ESET Endpoint Security

Руководство пользователя

Щелкните здесь чтобы отобразить этого документа (онлайн-справка)

Digital Security
Progress. Protected.

Авторское право ©2023 ESET, spol. s r.o.

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

Дополнительные сведения можно получить на сайте https://www.eset.com.

Все права защищены. Ни одна часть этой документации не может воспроизводиться, храниться в системе получения и передаваться в любой форме или любыми средствами, в том числе электронными и механическими способами, с помощью фотокопирования, записи, сканирования, а также любыми другими способами без письменного разрешения автора.

ESET, spol. s r.o. оставляет за собой право изменять любое описанное прикладное программное обеспечение без предварительного уведомления.

Служба технической поддержки: https://support.eset.com

ПРОВ. 19.03.2023

1 ESET Endpoint Security 8 ... 1
1.1 Новые возможности в этой версии? ... 2
1.2 Требования к системе ... 3
1.2 Поддерживаемые языки ... 5
1.3 Профилактика ... 6
1.4 Страницы справочной системы ... 7
2 Документация по конечным точкам под удаленным управлением ... 9
2.1 Знакомство с ESET PROTECT ... 9
2.2 Знакомство с ESET PROTECT Cloud ... 11
2.3 Защищенные паролем параметры ... 12
2.4 Что такое политики ... 13
2.4 Объединение политик ... 14
2.5 Принцип действия флажков ... 14
3 Использование только продукта ESET Endpoint Security ... 16
3.1 Способ установки ... 16
3.1 Установка с помощью средства ESET AV Remover ... 17
3.1 ESET AV Remover ... 17
3.1 Ошибка во время удаления с помощью средства ESET AV Remover ... 20
3.1 Установка (.exe) ... 20
3.1 Изменение папки установки (.exe) ... 22
3.1 Установка (.msi) ... 23
3.1 Расширенная установка (.msi) ... 25
3.1 Установка с помощью командной строки ... 27
3.1 Развертывание с помощью GPO или SCCM ... 32
3.1 Обновление до новой версии ... 33
3.1 Автоматическое обновление устаревшей версии продукта ... 34
3.1 Обновления для обеспечения безопасности и стабильности ... 34
3.1 Распространенные проблемы, возникающие при установке ... 35
3.1 Сбой активации ... 35
3.2 Активация продукта ... 35
3.3 Сканирование компьютера ... 36
3.4 Руководство для начинающих ... 36
3.4 Пользовательский интерфейс ... 36
3.4 Настройка обновлений ... 40
3.4 Настройка зон ... 42
3.4 Инструменты контроля доступа в Интернет ... 43
4 Работа с ESET Endpoint Security ... 43
4.1 Компьютер ... 46
4.1 Модуль обнаружения ... 48
4.1 Модуль обнаружения расширенных параметров ... 54
4.1 Действия при обнаружении заражения ... 54
4.1 Общий локальный кэш ... 57
4.1 Защита файловой системы в режиме реального времени ... 57
4.1 Проверка модуля защиты в режиме реального времени ... 59
4.1 Момент изменения конфигурации защиты в режиме реального времени ... 60
4.1 Решение проблем, возникающих при работе защиты файловой системы в режиме реального времени ... 60
4.1 Сканирование компьютера ... 61
4.1 Средство запуска выборочного сканирования ... 63
4.1 Ход сканирования ... 65
4.1 Журнал сканирования компьютера ... 66

4.1 Процессы сканирования вредоносных программ ... 67
4.1 Сканирование в состоянии простоя ... 67
4.1 Профили сканирования ... 68
4.1 Объекты сканирования ... 69
4.1 Расширенные параметры сканирования ... 70
4.1 Контроль устройств ... 70
4.1 Редактор правил для контроля устройств ... 71
4.1 Обнаруженные устройства ... 72
4.1 Группы устройств ... 73
4.1 Добавление правил контроля устройств ... 74
4.1 Система предотвращения вторжений на узел ... 76
4.1 Интерактивное окно HIPS ... 79
4.1 Потенциальное поведение Программ-вымогателей обнаружено ... 80
4.1 Управление правилами HIPS ... 81
4.1 Параметры правил HIPS ... 82
4.1 Расширенные параметры HIPS ... 85
4.1 Драйверы, загрузка которых разрешена всегда ... 85
4.1 Режим презентации ... 85
4.1 Сканирование файлов, исполняемых при запуске системы ... 86
4.1 Автоматическая проверка файлов при запуске системы ... 87
4.1 Защита документов ... 88
4.1 Исключения ... 88
4.1 Исключения для быстродействия ... 89
4.1 Добавление или изменение исключений для быстродействия ... 90
4.1 Формат исключения пути ... 92
4.1 Исключения из обнаружения ... 92
4.1 Добавление или изменение исключений из обнаружения ... 95
4.1 Создание исключения из обнаружения мастера ... 96
4.1 Исключения (версия 7.1 или более ранняя) ... 97
4.1 Исключения для процессов ... 97
4.1 Добавление или изменение исключений процессов ... 98
4.1 Исключения системы HIPS ... 99
4.1 ThreatSense параметры ... 99
4.1 Уровни очистки ... 103
4.1 Исключенные из сканирования расширения файлов ... 104
4.1 Дополнительные параметры ThreatSense ... 105
4.2 Сеть ... 105
4.2 Файервол ... 107
4.2 Режим обучения ... 109
4.2 Защита от сетевых атак ... 110
4.2 Расширенные параметры фильтрации ... 111
4.2 Правила IDS ... 114
4.2 Блокировка возможной угрозы ... 115
4.2 Устранение неполадок защиты сети ... 116
4.2 Подключенные сети ... 116
4.2 Известные сети ... 117
4.2 Редактор известных сетей ... 118
4.2 Аутентификация сети: конфигурация сервера ... 121
4.2 Профили файервола ... 122
4.2 Профили, назначаемые сетевым адаптерам ... 122
4.2 Обнаружение изменения приложений ... 123

4.2 Приложения, исключенные из проверки ... 123
4.2 Настройка и использование правил ... 124
4.2 Список правил файервола ... 124
4.2 Добавление и изменение правил файервола ... 126
4.2 Правило файервола — локальный ... 127
4.2 Правило файервола — удаленный ... 128
4.2 Временный черный список IP-адресов ... 129
4.2 Доверенная зона ... 130
4.2 Настройка зон ... 130
4.2 Зоны файервола ... 130
4.2 Журнал файервола ... 131
4.2 Установка соединения: обнаружение ... 131
4.2 Решение проблем с файерволом ESET ... 133
4.2 Мастер устранения неполадок ... 133
4.2 Ведение журнала и создание правил и исключений на основе журнала ... 133
4.2 Создание правил на основе журнала ... 134
4.2 Создание исключений на основе уведомлений файервола ... 134
4.2 Расширенное ведение журналов для защиты сети ... 134
4.2 Решение проблем с фильтрацией протоколов ... 135
4.3 Интернет и электронная почта ... 136
4.3 Фильтрация протоколов ... 138
4.3 Исключенные приложения ... 139
4.3 Исключенные IP-адреса ... 140
4.3 SSL/TLS ... 140
4.3 Сертификаты ... 142
4.3 Зашифрованный сетевой трафик ... 143
4.3 Список известных сертификатов ... 143
4.3 Список приложений, отфильтрованных с помощью SSL/TLS ... 144
4.3 Защита почтового клиента ... 145
4.3 Протоколы электронной почты ... 147
4.3 Оповещения и предупреждения для сообщений электронной почты ... 148
4.3 Интеграция с почтовыми клиентами ... 149
4.3 Панель инструментов Microsoft Outlook ... 149
4.3 Панель инструментов Outlook Express и Почты Windows ... 150
4.3 Окно подтверждения ... 151
4.3 Повторно сканировать сообщения ... 151
4.3 Защита от спама ... 151
4.3 Адресные книги модуля защиты от спама ... 153
4.3 «Черный» список/«белый» список/список исключений ... 154
4.3 Добавление или изменение адреса в черном списке, белом списке или исключениях ... 155
4.3 защита доступа в Интернет; ... 156
4.3 Расширенные параметры настройки защиты доступа в Интернет ... 158
4.3 Веб-протоколы ... 158
4.3 Управление URL-адресами ... 159
4.3 Список URL-адресов ... 160
4.3 Создание списка URL-адресов ... 161
4.3 Как добавить маску URL-адреса ... 162
4.3 Защита от фишинга ... 163
4.3 Расширенные параметры защищенного браузера ... 165
4.3 Защищенные веб-сайты ... 165
4.4 Контроль доступа в Интернет ... 166

4.4 Правила контроля доступа в Интернет ... 167
4.4 Добавление правил контроля доступа в Интернет ... 168
4.4 Группы категорий ... 170
4.4 Группы URL-адресов ... 172
4.4 Настройка сообщений о блокировке веб-страницы ... 173
4.5 Обновление программы ... 175
4.5 Настройка обновлений ... 179
4.5 Откат обновления ... 183
4.5 Обновление компонентов программы ... 184
4.5 Параметры подключения ... 185
4.5 Зеркало обновлений ... 187
4.5 HTTP-сервер и SSL для зеркала ... 189
4.5 Обновление с зеркала ... 189
4.5 Устранение проблем при обновлении с зеркала ... 191
4.5 Создание задач обновления ... 192
4.6 Служебные программы ... 192
4.6 Файлы журналов ... 194
4.6 Фильтрация журнала ... 196
4.6 Настройка ведения журнала ... 198
4.6 Журналы аудита ... 199
4.6 Планировщик ... 200
4.6 Мониторинг ... 204
4.6 ESET SysInspector ... 205
4.6 Защита на основе облака ... 206
4.6 Фильтр «Исключение» для защиты на основе облака ... 210
4.6 Запущенные процессы ... 210
4.6 Отчет по безопасности ... 212
4.6 Сетевые подключения ... 213
4.6 ESET SysRescue Live ... 215
4.6 Отправка образцов на анализ ... 215
4.6 Выбор образца для анализа — подозрительный файл ... 217
4.6 Выбор образца для анализа — подозрительный сайт ... 217
4.6 Выбор образца для анализа — ложно обнаруженный файл ... 217
4.6 Выбор образца для анализа — ложно обнаруженный сайт ... 218
4.6 Выбор образца для анализа — другое ... 218
4.6 Оповещения ... 218
4.6 Уведомления приложения ... 220
4.6 Уведомления на рабочем столе ... 221
4.6 Уведомления по электронной почте ... 222
4.6 Настройка уведомлений ... 225
4.6 Карантин ... 225
4.6 Настройка прокси-сервера ... 227
4.6 Временные интервалы ... 229
4.6 Центр обновления Microsoft Windows® ... 229
4.6 Проверка лицензии с интервалом ... 230
4.7 Интерфейс ... 230
4.7 Элементы интерфейса пользователя ... 231
4.7 Состояния приложения ... 232
4.7 Настройка доступа ... 233
4.7 Пароль для доступа к расширенным параметрам ... 234
4.7 Окна предупреждений и сообщений ... 235

4.7 Интерактивные предупреждения ... 237
4.7 Подтверждения ... 238
4.7 Ошибка «Конфликт дополнительных настроек» ... 240
4.7 Съемные носители ... 240
4.7 Требуется перезагрузка ... 241
4.7 Рекомендуется перезагрузка ... 243
4.7 Значок на панели задач ... 245
4.7 Контекстное меню ... 246
4.7 Справка и поддержка ... 246
4.7 О программе ESET Endpoint Security ... 247
4.7 Отправка данных о конфигурации системы ... 248
4.7 Служба технической поддержки ... 248
4.7 Диспетчер профилей ... 249
4.7 Сочетания клавиш ... 250
4.7 Диагностика ... 251
4.7 Сканер командной строки ... 252
4.7 ESET CMD ... 255
4.7 Сканирование в состоянии простоя ... 257
4.7 Импорт и экспорт параметров ... 258
4.7 Восстановление всех параметров по умолчанию ... 259
4.7 Восстановление всех параметров в этом разделе ... 259
4.7 При сохранении конфигурации произошла ошибка ... 259
4.7 Удаленный мониторинг и управление ... 260
4.7 Командная строка ERMM ... 260
4.7 Список команд ERMM JSON ... 262
4.7 получить состояние защиты ... 263
4.7 получить сведения о приложении ... 263
4.7 получить сведения о лицензии ... 266
4.7 получить журналы ... 266
4.7 получить состояние активации ... 267
4.7 получить сведения о сканировании ... 268
4.7 получить конфигурацию ... 269
4.7 получить состояние обновления ... 270
4.7 запуск сканирования ... 271
4.7 запуск активации ... 271
4.7 запуск деактивации ... 272
4.7 запуск обновления ... 273
4.7 настройка конфигурации ... 273
5 Часто задаваемые вопросы ... 274
5.1 Обновление ESET Endpoint Security ... 275
5.2 Активация ESET Endpoint Security ... 275
5.2 Ввод лицензионного ключа при активации ... 276
5.2 Вход в ESET Business Account ... 277
5.2 Использование устаревших учетных данных лицензии для активации более нового продукта ESET для конечных точек ... 277
5.3 Удаление вируса с компьютера ... 277
5.4 Разрешение обмена данными определенному приложению ... 278
5.5 Создание задачи в планировщике ... 279
5.5 Планирование еженедельного сканирования компьютера ... 280
5.6 Подключение ESET Endpoint Security к ESET PROTECT ... 280
5.6 Использование режима переопределения ... 281

5.6 Применение рекомендуемой политики для ESET Endpoint Security 283
5.7 Настройка зеркала 285
5.8 Как мне обновить свою систему до Windows 10, если у меня установлен продукт ESET Endpoint Security? 286
5.9 Активация удаленного мониторинга и управления 287
5.10 Блокировка загрузки файлов определенного типа из Интернета 289
5.11 Сведения о свертывании ESET Endpoint Security 290
5.12 Устранение ошибки «Не удалось перенаправить защищенный браузер на запрошенную веб-страницу» 291
6 Лицензионное соглашение с конечным пользователем 293
7 Политика конфиденциальности 302

ESET Endpoint Security 8

ESET Endpoint Security 8 представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Новейшая версия модуля сканирования ThreatSense® в сочетании со специализированными модулями файервола 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 8 — 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.

Решение ESET Endpoint Security 8 предназначено в первую очередь для рабочих станций в среде небольших предприятий.

В разделе Использование только продукта ESET Endpoint Security представлены справочные статьи с разделами и подразделами, в которых можно найти необходимые сведения, в том числе о загрузке, установке и активации.

Использование ESET Endpoint Security в сочетании с ESET PROTECT в среде предприятия позволяет с легкостью управлять любым количеством клиентских рабочих станций, применять политики и правила, отслеживать обнаруженные угрозы и удаленно настраивать клиенты с любого компьютера, подключенного к сети.

Раздел Часто задаваемые вопросы содержит ответы на некоторые из наиболее часто задаваемых вопросов и решения проблем пользователей.

Возможности и преимущества

Улучшенный интерфейс	Интерфейс в этой версии значительно улучшен и упрощен с учетом результатов тестирования на предмет удобства использования. Все формулировки и уведомления, присутствующие в графическом интерфейсе пользователя, были тщательно проанализированы, и теперь интерфейс поддерживает языки с написанием справа налево, например иврит и арабский. Интернет-справка теперь интегрирована в ESET Endpoint Security и содержит динамически обновляемые статьи по поддержке.

Защита от вирусов и шпионских программ	Упреждающее обнаружение и очистка большего количества известных и неизвестных вирусов, червей, троянских программ и руткитов. Метод расширенной эвристики идентифицирует даже раннее неизвестные вредоносные программы, обеспечивая защиту вашего компьютера от неизвестных угроз и нейтрализуя их до того, как они могут причинить какой-либо вред. Функции защиты доступа в Интернет и защиты от фишинга работают путем отслеживания обмена данными между веб-браузерами и удаленными серверами (в том числе SSL). Функция защиты почтового клиента обеспечивает контроль обмена сообщениями через протоколы POP3(S) и IMAP(S).
Регулярные обновления	Регулярное обновление модуля обнаружения (ранее известного, как база данных сигнатур вирусов) и программных модулей — лучший способ обеспечить максимальный уровень безопасности компьютера.
ESET LiveGrid® (репутация на основе облака)	Вы можете проверить репутацию запущенных процессов и файлов непосредственно с помощью ESET Endpoint Security.
Удаленное управление	ESET PROTECT или ESET Security Management Center дает возможность управлять продуктами ESET на рабочих станциях, серверах и мобильных устройствах в сетевой среде из одной центральной точки. С помощью веб-консоли ESET Security Management Center (веб-консоли ESMC) можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.
Защита от сетевых атак	Анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который расценивается как опасный, блокируется.
Контроль доступа в Интернет (только ESET Endpoint Security)	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.

Новые возможности в этой версии?

Для ESET Endpoint Security выпущена версия 8, доступная для скачивания.

Защищенный браузер

- защищает веб-браузер от других запущенных на компьютере процессов
- подход с нулевым доверием и предполагает, что компьютер или его возможности защиты нарушены или недостаточны, и не позволяет самовольно манипулировать пространством памяти браузера и, следовательно, содержимым окна браузера
- по умолчанию эта функция не активна, поэтому администраторы имеют достаточно времени для использования этой возможности в политиках безопасности

WMI и полное сканирование реестра

- улучшение сканирования реестра, которое позволяет обнаруживать и устранять вредоносные ссылки и опасное содержимое в любом месте реестра или репозитория WMI

- проверка может занять некоторое время; эти объекты сканирования необходимо выбирать для всех процессов сканирования по требованию, даже для профиля «глубокого» сканирования

Обновление компонентов микропрограммы (обновление компонентов)

- интеллектуальное решение, которое позволяет сократить до минимума обслуживание ESET Endpoint Security

- Обновление компонентов микропрограммы может ожидать перезагрузки неделями

- при этом не выполняется переустановка продукта со всеми недостатками, такими как отмена регистрации в системе во время процесса, включая передачу конфигурации

- загружается меньше данных (разностное обновление)

- идет с понятным или полностью убираемым напоминанием для пользователя и имеет совместимость с управляемыми сетями

Обновления для обеспечения безопасности и стабильности

- Обновления для обеспечения безопасности и стабильности будут автоматически распространяться на поддерживаемые версии (7.x и более новые). Такие обновления будут содержать только существенные изменения, которые будут задокументированы с абсолютной прозрачностью в журналах существенных изменений.

Эта версия содержит различные исправления ошибок и улучшения производительности.

Дополнительная информация о новых функциях ESET Endpoint Security и снимки экрана приведены в следующей статье базы знаний ESET:

- Новые возможности в ESET Endpoint Security версии 8.

Системные требования

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

Поддерживаемые процессоры:

Процессор Intel или AMD, 32-разрядный (x86) с набором инструкций SSE2 или 64-разрядный (x64), частотой 1 ГГц и выше

Операционные системы

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 с последними обновлениями Windows (по крайней мере KB4474419 и KB4490628)

Windows XP и Windows Vista больше не поддерживаются.

Регулярно обновляйте операционную систему.

Другое

• Операционная система и другое ПО, установленное на компьютере, должны соответствовать системным требованиям

• 0,3 ГБ свободной системной памяти (см. прим. 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. прим. 3)

• Две программы по защите от вирусов, работающие одновременно на одном устройстве, вызывают неизбежные конфликты системных ресурсов, например замедляют работу системы до нерабочего состояния.

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.

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.

Поддерживаемые языки

Продукт ESET Endpoint Security доступен для загрузки и установки на следующих языках.

Язык	Код языка	LCID
Английский (США)	en-US	1033
Арабский (Египет)	ar-EG	3073
Болгарский	bg-BG	1026
Китайский (упрощенное письмо)	zh-CN	2052
Китайский (традиционное письмо)	zh-TW	1028
Хорватский	hr-HR	1050
Чешский	cs-CZ	1029
Эстонский	et-EE	1061
Финский	fi-FI	1035
Французский (Франция)	fr-FR	1036
Французский (Канада)	fr-CA	3084
Немецкий (Германия)	de-DE	1031
Греческий	el-GR	1032
*Иврит	he-IL	1037
Венгерский	hu-HU	1038
* Индонезийский	id-ID	1057
Итальянский	it-IT	1040
Японский	ja-JP	1041
Казахский	kk-KZ	1087
Корейский	ko-KR	1042
*Латышский	lv-LV	1062
Литовский	lt-LT	1063
Nederlands	nl-NL	1043
Норвежский	nn-NO	1044
Польский	pl-PL	1045
Португальский (Бразилия)	pt-BR	1046
Румынский	ro-RO	1048
Русский	ru-RU	1049
Испанский (Чили)	es-CL	13322
Испанский (Испания)	es-ES	3082
Шведский (Швеция)	sv-SE	1053
Словацкий	sk-SK	1051
Словенский	sl-SI	1060
Тайский	th-TH	1054
Турецкий	tr-TR	1055

Язык	Код языка	LCID
Украинский (Украина)	uk-UA	1058
*Вьетнамский	vi-VN	1066

* Продукт ESET Endpoint Security доступен на этом языке, но онлайн-руководство пользователя на этом языке недоступно (выполняется перенаправление на английскую версию).

Чтобы изменить язык этого онлайн-руководства пользователя, используйте поле выбора языка (в верхнем правом углу).

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 удаленных 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.

Страницы справочной системы

Добро пожаловать в справочную систему ESET Endpoint Security. Представленная здесь информация ознакомит вас с программным продуктом и сделает использование компьютера более безопасным.

Начало работы

Перед началом работы с ESET Endpoint Security следует знать, что пользователи могут работать с самим продуктом или с использованием подключения через ESET Security Management Center. Также рекомендуется ознакомиться с различными типами обнаруженных угроз и удаленных атак, с которыми вы можете столкнуться при использовании компьютера.

См. сведения о новых возможностях, чтобы узнать о нововведениях в данной версии ESET Endpoint Security. Также к вашим услугам руководство по настройке и изменению основных параметров ESET Endpoint Security.

Использование страниц справочной системы ESET Endpoint

Security

Справочная система удобно разделена на главы и подразделы. Найти необходимую информацию можно, просматривая структуру справочной системы.

Чтобы получить дополнительную информацию о любом окне программы, нажмите клавишу **F1**. Откроется страница справки, содержащая информацию о текущем окне.

Осуществлять поиск в справочной системе можно по ключевому слову или путем ввода слов или фраз. Разница между этими двумя способами состоит в том, что ключевое слово, характеризующее содержимое справочной страницы, может отсутствовать в тексте этой страницы. Поиск по словам и фразам осуществляется в содержимом всех страниц. В результате отображаются все страницы, содержащие именно эти слова и фразы.

Для согласованности информации и во избежание путаницы в настоящем руководстве используется терминология, основанная на именах параметров программы ESET Endpoint Security. Кроме того, для выделения особо интересных или важных тем в настоящем документе использован единый набор символов.

Примечания содержат краткие сведения о наблюдениях. Вы можете пропускать их, однако в примечаниях содержится ценная информация, например сведения о конкретных функциях или ссылки на соответствующие материалы.

Эта информация требует вашего внимания, так что рекомендуем ее не пропускать. Обычно такая информация не является критически важной, однако она значима.

Это информация о том, что требует особого внимания и осторожности. Отметка «ВНИМАНИЕ!» используется для того, чтобы удержать вас от потенциально опасных ошибок. Прочитайте текст такого предупреждения и вникните в него, поскольку оно содержит сведения об исключительно важных системных настройках или о возможных угрозах.

Это образец использования или практический пример, помогающий понять, как можно использовать определенную функцию или компонент.

Условное обозначение	Значение
Жирный шрифт	Названия элементов интерфейса, например флажков или переключателей.
Курсив	Заполнители для предоставляемой вами информации. Например, если текст имя файла или путь указан с использованием курсива, это означает, что путь или имя файла должны ввести вы.
`Courier New`	Образцы кода или команд.
Гиперссылка	Обеспечивает простой и быстрый доступ к связанным разделам или внешним веб-страницам. Гиперссылки выделяются синим цветом и иногда подчеркиванием.
%ProgramFiles%	Системный каталог Windows, в котором хранятся программы, установленные в этой ОС.

Интернет-справка — основной источник справочных сведений. Если подключение к Интернету установлено, автоматически открывается последняя версия интерактивной справки.

Документация по конечным точкам под удаленным управлением

Продуктами ESET для бизнеса, а также решением ESET Endpoint Security на рабочих станциях, серверах и мобильных устройствах в сетевой среде можно управлять удаленно из одного центрального расположения. Системные администраторы, управляющие более чем 10 клиентскими рабочими станциями, могут развернуть одно из средств удаленного управления ESET, с помощью которых можно централизованно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.

Средства удаленного управления ESET

Решением ESET Endpoint Security можно управлять удаленно с помощью ESET Security Management Center или ESET Cloud Administrator.

- Знакомство с ESET PROTECT
- Знакомство с ESET PROTECT Cloud

Сторонние средства удаленного управления

- Удаленный мониторинг и управление (RMM)

Рекомендации

- Подключите все конечные точки с решением ESET Endpoint Security к ESET PROTECT.
- Защитите расширенные параметры на подключенных клиентских компьютерах от несанкционированного изменения.
- Примените рекомендуемую политику, чтобы активировать доступные функции безопасности.
- Уменьшите количество элементов пользовательского интерфейса, чтобы ограничить возможности взаимодействия пользователя с ESET Endpoint Security

Практические руководства

- Использование режима переопределения
- Развертывание ESET Endpoint Security с помощью GPO или SCCM

Знакомство с ESET PROTECT

ESET PROTECT дает возможность управлять продуктами ESET на рабочих станциях, серверах и мобильных устройствах в сетевой среде из одного центрального расположения.

С помощью веб-консоли ESET PROTECT можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и обнаружения, возникающие на удаленных компьютерах. Ознакомьтесь также с разделами Обзор архитектуры и элементов инфраструктуры ESET PROTECT, Начало работы с веб-консолью ESET PROTECT и Поддерживаемые среды подготовки рабочих столов.

ESET PROTECT состоит из следующих компонентов.

- Сервер ESET PROTECT. Сервер ESET PROTECT устанавливается на сервера под управлением Windows или Linux, а также в качестве виртуального устройства. Он управляет связью с агентами, собирает и сохраняет данные приложений в базе данных.

- Веб-консоль ESET PROTECT. Веб-консоль ESET PROTECT является основным интерфейсом, который позволяет управлять клиентскими компьютерами в вашей среде. В ней отображаются общие сведения о состоянии клиентов в сети, и ее можно использовать для удаленного развертывания решений ESET на неуправляемых компьютерах. После установки сервера ESET PROTECT (сервера) вы можете получить доступ к веб-консоли с помощью браузера. Если разрешить доступ к веб-серверу из Интернета, можно будет использовать ESET PROTECT практически в любом месте и на любом устройстве с подключением к Интернету.

- ESET Management Агент. Агент ESET Management облегчает обмен данными между сервером ESET PROTECT и клиентскими компьютерами. Агент должен быть установлен на клиентском компьютере, чтобы установить связь между этим компьютером и сервером ESET PROTECT. Поскольку он находится на клиентском компьютере и может хранить несколько сценариев безопасности, использование ESET Management значительно сокращает время реагирования на новые обнаружения. С помощью веб-консоли ESET PROTECT можно развернуть агент ESET Management на неуправляемых компьютерах, распознанных с помощью Active Directory или ESET RD Sensor. Можно также вручную установить агент ESET Management на клиентских компьютерах, если это необходимо.

- Rogue Detection Sensor. ESET PROTECT Rogue Detection (RD) Sensor обнаруживает неуправляемые компьютеры, присутствующие в сети, и отправляет сведения о них на сервер ESET PROTECT. Это позволяет легко добавлять новые клиентские компьютеры в защищенную сеть. Rogue Detection Sensor запоминает компьютеры, которые были обнаружены, и не будет отправлять одну и ту же информацию дважды.

