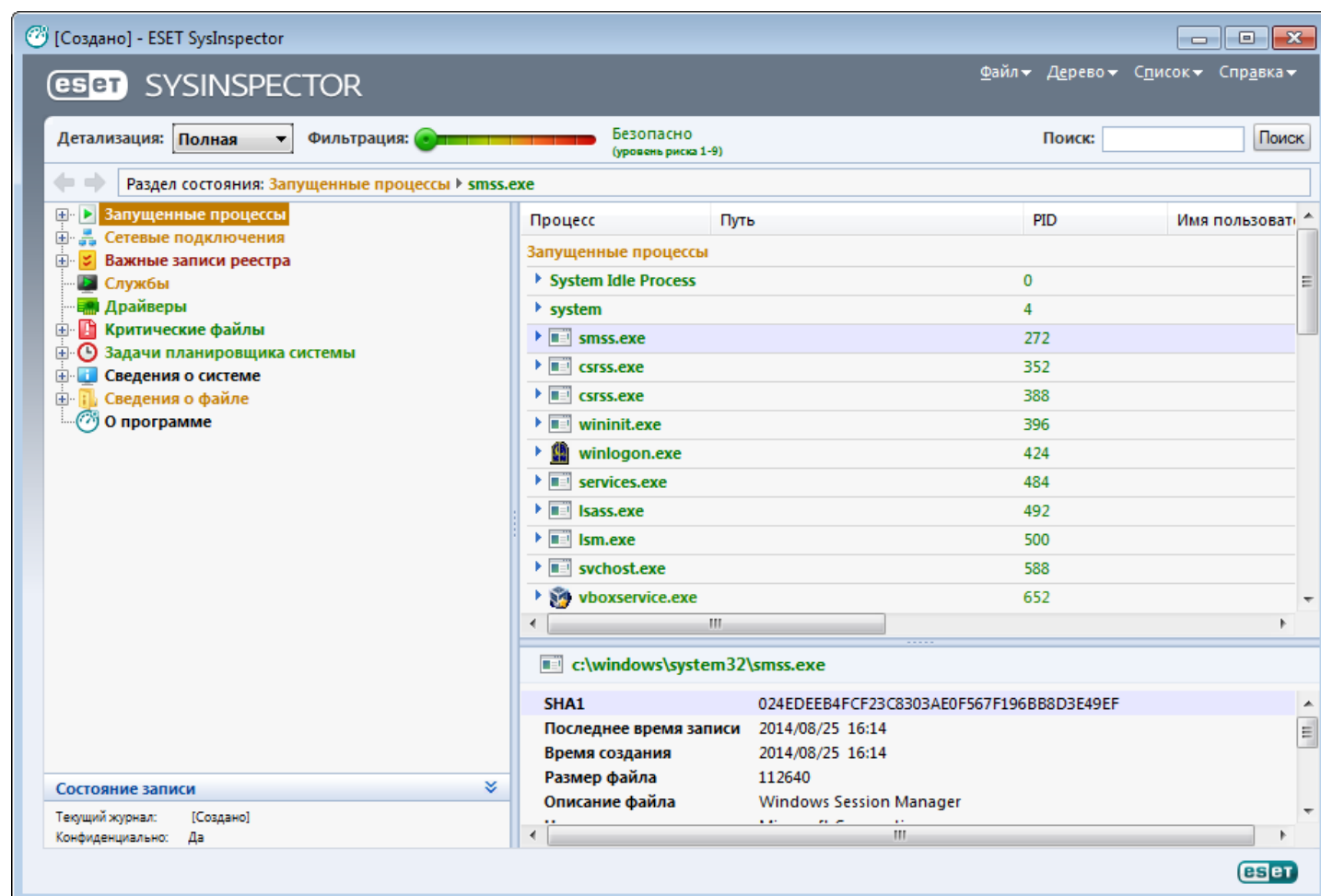
3.10.6.1.1 Запуск ESET SysInspector

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

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

3.10.6.2 Интерфейс пользователя и работа в приложении

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



3.10.6.2.1 Элементы управления программой

В этом разделе описаны все элементы управления приложением ESET SysInspector.

Файл

Щелкнув элемент **Файл**, можно сохранить данные о текущем состоянии системы для их последующего изучения или открыть ранее сохраненный журнал. Если планируется опубликовать журнал, при его создании рекомендуется использовать параметр **Подходит для отправки**. В этом случае из него исключается конфиденциальная информация (например, имя текущего пользователя, имя компьютера и домена, права текущего пользователя, переменные среды и т. п.).

i ПРИМЕЧАНИЕ.

Чтобы открыть сохраненные ранее отчеты ESET SysInspector, достаточно просто перетащить их в главное окно программы. Эта функция недоступна в операционной системе Windows Vista по соображениям безопасности.

Дерево

Позволяет развернуть или закрыть все узлы, а также экспортировать выбранные разделы в сценарий обслуживания.

Список

Содержит функции, облегчающие навигацию в программе, а также прочие функции, например средства поиска информации в Интернете.

Справка

Содержит сведения о приложении и его функциях.

Подробнее

Этот параметр влияет на выводимую в главном окне программы информацию, облегчая работу с ней. В базовом режиме пользователю доступна информация, необходимая для поиска решений стандартных проблем, возникающих в системе. В среднем режиме отображаются расширенные данные. В полном режиме программа ESET SysInspector отображает всю информацию, необходимую для решения самых нестандартных проблем.

Фильтрация

Используется для поиска подозрительных файлов или записей в реестре системы. 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 отфильтровывает все элементы с уровнем риска, который меньше текущего, и выводит на экран только те элементы, уровень подозрительности которых выше отображаемого уровня. Если ползунок находится в крайнем правом положении, программа отображает только известные вредоносные элементы.

Все элементы, имеющие уровень риска от 6 до 9, могут представлять угрозу для безопасности. Если вы не используете решение ESET по обеспечению безопасности, после нахождения программой ESET SysInspector такого элемента рекомендуется проверить систему с помощью [ESET Online Scanner](#). ESET Online Scanner является бесплатной службой.

ПРИМЕЧАНИЕ.

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

Сравнение

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

Поиск

Служит 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 окно 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.

ВАЖНО!

Элементы, выделенные красным цветом, являются неизвестными, поэтому программа помечает их как потенциально опасные. Если элемент выделен красным, это не означает, что его можно удалить. Перед удалением убедитесь в том, что эти файлы действительно опасны и не являются необходимыми.

3.10.6.2.2 Навигация в ESET SysInspector

ESET SysInspector распределяет информацию разного типа по нескольким базовым разделам, называемым узлами. Чтобы получить дополнительные сведения, разверните подузлы соответствующего узла. Чтобы развернуть или свернуть узел, дважды щелкните имя узла либо рядом с именем щелкните значок  или . При перемещении по древовидной структуре узлов и подузлов в окне навигации о каждом узле доступны различные сведения, отображаемые в окне описания. При переходе в окне описания к конкретному элементу в окне подробной информации появляются дополнительные сведения о нем.

Ниже описаны главные узлы в окне навигации и относящиеся к ним сведения в окнах описания и подробной информации.

Запущенные процессы

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

Окно подробной информации содержит дополнительные сведения об элементах, выбранных в окне описания, например 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 начинается в программе ESET SysInspector с символов «\??\». Эти символы обеспечивают таким процессам оптимизацию до запуска 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 в нем можно найти IP-адреса DNS-серверов.

Окно подробной информации содержит дополнительные сведения об элементах, выбранных в окне описания, например размер файла или его хэш.

Важные записи реестра

Содержит список определенных записей реестра, которые часто бывают связаны с различными проблемами в системе: например, записи с указанием автоматически загружаемых программ, вспомогательных объектов браузера и т. п.

В окне описания можно узнать, какие файлы связаны с определенными записями реестра. Дополнительная информация отображается в окне подробных сведений.

Службы

В окне описания перечислены файлы, зарегистрированные как службы Windows. В окне подробных сведений можно увидеть способ запуска службы, а также просмотреть некоторую дополнительную информацию.

Драйверы

Список драйверов, установленных в системе.

Критические файлы

В окне описания отображается содержимое критически важных файлов операционной системы Microsoft Windows.

Задачи системного планировщика

Отображается список задач, инициируемых планировщиком заданий Windows в определенное время/период времени.

Информация о системе

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

Сведения о файле

Список важных системных файлов и файлов из папки Program Files. В окнах описания и подробных сведений может отображаться дополнительная информация о них.

О программе

Сведения о версии программы ESET SysInspector и список программных модулей.

3.10.6.2.2.1 Сочетания клавиш

Ниже перечислены сочетания клавиш, которые можно использовать при работе с программой ESET SysInspector.

Файл

Ctrl+O открывает существующий журнал
Ctrl+S сохраняет созданные журналы

Создание

Ctrl+G создает стандартный снимок состояния компьютера
Ctrl+H создает снимок состояния компьютера, который также может содержать конфиденциальную информацию

Фильтрация элементов

1, O безопасно, отображаются элементы с уровнем риска 1–9
2 безопасно, отображаются элементы с уровнем риска 2–9
3 безопасно, отображаются элементы с уровнем риска 3–9
4, U неизвестно, отображаются элементы с уровнем риска 4–9
5 неизвестно, отображаются элементы с уровнем риска 5–9
6 неизвестно, отображаются элементы с уровнем риска 6–9
7, B опасно, отображаются элементы с уровнем риска 7–9
8 опасно, отображаются элементы с уровнем риска 8–9
9 опасно, отображаются элементы с уровнем риска 9
- понижает уровень риска
+ повышает уровень риска
Ctrl+9 режим фильтрации, равный или более высокий уровень
Ctrl+0 режим фильтрации, только равный уровень

Вид

Ctrl+5 просмотр по производителям, все производители
Ctrl+6 просмотр по производителям, только Майкрософт
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 развертывание дерева

Ctrl+Q свертывание дерева

Прочие элементы управления

Ctrl+T переход к исходному расположению элемента после его выбора в результатах поиска
Ctrl+P отображение базовых сведений об объекте
Ctrl+A отображение полных сведений об объекте
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 выбранный 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 обслуживания

Сравнение

Ctrl+Alt+O открытие исходного или сравнительного журнала
Ctrl+Alt+R отмена сравнения
Ctrl+Alt+1 отображение всех элементов
Ctrl+Alt+2 отображение только добавленных элементов (отображаются только элементы из текущего журнала)
Ctrl+Alt+3 отображение только удаленных элементов (отображаются элементы из предыдущей версии журнала)
Ctrl+Alt+4 отображение только замененных элементов (включая файлы)
Ctrl+Alt+5 отображение только различий между журналами
Ctrl+Alt+C отображение результатов сравнения
Ctrl+Alt+N отображение текущего журнала
Ctrl+Alt+P отображение предыдущей версии журнала

Разное

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

3.10.6.2.3 Сравнение

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

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

Преимуществом функции сравнения двух журналов является то, что она позволяет просматривать активный на данный момент журнал и журнал, сохраненный в файле. Для сравнения журналов в меню **Файл** выберите пункт **Сравнить журналы** и выполните команду **Выбрать файл**. Выбранный журнал сравнивается с активным журналом в главном окне программы. Сравнительный журнал будет содержать только различия между двумя сравниваемыми журналами.

i ПРИМЕЧАНИЕ.

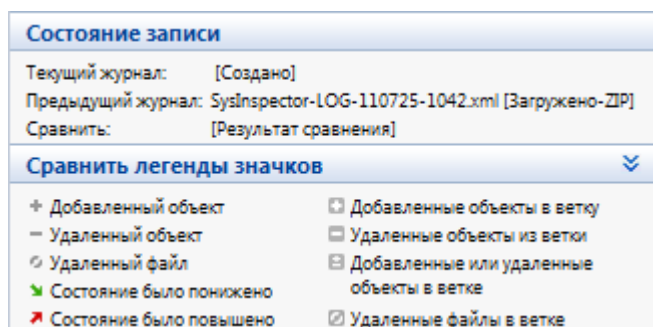
При сравнении двух файлов журнала в меню **Файл** выберите пункт **Сохранить журнал** и сохраните журнал как файл в формате ZIP. В результате будут сохранены оба файла. Если такой файл впоследствии открыть, содержащиеся в нем журналы сравниваются автоматически.

Рядом с отображенными элементами ESET SysInspector добавляет символы, указывающие на различия между журналами.

Ниже описаны все символы, которые могут отображаться рядом с элементами.

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

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



Любой сравниваемый журнал можно сохранить в файл и открыть позже.

Пример

Создайте и сохраните журнал, содержащий исходную информацию о системе, в файл с названием «предыдущий.xml». Внеся в систему изменения, откройте ESET SysInspector и создайте 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 с перечнем различий между исходными журналами.

Тот же результат можно получить с помощью следующей команды, вызываемой из командной строки:

```
SysInspector.exe текущий.xml предыдущий.xml
```

3.10.6.3 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 пользователя
/privacy	создание журнала без конфиденциальной информации
/zip	сохранение созданного журнала в ZIP-архиве
/silent	скрытие окна хода 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*

i ПРИМЕЧАНИЕ.

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

3.10.6.4 Сценарий обслуживания

Сценарий обслуживания является средством для пользователей программы ESET SysInspector, с помощью которого можно легко удалить из системы нежелательные объекты.

Сценарий обслуживания позволяет целиком или частично экспортировать журнал ESET SysInspector. После экспорта можно отметить нежелательные объекты для удаления. Затем можно запустить отредактированный журнал для удаления отмеченных объектов.

Сценарий обслуживания предназначен для пользователей, имеющих определенный опыт в диагностике компьютерных систем. Неквалифицированное использование данного средства может привести к неисправности 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. Выберите первый элемент в разделе слева (в древовидной структуре), нажмите клавишу SHIFT, а затем выберите последний объект, чтобы отметить все элементы в списке.
3. Щелкните выделенные объекты правой кнопкой мыши и в контекстном меню выберите пункт **Экспортировать выбранные разделы в сценарий службы**.
4. Выбранные объекты будут экспортированы в новый журнал.
5. Далее следует наиболее важный шаг всей процедуры: откройте созданный журнал и измените атрибут «-» на «+» для всех объектов, подлежащих удалению. Убедитесь, что не отмечены какие-либо важные для операционной системы файлы или объекты.
6. Откройте ESET SysInspector, выберите **Файл > Запустить сценарий обслуживания** и укажите путь к своему сценарию.
7. Нажмите кнопку **ОК**, чтобы запустить сценарий.

3.10.6.4.1 Создание сценария обслуживания

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

i ПРИМЕЧАНИЕ.

Сценарий обслуживания нельзя экспортировать в ходе сравнения двух журналов.

3.10.6.4.2 Структура сценария обслуживания

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

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

01) Запущенные процессы

Этот раздел содержит список всех процессов, запущенных в системе. Каждый процесс идентифицируется по UNC-пути, а также по хэшу 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 выбран (помечен символом «+») процесс module32.exe. При выполнении сценария этот процесс будет завершен.