- Прокси-сервер Apache HTTP. Это служба, которую можно использовать вместе с ESET PROTECT, чтобы:

  - Рассылать обновления на клиентские компьютеры и установочные пакеты — агенту ESET Management.

  - Пересылать данные с агентов ESET Management на сервер ESET PROTECT.

- Средство подключения для мобильных устройств — это компонент, позволяющий использовать средства управления мобильными устройствами в ESET PROTECT для управления мобильными устройствами (Android и iOS) и администрирования ESET Endpoint Security для Android.

- Виртуальное устройство ESET PROTECT — виртуальное устройство ESET PROTECT доступно для пользователей, которым требуется запустить ESET PROTECT в виртуализированной среде.

- Хост виртуального агента ESET PROTECT — компонент ESET PROTECT, который виртуализирует сущности агентов, позволяя управлять безагентными виртуальными машинами. Это решение обеспечивает автоматизацию, использование динамических групп и тот же уровень управления задачами, что и агент ESET Management на физических компьютерах. Виртуальный агент собирает информацию с виртуальных машин и передает ее на сервер ESET PROTECT.

- Средство «Зеркало». Это средство необходимо для автономного обновления модулей. Если у клиентских компьютеров нет подключения к Интернету и при этом им нужны обновления модулей, с помощью средства «Зеркало» можно загрузить файлы обновления с серверов обновления ESET и хранить эти файлы локально.

- ESET Remote Deployment Tool. Этот инструмент предназначен для развертывания комплексных пакетов, созданных в веб-консоли <%PRODUCT%>. Это удобный способ распространения агентов ESET Management с продуктом ESET на компьютерах по сети.

- ESET Business Account. Новый портал лицензирования для бизнес-продуктов ESET позволяет управлять своими лицензиями. См. раздел ESET Business Account этого документа, чтобы узнать больше об активации своего продукта, или см. ESET Business Account руководство пользователя, чтобы получить дополнительные сведения об использовании ESET Business Account. Если у вас уже есть имя пользователя и пароль, предоставленные компанией ESET и которые нужно преобразовать в лицензионный ключ, см. раздел Преобразование учетных данных устаревшей лицензии.

- ESET Enterprise Inspector (EEI) — это комплексная система обнаружения и реагирования конечных точек, которая включает в себя такие функции, как обнаружение инцидентов, управление инцидентами и реагированием, сбор данных, индикаторы обнаружения компромиссов, обнаружение аномалий, обнаружение поведения, нарушения политики.

С помощью веб-консоли ESET PROTECT можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.

> ℹ Дополнительные сведения см. в интерактивном руководстве пользователя ESET PROTECT.

Знакомство с ESET PROTECT Cloud

ESET PROTECT Cloud дает возможность управлять продуктами ESET на рабочих станциях и серверах в сетевой среде из одного центрального местоположения без необходимости использовать физический или виртуальный сервер, как в случае с ESET PROTECT или ESMC. С помощью веб-консоли ESET PROTECT Cloud можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.

- Дополнительные сведения см. в интерактивном руководстве пользователя ESET PROTECT Cloud

Защищенные паролем параметры

Чтобы обеспечить максимальную безопасность вашей системы, ESET Endpoint Security необходимо настроить правильно. Любые неквалифицированные изменения или настройки могут привести к снижению безопасности и уровня защиты клиента. Чтобы ограничить доступ пользователей к расширенным настройкам, администратор может защитить параметры паролем.

Администратор может создать политику защиты расширенных параметров паролем для ESET Endpoint Security на подключенных клиентских компьютерах. Чтобы создать новую политику, необходимо выполнить следующие действия.

1. В веб-консоли ESET PROTECT или ESMC щелкните **Политики** в главном меню слева.

2. Щелкните **Новая политика**.

3. Присвойте имя новой политике и дайте ей короткую характеристику. Нажмите кнопку **Продолжить**.

4. Из списка продуктов выберите **ESET Endpoint для Windows**.

5. Щелкните **Интерфейс пользователя** в списке **Параметры** и разверните **Настройку доступа**.

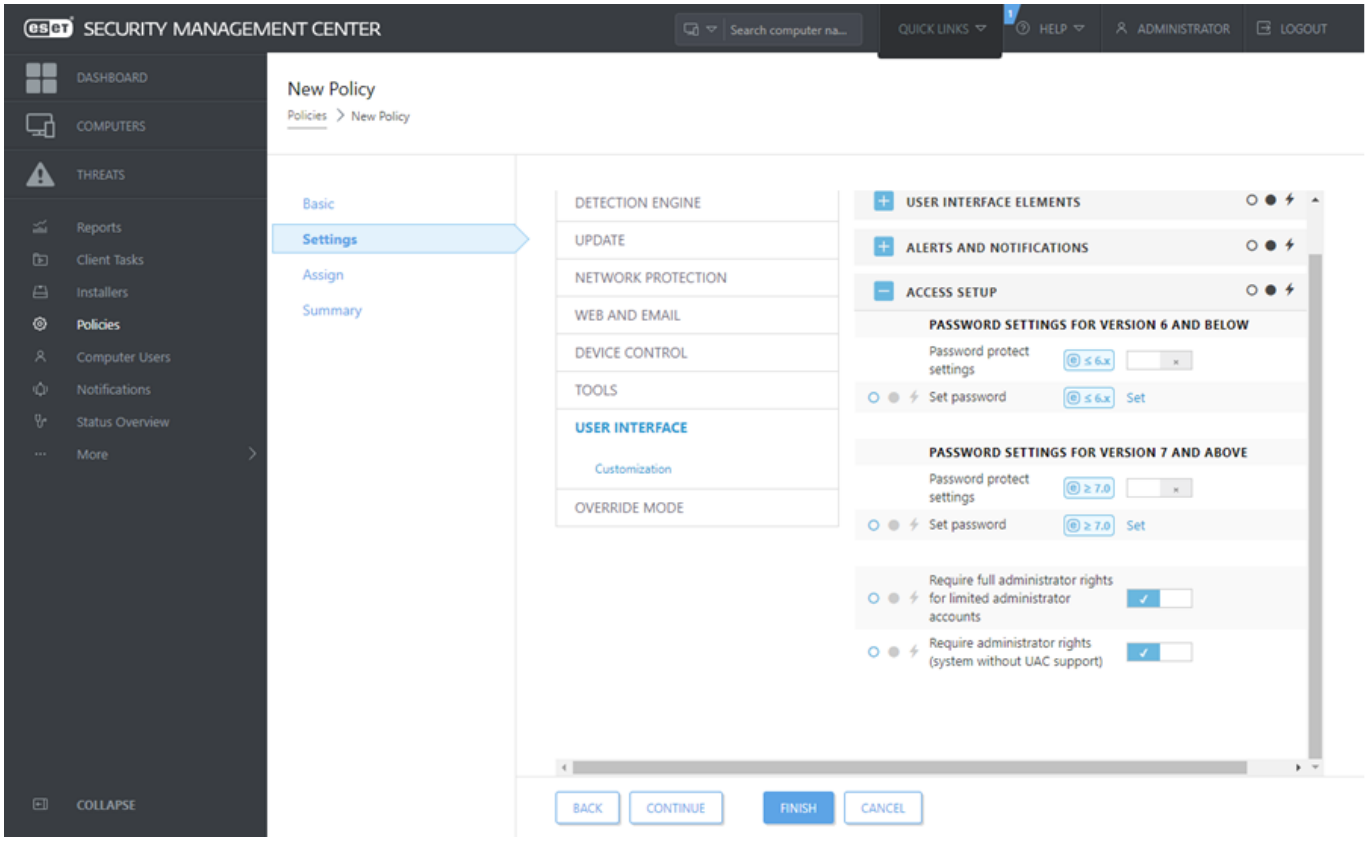
6. В соответствии с версией ESET Endpoint Security щелкните ползунок, чтобы включить **Пароль для защиты параметров**. Обратите внимание, что решения ESET Endpoint версии 7 предлагают расширенную защиту. Если в вашей сети есть версия 7 и версия 6 продуктов Endpoint, рекомендуем создать две отдельные политики с разными паролями для каждой версии.

7. В разделе всплывающего окна создайте новый пароль, подтвердите его и нажмите кнопку **OK**. Щелкните **Продолжить**.

8. Назначьте политику клиентам. Щелкните **Назначить** и выберите компьютеры или группы компьютеров для защиты паролем. Щелкните **OK**, чтобы подтвердить.

9. Убедитесь, что все целевые клиентские компьютеры находятся в целевом списке, и нажмите **Продолжить**.

10. Проверьте настройки политики в разделе «Сводка» и нажмите **Готово**, чтобы сохранить новую политику.



Что такое политики

Администратор может применять определенные конфигурации для продуктов ESET, работающих на клиентских компьютерах, используя политики из веб-консоли ESET PROTECT или ESMC. Политика может применяться непосредственно к отдельным компьютерам, а также к группам компьютеров. Кроме того, для компьютера или группы можно назначить несколько политик.

Пользователь должен иметь следующие разрешения для создания новой политики: **Чтение** — для чтения списка политик, **Использование** — для назначения политик целевым компьютерам и **Запись** — для создания, изменения или редактирования политик.

Политики применяются в том порядке, в котором расположены статические группы. Это не относится к динамическим группам, где политики сначала применяются к дочерним динамическим группам. Это позволяет применять политики с большим влиянием на верхние группы в иерархии и применять более конкретные политики для подгрупп. Используя флажки, ESET Endpoint Security пользователь, имеющий доступ к группам, расположенным выше в иерархии, может переопределить политики нижних групп. Алгоритм описан в Онлайн-справке ESET PROTECT.

> Рекомендуется назначать дополнительные общие политики (например, для сервера обновлений) группам, расположенным на вершине иерархии. Специализированные политики (касающиеся, например, контроля устройств) следует располагать ниже в иерархии групп. Это необходимо потому, что при объединении расположенная ниже политика обычно заменяет параметры расположенной выше политики (если иное не задано флажками политики).

Объединение политик

Политика, применяемая к клиенту, обычно является результатом объединения нескольких политик в одну окончательную. Политики объединяются одна за другой. При слиянии политик общее правило заключается в том, что более поздняя политика всегда заменяет настройки, установленные прежней. Чтобы изменить это поведение, можно использовать флажки политики (доступно для каждого параметра).

При создании политик вы заметите, что для некоторых параметров имеются дополнительные правила (заменить/присоединить/добавить), которые можно настроить.

- **Заменить**. Весь список заменяется, добавляются новые значения и удаляются все предыдущие.
- **Присоединить**. Элементы добавляются в нижнюю часть текущего списка (должна быть другая политика, локальный список всегда перезаписывается).
- **Добавить**. Элементы добавляются в верхнюю часть списка (локальный список перезаписывается).

ESET Endpoint Security поддерживает слияние локальных параметров с удаленными политиками по-новому. Если этот параметр представляет собой список (например, список заблокированных веб-сайтов), а удаленная политика конфликтует с существующим локальным параметром, удаленная политика перезаписывает его. Можно выбрать способ объединения локальных и удаленных списков, выбрав различные правила слияния.

- Настройки объединения для удаленных политик.
- Объединение удаленных и локальных политик. Локальные настройки можно получить в результате удаленной политики.

Дополнительные сведения о слиянии политик см. в интерактивном руководстве пользователя ESET PROTECT, а также в соответствующем примере.

Принцип действия флажков

Политика, применяемая на клиентском компьютере, обычно является результатом объединения нескольких политик в одну окончательную. При объединении политик можно настроить ожидаемое поведение конечной политики с помощью порядка применяемых политик, используя флажки политики. Флажки определяют, как политика будет обрабатывать определенный параметр.

Для каждого параметра можно выбрать один из следующих флажков.

Не применять	Любой параметр с этим флажком политикой игнорируется. Поскольку этот параметр не задан политикой, его можно изменить с помощью других политик, применяемых позже.

Применить	Параметры с флажком «**Применить**» будут применены к клиентскому компьютеру. Однако при слиянии политик он может быть перезаписан другими политиками, применяемыми позже. Когда политика передается на клиентский компьютер, содержащий параметры, отмеченные этим флажком, эти параметры изменят локальную конфигурацию клиентского компьютера. Поскольку для параметра не выбрано принудительное применение, его значение можно будет изменить другими политиками, применяемыми позже.
Принудительно применить	Настройки с флажком **Принудительно применить** имеют высший приоритет и не могут быть перезаписаны какой-либо политикой, примененной позже (даже если у нее также есть флажок **Принудительно применить**). Это гарантирует, что другие политики, примененные позже, не смогут изменить этот параметр при слиянии. Когда политика передается на клиентский компьютер, содержащий параметры, отмеченные этим флажком, эти параметры изменят локальную конфигурацию клиентского компьютера.

Сценарий. Администратору нужно разрешить пользователю *John* создавать или изменять политики в своей домашней группе, а также просматривать все политики, созданные Администратором, включаяПолитики, которые имеют флажки Применить принудительно. Администратор хочет, чтобы *John* мог просматривать все политики, но не редактировать существующие политики, созданные администратором. *John* может создавать или редактировать политики в своей домашней группе San Diego.
Решение. Администратор должен сделать следующее.
Создать настраиваемые статические группы и наборы разрешений
1. Создайте новую статическую группу с именем Санкт-Петербург.
2. Создайте новый набор разрешений с именем *Policy — All John* с доступом к статической группе *All* и с разрешением **Чтение** для объекта **Политики**.
3. Создайте новый набор разрешений с именем *Policy John* с доступом к статической группе *San Diego* и с разрешением доступа к функциональности **Запись** для объектов **Группы и компьютеры** и **Политики**. Этот набор разрешений позволяет пользователю *John* создавать или редактировать политики в своей домашней группе *San Diego*.
4. Создайте нового пользователя *John* и в разделе **Наборы разрешений** выберите *Policy — All John* и *Policy John*.
Создание политик
5. Создайте новую политику *All — Enable Firewall*, разверните раздел **Настройка**, выберите **ESET Endpoint для Windows**, выберите **Персональный файервол** > **Основная информация** и примените все настройки флажком **Применить принудительно**. Разверните раздел **Применить** и выберите статическую группу *All*.
6. Создайте новую политику *John Group — Enable Firewall*, разверните раздел **Настройка**, выберите **ESET Endpoint для Windows**, выберите **Персональный файервол** > **Основная информация** и примените все настройки флажком **Применить**. Разверните раздел **Применить** и выберите статическую группу *San Diego*.
Результат
Политики, созданные Администратором, будут применяться сначала, поскольку к параметрам политики были применены флажки **Применить принудительно**. Параметры с установленным этим флажком имеют приоритет и не могут быть перезаписаны другой политикой, применяемой позже. Политики, созданные пользователем *John*, будут применяться после политик, созданных Администратором. Чтобы увидеть окончательный порядок политик, перейдите в раздел **Дополнительно** > **Группы** > **SanDiego**. Щелкните компьютер и выберите **Показать подробности**. В разделе **Конфигурация** нажмите **Действующие политики**.

Использование только продукта ESET Endpoint Security

Эта часть руководства, как и раздел, посвященный работе с ESET Endpoint Security, предназначена для пользователей, использующих ESET Endpoint Security без ESET PROTECT, ESET Security Management Center или ESET PROTECT Cloud. Доступность тех или иных функций и возможностей ESET Endpoint Security полностью зависит от прав учетной записи пользователя.

Способ установки

Существует несколько методов установки ESET Endpoint Security версии 8.x на клиентской рабочей станции, если только вы не развертываете ESET Endpoint Security удаленно на клиентских рабочих станциях с помощью ESET PROTECT, ESET Security Management Center или ESET PROTECT Cloud.

- Установка или обновление ESET Endpoint Security до версии 6.6.x

Методы	Назначение	Ссылка для загрузки
Установка с помощью средства ESET AV Remover	Средство ESET AV Remover поможет удалить практически любую установленную в системе антивирусную программу, чтобы вы могли продолжить установку.	Загрузить 64-разрядную версию Загрузить 32-разрядную версию
*** Установка (.exe)	Процесс установки без ESET AV Remover.	N/A
Установка (.msi)	В бизнес-средах предпочтительнее использовать пакет установки MSI. В основном это связано с тем, что такая программа установки упрощает развертывание в автономном и удаленном режиме с помощью различных средств, например ESET Security Management Center.	Загрузить 64-разрядную версию Загрузить 32-разрядную версию
Установка с помощью командной строки	ESET Endpoint Security можно установить локально с помощью командной строки или удаленно с помощью клиентской задачи ESET PROTECT или ESET Security Management Center.	N/A
Развертывание с помощью GPO или SCCM	Используйте средства управления, например GPO или SCCM, чтобы развернуть ESET Management Agent и ESET Endpoint Security на клиентских рабочих станциях.	N/A
Развертывание с помощью средств RMM	С помощью плагинов ESET DEM для средства удаленного мониторинга и управления (RMM) можно развернуть ESET Endpoint Security на клиентских рабочих станциях.	N/A

Продукт ESET Endpoint Security предлагается на более чем 30 языках.

Установка с помощью средства ESET AV Remover

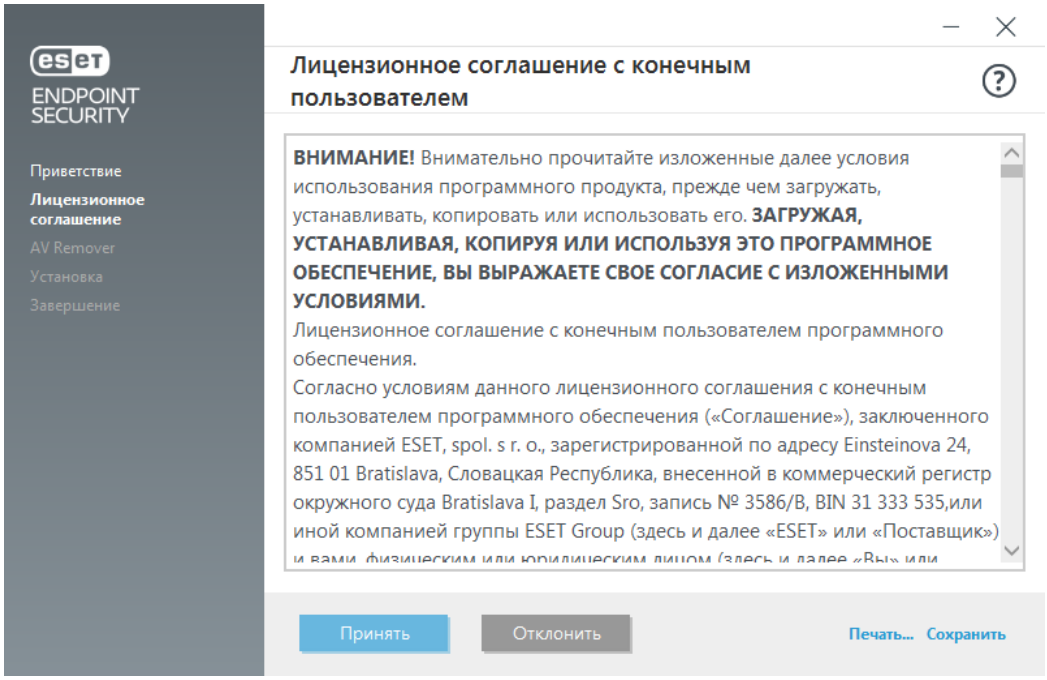
Прежде чем приступить к установке, необходимо удалить все установленные на компьютере приложения для обеспечения безопасности. Установите флажок **Я хочу удалить ненужные антивирусные программы с помощью средства ESET AV Remover**. Средство ESET AV Remover просканирует систему и удалит все поддерживаемые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

ESET AV Remover

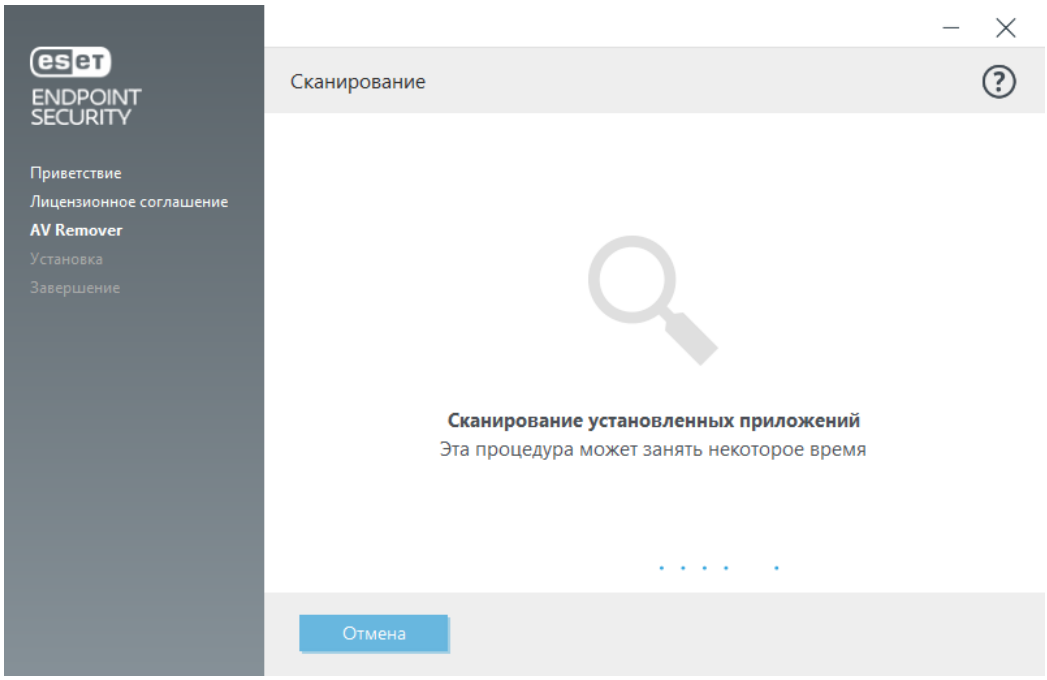
Средство ESET AV Remover поможет удалить практически любую установленную в системе антивирусную программу. Процедура удаления антивирусной программы с помощью средства ESET AV Remover приведена ниже.

1. Чтобы просмотреть список антивирусных программ, которые можно удалить с помощью ESET AV Remover, ознакомьтесь с соответствующей статьей базы знаний ESET.

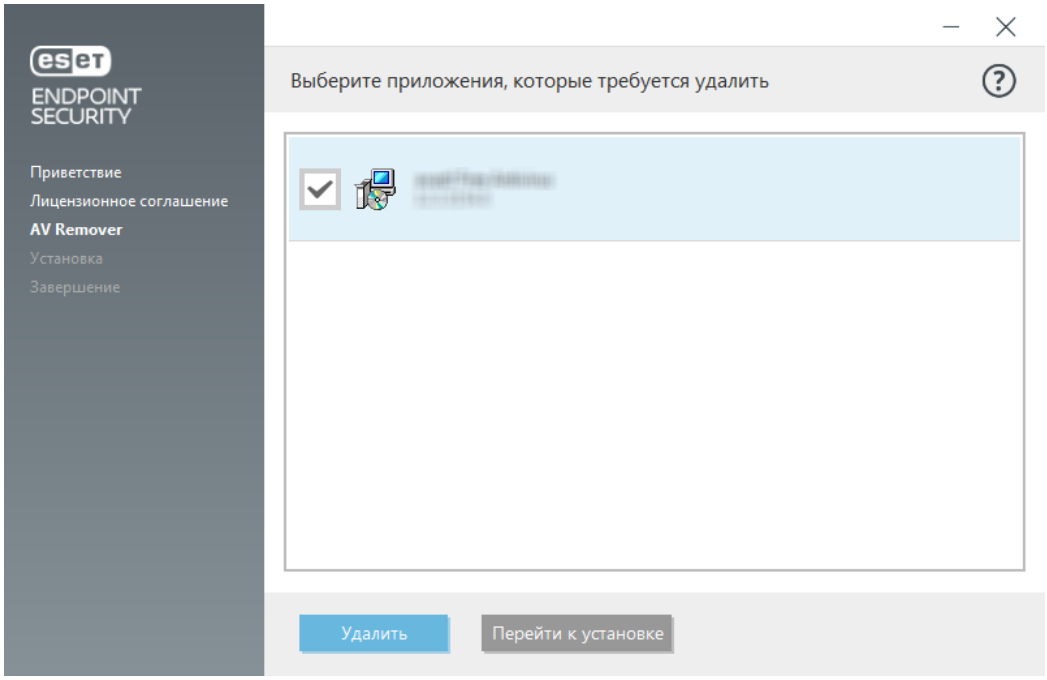
2. Прочтите лицензионное соглашение с конечным пользователем и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с его условиями. Нажав кнопку **Отклонить**, вы перейдете к установке ESET Endpoint Security. При этом уже установленное на компьютере приложение для обеспечения безопасности удалено не будет.



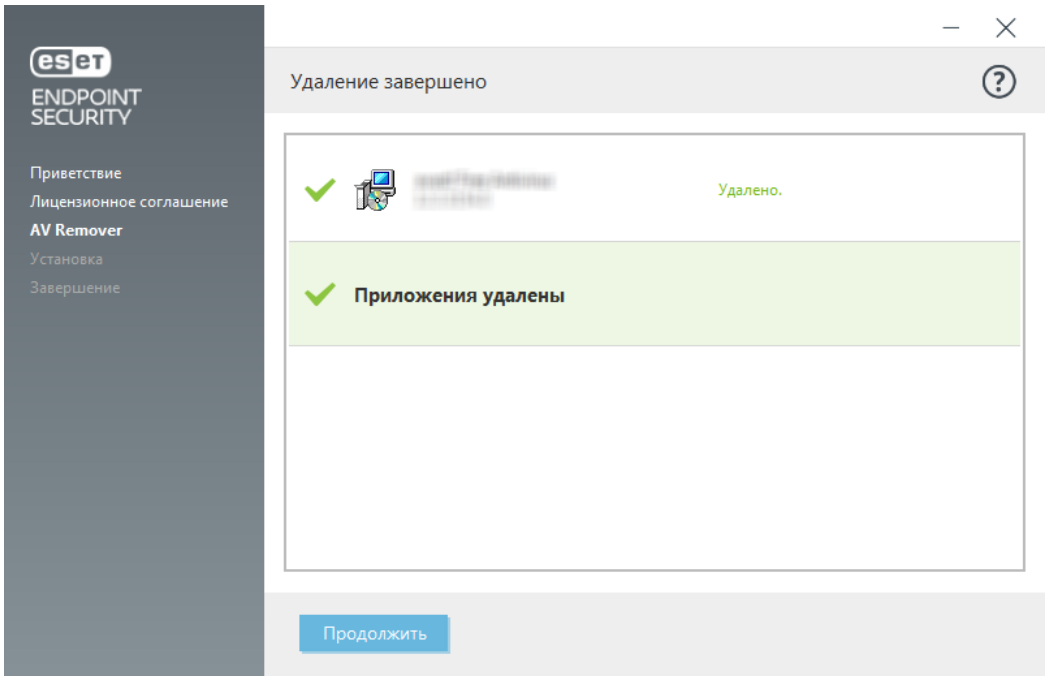
3. Средство ESET AV Remover начнет поиск установленного в системе антивирусного ПО.