02) 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\khbexb.dll
- c:\windows\system32\advapi32.dll
[...]
```

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

03) TCP-соединения

Этот раздел содержит данные о существующих TCP-соединениях.

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 этого сценария обнаруживается владелец сокета помеченного TCP-соединения, после чего сокет останавливается, высвобождая системные ресурсы.

04) 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) 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) 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 сброшены к значениям по умолчанию. Действия, применяемые к конкретным записям, зависят от категории и значения раздела в определенной записи реестра.

07) 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 и все зависящие от них службы будут остановлены и удалены.

08) 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 останавливаются. Следует учесть, что некоторые драйверы не позволяют остановить свою работу.

09) Важные файлы

Этот раздел содержит информацию о файлах, критически важных с точки зрения 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
[...]
```

Выбранные объекты будут удалены или возвращены к исходным значениям.

3.10.6.4.3 Выполнение сценариев обслуживания

Отметьте все нужные объекты, а затем сохраните и закройте сценарий. Запустите измененный сценарий непосредственно из главного окна программы ESET SysInspector с помощью команды **Запустить сценарий обслуживания** в меню «Файл». При открытии сценария появится следующее сообщение: **Выполнить сценарий обслуживания «%Scriptname%»? После подтверждения может появиться еще одно предупреждение, сообщающее о попытке запуска неподписанного сценария. Чтобы запустить сценарий, нажмите кнопку **Запуск**.**

В диалоговом окне появится подтверждение успешного выполнения сценария.

Если сценарий может быть обработан только частично, отобразится следующее сообщение: **Сценарий обслуживания выполнен частично. Показать отчет об ошибке?** Чтобы просмотреть полный отчет об ошибках, в котором перечислены невыполненные действия, нажмите кнопку **Да**.

Если сценарий не был признан действительным, отобразится следующее сообщение: **Выбранный сценарий обслуживания не подписан. Выполнение неподписанных и неизвестных сценариев может привести к повреждению данных на компьютере. Выполнить сценарий и все действия?** Это может быть вызвано несоответствиями в сценарии (поврежден заголовок, искажено название раздела, пропущена пустая строка между разделами и т. д.). В этом случае откройте файл сценария и исправьте ошибки либо создайте новый сценарий обслуживания.

3.10.6.5 Часто задаваемые вопросы

Требуется 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 с правами обычного пользователя или с ограниченными правами приведет к сбору меньшего объема данных о системе.

Создает ли ESET SysInspector файл журнала?

ESET SysInspector может создать файл журнала с конфигурацией системы. Для сохранения такого журнала в главном окне программы выберите **Файл > Сохранить журнал**. Журналы сохраняются в формате XML. По умолчанию файлы сохраняются в папке `%USERPROFILE%\Мои документы\` и получают название типа «SysInspector-`%COMPUTERNAME%`-ГГММДД-ЧЧММ.XML». Перед сохранением файла журнала можно изменить его расположение и имя.

Как просмотреть файл журнала ESET SysInspector?

Для просмотра файла журнала, созданного в ESET SysInspector, запустите программу и в главном окне выберите **Файл > Открыть журнал**. Кроме того, файлы журнала можно перетаскивать в окно приложения ESET SysInspector. Если вы часто просматриваете файлы журнала ESET SysInspector, создайте на рабочем столе ярлык для файла SYSINSPECTOR.EXE. После этого файлы для просмотра можно просто перетаскивать на этот ярлык. По соображениям безопасности в ОС Windows Vista/7 может быть запрещено перетаскивать элементы между окнами с разными настройками 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. После выхода окончательной версии программы мы можем предоставить эти данные по просьбам клиентов.

Как ESET SysInspector оценивает риск определенного объекта?

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

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

Анализ ESET SysInspector не гарантирует, что данный объект является вредоносным — эта оценка должна выполняться специалистом по безопасности. Приложение ESET SysInspector разработано для того, чтобы специалист по безопасности имел возможность быстро оценить, какие объекты системы следует проверить в связи с их необычным поведением.

Зачем ESET SysInspector в ходе работы подключается к Интернету?

Как и многие приложения, программа ESET SysInspector подписана цифровым сертификатом, гарантирующим, что издателем программы является компания ESET и что программа не была изменена. Для проверки сертификата и подлинности издателя программы операционная система связывается с центром сертификации. Это нормальное поведение программ с цифровой подписью в Microsoft Windows.

Что такое технология Anti-Stealth?

Технология Anti-Stealth обеспечивает эффективное обнаружение руткитов.

Если система атакована вредоносной программой, которая ведет себя как руткит, пользователь может подвергнуться риску потери или кражи данных. Без специального инструмента для борьбы с руткитами такие программы практически невозможно обнаружить.

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

В ходе идентификации цифровой подписи исполняемого файла программа ESET SysInspector сначала проверяет наличие в файле встроенной цифровой подписи. Если цифровая подпись найдена, файл будет проверен с использованием этих данных. Если цифровая подпись не найдена, программа ESI начинает поиск соответствующего CAT-файла (в каталоге безопасности `%systemroot%\system32\catroot`), содержащего сведения об обрабатываемом исполняемом файле. Если соответствующий CAT-файл найден, его цифровая подпись применяется при проверке исполняемого файла.

Поэтому иногда в некоторых файлах с пометкой «Подписано MS» имеется запись с названием другой компании.

3.10.6.6 ESET SysInspector как часть приложения ESET Endpoint Security

Чтобы открыть раздел ESET SysInspector в ESET Endpoint Security, выберите **Службные программы > ESET SysInspector**. В окне ESET SysInspector используется примерно такая же система управления, как и в окнах журналов сканирования и запланированных задач. Чтобы выполнить любую операцию со снимками системы (создание, просмотр, сравнение, удаление и экспорт), требуется всего несколько простых действий.

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, создания или 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 выбранный снимок в файл, щелкните его правой кнопкой мыши и выберите команду **Экспорт....**

Ниже приведено подробное описание каждой из функций.

- **Сравнить** — сравнение двух существующих журналов. Эта функция пригодится, если вам потребуется проследить различия между текущим и более старым журналом. Для сравнения необходимо выбрать два снимка.
- **Создать...** — создание новой записи. Перед созданием записи нужно ввести краткий комментарий к ней. В столбце **Состояние** отображается ход создания снимка. Все уже созданные снимки помечены надписью **Создано**.
- **Удалить/Удалить все** — удаление записей из списка.
- **Экспорт...** — сохранение выбранной записи в XML-файл с возможностью упаковки в ZIP-архив.

3.10.7 Удаленный мониторинг и управление

Remote Monitoring and Management (RMM) is the process of supervising and controlling software systems using a locally installed agent that can be accessed by a management service provider. The default ESET Endpoint Security installation contains the file *ermm.exe* located in the Endpoint application within the directory `c:\Program Files\ESET\ESET Security`. *ermm.exe* is a command line utility designed to facilitate the management of endpoint products and communications with any RMM Plugin. *ermm.exe* exchanges data with the RMM Plugin, which communicates with the RMM Agent linked to an RMM Server. By default, the ESET RMM tool is disabled. For more information, see [Активация удаленного мониторинга и управления](#).

The default ESET Endpoint Security installation contains file *ermm.exe* located in the Endpoint application directory (default path `c:\Program Files\ESET\ESET Security`). *ermm.exe* exchanges data with the RMM Plugin, which communicates with the RMM Agent that is linked to an RMM Server.

- *ermm.exe* – command line utility developed by ESET that allows managing of Endpoint products and communication with any RMM Plugin.

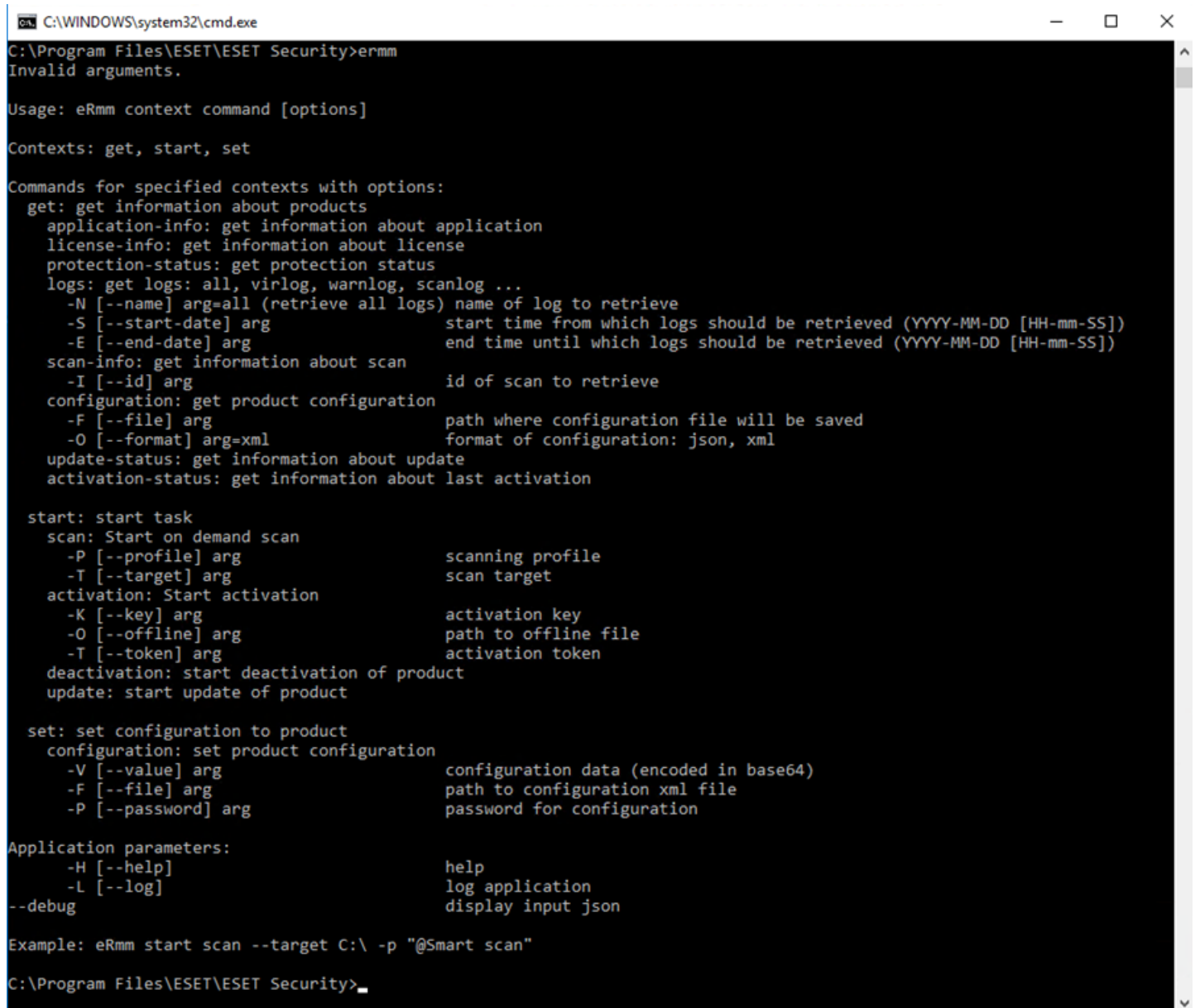
3.10.7.1 Командная строка RMM

Remote monitoring management is run using the command line interface. The default ESET Endpoint Security installation contains the file *ermm.exe* located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (*cmd.exe*) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a *cmd.exe* into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\ESET\ESET Security>ermm
Invalid arguments.

Usage: eRmm context command [options]

Contexts: get, start, set

Commands for specified contexts with options:
get: get information about products
  application-info: get information about application
  license-info: get information about license
  protection-status: get protection status
  logs: get logs: all, virlog, warnlog, scanlog ...
    -N [--name] arg=all (retrieve all logs) name of log to retrieve
    -S [--start-date] arg start time from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
    -E [--end-date] arg end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
  scan-info: get information about scan
    -I [--id] arg id of scan to retrieve
  configuration: get product configuration
    -F [--file] arg path where configuration file will be saved
    -O [--format] arg=json,xml format of configuration: json, xml
  update-status: get information about update
  activation-status: get information about last activation

start: start task
scan: Start on demand scan
  -P [--profile] arg scanning profile
  -T [--target] arg scan target
activation: Start activation
  -K [--key] arg activation key
  -O [--offline] arg path to offline file
  -T [--token] arg activation token
deactivation: start deactivation of product
update: start update of product

set: set configuration to product
configuration: set product configuration
  -V [--value] arg configuration data (encoded in base64)
  -F [--file] arg path to configuration xml file
  -P [--password] arg password for configuration

Application parameters:
  -H [--help] help
  -L [--log] log application
--debug display input json

Example: eRmm start scan --target C:\ -p "@Smart scan"

C:\Program Files\ESET\ESET Security>
```

ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get	get	Get information about products

Context	Command	Description
	сведения о приложении	Get information about product
	сведения о лицензии	Get information about license
	состояние защиты	Get protection status
	журналы	Get logs
	сведения о сканировании	Get information about running scan
	конфигурация	Get product configuration
	состояние обновления	Get information about update
	состояние активации	Get information about last activation
start		Start task
	сканирование	Start on demand scan
	активация	Start activation of product
	деактивация	Start deactivation of product
	обновление	Start update of product
set		Set options for product
	конфигурация	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

3.10.7.2 Список команд JSON

- [получить состояние защиты](#)
- [получить сведения о приложении](#)
- [получить сведения о лицензии](#)
- [получить журналы](#)
- [получить состояние активации](#)
- [получить сведения о сканировании](#)
- [получить конфигурацию](#)
- [получить состояние обновления](#)
- [запуск сканирования](#)
- [запуск активации](#)
- [запуск деактивации](#)
- [запуск обновления](#)
- [настройка конфигурации](#)

3.10.7.2.1 получить состояние защиты

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call
<pre>{ "command": "get_protection_status", "id": 1, "version": "1" }</pre>

result
<pre>{ "id": 1, "result": { "statuses": [{ "id": "EkrrnNotActivated", "status": 2, "priority": 768, "description": "Product not activated" }], "status": 2, } }</pre>

```
"description":"Security alert"
},
"error":null
}
```

3.10.7.2.2 получить сведения о приложении

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

```
call
{
  "command":"get_application_info",
  "id":1,
  "version":"1"
}
```

```
result
{
  "id":1,
  "result":{
    "description":"ESET Endpoint Antivirus",
    "version":"6.6.2018.0",
    "product":"eea",
    "lang_id":1033,
    "modules":[{"id":"SCANNER32",
      "description":"Detection engine",
      "version":"15117",
      "date":"2017-03-20"}],{
      "id":"PEGASUS32",
      "description":"Rapid Response module",
      "version":"9734",
      "date":"2017-03-20"
    }
  }
}
```