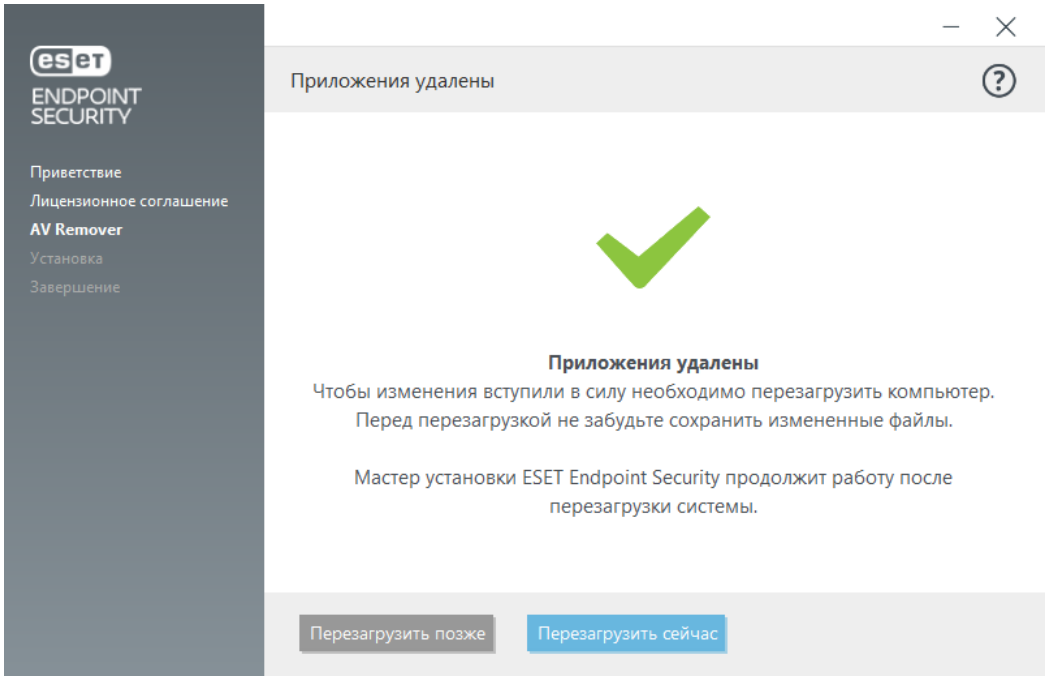
4. Выберите все обнаруженные приложения и нажмите кнопку **Удалить**. Процедура удаления может занять некоторое время.



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



6. Чтобы изменения вступили в силу и продолжить установку ESET Endpoint Security, перезагрузите компьютер. Если во время удаления произошла ошибка, см. раздел настоящего руководства Ошибка во время удаления с помощью средства ESET AV Remover.



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 распространенного антивирусного ПО для Windows. Эти списки можно найти в базе знаний ESET.

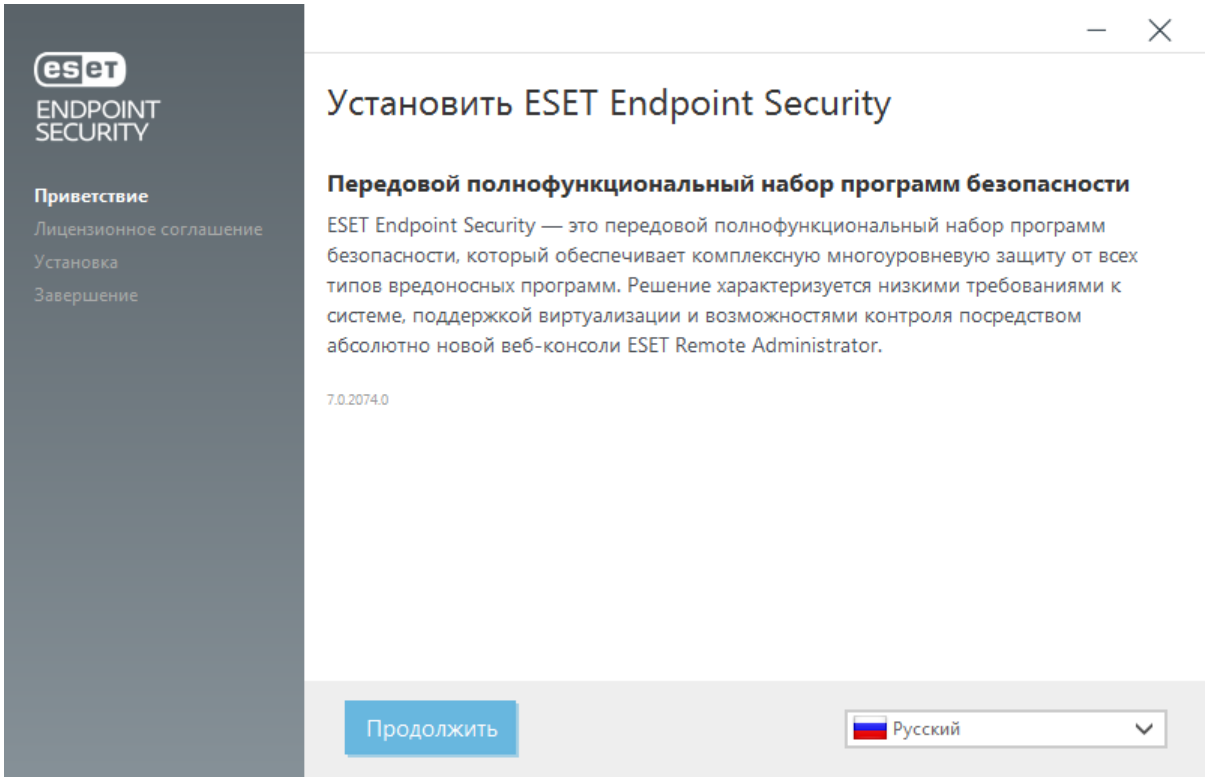
Если удалить продукт для обеспечения безопасности не удалось или некоторые из его компонентов были удалены частично, появится предложение **Перезагрузить компьютер и повторно выполнить сканирование**. После перезагрузки появится предупреждение системы контроля учетных записей. Разрешите запуск программы, повторно просканируйте систему и удалите имеющиеся антивирусные приложения.

В случае необходимости обратитесь в службу технической поддержки ESET, создайте запрос на обслуживание и приготовьте 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 технической поддержки ESET свяжутся с вами, как только появится возможность.

Установка (.exe)

После запуска EXE-файла мастер установки поможет установить программу.

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).

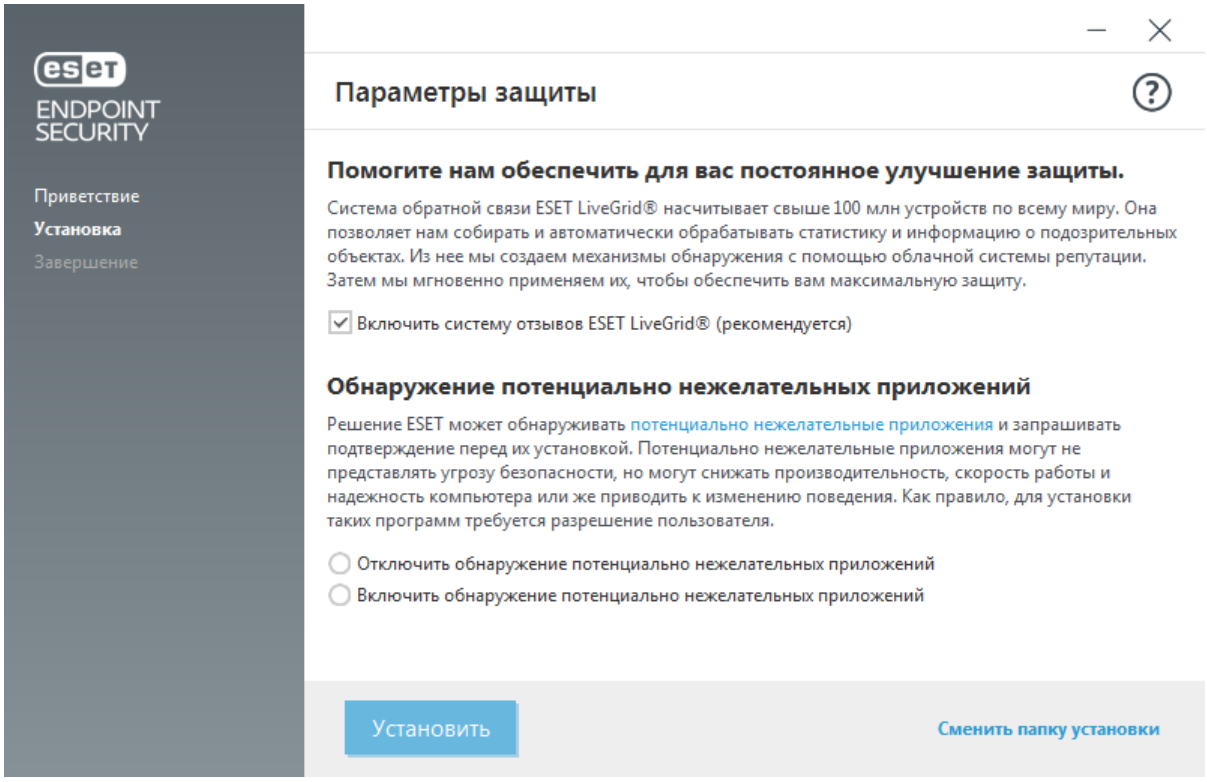


1. Прочтите Лицензионное соглашение и нажмите кнопку **Я принимаю**, чтобы подтвердить свое согласие с его условиями. Приняв условия, нажмите кнопку **Далее**, чтобы продолжить установку.

2. Выберите, следует ли включить систему обратной связи 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.

3. Следующий шаг установки: следует настроить обнаружение потенциально нежелательных приложений. Дополнительные сведения см. в главе Потенциально нежелательные приложения.

4. Последний шаг: подтверждение установки. Для этого нужно нажать **Установить**. Вы можете установить ESET Endpoint Security в определенную папку, нажав **Изменить папку установки**. После завершения установки отобразится запрос на активацию ESET Endpoint Security.



Изменение папки установки (.exe)

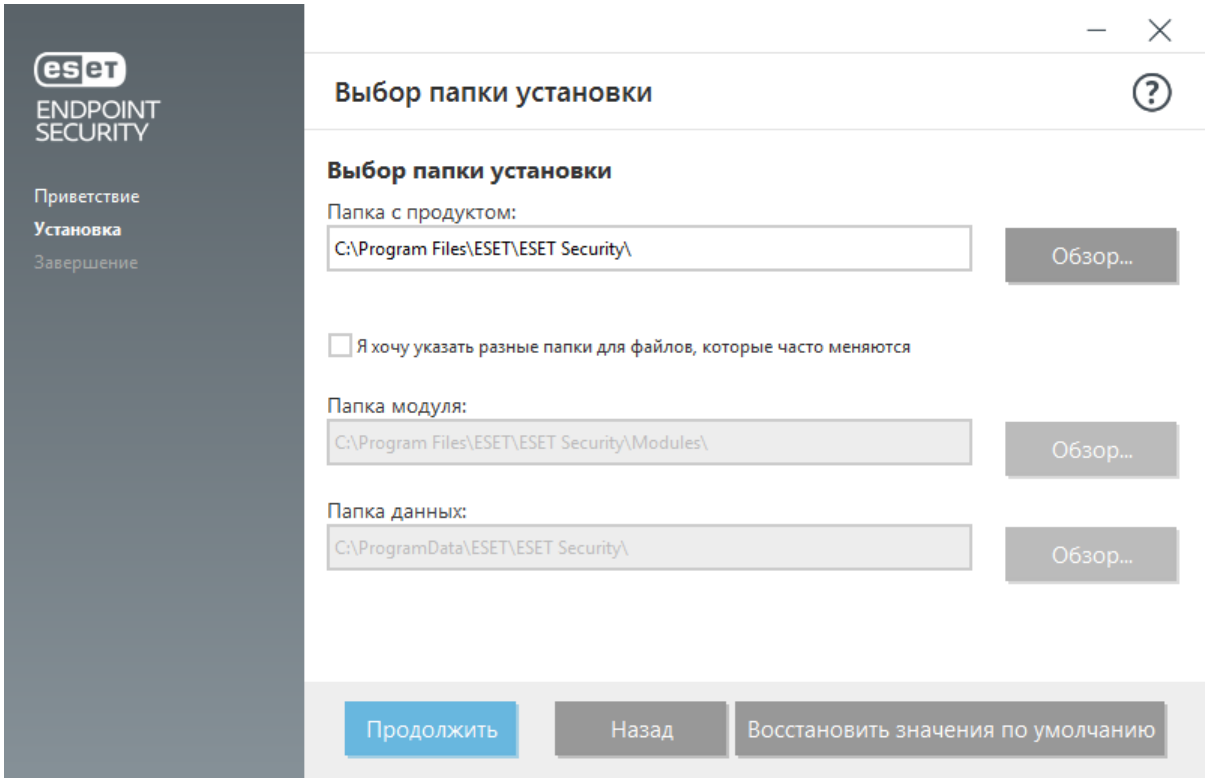
Когда вы включите обнаружение потенциально нежелательных приложений и нажмете **Изменить папку установки**, вам будет предложено выбрать расположение для папки установки продукта ESET Endpoint Security. По умолчанию программа устанавливается в указанную ниже папку.

C:\Program Files\ESET\ESET 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 Security\Modules
C:\ProgramData\ESET\ESET Security

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



Щелкните **Продолжить**, а затем — **Установить**, чтобы начать установку.

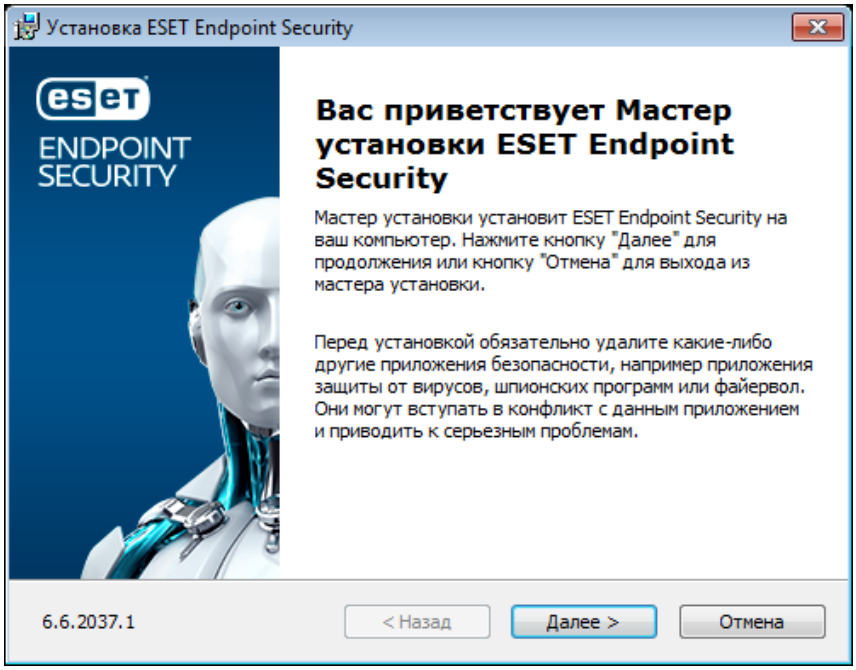
Установка (.msi)

После запуска MSI-файла мастер установки поможет установить программу.

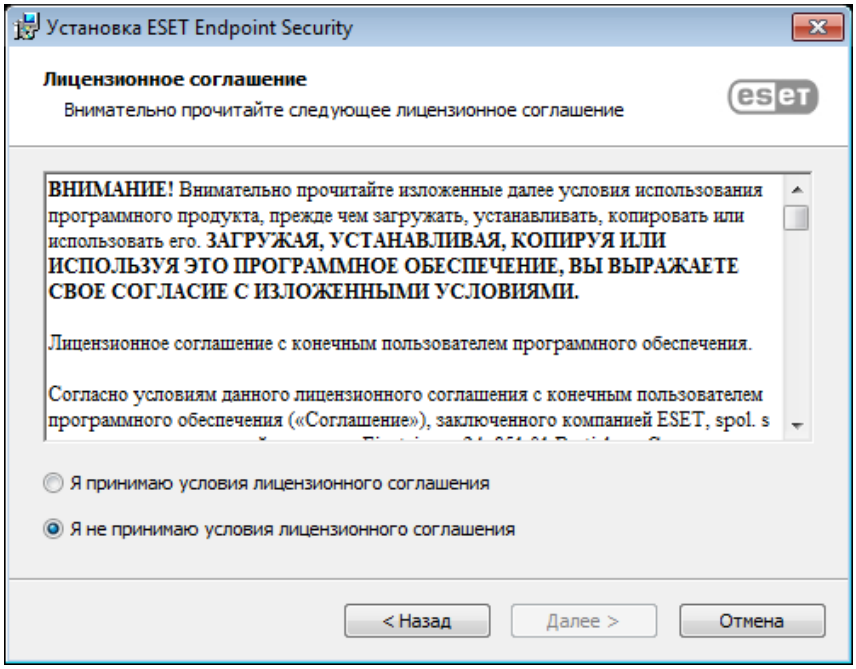
В бизнес-средах предпочтительнее использовать пакет установки MSI. В основном это связано с тем, что такая программа установки упрощает развертывание в автономном и удаленном режиме с помощью различных средств, например ESET Security Management Center.

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).

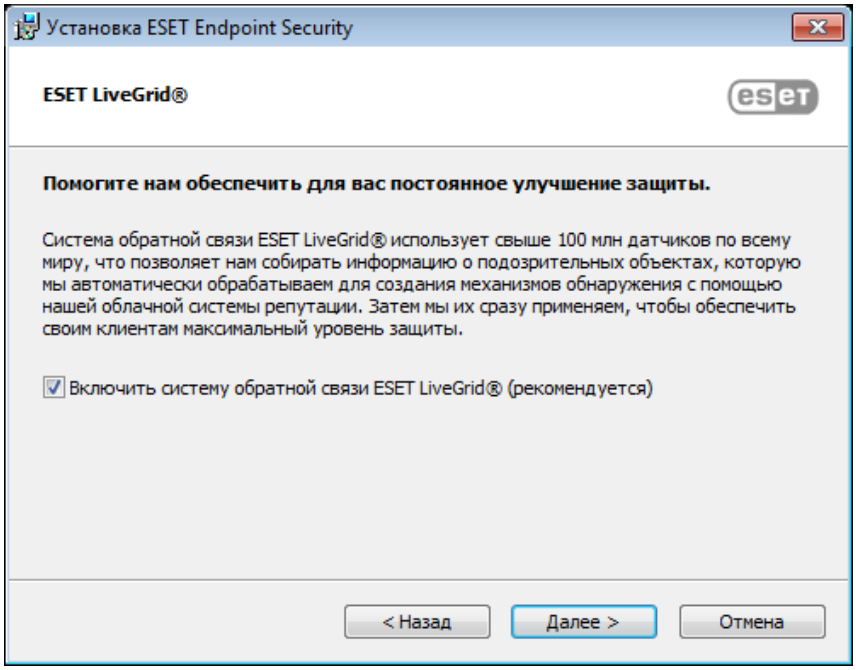
1. Выберите нужный язык и нажмите кнопку **Далее**.



2. Прочтите Лицензионное соглашение и нажмите кнопку **Я принимаю условия лицензионного соглашения**, чтобы подтвердить свое согласие с его условиями. Приняв условия, нажмите кнопку **Далее**, чтобы продолжить установку.

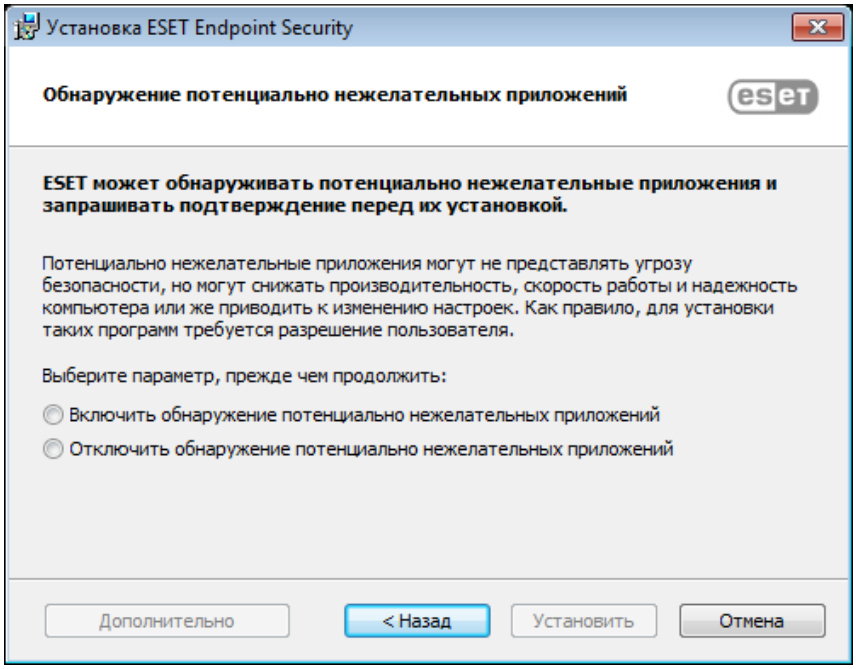


3. Настройте предпочтения для системы обратной связи ESET LiveGrid®. ESET LiveGrid® дает возможность незамедлительно и постоянно информировать компанию ESET о новых заражениях, благодаря чему мы можем защищать своих клиентов более качественно. С помощью этой системы вы можете отправлять новые угрозы в вирусную лабораторию ESET, где они анализируются, обрабатываются и добавляются в модуль обнаружения.



4. Следующий шаг установки: следует настроить обнаружение потенциально нежелательных приложений. Дополнительные сведения см. в главе Потенциально нежелательные приложения.

Нажмите кнопку **Дополнительные параметры**, чтобы выбрать пункт Расширенная установка (MSI).



5. Последний шаг: подтверждение установки. Для этого нужно нажать **Установить**. После завершения установки отобразится запрос на активацию ESET Endpoint Security.

Расширенная установка (.msi)

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

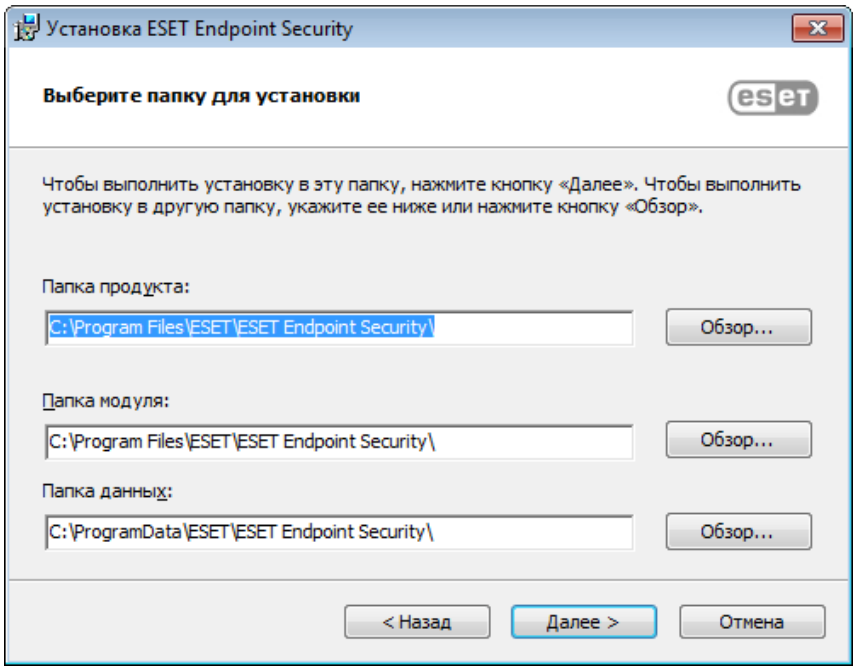
5. Когда вы включите обнаружение потенциально нежелательных приложений и нажмете **Дополнительные настройки**, вам будет предложено выбрать расположение для папки установки продукта ESET Endpoint Security. По умолчанию программа устанавливается в указанную ниже папку.

C:\Program Files\ESET\ESET Security

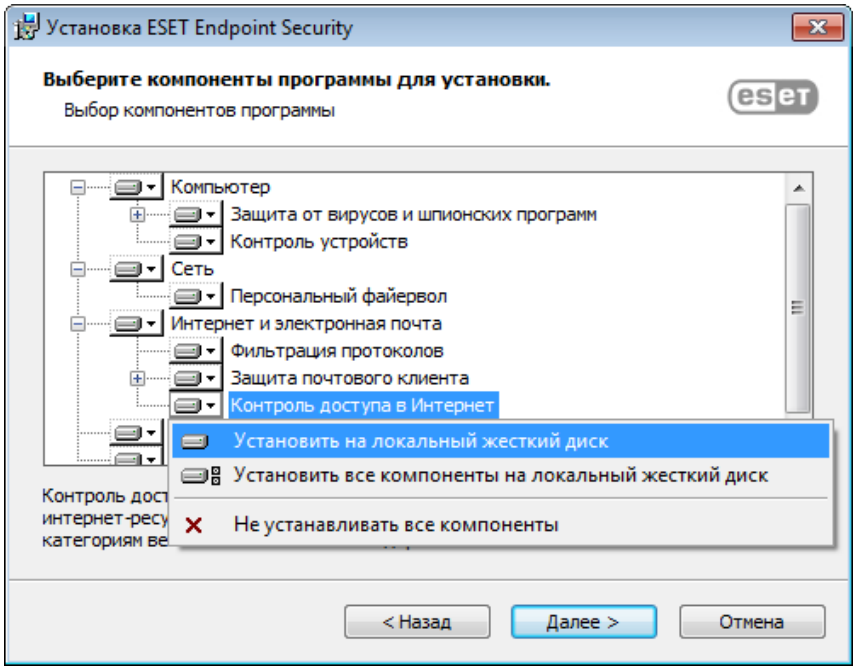
Можно указать расположение для модулей и данных программы. По умолчанию они устанавливаются в указанные ниже папки (в том же порядке):

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

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



6. Выберите компоненты продукта, которые следует установить. В разделе Компьютер находятся в том числе такие компоненты: защита файловой системы в реальном 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 файервол ESET, который отслеживает входящий и исходящий трафик и на основе правил работает с отдельными сетевыми подключениями. Файервол также обеспечивает защиту от атак с удаленных компьютеров. Компонент Защита от сетевых атак (IDS) анализирует сетевой трафик и защищает от сетевых атак. Любой трафик, который расценивается как опасный, блокируется. 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. Удаленный мониторинг и управление (RMM) — это процесс контроля систем программного обеспечения с помощью локально установленного агента, к которому может получать доступ поставщик службы управления.



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

Установка с помощью командной строки

ESET Endpoint Security Можно установить локально с помощью командной строки или удаленно с помощью клиентской задачи в ESET PROTECT или ESET Security Management Center.

Поддерживаемые параметры

APPDIR=<path>

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

APPDATADIR=<path>

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

MODULEDIR=<path>

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

ADDLOCAL=<list>

- Установка компонентов — список необязательных компонентов, которые нужно установить локально.
- Использование с пакетами .msi продуктов 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.

ADDEXCLUDE=<list>

• В списке ADDEXCLUDE через запятую перечислены имена всех компонентов, которые не следует устанавливать. Он используется в качестве замены устаревшему списку REMOVE.

• Если в этот список входит какой-либо компонент, который не следует устанавливать, то в список нужно явным образом добавить полный путь компонента (т.е. все его вложенные компоненты) и связанные невидимые компоненты.

• Использование с пакетами .msi продуктов ESET: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> i **ADDEXCLUDE** нельзя использовать вместе с **ADDLOCAL**.

Соответствующие параметры командной строки см. в документации для используемой версии **msiexec**.

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.

Компоненты и функции

> i ESET Endpoint Antivirus не поддерживает установку компонентов с помощью параметров ADDLOCAL/ADDEXCLUDE.