```
},{
  "id":"LOADER32",
  "description":"Update module",
  "version":"1009",
  "date":"2016-12-05"
},{
  "id":"PERSEUS32",
  "description":"Antivirus and antispysware scanner module",
  "version":"1513",
  "date":"2017-03-06"
},{
  "id":"ADVHEUR32",
  "description":"Advanced heuristics module",
  "version":"1176",
  "date":"2017-01-16"
},{
  "id":"ARCHIVER32",
  "description":"Archive support module",
  "version":"1261",
  "date":"2017-02-22"
},{
  "id":"CLEANER32",
  "description":"Cleaner module",
  "version":"1132",
  "date":"2017-03-15"
},{
  "id":"ANTISTEALTH32",
  "description":"Anti-Stealth support module",
  "version":"1106",
  "date":"2016-10-17"
},{
  "id":"SYSTEMSTATUS32",
  "description":"ESET SysInspector module",
  "version":"1266",
  "date":"2016-12-22"
},{
  "id":"TRANSLATOR32",
  "description":"Translation support module",
  "version":"1588B",
  "date":"2017-03-01"
},{
  "id":"HIPS32",
```



```
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

3.10.7.2.3 получить сведения о лицензии

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call
<pre>{ "command": "get_license_info", "id": 1, "version": "1" }</pre>

result
<pre>{ "id": 1, "result": { "type": "NFR", "expiration_date": "2020-12-31", "expiration_state": "ok", "public_id": "3XX-7ED-7XF", "seat_id": "6f726793-ae95-4e04-8ac3-e6a20bc620bf", "seat_name": "M" }, "error": null }</pre>

3.10.7.2.4 получить журналы

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

Parameters

Name	Value
------	-------

name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrlog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call
<pre>{ "command": "get_logs", "id": 1, "version": "1", "params": { "name": "warnlog", "start_date": "2017-04-04 06-00-00", "end_date": "2017-04-04 12-00-00" } }</pre>

result
<pre>{ "id": 1, "result": { "warnlog": { "display_name": "Events", "logs": [{ "Time": "2017-04-04 06-05-59", "Severity": "Info", "PluginId": "ESET Kernel", "Code": "Malware database was successfully updated to version 15198 (20170404).", "UserData": "" }, { "Time": "2017-04-04 11-12-59", "Severity": "Info", "PluginId": "ESET Kernel", "Code": "Malware database was successfully updated to version 15199 (20170404).", "UserData": "" }] } } }</pre>

```
"error":null
}
```

3.10.7.2.5 получить состояние активации

Get information about the last activation. Result of status can be { success, error }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
  "command":"get_activation_status",
  "id":1,
  "version":"1"
}
```

result

```
{
  "id":1,
  "result":{
    "status":"success"
  },
  "error":null
}
```

3.10.7.2.6 получить сведения о сканировании

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{
  "command": "get_scan_info",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "scan-info": {
      "scans": [
        {
          "scan_id": 65536,
          "timestamp": 272,
          "state": "finished",
          "pause_scheduled_allowed": false,
          "pause_time_remain": 0,
          "start_time": "2017-06-20T12:20:33Z",
          "elapsed_tickcount": 328,
          "exit_code": 0,
          "progress_filename": "Operating memory",
          "progress_arch_filename": "",
          "total_object_count": 268,
          "infected_object_count": 0,
          "cleaned_object_count": 0,
          "log_timestamp": 268,
          "log_count": 0,
          "log_path": "C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
          "username": "test-PC\\test",
          "process_id": 3616,
          "thread_id": 3992,
          "task_type": 2
        }
      ],
      "pause_scheduled_active": false
    }
  },
}
```

```
"error":null
}
```

3.10.7.2.7 получить конфигурацию

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

```
call
{
  "command": "get_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml"
  }
}
```

```
result
{
  "id": 1,
  "result": {
    "configuration": "PD94bWwgdmVyc2lvcj0iMS4w=="
  },
  "error": null
}
```

3.10.7.2.8 получить состояние обновления

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call
<pre>{ "command": "get_update_status", "id": 1, "version": "1" }</pre>

result
<pre>{ "id": 1, "result": { "last_update_time": "2017-06-20 13-21-37", "last_update_result": "error", "last_successful_update_time": "2017-06-20 11-21-45" }, "error": null }</pre>

3.10.7.2.9 запуск сканирования

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

```
call
{
  "command":"start_scan",
  "id":1,
  "version":"1",
  "params":{
    "profile":"Smart scan",
    "target":"c:\\\"
  }
}
```

```
result
{
  "id":1,
  "result":{
    "task_id":458752
  },
  "error":null
}
```


3.10.7.2.10 запуск активации

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file" | --token "activation token"
```

Parameters

Name	Value
key	Activation key
offline	Path to offline file
token	Activation token

Example

```
call
{
  "command": "start_activation",
  "id": 1,
  "version": "1",
  "params": {
    "key": "XXXX-XXXX-XXXX-XXXX-XXXX"
  }
}
```

```
result
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

3.10.7.2.11 запуск деактивации

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call
<pre>{ "command": "start_deactivation", "id": 1, "version": "1" }</pre>

result
<pre>{ "id": 1, "result": { }, "error": null }</pre>

3.10.7.2.12 запуск обновления

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call
<pre>{ "command": "start_update", "id": 1, }</pre>

```
"version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
  },
  "error": {
    "id": 4,
    "text": "Task already running."
  }
}
```

3.10.7.2.13 настройка конфигурации

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
  "command": "set_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml",
    "password": "pass"
  }
}
```

```
result
{
  "id":1,
  "result":{
  },
  "error":null
}
```

3.11 Глоссарий

3.11.1 Типы угроз

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

3.11.1.1 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 это понятие 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 удастся очистить, отправьте соответствующие файлы в лабораторию ESET для изучения. В ряде случаев зараженные файлы изменяются настолько, что их невозможно очистить. В таком случае их нужно заменять чистыми копиями.

3.11.1.2 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 считанные часы или даже минуты после запуска. Эта способность быстро самостоятельно реплицироваться делает черви более опасными, чем другие типы вредоносных программ.

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

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

3.11.1.3 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 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.

3.11.1.4 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 Endpoint Security доступны преимущества технологии Anti-Stealth, которая также позволяет обнаруживать и устранять активные руткиты.

3.11.1.5 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 стоит 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.

3.11.1.6 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 списка контактов пользователя или список нажатий клавиш на клавиатуре.

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 шпионской программы во время установки основной программы, чтобы поощрить их к приобретению платной версии, в которой шпионской программы нет.

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.

3.11.1.7 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.

3.11.1.8 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 Endpoint Security позволяет обнаруживать такие угрозы.

В качестве **потенциально опасных приложений** выступает нормальное коммерческое программное обеспечение. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (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.

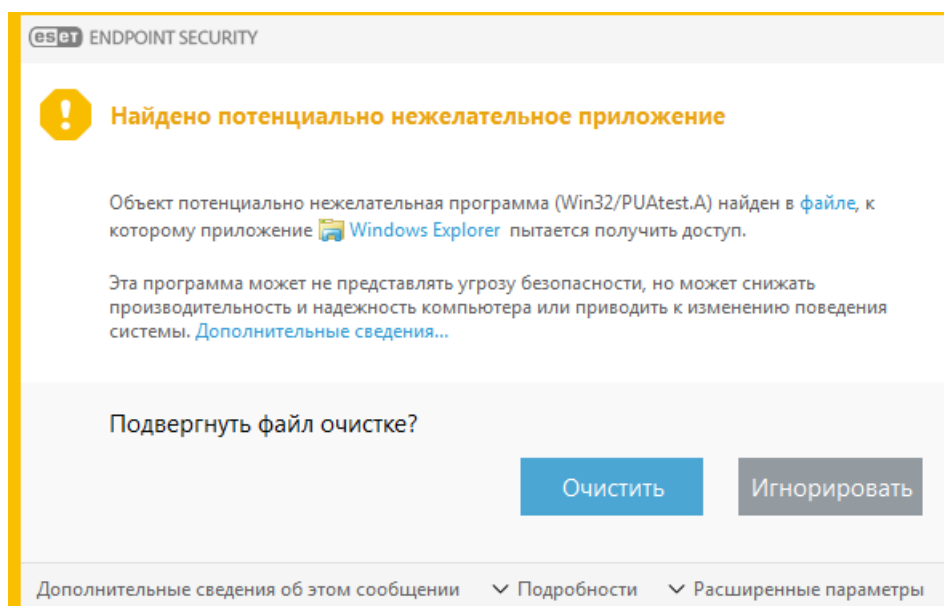
3.11.1.9 Потенциально нежелательные приложения

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

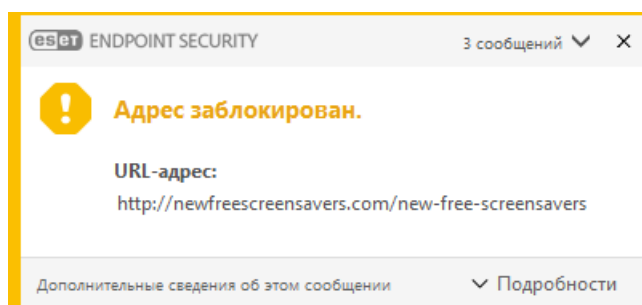
Предупреждение — обнаружена потенциальная угроза

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. **Ничего не предпринимать:** эта функция позволяет потенциальной угрозе проникнуть на компьютер.
3. Чтобы разрешить приложению и впредь работать на компьютере без прерываний, щелкните элемент **Дополнительные сведения/показать параметры** и установите флажок **Исключить из проверки**.

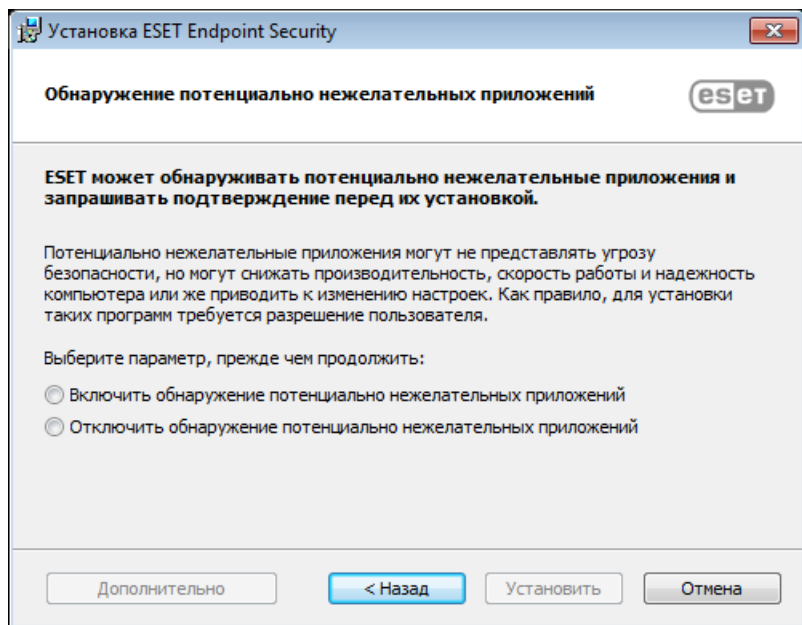


Если обнаружено потенциально нежелательное приложение и его невозможно очистить, в правом нижнем углу экрана отобразится окно уведомлений **Адрес заблокирован**. Дополнительные сведения об этом событии можно получить, последовательно щелкнув в главном меню элементы **Сервис > Файлы журнала > Отфильтрованные веб-сайты**.



Потенциально нежелательные приложения — параметры

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

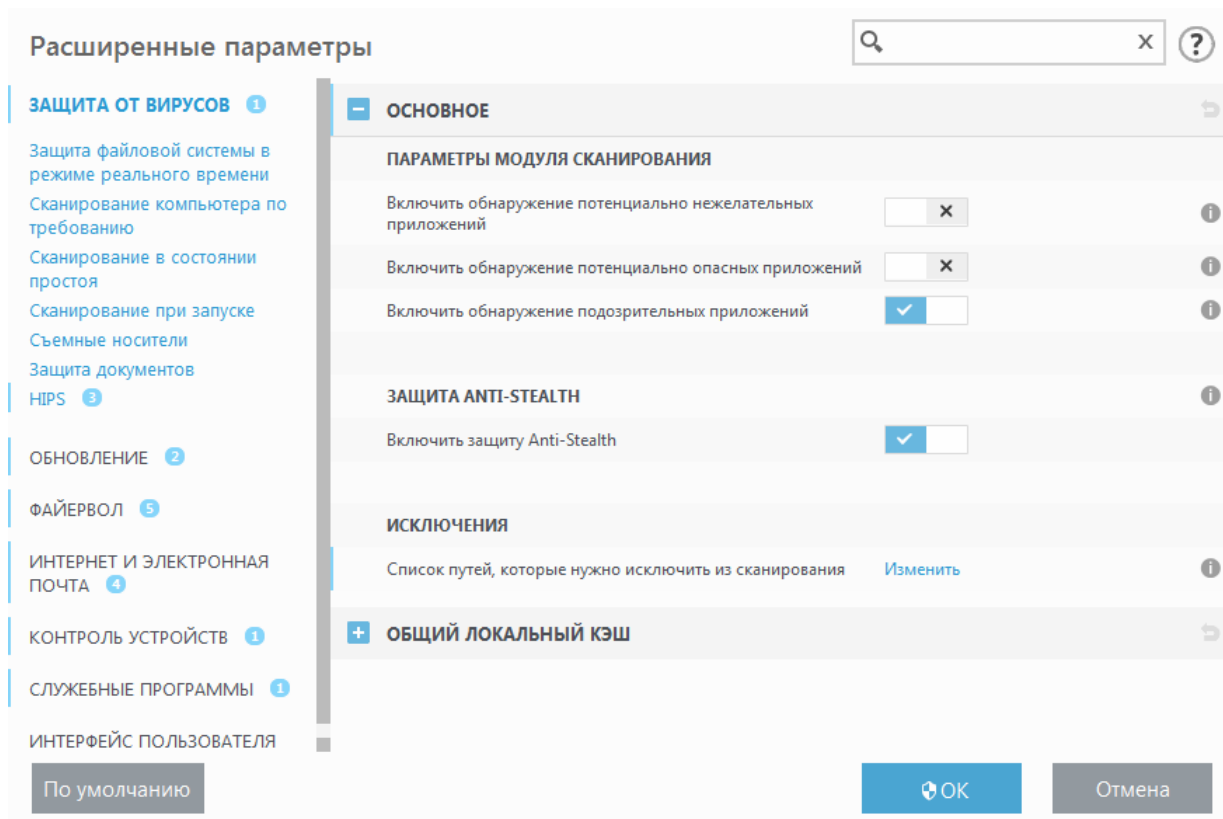


⚠ ВНИМАНИЕ!

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 нижеприведенным инструкциям.

1. Откройте программу ESET. [Как открыть мой продукт ESET?](#)
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 рекламой, которые изменяют домашнюю страницу браузера или параметры поиска. При этом файлообменные ресурсы часто не уведомляют производителя программного обеспечения или пользователей 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 этой страницы справочной системы см. в этой [статье базы знаний ESET](#).

Для получения дополнительных сведений щелкните [здесь](#).

3.11.1.10 Ботнет

Бот или веб-робот — это автоматизированная вредоносная программа, которая сканирует блоки сетевых адресов и заражает уязвимые компьютеры. Это позволяет хакерам получить контроль над множеством компьютеров одновременно и превратить их в ботов (называемых также «зомби»). Чтобы заразить большое количество компьютеров, хакеры обычно используют боты. Большая группа зараженных компьютеров называется ботнетом. Зараженный компьютер, являющийся частью ботнета, может использоваться для проведения распределенных атак типа «отказ в обслуживании» (DDoS) и выполнения автоматизированных задач в Интернете без вашего ведома (например, отправка спама и вирусов, кража личной и конфиденциальной информации, включающей банковские учетные данные или номера кредитных карт).

3.11.2 Типы удаленных атак

Существует множество специальных технологий, с помощью которых злоумышленники могут атаковать удаленные компьютеры. Они подразделяются на несколько категорий.

3.11.2.1 Атаки червей

Компьютерные черви — это содержащие злонамеренный код программы, которые атакуют главные компьютеры и распространяются через сеть. Сетевые черви используют уязвимости системы безопасности различных приложений. Благодаря Интернету они распространяются по всему земному шару за считанные часы после запуска в сеть.

Большинство атак червей можно избежать, используя в файрволе настройки безопасности по умолчанию. Кроме того, следует выбрать тип защиты для **Сети общего пользования**, работая в такой сети, и постоянно скачивать актуальные обновления безопасности для своих программ и ОС.

3.11.2.2 DoS-атаки

DoS-атаки (атаки типа *отказ в обслуживании*) представляют собой попытку сделать компьютер или сеть недоступными тем пользователям, для которых они предназначены. Обмен данными между пользователями пораженного компьютера затруднен или невозможен в приемлемом режиме. Компьютеры, подвергшиеся действию DoS-атаки, обычно должны быть перезагружены для восстановления нормальной работы.

В большинстве случаев объектами этой атаки становятся веб-серверы, а целью является вывод их из строя и, как следствие, их недоступность на некоторое время.

3.11.2.3 Сканирование портов

Сканирование портов используется, чтобы определить, какие порты компьютера открыты на узле сети. Сканер портов представляет собой программное обеспечение, которое предназначено для поиска таких портов.

Компьютерный порт является виртуальной точкой, которая управляет сетевым трафиком в обоих направлениях. Это является критичным с точки зрения сетевой безопасности. В больших сетях данные, которые собираются с помощью сканера портов, могут помочь выявить потенциальные уязвимости компьютерных систем. Такое использование является допустимым.

Однако сканеры часто используются злоумышленниками для взлома систем безопасности. Первым шагом отправляется серия пакетов на каждый из портов. В зависимости от полученных ответов определяется, какой из портов можно использовать. Сканирование не причиняет вреда само по себе, но следует иметь в виду, что такая активность зачастую является признаком попытки выявления уязвимости и последующей атаки злоумышленников на систему.