Функции разделены на 4 категории:

• **Обязательная**: функция всегда будет устанавливаться.

• **Необязательная**: с функции можно снять выделение, чтобы она не устанавливалась.

• **Невидимая**: логическая функция, необходимая для правильной работы других функций.

• **Заполнитель**: функция, которая никак не влияет на продукт и которую нужно указать с подчиненными функциями.

ESET Endpoint Security включает такой набор функций:

Описание	Имя функции	Родительский элемент функции	Наличие

Описание	Имя функции	Родительский элемент функции	Наличие
Базовые компоненты программы	Computer		Заполнитель
Модуль обнаружения	Antivirus	Computer	Обязательная
Модуль обнаружения/сканирование на наличие вредоносных программ	Scan	Computer	Обязательная
Модуль обнаружения/защита файловой системы в реальном времени	RealtimeProtection	Computer	Обязательная
Модуль обнаружения/сканирование на наличие вредоносных программ/защита документов	DocumentProtection	Antivirus	Необязательная
Контроль устройств	DeviceControl	Computer	Необязательная
Защита сети	Network		Заполнитель
Защита сети/файервол	Firewall	Network	Необязательная
Защита сети/защита от сетевых атак/...	IdsAndBotnetProtection	Network	Необязательная
Защищенный браузер	OnlinePaymentProtection	WebAndEmail	Необязательная
Интернет и электронная почта	WebAndEmail		Заполнитель
Интернет и электронная почта/фильтрация протоколов	ProtocolFiltering	WebAndEmail	Невидимая
Интернет и электронная почта/Защита доступа в Интернет	WebAccessProtection	WebAndEmail	Необязательная
Интернет и электронная почта/Защита почтового клиента	EmailClientProtection	WebAndEmail	Необязательная
Интернет и электронная почта/защита почтового клиента/почтовые клиенты	MailPlugins	EmailClientProtection	Невидимая
Интернет и электронная почта/Защита почтового клиента/Защита от спама	Antispam	EmailClientProtection	Необязательная
Интернет и электронная почта / контроль доступа в Интернет	WebControl	WebAndEmail	Необязательная
Средства/ESET RMM	Rmm		Необязательная
Обновление/профили/зеркало обновления	UpdateMirror		Необязательная
Плагин ESET Enterprise Inspector	EnterpriseInspector		Невидимая

Набор групповых функций:

Описание	Имя функции	Наличие функции
Все обязательные функции	_Base	Невидимая
Все доступные функции	ALL	Невидимая

Дополнительные правила

• Если для установки выбраны какие-либо из функций «**WebAndEmail**», в список нужно включить невидимую функцию «**ProtocolFiltering**».

• В именах всех функций учитывается регистр, например имя UpdateMirror не равнозначно UPDATEMIRROR.

Список свойств конфигурации

Свойство	Значение	Компонент
CFG_POTENTIALLYUNWANTED_ENABLED=	0 — отключено 1 — включено	Обнаружение потенциально нежелательных приложений
CFG_LIVEGRID_ENABLED=	См. ниже	См. свойство LiveGrid ниже
FIRSTSCAN_ENABLE=	0 — отключено 1 — включено	Запланируйте и выполните сканирование компьютера после установки
CFG_PROXY_ENABLED=	0 — отключено 1 — включено	Параметры прокси-сервера
CFG_PROXY_ADDRESS=	<ip>	IP-адрес прокси-сервера
CFG_PROXY_PORT=	<port>	Номер порта прокси-сервера
CFG_PROXY_USERNAME=	<username>	Имя пользователя для проверки подлинности
CFG_PROXY_PASSWORD=	<password>	Пароль для аутентификации
ACTIVATION_DATA=	См. ниже	Активация программы, лицензионный ключ или автономный файл лицензии
ACTIVATION_DLG_SUPPRESS=	0 — отключено 1 — включено	При значении «1» диалоговое окно активации программы не отображается при первом запуске
ADMINCFG=	<path>	Путь к экспортированному файлу конфигурации в формате XML (значение по умолчанию: *cfg.xml*)

Свойства конфигурации только в ESET Endpoint Security

CFG_EPFW_MODE=	0 — автоматически (по умолчанию) 1 — интерактивный режим 2 — на основе политики 3 — режим обучения	Режим фильтрации файервола
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Дата окончания режима обучения в виде метки времени Unix

Свойство LiveGrid®

При установке ESET Endpoint Security с `CFG_LIVEGRID_ENABLED`, продукт после установки будет работать следующим образом:

Компонент	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
Система репутации ESET LiveGrid®	Вкл.	Вкл.
Система отзывов ESET LiveGrid®	Выкл.	Вкл.
Отправить анонимную статистическую информацию	Выкл.	Вкл.

Свойство ACTIVATION_DATA

Формат	Методы
`ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`	Активация с помощью лицензионного ключа ESET (необходим доступ в Интернет)
`ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf`	Активация с помощью автономного файла лицензии

Свойства языка

Язык ESET Endpoint Security (нужно указать оба свойства).

Свойство	Значение
`PRODUCT_LANG=`	LCID Decimal (идентификатор языка в формате десятичного числа): например, языку «Английский (США)» соответствует значение 1033. См. список кодов языков.
`PRODUCT_LANG_CODE=`	LCID String (имя языка и культуры) строчными буквами: например, «en-us» означает «Английский (США)». См. список кодов языков.

Примеры установки с помощью командной строки

Прежде чем начинать установку, обязательно прочитайте лицензионное соглашение и убедитесь, что у вас есть права администратора.

Исключите раздел **NetworkProtection** из устанавливаемых компонентов (также укажите все дочерние компоненты):
`msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection`

Чтобы после установки продукта ESET Endpoint Security была произведена его автоматическая настройка, в команде установки можно указать основные параметры конфигурации.
Установите ESET Endpoint Security со включенной функцией ESET LiveGrid®:
`msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1`

Установите приложение в каталог, который отличается от каталога установки по умолчанию.
`msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\`

Установите и активируйте ESET Endpoint Security с помощью лицензионного ключа ESET.
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Автоматическая установка с ведением подробного журнала (полезно для устранения проблем) и только RMM с обязательными компонентами:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

Принудительная автоматическая полная установка с заданным языком.
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Параметры командной строки после установки

- ESET CMD: импорт файла конфигурации .xml или включение/выключение функции системы безопасности

- Модуль сканирования командной строки: запуск сканирования компьютера с помощью командной строки

Развертывание с помощью GPO или SCCM

Кроме прямой установки ESET Endpoint Security на клиентской рабочей станции или удаленного развертывания с помощью серверной задачи в ESMC, можно выполнить установку с помощью таких средств управления, как объект групповой политики (GPO), диспетчер конфигурации центра программного обеспечения (SCCM), Symantec Altiris или Puppet.

Управляемый (рекомендуется)

Если компьютер управляемый, сначала нужно установить ESET Management Agent, затем развернуть ESET Endpoint Security с помощью ESET Security Management Center (ESMC). В вашей сети должно быть установлено решение ESMC.

1. Загрузите автономный установщик для ESET Management Agent.

2. Подготовьте сценарий удаленного развертывания с помощью GPO/SCCM.

3. Разверните ESET Management Agent с помощью GPO или SCCM.

4. Убедитесь, что клиентские компьютеры добавлены в ESMC.

5. Разверните и активируйте ESET Endpoint Security на клиентских компьютерах.

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
- Разверните ESET Management Agent с помощью SCCM или GPO
- Развертывание агента ESET Management Agent с помощью объекта групповой политики (GPO)

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 с помощью ESET PROTECT, ESET Security Management Center (ESMC) или ESET PROTECT Cloud. Управлять приложением ESET Endpoint Security версии 8 с помощью ESET Remote Administrator нельзя.

2. Автоматически с помощью GPO или SCCM.

3. Автоматически путем обновления программы.
Поскольку обновления программы распространяются среди всех пользователей и могут повлиять на некоторые системные конфигурации, они выпускаются только после длительного тестирования с целью обеспечения бесперебойной работы на всех возможных конфигурациях. Чтобы перейти на новую версию сразу после ее выпуска, воспользуйтесь одним из перечисленных ниже способов.
Убедитесь, что включен параметр **Режим обновления** в разделе **Расширенные параметры** (F5) > **Обновление** > **Профили** > **Обновление компонентов программы**.

4. Вручную путем загрузки и установки новой версии поверх предыдущей.

Рекомендуемые сценарии обновления

Я управляю или желаю управлять продуктами ESET в удаленном режиме

Если вы управляете более чем 10 продуктами ESET для конечных точек, рекомендуем для установки обновлений использовать ESET PROTECT, ESET PROTECT Cloud или ESMC.

Ознакомьтесь со следующей документацией:

- ESET PROTECT | Обновление программного обеспечения ESET с помощью клиентской задачи
- ESET PROTECT | Руководство для предприятий малого и среднего бизнеса, которые имеют в управлении до 250 Windows-продуктов ESET для конечных точек
- Знакомство с ESET PROTECT Cloud

Обновление вручную на клиентской рабочей станции

Не устанавливайте версию 8 поверх версии 4.x. Аналогично, если у вас старый или неработающий продукт ESET Endpoint Security версии 5.x или 6.x.

Если вы планируете вручную устанавливать обновления на отдельных клиентских рабочих станциях:

1. Убедитесь, что ваша операционная система поддерживается Windows Vista и Windows XP не поддерживается для версии.

2. Загрузите и установите более новую версию поверх предыдущей.

Чтобы обновление до последней версии 8.x прошло максимально успешно, обновляйте одну из следующих версий ESET Endpoint Security:
- 5.0.2272.x
- 6.5.2132.x
- 7.3.2044.x

Если у вас другая версия продукта, то сначала удалите ESET Endpoint Security. Дополнительная информация об обновлении ESET Endpoint Security на клиентской рабочей станции приведена в этой статье базы знаний ESET.

Автоматическое обновление устаревшей версии продукта

Версия продукта ESET больше не поддерживается. Ваш продукт был обновлен до последней версии.

Распространенные проблемы, возникающие при установке

Каждая новая версия продуктов ESET содержит множество исправлений ошибок и улучшений. Имеющиеся клиенты с действующей лицензией для продукта ESET могут бесплатно перейти на последнюю версию того же продукта.

Чтобы завершить установку, выполните следующие действия.

1. Нажмите **Принять и продолжить**, чтобы принять лицензионное соглашение с конечным пользователем и подтвердить свое согласие с политикой конфиденциальности. Если вы не согласны с лицензионным соглашением, нажмите **Удалить**. Восстановить предыдущую версию невозможно.

2. Щелкните **Разрешить все и продолжить**, чтобы разрешить Систему обратной связи ESET LiveGrid®, или щелкните **Продолжить**, если вы не хотите участвовать.

3. После активации нового продукта ESET с помощью лицензионного ключа откроется домашняя страница. Если сведения о лицензии не найдены, вы сможете продолжить с новой лицензией на пробное использование. Если лицензия, используемая в предыдущем продукте, недействительна, активируйте продукт ESET.

4. Для завершения установки необходимо перезагрузить устройство.

Обновления для обеспечения безопасности и стабильности

Обновление ESET Endpoint Security — это важный аспект поддержания полной защиты от вредоносного кода. Каждая новая версия ESET Endpoint Security включает множество улучшений и исправлений ошибок. Настоятельно рекомендуется периодически обновлять ESET Endpoint Security, чтобы предотвратить появление уязвимостей и угроз безопасности. ESET Endpoint Security проходит определенные этапы жизненного цикла продукта, как любой другой продукт ESET. Ознакомьтесь более подробно с политикой относительно завершения срока службы (для бизнес-продуктов).

Дополнительные сведения об изменениях в ESET Endpoint Security см. в следующей статье базы знаний ESET.

> Функция автоматического обновления обеспечивает максимальную безопасность и стабильность вашего продукта. Вы не можете отключить обновление функций по обеспечению безопасности и стабильности.

Распространенные проблемы, возникающие при установке

Если при установке возникают проблемы, способ их решения можно найти в списке Распространенные ошибки, возникающие при установке, и способы их разрешения.

Сбой активации

Если активация ESET Endpoint Security была неуспешной, наиболее распространенные возможные сценарии приведены ниже.

- Лицензионный ключ уже используется.
- Недействительный лицензионный ключ. Ошибка в форме активации продукта.
- Дополнительная информация, необходимая для активации, отсутствует или неверна.
- Ошибка обмена данными с базой данных активации. Повторите попытку активации через 15 минут.
- Подключение к серверам активации ESET отсутствует или отключено

Убедитесь, что вы ввели правильный лицензионный ключ или подключили офлайн-лицензию, и повторите попытку активации.

Если вам не удается выполнить активацию, воспользуйтесь нашим пакетом начальной настройки, который содержит ответы на часто задаваемые вопросы, сведения об ошибках и способы решения проблем с активацией и лицензированием (доступен на английском и нескольких других языках).

- Запуск процесса устранения проблем с активацией программы ESET

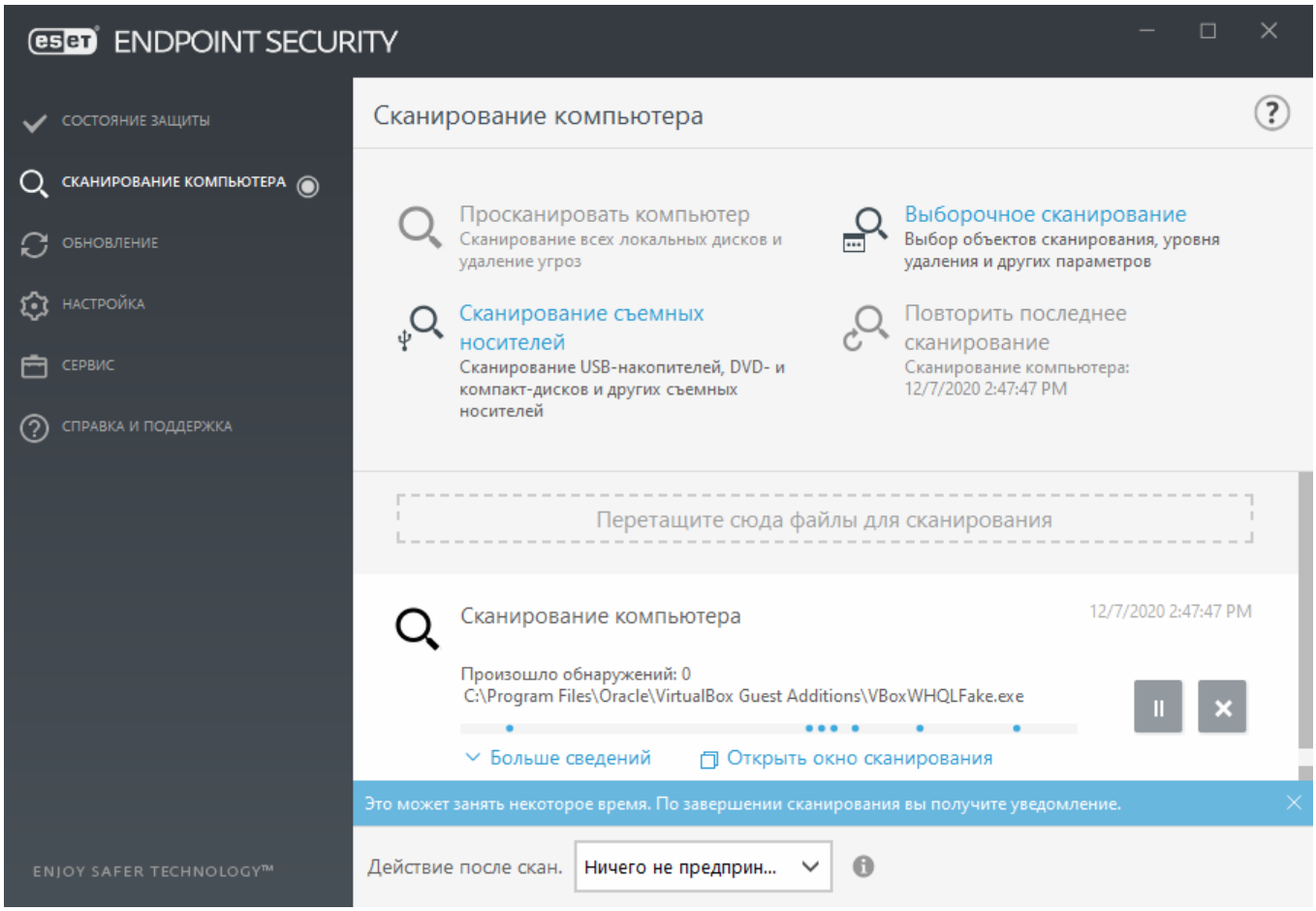
Активация программы

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.

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.



Руководство для начинающих

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

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

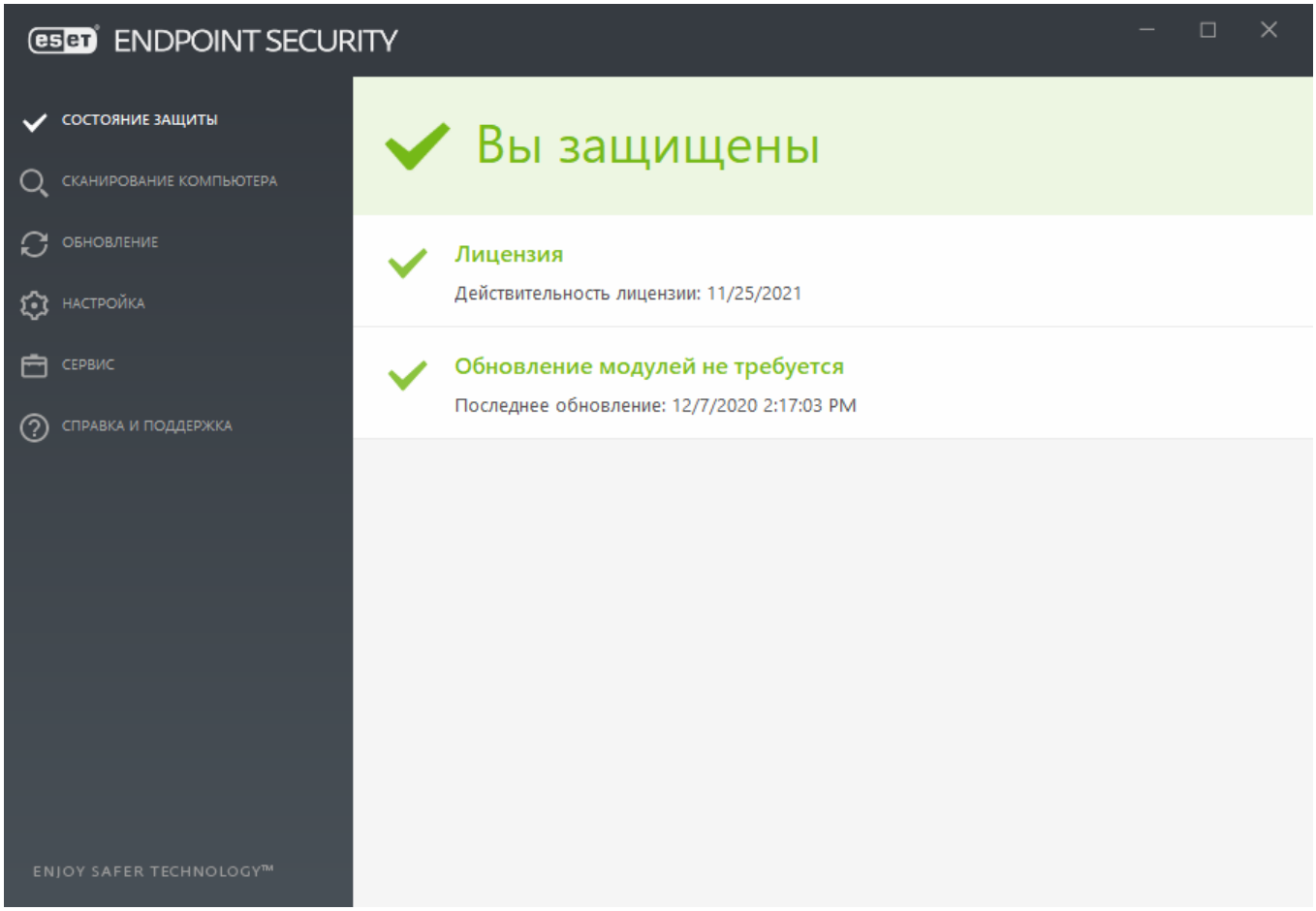
запустить последнюю операцию сканирования.

Обновление: отображение информации о модуле обнаружения и возможность проверки наличия обновлений вручную.

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 технической поддержки, средства поддержки и информацию об активации программы.

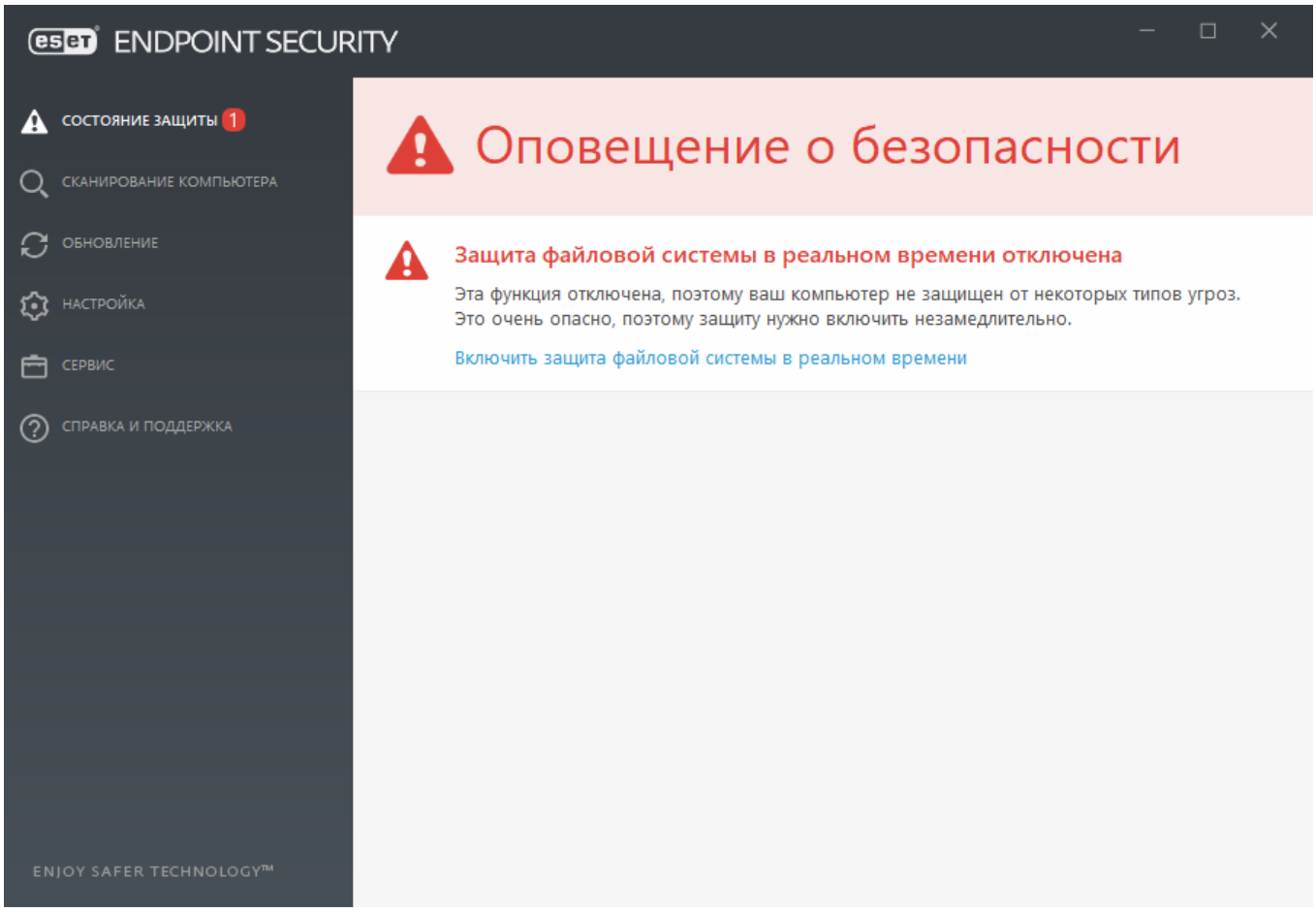


Окно **Состояние защиты** информирует пользователя об уровне безопасности и текущем уровне защиты компьютера. Зеленый значок **Максимальная защита** означает, что обеспечивается максимальная степень защиты.

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**: эта ошибка появляется после нескольких неудачных попыток обновить модуль обнаружения (ранее база данных сигнатур вирусов). Рекомендуется проверить параметры обновлений. Наиболее частая причина этой ошибки — неправильно введенные данные для аутентификации или неверно сконфигурированные параметры подключения.

• **Продукт не активирован**, или **Срок действия лицензии истек** — об этом сигнализирует красный значок состояния защиты. С этого момента программа больше не сможет выполнять обновления. Для продления лицензии следуйте инструкциям в окне предупреждения.

• **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.

• **Доступ к сети заблокирован** – отображается, если клиентское задание **Изолировать компьютер от сети** этой рабочей станции сработает от ESMC. Обратитесь к системному администратору, чтобы получить дополнительные сведения.

• **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 некритичной 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.

Чтобы настроить видимость состояния продуктов на первой панели ESET Endpoint Security, см. Состояния приложений.

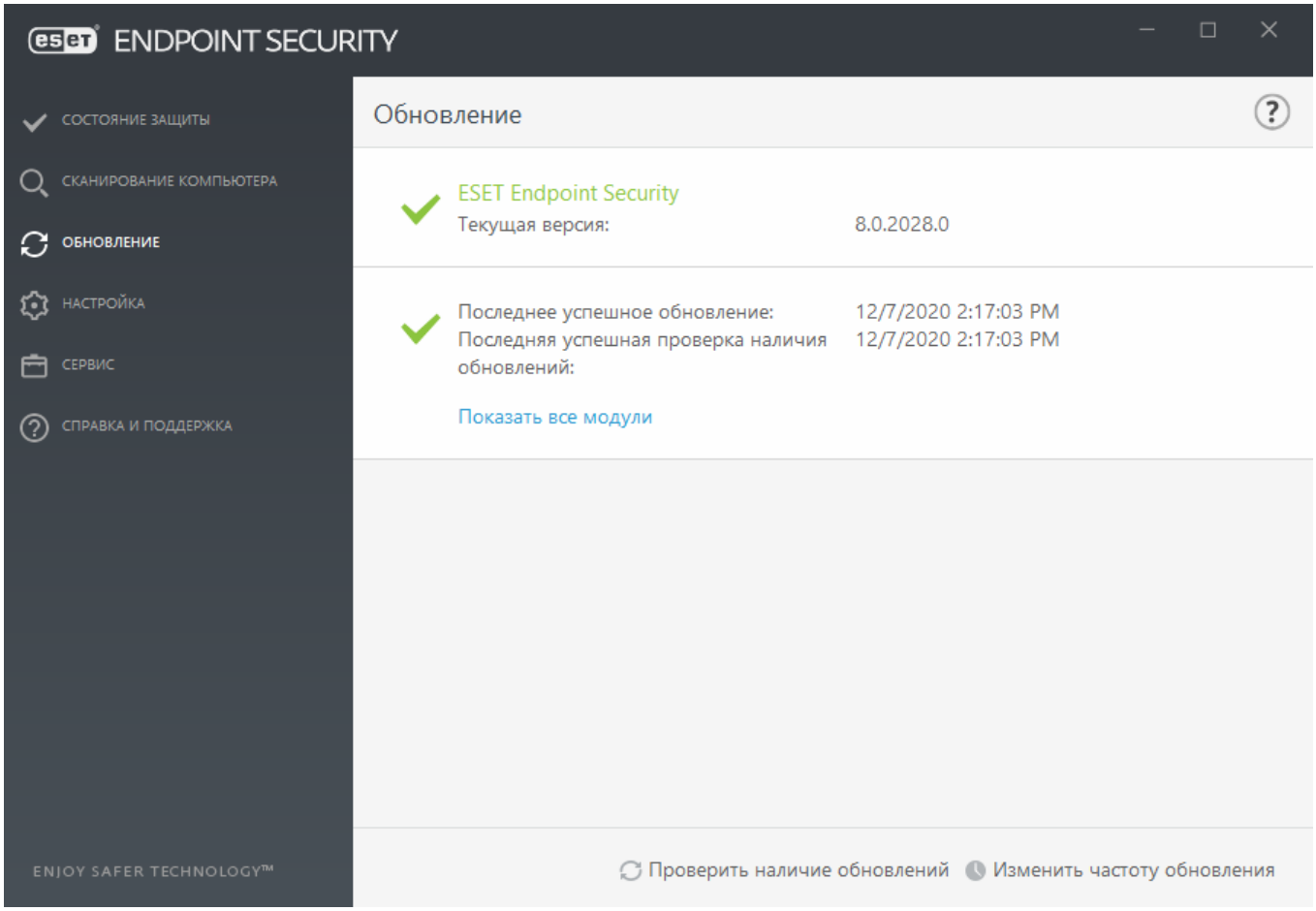
Если предложенные решения не позволяют устранить проблему, выберите пункт **Справка и поддержка** и просмотрите файлы справки или поищите нужную информацию в базе знаний ESET. Если вам по-прежнему нужна помощь, отправьте свой запрос в службу технической поддержки ESET. Ее специалисты оперативно ответят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

> i Если состояние относится к функции, заблокированной политикой ESMC или ESET PROTECT, ссылка будет неактивна.