Сетевые администраторы обычно советуют блокировать все неиспользуемые порты и защищать используемые от неавторизованного доступа.

3.11.2.4 Атака путем подделки записей кэша DNS

Атака путем подделки записей кэша DNS (сервер доменных имен) позволяет хакерам убедить DNS-сервер любого компьютера в том, что предоставляемые подложные данные являются истинными. Ложная информация кэшируется на определенное время, давая злоумышленникам возможность перезаписать ответы DNS-сервера с IP-адресами. В результате при попытке посещения веб-сайтов пользователь загружает компьютерные вирусы и черви вместо исходного содержимого.

3.11.3 Электронная почта

Электронная почта является современным средством общения, которое применяется во многих областях. Отличаясь гибкостью, высокой скоростью и отсутствием посредников, она сыграла ключевую роль в становлении Интернета в начале 90-х годов прошлого века.

К сожалению, вследствие высокого уровня анонимности электронная почта и Интернет оставляют пространство для незаконных действий, таких как рассылка спама. Спам может содержать нежелательные рекламные объявления, мистификации или вложения, распространяющие вредоносные программы. Доставляемые пользователю неудобства и опасность увеличиваются из-за того, что стоимость рассылки минимальна, а в распоряжении авторов спама есть множество средств для получения новых адресов электронной почты. Кроме того, количество и разнообразие спама 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 полученные нежелательные сообщения.
- Будьте осторожны при заполнении форм на веб-сайтах (особенно если они содержат пункты типа «Да, я хочу получать информацию»).
- Используйте разные 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.

3.11.3.1 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.

3.11.3.2 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 у получателей страх, неуверенность и сомнения, побуждая их верить в то, что «не поддающийся обнаружению вирус» удаляет их файлы, крадет пароли или выполняет какие-либо другие вредоносные действия на их компьютерах.

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.

3.11.3.3 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 (например, финансового учреждения или страховой компании). Сообщение может казаться благонадежным и содержать изображения и текст, которые могли изначально быть получены от источника, якобы являющегося отправителем данного сообщения. Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какую-либо личную информацию, такую как номера банковских счетов, имена пользователя, пароли и т. д. Если такие данные предоставляются, они легко могут быть украдены и использованы в преступных целях.

Банки, страховые компании и другие легитимные организации никогда не запрашивают имена пользователей и пароли в незапрошенных сообщениях электронной почты.

3.11.3.4 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, «ваигра» вместо «виагра» и т. п.

3.11.3.4.1 Правила

В контексте решений для защиты от спама и почтовых клиентов под правилами понимаются инструменты обработки электронной почты. Правило состоит из двух логических частей:

1. условие (например, получение сообщения с определенного адреса);
2. действие (например, удаление сообщения, перемещение его в указанную папку).

Количество и сочетания правил зависят от конкретного решения по защите от спама. Правила предназначены для борьбы со спамом (нежелательными сообщениями). Стандартные примеры приведены далее.

- 1. Условие: во входящем сообщении содержатся некоторые слова, часто присутствующие в нежелательных сообщениях.
2. Действие: удалить сообщение.
- 1. Условие: у входящего сообщения есть вложение с расширением .exe.
2. Действие: удалить вложение и доставить сообщение в почтовый ящик.
- 1. Условие: входящее сообщение отправлено сотрудником компании, в которой работает пользователь.
2. Действие: переместить сообщение в папку «Работа».

Рекомендуется использовать сочетание правил в программах защиты от спама, чтобы упростить администрирование и более эффективно отфильтровывать спам.

3.11.3.4.2 «Белый» список

Вообще под «белым» списком понимается перечень объектов или лиц, которые являются приемлемыми или имеют доступ. Термин «белый список электронной почты» означает список контактов, от которых разрешено получать сообщения. Такого рода списки создаются на основе поиска по ключевым словам в адресах электронной почты, именах домена или IP-адресах.

Если «белый» список работает в «исключительном» режиме, получение сообщений с других адресов, доменов или IP-адресов будет блокироваться. Если же «белый» список не является исключительным, такие сообщения не будут удаляться, а будут обрабатываться каким-либо другим способом.

«Белый» список обладает противоположным [«черному» списку](#) назначением. «Белые» списки сравнительно просто поддерживать, значительно проще, чем «черные». Для большей эффективности фильтрации спама рекомендуется использовать и «белый», и «черный» списки.

3.11.3.4.3 «Черный» список

В общем случае «черный» список является списком неприемлемых или запрещенных объектов или лиц. В виртуальном мире это метод, позволяющий принимать сообщения, которые приходят от всех пользователей, отсутствующих в таком списке.

Существует два типа «черных» списков. К первому типу относятся списки, созданные самими пользователями, в их приложениях для защиты от спама, а ко второму — профессиональные регулярно обновляемые «черные» списки, которые создаются специализированными учреждениями и распространяются через Интернет.

Принципиально важно использовать «черный» список для блокировки спама, но при этом вести такой список сложно, так как новые объекты блокирования появляются ежедневно. Рекомендуется использовать и «белый», и «черный» список, чтобы максимально эффективно отфильтровывать спам.

3.11.3.4.4 Список исключений

Список исключений обычно включает адреса электронной почты, которые могут быть подделаны и использоваться для отправки спама. Сообщения электронной почты, полученные с адресов, присутствующих в списке исключений, всегда будут сканироваться на предмет наличия спама. По умолчанию в списке исключений присутствуют все адреса электронной почты из существующих учетных записей почтовых клиентов.

3.11.3.4.5 Контроль на стороне сервера

Контроль на стороне сервера — это метод выявления массовых рассылок спама на основе количества полученных сообщений и реакции пользователей на них. Каждое сообщение оставляет уникальный цифровой «отпечаток», который основан на его содержимом. Уникальный идентификационный номер ничего не говорит о содержимом сообщения. Однако два одинаковых сообщения имеют одинаковые отпечатки, тогда как два различающихся — разные.