Настройка обновлений

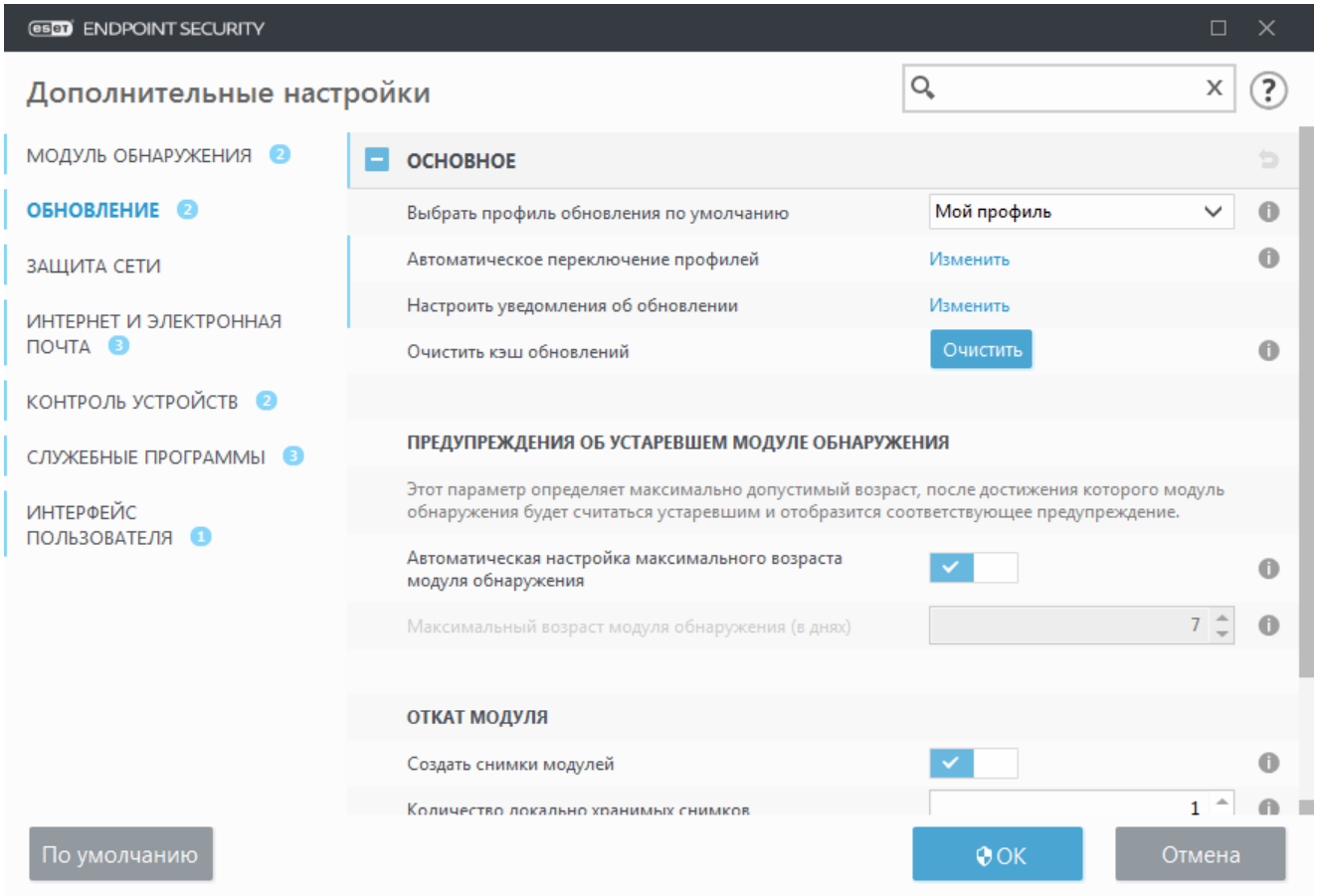
Обновление модулей является важной частью обеспечения полной защиты компьютера от вредоносного кода. Уделите особенное внимание изучению конфигурации и работы этого процесса. В главном меню выберите **Обновление** > **Проверить наличие обновлений**, чтобы проверить наличие обновлений модуля.

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



В окне «Расширенные параметры» (в главном меню выберите **Настройка** > **Расширенные параметры** 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 расширенных параметров пункт **Обновление**.

- Если при обновлении возникнут проблемы, щелкните **Очистить**, чтобы удалить временный кэш обновлений.



- Параметр **Выбирать автоматически** в разделе **Профили** > **Обновления** > **Обновления модулей** по умолчанию включен. Если для получения обновлений вы используете сервер обновлений ESET, рекомендуем не менять его значение.

- Если вы не хотите, чтобы при успешном выполнении обновления на панели задач в нижнем правом углу экрана появлялось уведомление, разверните элемент **Профили** > **Обновления**, щелкните **Изменить** возле пункта **Выбрать полученные уведомления об обновлении** и установите либо снимите флажки для уведомления **Модуль обнаружения успешно обновлен**.

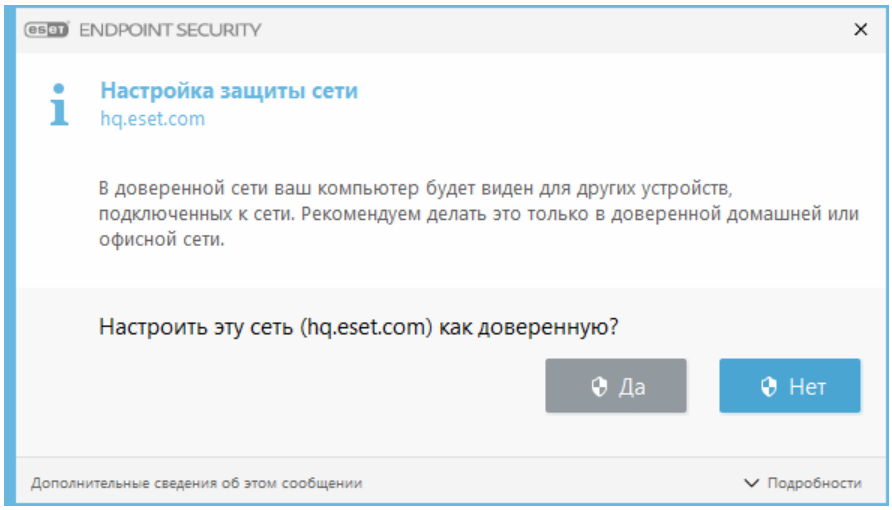
Для того чтобы использовать программу наилучшим образом, необходимо включить ее автоматическое обновление. Это возможно только в случае, если в разделе **Справка и поддержка** > **Активировать продукт** указан правильный **Лицензионный ключ**.

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**.

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 **Расширенные параметры** (F5) > **Защита сети** > **Файервол** > **Дополнительно** > **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.



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

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.

Дополнительные сведения об этой функции см. в статье базы знаний ESET:

- Обнаружено новое сетевое подключение ESET Endpoint Security

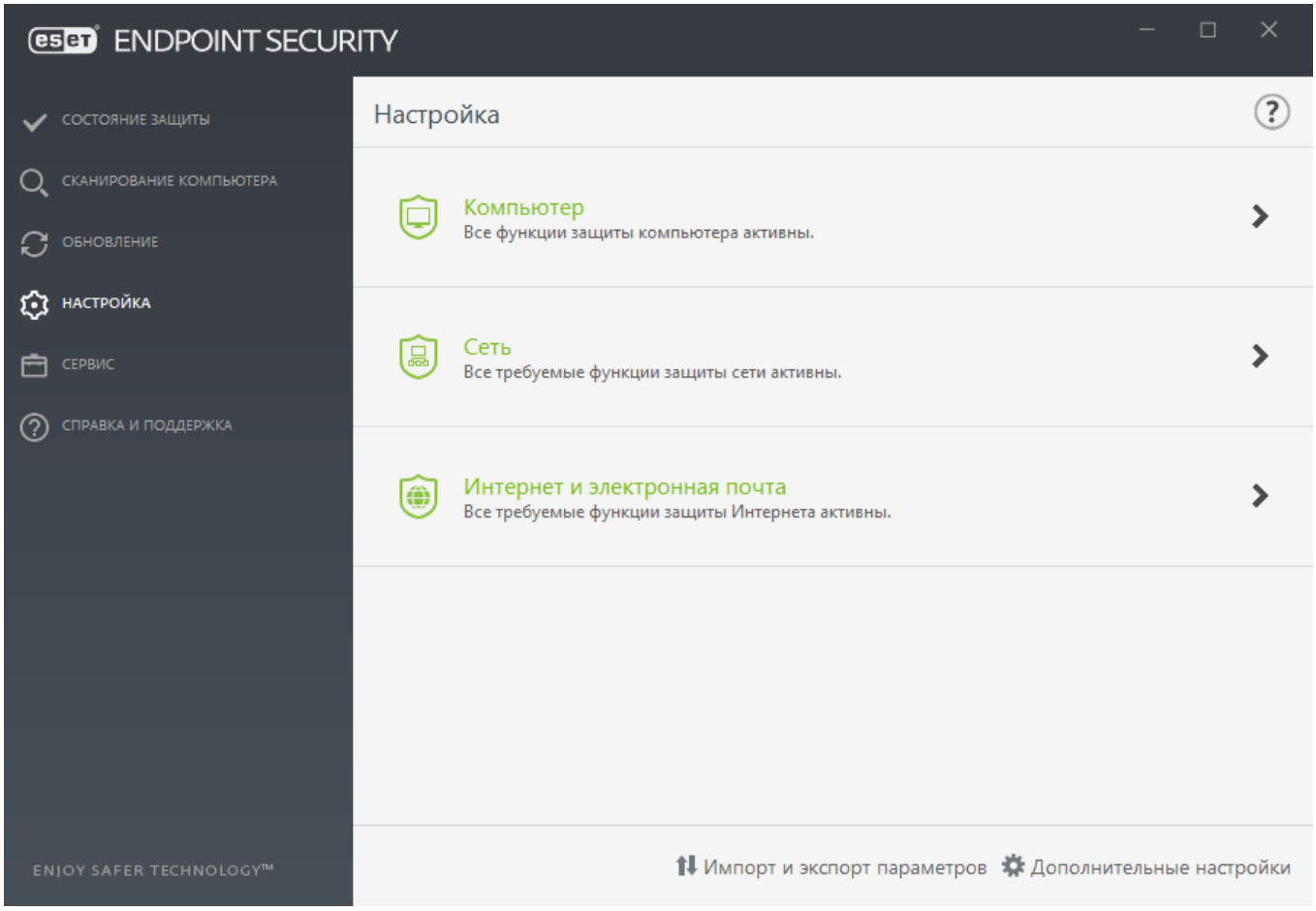
Инструменты контроля доступа в Интернет

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.

Работа с ESET Endpoint Security

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

При создании политики из веб-консоли ESET PROTECT или веб-консоли ESET Security Management Center можно выбрать флажок для каждого параметра. Параметры с флагом «Применить принудительно» 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 флажках в ESET PROTECT в Интернете.



Меню **Настройка** содержит следующие разделы.

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

В разделе Компьютер можно включать и отключать следующие компоненты:

- **Защита файловой системы в режиме реального времени**: при открытии, создании или исполнении файлов они сканируются на наличие вредоносного кода.
- **Контроль устройств**. Обеспечивает автоматическое управление устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). Этот модуль позволяет блокировать или изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним.

• **Host Intrusion Prevention System (HIPS)**: система предотвращения вторжений на узел (HIPS) отслеживает события, происходящие в операционной системе, и реагирует на них в соответствии с настраиваемым набором правил.

• **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-вымогателей**: это еще один уровень защиты, функционирующий как компонент системы HIPS. Для работы модуля защиты от программы-вымогателей необходимо, чтобы система репутации ESET LiveGrid® была включена. Дополнительная информация об этом типе защиты.

• **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.

Раздел **Защита сети** используется для конфигурации файервола, защиты от сетевых атак (IDS) и защиты от ботнетов.

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

• **Защищенный браузер**: защищает конфиденциальные данные при просмотре в Интернете (например, финансовые данные при финансовых операциях в Интернете).

• **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 ESET PROTECT/ESMC будет отображаться значок блокировки рядом с определенным компонентом. Политика, примененная решением ESET Security Management Center или ESET PROTECT, может быть переопределена локально после проверки подлинности пользователя, вошедшего в систему (например, администратора). Дополнительные сведения см. в справке о решении ESET PROTECT в Интернете.

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

Чтобы открыть подробные настройки определенного компонента безопасности, щелкните значок шестеренки рядом с любым компонентом.

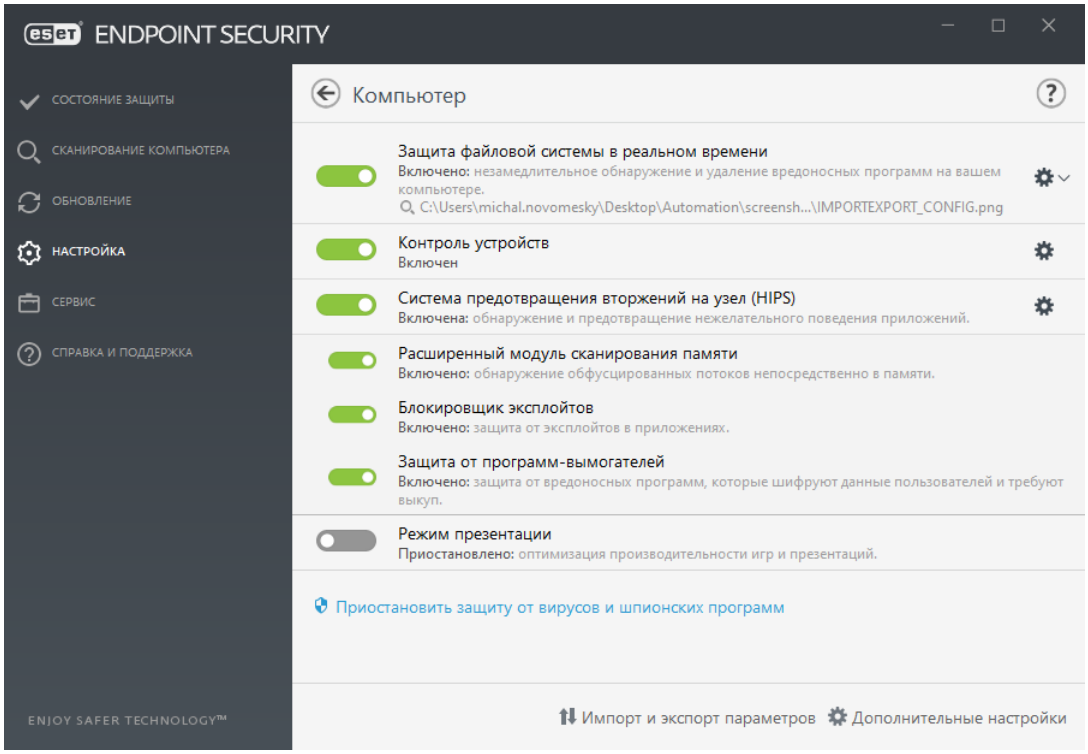
В нижней части окна настройки есть дополнительные параметры. Чтобы загрузить параметры настройки из файла конфигурации в формате *XML* или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией **Импорт и экспорт параметров**. Для получения дополнительных сведений см. раздел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

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

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 реальном времени**, затем выберите **Изменить исключения**. После этого откроется окно настроек исключения, в котором можно исключить файлы и папки из сканирования. Чтобы открыть расширенные параметры для элемента **Защита файловой системы в реальном времени**, щелкните **Настроить**.



В разделе **Компьютер** можно включать и отключать следующие компоненты:

• **Защита файловой системы в режиме реального времени**: при открытии, создании или исполнении файлов они сканируются на наличие вредоносного кода.

• **Контроль устройств**. Обеспечивает автоматическое управление устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). Этот модуль позволяет блокировать или изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним.

• **Host Intrusion Prevention System (HIPS)**: система предотвращения вторжений на узел (HIPS) отслеживает события, происходящие в операционной системе, и реагирует на них в соответствии с настраиваемым набором правил.

• **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-вымогателей**: это еще один уровень защиты, функционирующий как компонент системы HIPS. Для работы модуля защиты от программы-вымогателей необходимо, чтобы система репутации ESET LiveGrid® была включена. Дополнительная информация об этом типе защиты.

• **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.

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**.

Модуль обнаружения

Модуль обнаружения блокирует вредоносные атаки системы, контролируя информационное взаимодействие с помощью файлов, электронной почты, и Интернета. Например, при обнаружении объекта, который классифицируется как «вредоносная программа» начнется процесс исправления. Модуль обнаружения может устранить его, сначала заблокировав его, а затем очистив, удалив или переместив в карантин.

Для детальной настройки параметров модуля обнаружения щелкните элемент **Расширенные параметры** или нажмите клавишу **F5**.

В этом разделе:

- Защита в режиме реального времени и категории защиты машинного обучения
- Процессы сканирования вредоносных программ
- Настройка обнаружения
- Настройка защиты
- Рекомендации

> Начиная с версии 7.2, раздел «Модуль обнаружения» больше не оснащен переключателями ВКЛ/ВЫКЛ по сравнению с версией 7.1 и более ранней.. Кнопки ВКЛ/ВЫКЛ заменяются четырьмя пороговыми значениями — «Агрессивный», «Сбалансированный», «Осторожный» и «Отключено».

Защита в режиме реального времени и категории защиты машинного обучения

Защита в режиме реального времени и на основе машинного обучения для всех модулей защиты (например, защита файловой системы в режиме реального времени, защита веб-доступа и т. д.) позволяет настраивать уровни защиты и отчетности по следующим

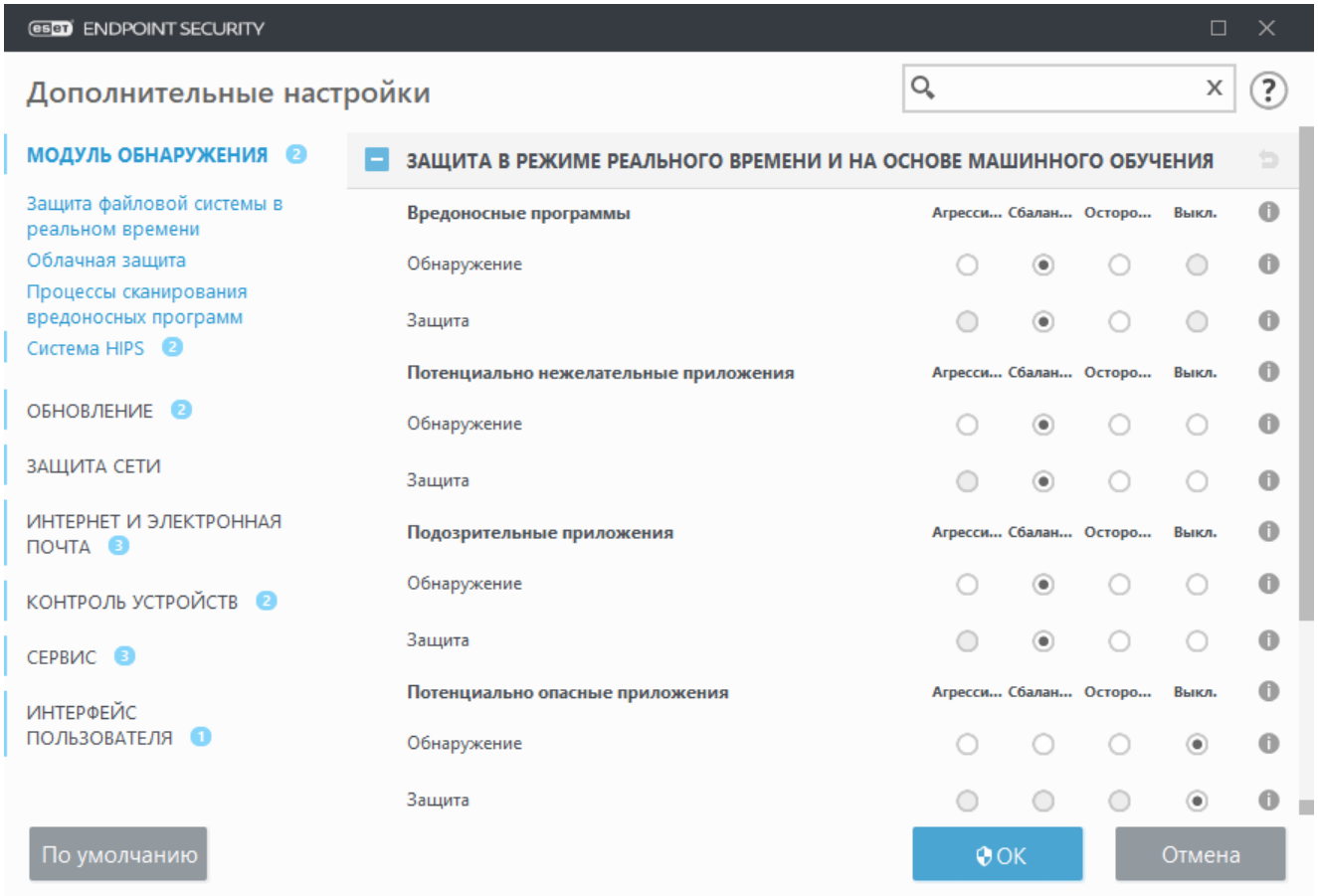
категориям:

- **Вредоносные программы**. Компьютерный вирус — это фрагмент вредоносного кода, который добавляется в начало или конец файлов на вашем компьютере. Тем не менее термин «вирус» часто используется не по назначению. Более точный термин — «вредоносная программа» («вредоносное ПО»). Обнаружение вредоносных программ осуществляется модулем обнаружения в сочетании с компонентом машинного обучения. Дополнительную информацию о приложениях этого типа см. в глоссарии.

- **Потенциально нежелательные приложения** . Потенциально нежелательные приложения представляют собой довольно широкую категорию программного обеспечения, задачей которого не является однозначно вредоносная деятельность в отличие от других типов вредоносных программ, например вирусов или троянских программ. Однако такое приложение может устанавливать дополнительное нежелательное программное обеспечение, изменять поведение цифрового устройства, а также выполнять действия без запроса или разрешения пользователя. Дополнительную информацию о приложениях этого типа см. в глоссарии.

- **Потенциально опасные приложения** . Определениеотносится 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). 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.



> Расширенное машинное обучение — это часть модуля обнаружения, которая является дополнительным уровнем защиты на основе машинного обучения, который улучшает работу функции обнаружения. Дополнительную информацию об этом типе защиты см. в глоссарии.

Процессы сканирования вредоносных программ

Параметры модуля сканирования можно настроить отдельно для сканера в режиме реального времени и для сканера по запросу. По умолчанию, **использование настроек защиты в режиме реального времени** включено. При включении этой функции соответствующие настройки сканирования по требованию происходят от раздела **Защита в режиме реального времени и на основе машинного обучения**.

Настройка обнаружения

При обнаружении (например, угроза обнаруживается и классифицируется, как вредоносная программа) информация передается в Журнал обнаружения и появляются Уведомления на рабочем столе, если они настроены в меню ESET Endpoint Security.

Пороговое значение обнаружения настраивается для каждой категории (далее — «КАТЕГОРИЯ»):

1. Вредоносные программы
2. Потенциально нежелательные приложения
3. Потенциально опасный
4. Подозрительные приложения

Создание отчетов выполняется с помощью модуля обнаружения, включая компонент машинного обучения. Можно установить более высокое пороговое значение отчетности по сравнению с текущим значением защиты. Эти настройки отчетности не влияют на блокировку, очищение или удаление объектов.

Перед изменением порогового значения (или уровня) отчетности для КАТЕГОРИИ ознакомьтесь со следующим:

Пороговое значение	Описание
Агрессивный	Функция обнаружения КАТЕГОРИИ настроена на максимальную чувствительность. Случаев обнаружения будет больше. При уровне **Агрессивный** функция может ошибочно считать объекты КАТЕГОРИЯМИ.

Пороговое значение	Описание
Сбалансированный	Установлен сбалансированный уровень функции обнаружения КАТЕГОРИИ. Эта настройка должна обеспечивать оптимальный баланс производительности, точности обнаружения и количества ложных обнаружений.
Осторожный	Уровень функции обнаружения КАТЕГОРИИ настроен таким образом, чтобы уменьшить количество ложных обнаружений, но при этом сохранить достаточный уровень защиты. Объекты считаются такими, только если их поведение явно соответствует поведению КАТЕГОРИИ.
Выкл.	Функция обнаружения для КАТЕГОРИИ не активна, и обнаружения такого рода не обнаруживаются, не регистрируются и не очищаются. В результате, данная настройка отключает защиту от этого типа обнаружения. Значение «Выкл» недоступно для оповещения о вредоносных программах и по умолчанию используется для потенциально опасных приложений.

Доступность модулей защиты ESET Endpoint Security

Доступность (включено или выключено) модуля защиты для выбранного порогового значения КАТЕГОРИИ выглядит следующим образом:

	Агрессивный	Сбалансированный	Осторожный	Викл**
Модуль расширенного машинного обучения*	✔ (агрессивный режим)	✔ (консервативный модуль)	X	X
Модуль обнаружения	✔	✔	✔	X
Другие модули защиты	✔	✔	✔	X

* Доступно в ESET Endpoint Security версии 7.2 и более поздних версиях.
** Не рекомендуется

Определение версии продукта, версий модуля программы и даты сборки

1. Щелкните элемент **Справка и поддержка** > **О продукте ESET Endpoint Security**.

2. На экране **О продукте** в первой строке текста отображается номер версии вашего продукта ESET.

3. Щелкните элемент **Установленные компоненты** для доступа к информации о конкретных модулях.