Если сообщение помечено как спам, его отпечаток отправляется на сервер. Если сервер получает и другие идентичные отпечатки (соответствующие одному и тому же нежелательному сообщению), этот отпечаток сохраняется в базе данных отпечатков спама. При сканировании входящих сообщений программа отправляет отпечатки сообщений на сервер. Сервер возвращает данные о тех отпечатках, которые соответствуют сообщениям, уже помеченным пользователями как спам.

3.11.4 Технологии ESET

3.11.4.1 Блокировщик эксплойтов

Блокировщик эксплойтов отслеживает приложения, которые обычно имеют уязвимость (браузеры, приложения для чтения документов, почтовые клиенты, Flash, Java и т. д.), и не просто блокирует определенные идентификаторы CVE, а уделяет основное внимание техникам злонамеренного использования уязвимостей. После срабатывания блокировщик анализирует поведение процесса, и если он вызывает подозрения, угрозу можно незамедлительно заблокировать на компьютере.

В отличие от модуля сканирования ESET, который обнаруживает эксплойты в файлах документов неправильного формата, и модуля защиты от сетевых атак, который функционирует на уровне обмена данными, технология блокировщика эксплойтов блокирует непосредственно процесс, использующий уязвимость, и записывает данные об угрозе, которые затем отправляются в облачную систему ESET LiveGrid®. Эти данные обрабатываются в лаборатории ESET по изучению угроз 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).

3.11.4.2 Расширенный модуль сканирования памяти

Расширенный модуль сканирования памяти работает в сочетании с [блокировщиком эксплойтов](#) для усиления защиты от вредоносных программ, которые обычные продукты, предназначенные для защиты от вредоносных программ, могут не обнаруживать из-за 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 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.

3.11.4.3 ESET LiveGrid®

Сеть ESET LiveGrid®, основанная на передовой системе раннего обнаружения 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 в реальных условиях, 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 версию модуля обнаружения на компьютере пользователя (что происходит несколько раз в день).

3.11.4.4 Защита от ботнетов

Защита от ботнетов обнаруживает вредоносные программы, анализируя их протоколы обмена данными по сети. В отличие от сетевых протоколов, которые не меняются годами, вредоносные ботнеты меняются часто. Эта новая технология помогает ESET обезвреживать вредоносные программы, которые пытаются подключить компьютер к ботнет-сети.

3.11.4.5 Блокировщик эксплойтов Java

Блокировщик эксплойтов Java — это расширение для существующего блокировщика эксплойтов ESET. Он осуществляет мониторинг Java на предмет поведения, которое напоминает поведение 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.).

3.11.4.6 Защита от атак на основе сценариев

Защита от атак на основе сценариев — это защита от злонамеренного кода на языке Javascript в браузерах и защита на базе Antimalware Scan Interface (AMSI) от сценариев в Powershell.

ВНИМАНИЕ!

Для работы этой функции необходимо, чтобы система HIPS была включена.

Функция защиты от атак на основе сценариев поддерживается для таких браузеров:

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

ПРИМЕЧАНИЕ.

Минимальные поддерживаемые версии браузеров могут различаться, поскольку файловые сигнатуры браузеров часто меняются. Последняя версия браузера поддерживается всегда.

3.11.4.7 Защита от программ-вымогателей

Программа-шантажист — это тип вредоносного ПО, блокирующий доступ пользователей к системе путем блокирования ее экрана или шифрования файлов. Модуль защиты от программ-шантажистов отслеживает поведение приложений и процессов, которые пытаются изменить ваши личные данные. Если поведение приложения определяется как злонамеренное или репутационное сканирование показывает, что приложение является подозрительным, это приложение блокируется или пользователю [предлагается](#) принять решение о его блокировании.

ВАЖНО!

Для правильной работы модуля защиты от программ-шантажистов должна быть включена система ESET LiveGrid®.

3.11.4.8 Система обнаружения DNA Detections

Методы обнаружения варьируются от точно определенных хэшей до системы обнаружения ESET DNA Detections, которая содержит комплексные определения вредоносного поведения и характеристики вредоносных программ. В отличие от вредоносного кода, который может быть легко изменен или скрыт злоумышленниками, поведение объектов не так просто изменить, поэтому система обнаружения ESET DNA Detections использует это в свою пользу.

Мы выполняем глубокий анализ кода и извлекаем «гены», которые определяют его поведение и позволяют системе обнаружения ESET DNA Detections получать доступ к потенциально подозрительному коду, который может находиться как на диске, так и в памяти запущенного процесса. Система обнаружения DNA Detections способна распознавать образцы известных вредоносных программ, новые варианты известных семейств вредоносных программ и даже незнакомые и неизвестные вредоносные программы по содержащимся в них «генам», указывающим на вредоносное поведение.

3.11.4.9 Модуль сканирования UEFI

Модуль сканирования единого интерфейса EFI (UEFI) является частью системы HIPS (системы предотвращения вторжений на узел), которая обеспечивает защиту интерфейса UEFI на вашем компьютере. UEFI — это встроенное ПО, которое загружается в память в начале процесса загрузки. Его код размещается в микросхеме флэш-памяти, которая находится на материнской плате. Вследствие ее заражения злоумышленники могут развернуть вредоносное ПО, которому не страшна переустановка системы и перезагрузка компьютера. Кроме того, такое вредоносное ПО может запросто оставаться невидимым для решений, предназначенных для защиты от вредоносных программ, поскольку большинство из них не выполняют сканирование такого уровня.

Модуль сканирования UEFI включается автоматически. Вы также можете запустить сканирование компьютера вручную в главном окне программы, последовательно открыв **Сканирование компьютера > Расширенное сканирование > Выборочное сканирование** и выбрав объект **Загрузочные секторы/UEFI**. Для получения дополнительных сведений о сканировании компьютера см. раздел [Сканирование компьютера](#).

Если ваш компьютер уже подвергся заражению вредоносным ПО для интерфейса UEFI, прочитайте следующую статью базы знаний ESET:

[My computer is infected with UEFI malware, what should I do? \(Мой компьютер заражен вредоносным ПО для интерфейса UEFI. Что делать?\)](#)