Ключевые моменты

Несколько ключевых моментов при установке соответствующего порогового значения для вашей среды:

- **Сбалансированное** пороговое значение рекомендуется для большинства настроек.
- **Осторожное** пороговое значение представляет собой сопоставимый уровень защиты по

сравнению с предыдущими версиями ESET Endpoint Security (версия 7.1 или более ранние). Это рекомендуется для сред, где приоритетом является свертывание ложно идентифицированных объектов с помощью защитного программного обеспечения.

• Более высокий порог отчетности — более высокий уровень обнаружения, но более высокий шанс ложно идентифицированных объектов.

• С реальной точки зрения, нет гарантии 100 % обнаружения, а также 0 % шансов избежать неправильной классификации чистых объектов как вредоносных программ.

• Сохраняйте ESET Endpoint Security и его модули в актуальном состоянии, чтобы обеспечить максимальный баланс между производительностью и точностью обнаружения и количеством ошибочно зарегистрированных объектов.

Настройка защиты

Если объект, классифицированный как КАТЕГОРИЯ, отображается в отчете, программа блокирует объект и затем очищает, удаляет или перемещает его в карантин.

Перед изменением порогового значения (или уровня) защиты для КАТЕГОРИИ ознакомьтесь со следующим:

Пороговое значение	Описание
Агрессивный	Сообщения об обнаружении агрессивного (или более низкого) уровня блокируются, и запускается автоматическое устранение неисправностей (т. е. очистка). Этот параметр рекомендуется, если все конечные точки были отсканированы с агрессивными настройками и в исключения обнаружения были добавлены объекты с ложным классифицированием.
Сбалансированный	Обнаружения сбалансированного (или более низкого) уровня блокируются, после чего запускается автоматическое исправление (т. е. очистка).
Осторожный	Обнаружения осторожного уровня блокируются, и запускается автоматическое исправление (т. е. очистка).
Выкл.	Полезно для идентификации и исключения ложных сообщений об объектах. Значение «Выкл» недоступно для защиты вредоносных программ и по умолчанию используется для потенциально опасных приложений.

⊟ Таблица преобразования политики ESET PROTECT для ESET Endpoint Security версии 7.1 или более ранней

Редактор политик ESET PROTECT для параметров модуля сканирования больше не содержит переключателей ВКЛ/ВЫКЛ для каждой КАТЕГОРИИ. В следующей таблице представлено приведение порогового значения защиты и финального состояния переключателя в ESET Endpoint Security версии 7.1 или более ранней.

Состояние порогового значения КАТЕГОРИИ	Агрессивный	Сбалансированный	Осторожный	Выкл.
Примененный переключатель КАТЕГОРИИ	✓	✓	✓	×

При обновлении с версии 7.1 и более ранней до версии 7.2 и более поздней, новое состояние порогового значения будет выглядеть следующим образом:

Переключатель категорий перед обновлением	✓	×
Новое пороговое значение КАТЕГОРИИ после обновления	Сбалансированный	Выкл.

Рекомендации

НЕУПРАВЛЯЕМАЯ (Индивидуальная рабочая станция клиента)

Сохраняйте рекомендуемые значения по умолчанию.

УПРАВЛЯЕМАЯ СРЕДА

Обычно эти настройки применяются к рабочим станциям с помощью политики.

1. Начальная фаза

Эта фаза может занять до недели.

- Настройте все пороговые значения **Обнаружения** на **Сбалансированный**.
ПРИМЕЧАНИЕ: При необходимости настройте на **Агрессивный**.
- Настройте или оставьте **Защиту** для вредоносных программ на **Сбалансированный**.
- Настройте **Защиту** для других КАТЕГОРИЙ на **Осторожный**.
ПРИМЕЧАНИЕ: На этой фазе не рекомендуется настраивать пороговое значение **Защиты** на **Агрессивный**, поскольку будут исправлены все обнаруженные объекты, в том числе и ложно идентифицированные.
- Определите фальшиво идентифицированные объекты из Журнала обнаружения и добавьте их в Исключения из обнаружения.

2. Переходная фаза

- Внедрите «производственную фазу» в некоторые рабочие станции в качестве тестовой (не для всех рабочих станций в сети).

3. Производственная фаза

- Настройте все пороговые значения **Защиты** на **Сбалансированный**.
- При удаленном управлении используйте соответствующую предопределённую политику защиты от вирусов для ESET Endpoint Security.
- **Агрессивное** пороговое значение защиты можно установить, если требуется

максимальный уровень обнаружения и принимаются ошибочно идентифицированные объекты.

- Проверьте Журнал обнаружения или ESET PROTECT отчеты на наличие возможных пропущенных обнаружений.

Модуль обнаружения расширенных параметров

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.

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

Действия при обнаружении заражения

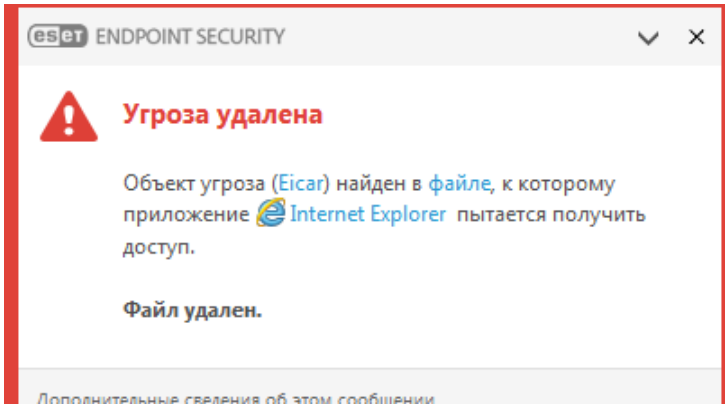
Заражения могут попасть на компьютер из различных источников, таких как веб-сайты, общие папки, электронная почта или съемные носители (накопители USB, внешние диски, компакт- или DVD-диски и т. д.).

Стандартное поведение

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

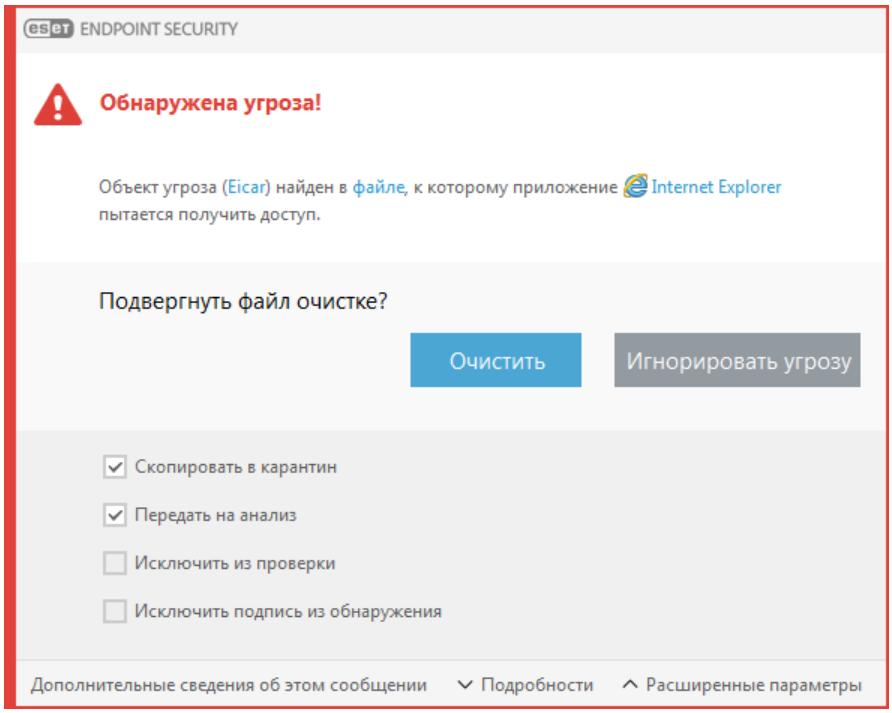
- Защита файловой системы в режиме реального времени
- Защита доступа в Интернет
- Защита почтового клиента
- сканирование компьютера по требованию;

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. Подробные сведения об обнаруженных и очищенных объектах можно найти в файлах журнала. 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.

Восстановление из карантина

Карантин можно открыть из главного окна программы ESET Endpoint Security, щелкнув элемент **Сервис** > **Карантин**.

Файлы, помещенные на карантин, можно также восстановить в исходное расположение.

- Для этого щелните правой кнопкой мыши файл, помещенный на карантин, и в контекстном меню нажмите кнопку **Восстановить**.
- Если файл помечен как потенциально нежелательное приложение, параметр **Восстановить и исключить из сканирования** включен. См. также Исключения.
- Контекстное меню содержит также функцию **Восстановить в**, которая позволяет восстановить файл в расположение, отличное от исходного.
- Функция восстановления недоступна в некоторых случаях, например, для файлов, расположенных в сетевой папке, доступной только для чтения.

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.

Общий локальный кэш

Общий локальный кэш может повысить производительность в изолированных средах (например, виртуальных машинах) за счет устранения дублирования сканирования в сети. Это гарантирует, что каждый файл будет отсканирован только один раз и сохранен в общем кэше.

ESET Shared Local Cache следует установить и настроить в первую очередь.

- Загрузить ESET Shared Local Cache.
- Для получения дополнительных сведений см. онлайн-справку по ESET Shared Local Cache.

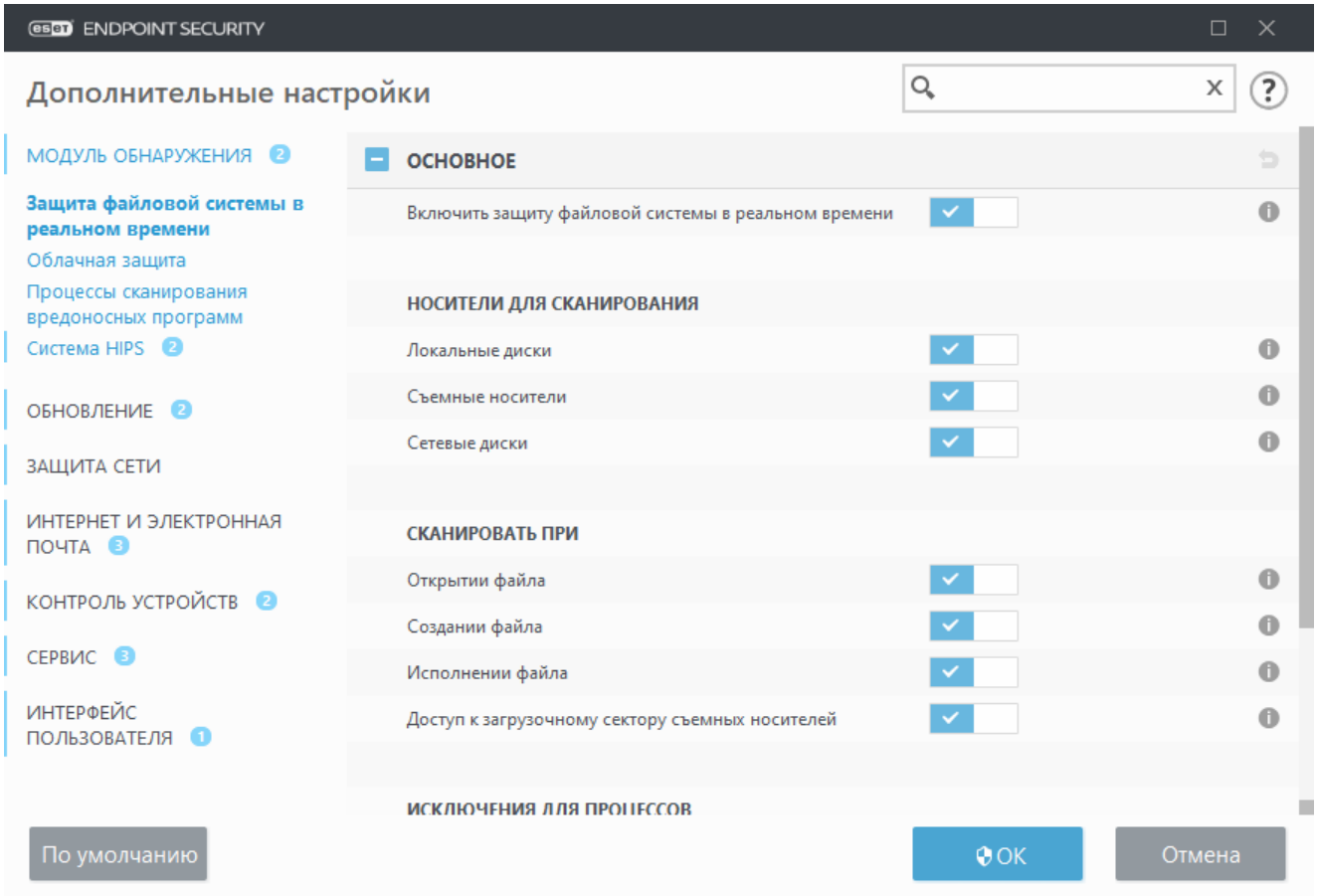
Включите **Параметры кэширования**, чтобы сохранить сведения о сканировании файлов и папок в сети в ESET Shared Local Cache. При новом сканировании ESET Endpoint Security будет искать отсканированные файлы в ESET Shared Local Cache. Если файлы совпадают, они исключаются из сканирования.

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

- **Имя хоста**. Имя хоста или IP-адрес компьютера, где расположен ESET Shared Local Cache.
- **Порт**. Номер порта, используемого для связи (такой же, как был установлен в ESET Shared Local Cache).
- **Пароль**. Укажите пароль для ESET Shared Local Cache, если это необходимо.

Защита файловой системы в режиме реального времени

Защита файловой системы в режиме реального времени контролирует все файлы в системе на наличие вредоносного кода при открытии, создании или запуске.



По умолчанию функция защиты файловой системы в реальном времени запускается при загрузке системы и обеспечивает постоянное сканирование. Мы не рекомендуем снимать флажок **Включить защиту файловой системы в реальном времени** в окне **Расширенные параметры** в разделе **Модуль обнаружения** > **Защита файловой системы в реальном времени** > **Основное**.

Носители для сканирования

По умолчанию все типы носителей сканируются на наличие возможных угроз.

- **Жесткие диски** — Сканирование всех системных и стационарных жестких дисков (например: *C:*\, *D:*\).

- **Съемные носители**: сканирование съемных носителей CD/DVD, USB-хранилища, карт памяти и т д.

- **Сетевые диски**: сканирование подключенных сетевых дисков (пример: *H:*\ как *store04*) или сетевых дисков прямого доступа (пример: *store08*).

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.

- **Открытии файла**: сканирование при открытии файла.
- **Создании файла**: сканирование созданного или измененного файла.
- **Исполнении файла**: сканирование при выполнении или запуске файла.
- **Доступ к загрузочному сектору съемных носителей**: сканирование сразу при вставке съемного носителя, содержащего загрузочный сектор, в устройство. Этот параметр не включает сканирование файлов на съемных носителях. Сканирование файлов на съемных носителях можно включить в разделе **Носители для сканирования** > **Съемные носители**. Чтобы **доступ к загрузочному сектору съемных носителей** работал корректно, включите настройку **Загрузочные секторы/UEFI** в параметрах ThreatSense.

Процессы, которые нужно исключить из сканирования — подробнее об этом типе исключений см. в главе Исключения для процессов.

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 Параметры 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**.

Проверка модуля защиты в режиме реального времени

Чтобы убедиться, что защита в режиме реального времени работает и обнаруживает вирусы, используйте проверочный файл eicar.com. Этот тестовый файл является безвредным, и его обнаруживают все программы защиты от вирусов. Файл создан компанией EICAR (Европейский институт антивирусных компьютерных исследований) для проверки функционирования программ защиты от вирусов.

Файл доступен для загрузки с веб-сайта http://www.eicar.org/download/eicar.com.
После ввода этого URL-адресса в браузере вы должны увидеть сообщение об удалении угрозы.

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**).

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 пользователь непреднамеренно отключит защиту в реальном времени, необходимо повторно активировать эту функцию. Чтобы повторно активировать защиту в реальном времени, перейдите в раздел **Настройка** в главном окне программы и щелкните **Защита компьютера** > **Защита файловой системы в реальном времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке системы, обычно это связано с тем, что отключен параметр **Включить защиту файловой системы в реальном времени**. Чтобы включить этот параметр, перейдите в раздел **Расширенные параметры** (**F5**) и последовательно выберите **Модуль обнаружения** > **Защита файловой системы в реальном времени**.

Защита в режиме реального времени не обнаруживает и не очищает заражения

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

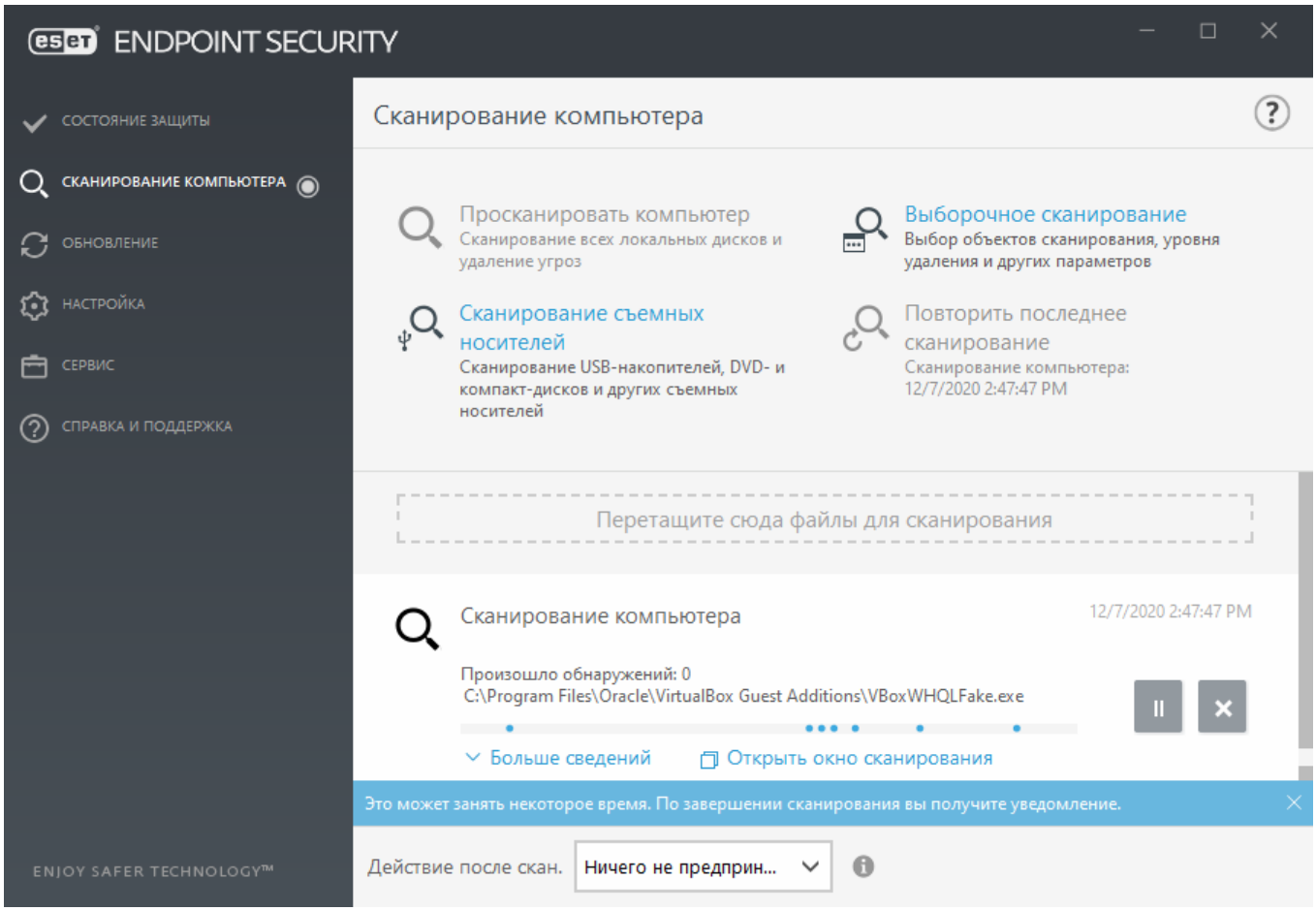
Защита в режиме реального времени не запускается

Если защита 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 в решении этой проблемы, обратитесь в службу технической поддержки ESET. Создайте журнал SysInspector и предоставьте его в службу поддержки ESET для анализа. Это поможет решить проблему. Более подробная информация приведена в этой статье базы знаний ESET.

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**. Функция **Просканировать компьютер** позволяет быстро просканировать систему без необходимости дополнительной настройки параметров сканирования. **Выборочное сканирование** позволяет выбрать предопределенный профиль сканирования и указать объекты, которые нужно просканировать.

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

Просканировать 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 функции **Просканировать компьютер** эта 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**.

Повторить последнее сканирование

Позволяет быстро запустить последнее выполненное сканирование с использованием тех же настроек.

Вы можете выбрать варианты **Ничего не предпринимать**, **Выключить**, **Перезагрузить** или **Перезагрузка при необходимости** в раскрывающемся меню **Действие после сканирования**. Доступность действий **Сон** и **Гибернация** зависит от параметров питания и спящего режима операционной системы и возможностей вашего ноутбука или компьютера. Выбранное действие будет запущено после того, как все запущенные процессы сканирования будут завершены. Если выбран вариант **Выключить**, в диалоговом окне подтверждения выключения будет отображаться 30-секундный обратный отсчет (щелкните **Отмена**, чтобы отменить выключение). Дополнительные сведения см. в разделе Расширенные параметры сканирования.

> Рекомендуется запускать сканирование компьютера не реже одного раза в месяц. Можно настроить сканирование как запланированную задачу в меню **Сервис** > **Планировщик**. См. статью Планирование еженедельного сканирования компьютера

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.

В раскрывающемся меню **Объекты сканирования** можно выбрать предварительно определенные объекты сканирования.

- **По параметрам профиля**: выбираются объекты сканирования, 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.
- **Пользовательский выбор**: отмена всех предыдущих выборов.

Структура папок (дерево) также содержит определенные объекты сканирования.

- **Оперативная память**: сканирование всех процессов и данных, которые в данный

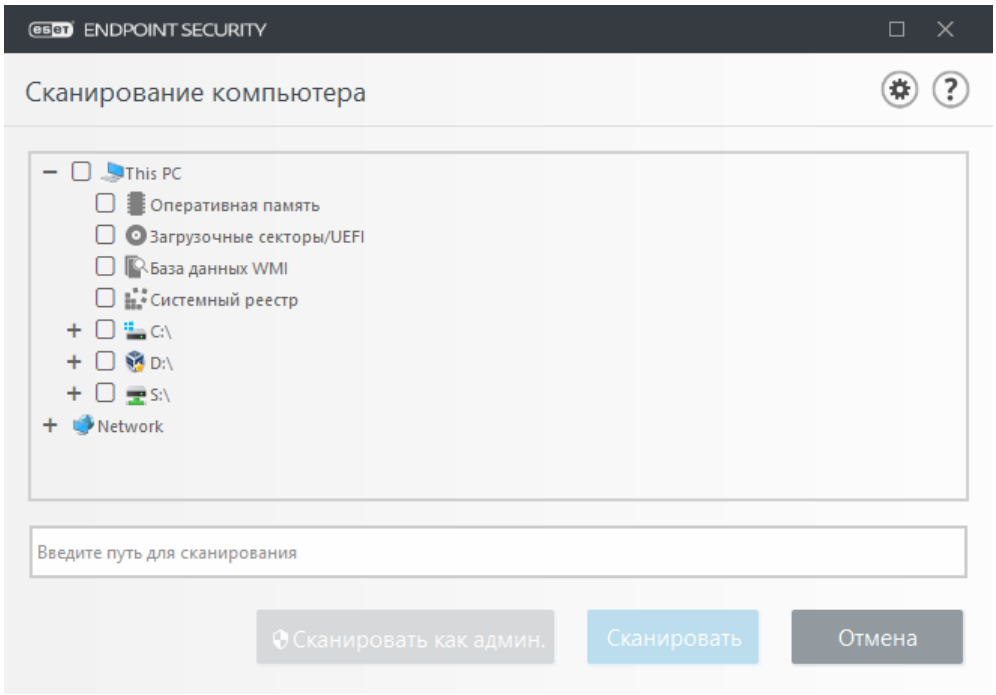
момент используются оперативной памятью.

• **Загрузочные секторы/UEFI**: сканирование загрузочных секторов и UEFI на наличие вредоносных программ. Дополнительные сведения о модуле сканирования UEFI приведены в глоссарии.

• **База данных WMI**: сканирование всей базы данных Windows Management Instrumentation (WMI), всех пространств имен, экземпляров классов и всех свойств. Поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных.

• **Системный реестр**: сканирование всего системного реестра, всех разделов и подразделов. Поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных. При очистке обнаружений ссылка остается в реестре во избежание потери каких-либо важных данных.

Чтобы быстро перейти к какому-либо объекту сканирования или добавить папку или файл для сканирования, введите имя целевой папки в пустое поле под списком папок.



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 **Интеллектуальное сканирование**. Существует еще три предварительно заданных профиля сканирования — **Сканирование через контекстное меню**, **Глубокое сканирование** и

Сканирование компьютера. В этих профилях сканирования используются другие параметры ThreatSense. Чтобы ознакомиться с доступными параметрами, последовательно выберите **Расширенные параметры** > **Модуль обнаружения** > **Сканирование на наличие вредоносных программ** > **Сканирование по требованию** > Параметры ThreatSense.

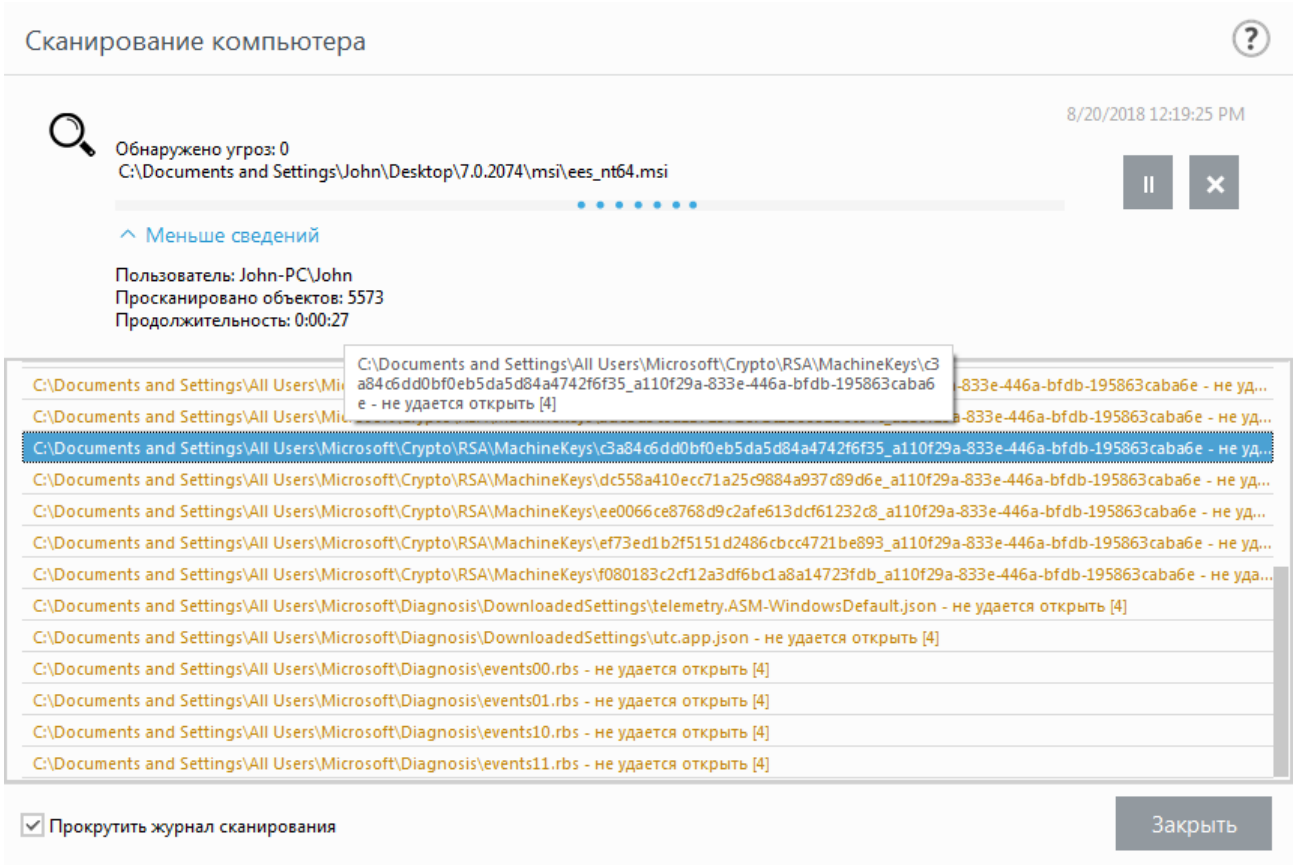
Нажмите кнопку **Сканировать**, чтобы выполнить сканирование с выбранными параметрами.

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.

> Журнал сканирования можно просмотреть по завершении сканирования, нажав кнопку **Показать журналы**.

Ход сканирования

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



> 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.

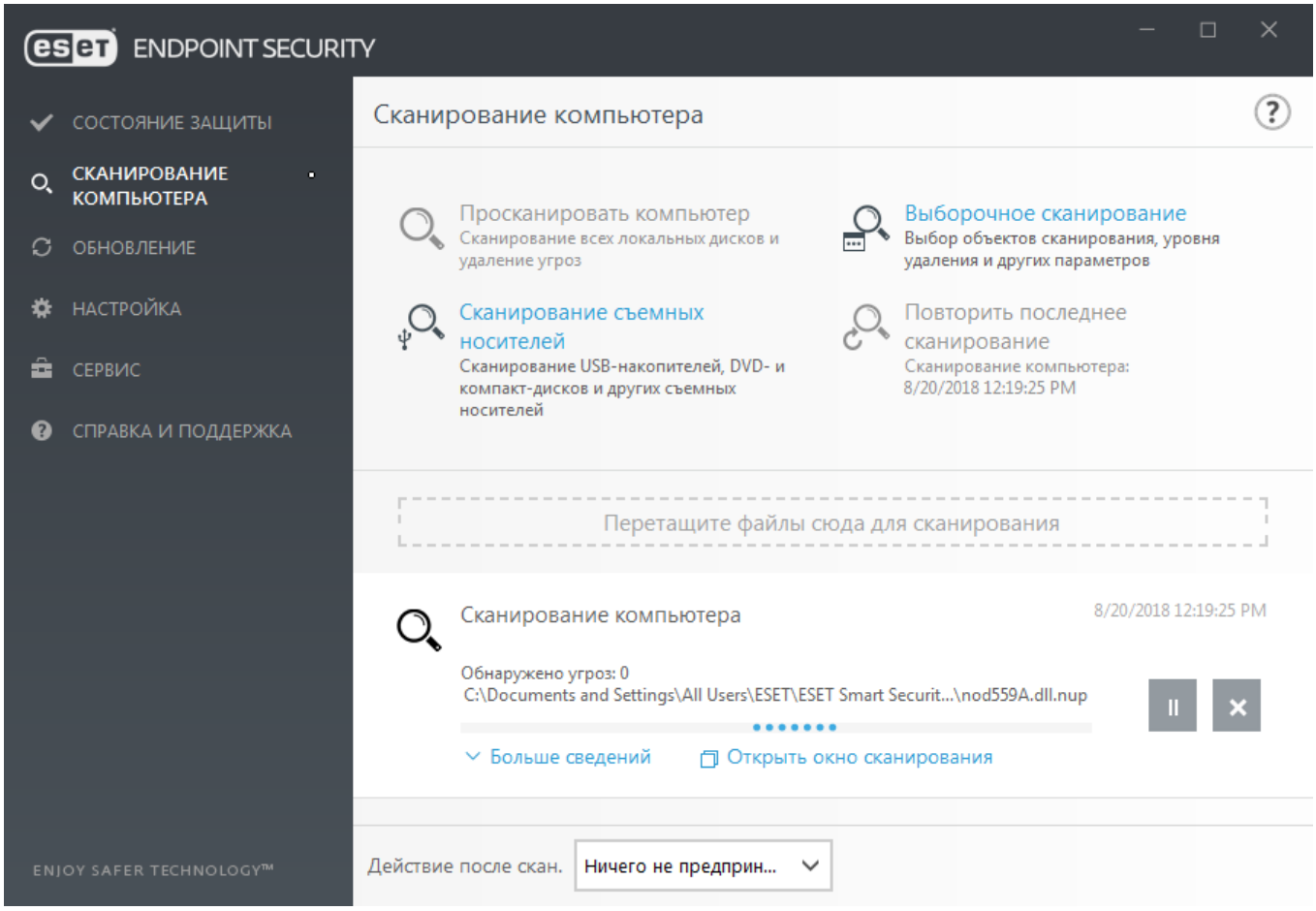
Обнаружены угрозы: общее число угроз, обнаруженных при сканировании.

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.



Журнал сканирования компьютера

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

- дата и время сканирования;
- просканированные диски, папки и файлы;
- число просканированных объектов;

- число обнаруженных угроз;
- время завершения;
- общее время сканирования.

Процессы сканирования вредоносных программ

Раздел **Процессы сканирования вредоносных программ** находится в меню «Расширенные параметры». Нажмите клавишу **F5**, щелкните **Модуль обнаружения** > **Процессы сканирования вредоносных программ** и выберите параметры сканирования. В этом разделе доступны следующие параметры:

- **Выбранный профиль** – конкретный набор параметров, используемых сканером по запросу.
  Чтобы создать новый профиль, нажмите Изменить возле списка профилей.
  Дополнительные сведения см. в разделе Профили сканирования.
- **По требованию и Защита машинного обучения** – см. Модуль обнаружения (версии 7.2 или более поздние версии).
- **Объекты сканирования**. Чтобы просканировать только определенный объект, рядом с параметром **Объекты сканирования** щелкните **Изменить** и укажите вариант из раскрывающегося меню или выберите нужные объекты из структуры папок (дерева).
  Дополнительные сведения см. в разделе Объекты сканирования.
- **Параметры ThreatSense**. В этом разделе доступны расширенные параметры, такие как расширения файлов, которыми нужно управлять, используемые методы обнаружения и т. п. Щелкните, чтобы открыть вкладку с расширенными параметрами сканирования.

Сканирование в состоянии простоя

Вы можете разрешить сканирование в состоянии простоя, выбрав **Расширенные параметры** в меню **Модуль обнаружения**, а затем **Процессы сканирования вредоносных программ** > **Сканирование в состоянии простоя**.

Сканирование в состоянии простоя

Установите переключатель **Включить сканирование в состоянии простоя** в положение **Включено**, чтобы включить эту функцию. Когда компьютер находится в состоянии простоя, автоматически выполняется сканирование всех жестких дисков.

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**).

Сканирование в состоянии простоя

Полный список условий для запуска сканирования в состоянии простоя см. в разделе Сканирование в состоянии простоя.

Выберите Параметры ThreatSense для изменения параметров сканирования (например, методов обнаружения) для сканирования в состоянии простоя.

Профили сканирования

В ESET Endpoint Security есть четыре предварительно заданных профиля сканирования:

- **Интеллектуальное сканирование** — это профиль расширенного сканирования по умолчанию. Для профиля интеллектуального сканирования используется технология интеллектуальной оптимизации, исключающая файлы, которые во время предыдущего сканирования были определены как чистые и с того времени не изменялись. Это обеспечивает сокращение времени сканирования при минимальном влиянии на безопасность системы.

- **Сканирование через контекстное меню** — вы можете запустить в контекстном меню сканирование по требованию для любого файла. Профиль «Сканирование через контекстное меню» позволяет определить конфигурацию сканирования, которая будет использоваться при запуске сканирования таким способом.

- **Глубокое сканирование** — Для профиля глубокого сканирования интеллектуальная оптимизация по умолчанию не используется, поэтому при использовании этого профиля никакие файлы из сканирования не исключаются.

- **Сканирование компьютера** — этот профиль по умолчанию используется при стандартном сканировании компьютера.

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

Для создания профиля откройте окно «Расширенные параметры» (F5) и щелкните **Модуль обнаружения** > **Сканирование на наличие вредоносных программ** > **Сканирование по требованию** > **Список профилей**. В окне **Диспетчер профилей** доступно раскрывающееся меню **Выбранный профиль** со списком существующих профилей сканирования и опцией для создания нового. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, где описывается каждый параметр, используемый для настройки сканирования.

Предположим, вам требуется создать собственный профиль сканирования. Хотя конфигурация **Сканировать компьютер** частично подходит, сканировать программы-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 меня **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **OK**, чтобы сохранить новый профиль.

Объекты сканирования

В окне объектов сканирования можно определить, какие объекты (оперативная память, жесткие диски, секторы, файлы и папки) будут сканироваться на предмет выявления заражений.

В раскрывающемся меню **Объекты сканирования** можно выбрать предварительно определенные объекты сканирования.

- **По параметрам профиля**: выбираются объекты сканирования, 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.
- **Пользовательский выбор**: отмена всех предыдущих выборов.

Структура папок (дерево) также содержит определенные объекты сканирования.

- **Оперативная память**: сканирование всех процессов и данных, которые в данный момент используются оперативной памятью.
- **Загрузочные секторы/UEFI**: сканирование загрузочных секторов и UEFI на наличие вредоносных программ. Дополнительные сведения о модуле сканирования UEFI приведены в глоссарии.
- **База данных WMI**: сканирование всей базы данных Windows Management Instrumentation (WMI), всех пространств имен, экземпляров классов и всех свойств. Поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных.
- **Системный реестр**: сканирование всего системного реестра, всех разделов и подразделов. Поиск ссылок на зараженные файлы или вредоносные программы, внедренные в виде данных. При очистке обнаружений ссылка остается в реестре во избежание потери каких-либо важных данных.

Чтобы быстро перейти к какому-либо объекту сканирования или добавить папку или файл для сканирования, введите имя целевой папки в пустое поле под списком папок.

Расширенные параметры сканирования

В этом окне можно задать расширенные параметры для запланированных задач сканирования компьютера. Действие, которое нужно автоматически выполнить после сканирования, можно выбрать в раскрывающемся меню.

- **Выключить**: после сканирования компьютер отключается.
- **Перезагрузить**: после сканирования открытые программы закрываются, а компьютер перезагружается.
- **Перезагрузка при необходимости**: если необходимо, после сканирования открытые программы закрываются, а компьютер перезапускается.
- **Спящий режим**: сеанс сохраняется, и компьютер переходит в режим пониженного энергопотребления (т. е. пользователь может быстро возобновить работу).
- **Режим гибернации**: все компоненты, использующие ОЗУ, переносятся в специальный файл на жестком диске. Компьютер выключается, и при следующем включении вернется в предыдущее состояние.
- **Ничего не предпринимать**: после сканирования действия предприниматься не будут.

> i Обратите внимание, что компьютер в спящем режиме все же работает. Когда он работает от батареи, выполняются основные функции и используется электричество. Чтобы сохранить время работы батареи (например, если вы находитесь в пути), рекомендуется перевести компьютер в режим гибернации.

Выберите элемент **Пользователь не может отменить действие**, чтобы пользователи, не обладающие нужными правами, не могли отменить действие, которое выполняется после сканирования.

Включите параметр **Сканирование может быть приостановлено пользователем на (мин.)**, чтобы пользователи, обладающие ограниченными правами, могли приостанавливать сканирование компьютера на определенный период времени.

Дополнительные сведения см. в главе Ход сканирования.

Контроль устройств

ESET Endpoint Security обеспечивает автоматическое управление устройствами (CD- 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 содержимым.

Поддерживаемые внешние устройства:

- Дисковый накопитель (HDD, съемный USB-диск)

- CD/DVD
- принтер USB
- FireWire Хранилище
- Устройство Bluetooth
- Устройство чтения смарт-карт
- Устройство обработки изображений
- Модемы
- LPT/COM порт
- Портативное устройство
- Все типы устройств

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

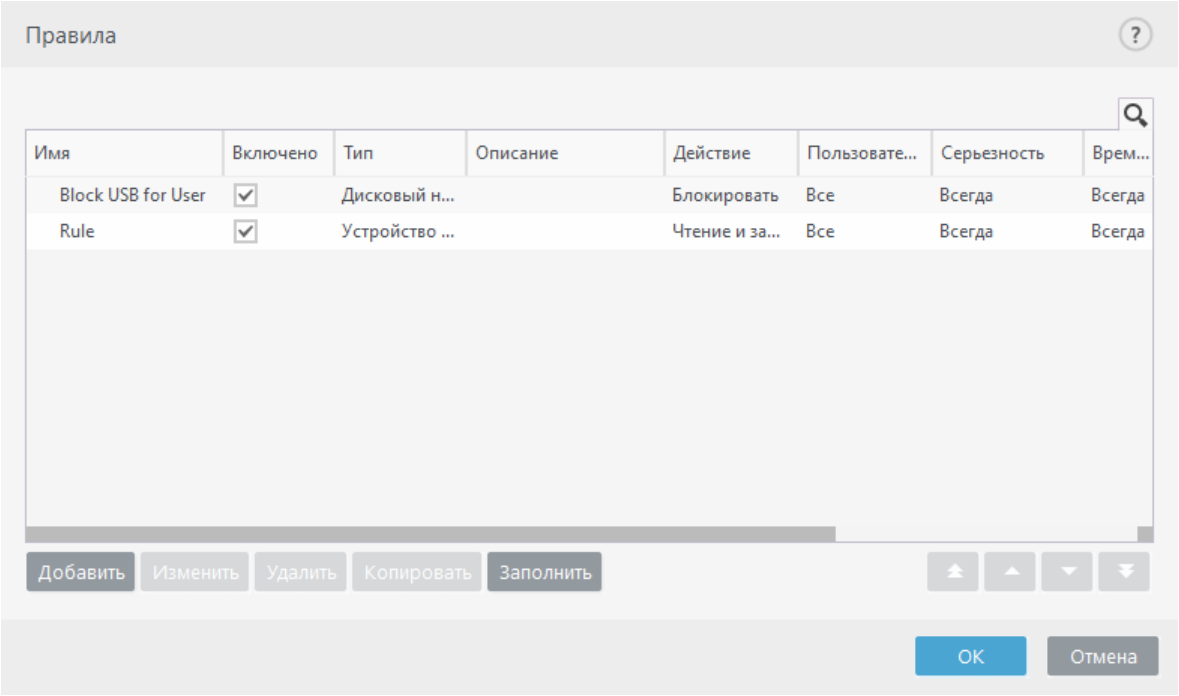
Если активировать переключатель, расположенный рядом с элементом **Включить контроль устройств**, в программе ESET Endpoint Security будет включена функция контроля устройств. Чтобы это изменение вступило в силу, необходимо перезагрузить компьютер. После включения контроля устройств кнопка **Правила** станет активной и вы сможете открыть окно Редактор правил.

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

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. См. также Добавление правил для контроля устройств.

> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> - Добавление и изменение правил для контроля устройств с помощью продуктов ESET для конечных точек



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**.

Обнаруженные устройства

С помощью кнопки **Заполнить** можно ознакомиться со следующей информацией о подключенных на данный момент устройствах: тип устройства, производитель, модель и серийный номер (если есть).

Выбрав устройство в списке обнаруженных устройств и нажав кнопку **OK**, в открывшемся окне редактора правил можно ознакомиться с предварительно заданной информацией (все

параметры можно настраивать).

Группы устройств

⚠ Устройство, подключенное к компьютеру, может представлять угрозу безопасности.

Окно групп устройств разделено на две части. В правой части окна отображается список устройств, входящих в выбранную группу, а в левой части — созданные группы. Выберите группу со списком устройств, которую нужно отобразить на правой панели.

Открыв окно групп устройств и выбрав группу, вы можете добавлять устройства в список или удалять их из него. Добавлять устройства в группу также можно посредством импорта данных об устройствах из файла. Или же можно нажать кнопку **Заполнить**. В этом случае все устройства, подключенные к компьютеру, отобразятся в окне **Обнаруженные устройства**. Выберите устройства из этого списка и нажмите кнопку **OK**, чтобы добавить их в группу.

Элементы управления

Добавить. Позволяет создать новую группу или добавить устройство в существующую (в зависимости от того, где нажата кнопка). При необходимости можно указать такие сведения, как имя поставщика, модель и серийный номер.

Изменить. Позволяет изменить имя выбранной группы или параметров устройства (производитель, модель, серийный номер).

Удалить: удаление выбранной группы или устройства (в зависимости от того, в какой части окна нажата кнопка).

Импорт. Импортирует список устройств из текстового файла. Для импорта устройств из текстового файла требуется правильное форматирование:

- каждое устройство должно быть указано с новой строки;
- для каждого устройства должны быть указаны через запятую сведения о **производителе**, **модели** и **серийном номере**.

✔ Вот пример содержимого такого текстового файла:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Экспорт. Экспортирует список устройств в файл.

С помощью кнопки **Заполнить** можно ознакомиться со следующей информацией о подключенных на данный момент устройствах: тип устройства, производитель, модель и серийный номер (если есть).

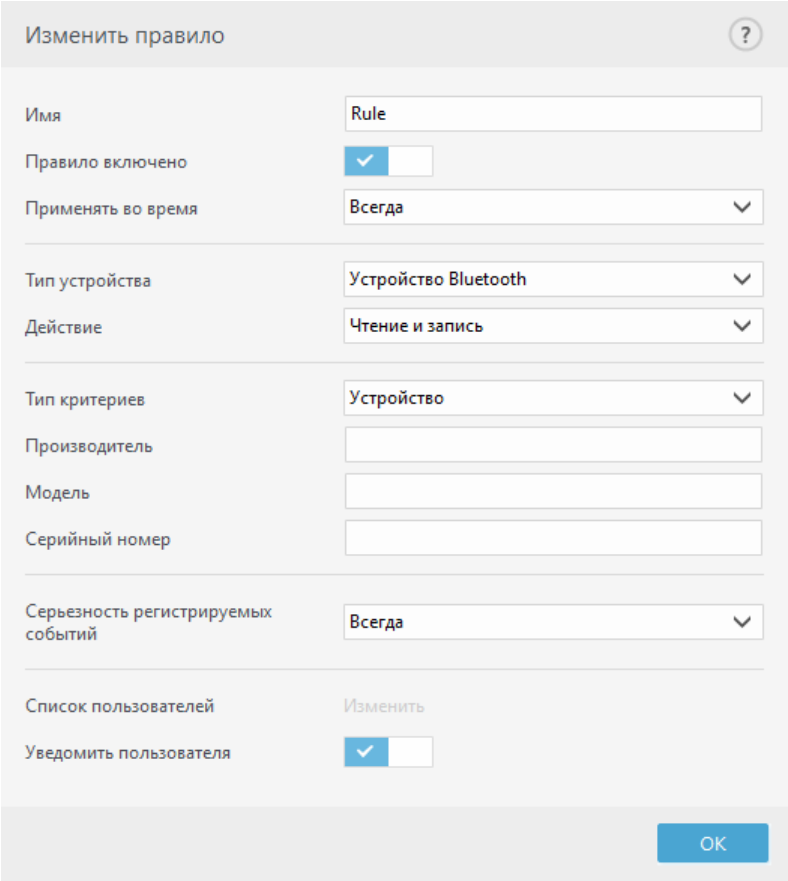
Завершив настройки, нажмите кнопку **OK**. Чтобы закрыть окно **Группы устройств** без сохранения изменений, нажмите кнопку **Отмена**.

> Вы можете создать разные группы устройств, к которым будут применяться разные правила. Группу, к которой применяется правило с действием **Чтение и запись** или **Только для чтения**, можно создать только одну. Благодаря этому, когда к компьютеру подключаются нераспознанные устройства, функция контроля устройств их блокирует.

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.

Добавление правил контроля устройств

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



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

Применять во время: позволяет применять созданное правило в определенное время. В раскрывающемся меню выберите созданный временной интервал. Ознакомьтесь с дополнительными сведениями о временных интервалах.

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 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.

> 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 (*, ?).

> 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.

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

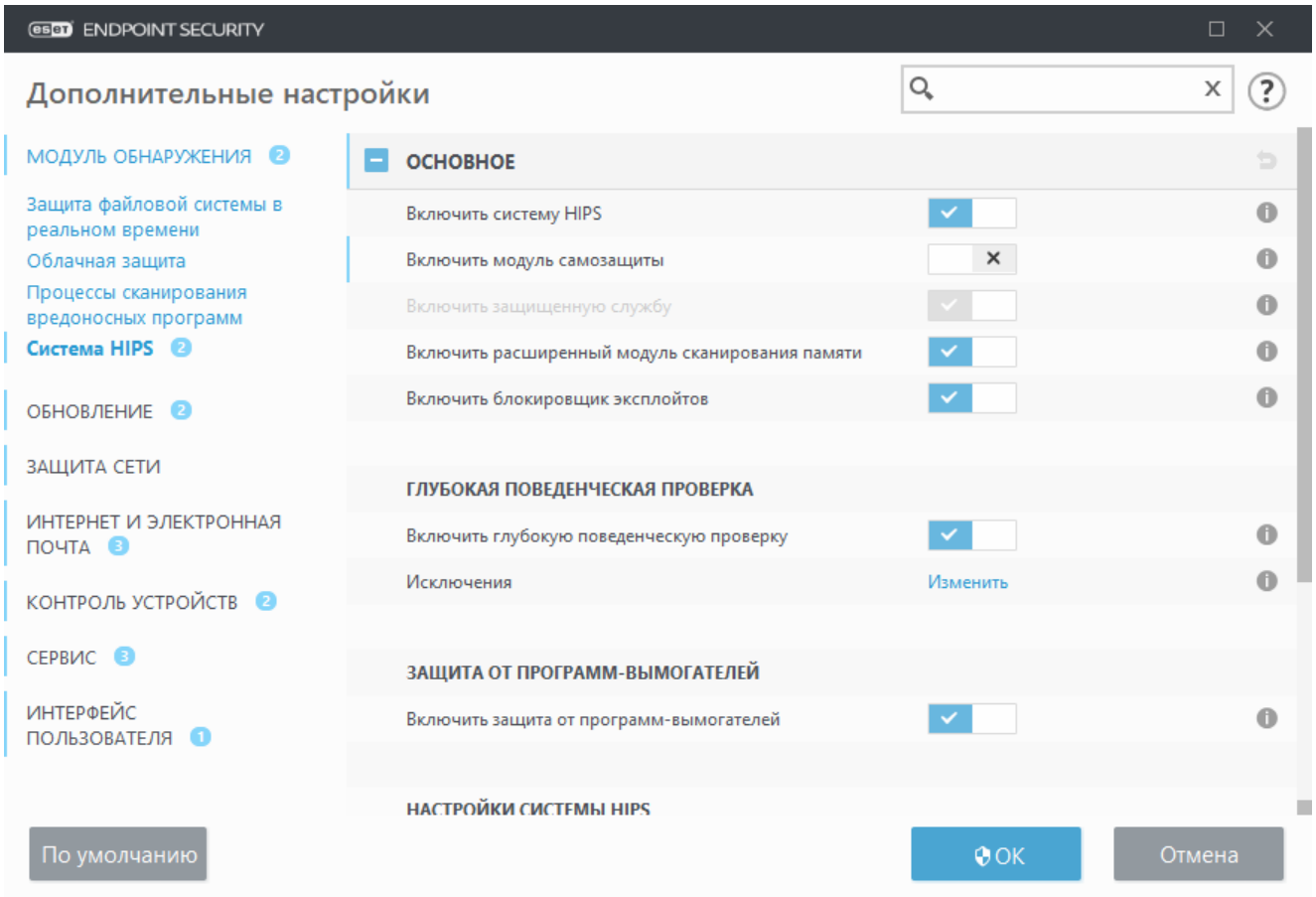
Система предотвращения вторжений на узел

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

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

реального времени и не является файерволом; она только отслеживает процессы, запущенные в операционной системе.

Параметры HIPS доступны в разделе **Расширенные параметры** (F5) > **Модуль обнаружения** > **HIPS** > **Основная информация**. Состояние системы HIPS (включено/отключено) отображается в главном окне программы ESET Endpoint Security в разделе **Настройка** > **Компьютер**.



Основные сведения

Включить систему HIPS. В ESET Endpoint Security система HIPS включена по умолчанию. Отключение системы HIPS приведет к отключению ее функций, Блокировщика эксплойтов.

Включить модуль самозащиты. 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. При установке агента ESET Management для него также включается защита.

Включить защищенную службу. Включается защита службы ESET (ekrn.exe). Если параметр включен, служба запускается в виде защищенного процесса Windows для защиты от атак вредоносных программ. Этот параметр доступен в Windows 8.1 и Windows 10.

Включить 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.

Глубокая поведенческая проверка

Включить глубокую поведенческую проверку — это еще один уровень защиты, используемый системой HIPS. Это расширение системы HIPS анализирует поведение всех программ, запущенных на компьютере, и предупреждает вас, если процесс ведет себя, как вредоносный.

Исключения системы HIPS из глубокой поведенческой проверки позволяют исключить из анализа определенные процессы. Чтобы обеспечить сканирование всех процессов на наличие угроз, рекомендуется создавать исключения только в случае крайней необходимости.

Защита от программ-шантажистов

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 ESET LiveGrid® была включена. Дополнительную информацию об этом типе защиты см. здесь.

Включить режим аудита: объекты, обнаруженные защитой от программ-вымогателей, не блокируются автоматически, а заносятся в журнал со статусом «Предупреждение» и отправляются в консоль управления с пометкой «РЕЖИМ АУДИТА». Администратор может решить либо исключить такое обнаружение, чтобы оно больше не повторялось, либо оставить его активным. Во втором случае после выхода из режима аудита обнаруженный объект будет заблокирован и удален. Факт включения и отключения режима аудита также будет занесен в журнал ESET Endpoint Security. Этот параметр доступен только в ESET PROTECT и редакторе конфигурации политики ESMC.

Настройки системы HIPS

Режим фильтрации можно выполнять в одном из следующих режимов:

Режим фильтрации	Описание
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	блокируются все операции, кроме тех, что разрешены определенным правилом.

Режим фильтрации	Описание
Режим обучения	Операции включены, и после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в редакторе **Правила HIPS**, но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. При выборе элемента **Режим обучения** в раскрывающемся меню **Режим фильтрации** 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. Выберите режим фильтрации, который будет действовать по окончании использования режима обучения. Чтобы после завершения режима обучения изменить режим фильтрация HIPS на **Спросить пользователя**, нужны права администратора.

Система HIPS отслеживает события в операционной системе и реагирует на них соответствующим образом на основе правил, которые аналогичны правилам файервола. Нажмите кнопку **Настроить** рядом с элементом **Правила**, чтобы открыть редактор **правил системы HIPS**. В этом окне можно выбирать, создавать, изменять и удалять правила. Дополнительные сведения о создании правил и операциях системы HIPS см. в разделе Изменение правила системы предотвращения вторжений на узел.

Интерактивное окно HIPS

В окне уведомлений HIPS можно создать правило на основе новых действий, обнаруженных системой HIPS, и определить условия, при которых такое действие будет разрешено или запрещено.

Правила, создаваемые в окне уведомлений, считаются равнозначными правилам, созданным вручную. Правило, созданное в окне уведомлений, может быть менее подробным, чем правило, которое вызвало появление этого диалогового окна. Это значит, что после создания такого правила в диалоговом окне эта же операция может вызвать появление такого же окна. Дополнительные сведения см. в разделе Приоритетность для правил HIPS.

Если для правила по умолчанию установлено действие **Спрашивать каждый раз**, 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.

Выбор параметра **Запомнить до закрытия приложения** 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.

Если выбрать параметр **Создать правило и запомнить навсегда**, будет создано новое правило HIPS, которое позже можно изменить в разделе Управление правилами HIPS (нужны

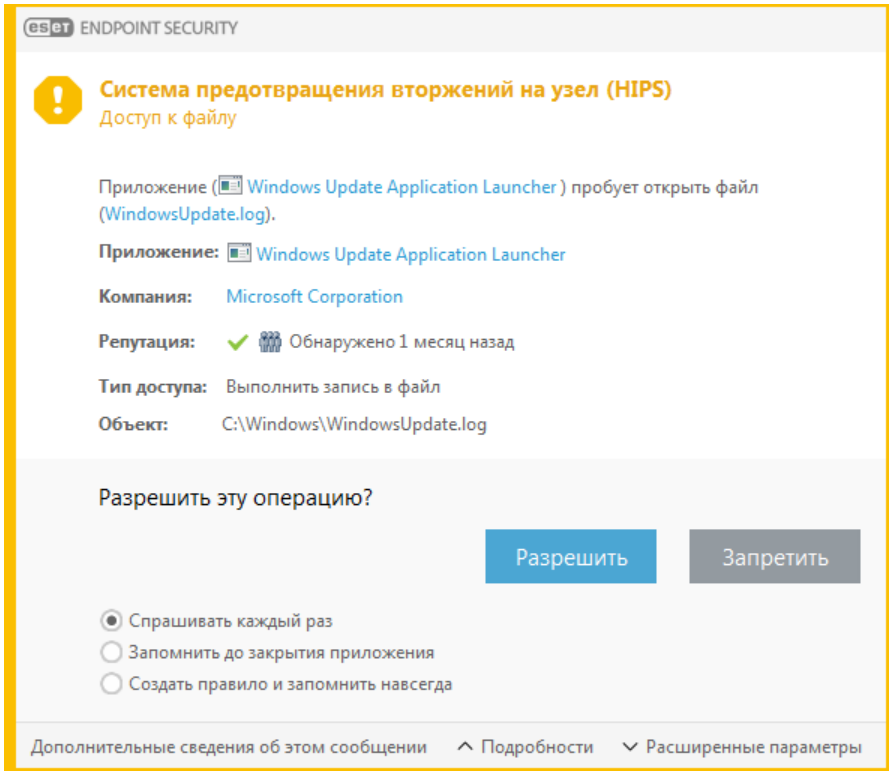
права администратора).

Внизу щелкните **Сведения**, чтобы узнать, какое приложение запускает операцию, какова репутация файла и какую операцию нужно разрешить или запретить.

Чтобы установить параметры правила более детально, щелкните **Расширенные параметры**. Если выбран параметр **Создать правило и запомнить навсегда**, доступны перечисленные ниже варианты.

- **Создать правило, действительное только для этого приложения**. Если установлен этот флажок, правило будет создано для всех исходных приложений.
- **Только для операции**. Выберите операции для файла, приложения или реестра правила. См. описания всех операций HIPS.
- **Только для цели**. Выберите целевые объекты для файла, приложения или реестра правила.

> Чтобы уведомления не отображались, установите **автоматический режим** фильтрации, поочередно щелкнув **Расширенные параметры** (F5) > **Модуль обнаружения** > **HIPS** > **Основные сведения**.



Потенциальное поведение Программ-вымогателей обнаружено

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

Щелкните **Сведения**, чтобы просмотреть конкретные параметры обнаружения. В этом диалоговом окне можно выбрать **Передать на анализ** или **Исключить из проверки**.

> Для правильной работы модуля защиты от программ-вымогателей система ESET LiveGrid® должна быть включена.

Управление правилами HIPS

Это список пользовательских и добавленных автоматически правил в системе HIPS. Дополнительные сведения о создании правила и операциях HIPS см. в разделе Параметры правил HIPS. См. также Общие принципы работы системы HIPS.

Столбцы

Правило: указанное пользователем или автоматически выбранное имя правила.

Включено. Отключите этот параметр, чтобы оставить правило в списке, но при этом не использовать его.
Действие. Правило задает действие (**Разрешить**, **Блокировать** или **Запросить**), которое должно быть выполнено при соблюдении условий.

Исходные объекты: правило будет использоваться только в том случае, если событие вызывается этими приложениями.

Целевые объекты: правило будет использоваться, только если операция связана с определенным файлом, приложением или записью реестра.

Серьезность регистрируемых событий: если активировать этот параметр, информация об указанном правиле будет записываться в журнал HIPS.

Уведомить. Если запускается событие, в правом нижнем углу экрана выводится маленькое всплывающее уведомление.

Элементы управления

Добавить: создание правила.

Изменить: изменение выделенных записей.

Удалить. Удаление выбранных записей.

Приоритетность для правил HIPS

Настройка уровня приоритета для правил HIPS с помощью кнопок «вверх» и «вниз» (как в разделе Правила файервола, где правила последовательно выполняются сверху вниз) не предусмотрена.

- Все правила, которые вы создаете, имеют одинаковый приоритет.
- Чем более подробное правило, тем выше его приоритет (например, правило для конкретного приложения имеет более высокий приоритет, чем правило для всех приложений).

• Система HIPS содержит внутренние правила с более высоким приоритетом, которые недоступны пользователю (например, нельзя переопределить правила самозащиты).

• Созданное пользователем правило, которое может заморозить работу операционной системы, не применяется (имеет самый низкий приоритет).

Параметры правил HIPS

Сначала ознакомьтесь с разделом Правила HIPS.

Имя правила: указанное пользователем или автоматически выбранное имя правила.

Действие: правило задает действие (Разрешить, Блокировать или Запросить), которое должно быть выполнено при соблюдении условий.

Операции влияния: выберите тип операции, к которому будет применяться правило. Правило будет использоваться только для этого типа операции и для выбранного объекта.

Включено: отключите этот параметр, если правило нужно оставить в списке, но при этом не использовать его.

Серьезность регистрируемых событий: если активировать этот параметр, информация об указанном правиле будет записываться в журнал HIPS.

Уведомить пользователя: если запускается событие, в правом нижнем углу экрана выводится небольшое всплывающее окно.

Правило состоит из частей, в которых описываются условия выполнения правила.

Исходные приложения: правило будет использоваться только в том случае, если событие вызывается этими приложениями. Выберите пункт **Определенные приложения** в раскрывающемся меню и нажмите кнопку **Добавить**, чтобы добавить новые файлы, или выберите пункт **Все приложения**, чтобы добавить все приложения.

Целевые файлы: это правило будет использоваться, только если операция относится к данному целевому объекту. Выберите пункт **Определенные файлы** в раскрывающемся меню и щелкните **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все файлы**, чтобы добавить все файлы.

Приложения: это правило будет использоваться, только если операция относится к данному целевому объекту. Выберите пункт **Определенные приложения** в раскрывающемся меню и нажмите кнопку **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все приложения**, чтобы добавить все приложения.

Записи реестра: это правило будет использоваться, только если операция относится к данному целевому объекту. Выберите пункт **Определенные записи** в раскрывающемся меню и нажмите кнопку **Добавить**, чтобы добавить новые файлы или папки, или выберите пункт **Все записи**, чтобы добавить все приложения.

Некоторые операции определенных правил, предварительно заданных системой HIPS, невозможно заблокировать, и они разрешены по умолчанию. Кроме того, не все системные операции отслеживаются системой HIPS. Система HIPS отслеживает операции, которые могут считаться небезопасными.

При указании пути строка C:\example влияет на действия с самой папкой, а строка C:\example*.* влияет на файлы в папке.

Операции с приложениями

• **Выполнить отладку другого приложения**: прикрепление отладчика к процессу. При отладке приложения можно просмотреть и изменить многие сведения о его поведении и получить доступ к его данным.

• **Перехватывать события другого приложения**: исходное приложение пытается записать события, направленные на другое приложение (например, клавиатурный шпион, пытающийся записать события браузера).

• **Завершить/приостановить работу другого приложения**: приостановка, возобновление или завершение процесса (можно получить доступ непосредственно из обозревателя процессов или панели «Процессы»).

• **Запустить новое приложение**: запуск новых приложений или процессов.

• **Изменить состояние другого приложения**: исходное приложение пытается осуществить запись в память целевого приложения или выполнить код от его имени. Эта функциональность может быть полезна для защиты важного приложения путем его настройки как целевого в правиле, блокирующем использование данной операции.

В 64-разрядных версиях Windows XP перехватывать операции процессов невозможно.

Операции с реестром

• **Изменить параметры запуска**: любые изменения параметров, которые определяют, какие приложения будут выполнены при запуске ОС Windows. Их можно найти, например, выполнив поиск раздела Run в реестре Windows.

• **Удалить из реестра**: удаление раздела реестра или его значения.

• **Переименовать раздел реестра**: переименование разделов реестра.

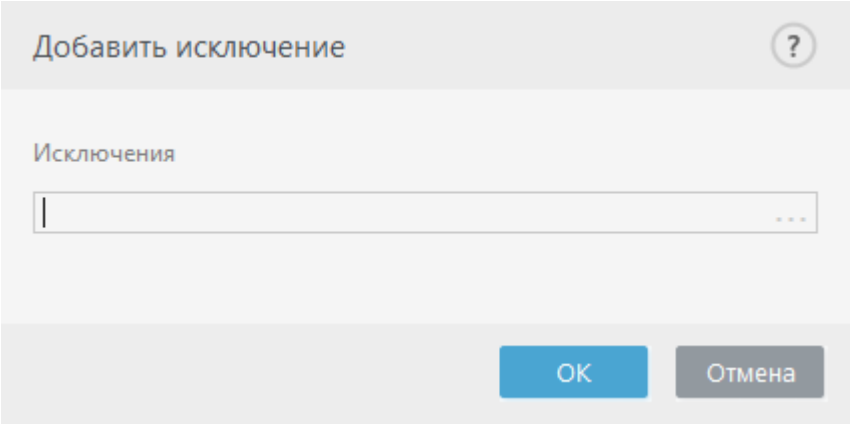
• **Изменить реестр**: создание новых значений разделов реестра, изменение существующих значений, перемещение данных в древовидной структуре базы данных или настройка прав пользователя или группы для разделов реестра.

Использование подстановочных знаков в правилах
Звездочка в правилах может использоваться только для замены конкретного ключа, например HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start. Другие способы использования подстановочных символов не поддерживаются.
Создание правил для ключа HKEY_CURRENT_USER
Этот ключ является лишь ссылкой на соответствующий подраздел HKEY_USERS, специфичный для пользователя, идентифицированного защищенным идентификатором (SID). Чтобы создать правило только для текущего пользователя, вместо того чтобы использовать путь к HKEY_CURRENT_USER, используйте путь, указывающий на HKEY_USERS\%SID%. В качестве SID можно использовать звездочку, чтобы сделать правило применимым для всех пользователей.

Если созданное правило будет слишком общим, появится соответствующее предупреждение.

В следующем примере будет показано, как ограничить нежелательное поведение конкретного приложения.

1.Присвойте правилу имя и выберите **Блокировать** (или **Запросить**, если вы хотите выбрать действие позже) в раскрывающемся меню **Действие**.
2.Активируйте переключатель **Уведомить пользователя**, чтобы уведомление отображалось при каждом применении правила.
3.Выберите хотя бы одну операцию в разделе **Операции влияния**, для которой будет применяться правило.
4.Нажмите кнопку **Далее**.
5.В окне **Исходные приложения** выберите в раскрывающемся списке вариант **Определенные приложения**. Новое правило будет применяться ко всем приложениям, которые будут пытаться выполнить любое из выбранных действий с указанными приложениями.
6.Нажмите кнопку **Добавить** и **...**, чтобы выбрать путь к определенному приложению. Затем нажмите кнопку **OK**. При необходимости добавьте дополнительные приложения. Например: *C:\Program Files (x86)\Untrusted application\application.exe*
7.Выберите операцию **Выполнить запись в файл**.
8.Выберите **Все файлы** в раскрывающемся меню. Это позволит заблокировать все попытки записи в файлы приложениями, которые были выбраны на предыдущем шаге.
9.Нажмите кнопку **Готово**, чтобы сохранить новое правило.



Расширенные параметры HIPS

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.

Драйверы, загрузка которых разрешена всегда

Загрузка драйверов, отображенных в этом списке, разрешена всегда вне зависимости от режима фильтрации HIPS. Это не касается случаев, когда загрузка драйвера явным образом заблокирована правилом пользователя.

Добавить: добавление нового драйвера.

Изменить: изменение выбранного драйвера.

Удалить: удаление драйвера из списка.

Сброс: перезагрузка системных драйверов.

> Если щелкнуть элемент **Сброс**, драйверы, добавленные вручную, будут удалены из списка. Это может пригодиться, если вы добавили несколько драйверов и не можете удалить их из списка вручную.

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.

> Если файервол 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 файерволе. 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.

сканирование при запуске

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.

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.

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 реальном времени. Ее можно отключить, чтобы улучшить производительность систем, которые не содержат большое количество документов Microsoft Office.

Чтобы активировать функцию защиты документов, откройте окно **Расширенные параметры** (нажмите клавишу **F5**), щелкните **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Защита документов** и выберите **Включить защиту документов**.

> i 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).

Исключения

Исключения позволяют исключить объекты из модуля обнаружения. 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 баз данных большой емкости, которые замедляет работу или программное обеспечение, которое противоречит сканированию.

Исключения для быстродействия позволяют исключить из сканирования файлы и папки. Исключения для быстродействия полезны для исключения при сканировании игровых приложений на уровне файлов, неправильном поведении системы или повышенной производительности.

Исключения из обнаружения позволяют исключить объекты из очистки, используя имя обнаружения, путь или хеш. Они не исключают файлы и папки из сканирования как делают исключения для быстродействия. Исключения обнаружения исключают объекты только при их обнаружении модулем обнаружения и если в списке исключений присутствует соответствующее правило.

Исключения в версии 7.1 и более ранних версиях включают в себя Исключения для быстродействия и Исключения из обнаружения, которые объединены.

Не стоить путать с другими типами исключений:

- Исключения из операции: все операции с файлами, относящиеся к исключенным из сканирования процессам приложения (может понадобится для повышения скорости резервного копирования и доступности служб).
- Исключенные расширения файлов
- Исключения системы HIPS
- Фильтр «Исключение» для защиты на основе облака

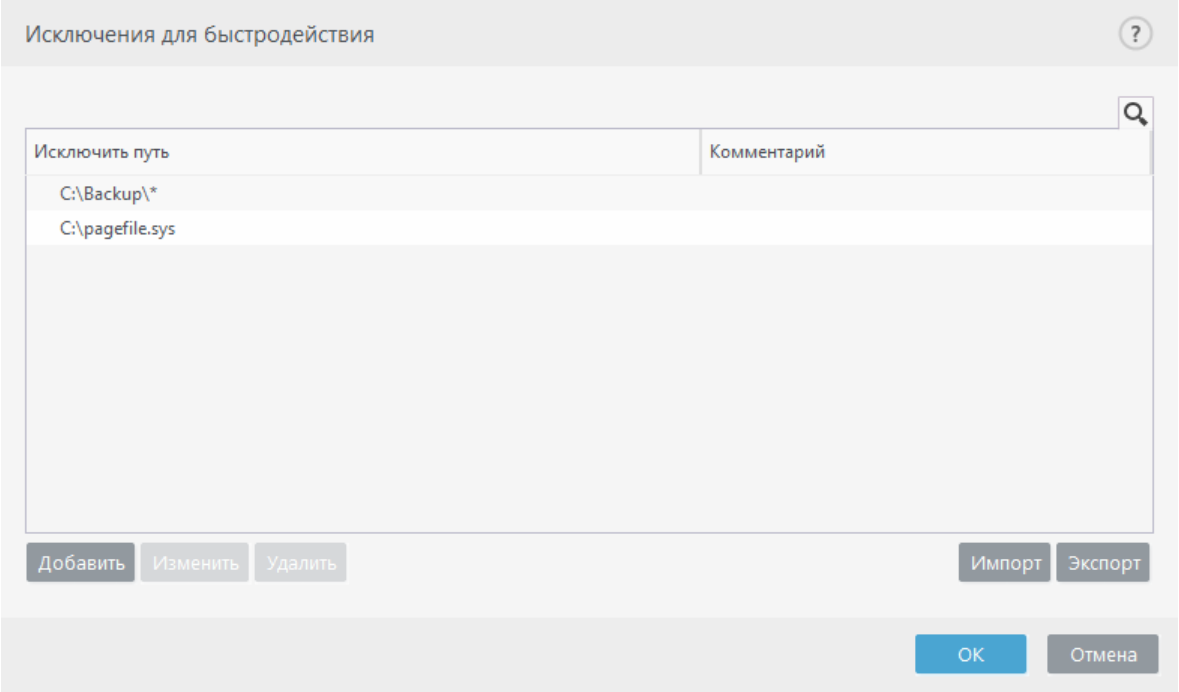
Исключения для быстродействия

Исключения для быстродействия позволяют исключить файлы и папки из сканирования.

Мы рекомендуем создавать исключения для быстродействия только при абсолютной необходимости, чтобы гарантировать, что все объекты просканированы на наличие угроз. Однако, все же могут быть ситуации, когда вам понадобится исключить объект, например, данные базы данных большой емкости, которые замедляют компьютер во время сканирования, или ПО, которое создает препятствия для сканирования.

Файлы и папки можно исключить из сканирования и поместить в перечень исключений, выбрав **Расширенные параметры** (клавиша F5) > **Модуль обнаружения** > **Исключения** > **Исключения для быстродействия** > **Изменить**.

Чтобы исключить объект (путь: файл или папка) из сканирования, щелкните **Добавить** и введите соответствующий путь или выделите его в древовидной структуре.



> Угроза в файле не будет обнаружена модулем **Защиты файловой системы в реальном времени** или модулем **сканирования компьютера**, если файл соответствует критериям для исключения из сканирования.

Элементы управления

- **Добавить**: добавление новой записи для исключения объектов из сканирования.
- **Изменить**: изменение выделенных записей.
- **Удалить**: удаление выбранных записей (чтобы выбрать несколько записей, щелкайте их, удерживая нажатой клавишу CTRL).
- **Импорт**/**Экспорт**: выполнять импорт и экспорт исключений для быстродействия удобно, если нужно создать резервную копию текущих исключений для использования в будущем. Экспорт параметров также удобен для пользователей в неуправляемых средах,

если необходимо использовать предпочитаемую конфигурацию на нескольких компьютерах. С этой целью можно легко импортировать TXT-файл для переноса нужных параметров.

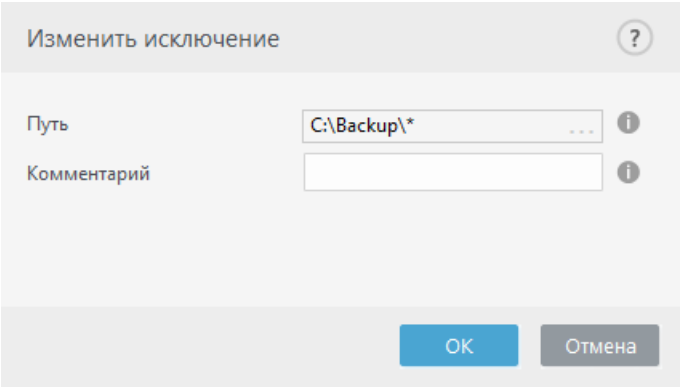
Отображение образца формата для файла импорта/экспорта

```
# {"product":"endpoint","version":"7.2.2055","path":"plugins.01000600.settings.Perfo
rmanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys
```

Добавление или изменение исключений для быстродействия

Диалоговое окно исключает определённый путь (файл или каталог) для этого компьютера.

> Чтобы выбрать нужный путь, выберите **...** в поле **Путь**.
> При ручном вводе см. примеры формата исключения ниже.



Для исключения групп файлов можно использовать символы подстановки. Вопросительный знак (*?*) обозначает один символ, а звездочка (***) — строку из любого количества символов.

• Чтобы исключить все файлы и вложенные папки в определенной папке, укажите путь к папке и используйте маску *
• 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 (знаки вопроса заменяют отсутствующие или неизвестные символы)
Примеры
• *C:\Tools**: путь должен заканчиваться обратной косой чертой ((\)) и звездочкой ((*)), указывающими, что это папка, все содержимое которое (файлы и вложенные папки) следует исключить.
• *C:\Tools*.**: поведение будет аналогично варианту *C:\Tools**
• *C:\Tools*: папку *Tools* не будет исключено. С точки зрения модуля сканирования *Tools* может также быть именем файла.
• *C:\Tools*.dat*: это применяется для исключения файлов .dat в папке *Tools*.
• *C:\Tools\sg.dat*: применяется для исключения отдельного файла, размещенного в точном пути.

Для определения исключений из сканирования можно использовать системные переменные, например *%PROGRAMFILES%*.
• Чтобы исключить папку «Program Files» с помощью такой системной переменной, укажите в исключениях путь *%PROGRAMFILES%** (не забудьте добавить обратную косую черту и звездочку в конце пути).
• Чтобы исключить все файлы и папки в подкаталоге *%PROGRAMFILES%*, укажите путь *%PROGRAMFILES%\Excluded_Directory**
Развернуть список поддерживаемых системных переменных
Формат исключения пути поддерживает следующие переменные:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
Пользовательские системные переменные (например, *%TEMP%* или *%USERPROFILE%*) и переменные среды (например, *%PATH%*) не поддерживаются.

Программа иногда может правильно исключать из обработки пути с подстановочными знаками в середине (например, *C:\Tools*\Data\file.dat*), но официально эта возможность не поддерживается. Дополнительные сведения см. в следующей статье базы знаний.
При использовании исключений из обнаружения ограничения на использование специальных символов в середине пути не применяются.

Порядок исключений:
• Варианты настройки уровня приоритета для исключений с помощью кнопок «вверх» и «вниз» не предусмотрены (как в разделе Правила файервола, где правила последовательно выполняются сверху вниз) не предусмотрена.
• Когда модуль сканирования обнаруживает совпадение с первым применимым правилом, второе применимое правило не проверяется.
• Чем меньше правил, тем быстрее происходит сканирование.
• Не следует создавать совпадающие правила.

Формат исключения пути

Для исключения групп файлов можно использовать символы подстановки. Вопросительный знак (*?*) обозначает один символ, а звездочка (***) — строку из любого количества символов.

- Чтобы исключить все файлы и вложенные папки в определенной папке, укажите путь к папке и используйте маску ***
- 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 (знаки вопроса заменяют отсутствующие или неизвестные символы)

Примеры

- *C:\Tools**: путь должен заканчиваться обратной косой чертой ((\)) и звездочкой ((*)), указывающими, что это папка, все содержимое которое (файлы и вложенные папки) следует исключить.
- *C:\Tools*.**: поведение будет аналогично варианту *C:\Tools**
- *C:\Tools*: папку *Tools* не будет исключено. С точки зрения модуля сканирования *Tools* может также быть именем файла.
- *C:\Tools*.dat*: это применяется для исключения файлов .dat в папке *Tools*.
- *C:\Tools\sg.dat*: применяется для исключения отдельного файла, размещенного в точном пути.

Для определения исключений из сканирования можно использовать системные переменные, например *%PROGRAMFILES%*.

- Чтобы исключить папку «Program Files» с помощью такой системной переменной, укажите в исключениях путь *%PROGRAMFILES%** (не забудьте добавить обратную косую черту и звездочку в конце пути).
- Чтобы исключить все файлы и папки в подкаталоге *%PROGRAMFILES%*, укажите путь *%PROGRAMFILES%\Excluded_Directory**

Развернуть список поддерживаемых системных переменных

Формат исключения пути поддерживает следующие переменные:

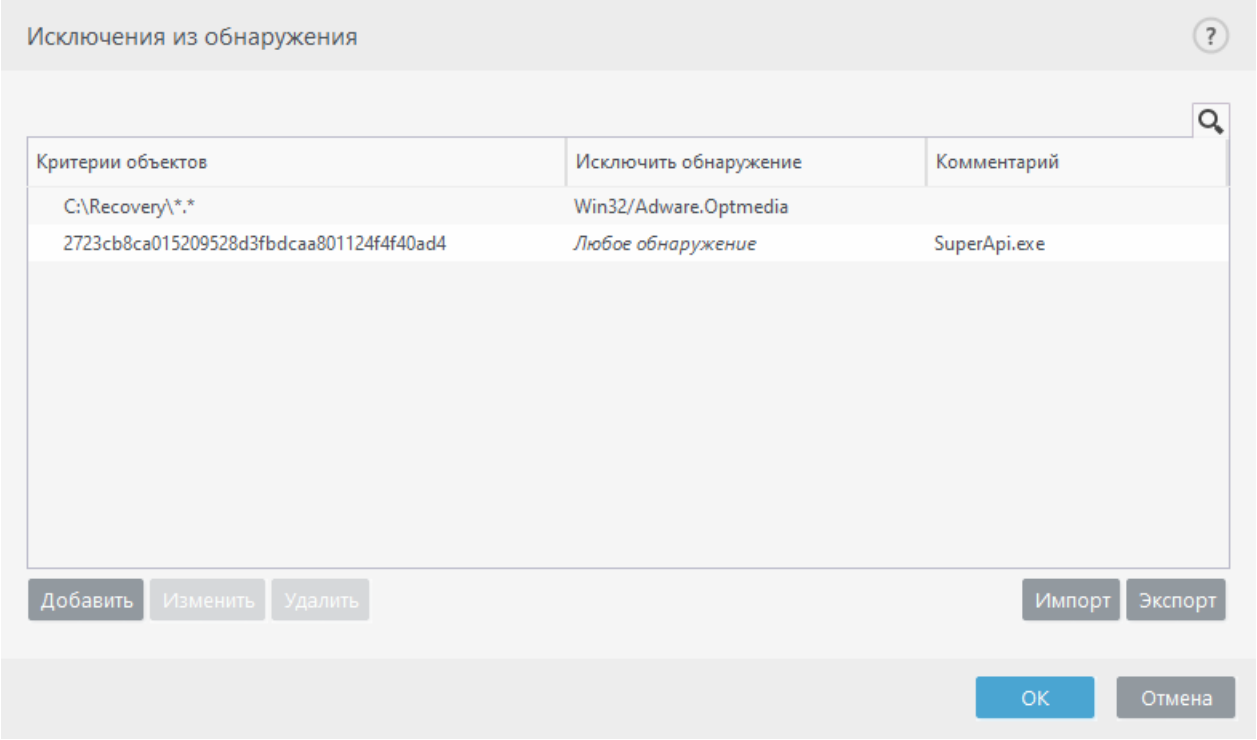
- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Пользовательские системные переменные (например, *%TEMP%* или *%USERPROFILE%*) и переменные среды (например, *%PATH%*) не поддерживаются.

Исключения из обнаружения

Исключения из обнаружения позволяют исключить объекты из списка очищения путем фильтрации имени обнаружения, пути объекта или его хеша.

Исключения из обнаружения не исключают файлы и папки из сканирования, как делают Исключения для быстродействия. Исключения обнаружения исключают объекты только тогда, когда они обнаружены механизмом обнаружения и в списке исключений присутствует соответствующее правило.
Например (см. первый ряд на изображении ниже), когда объект определяется как Win32/Adware.Optmedia и обнаруженный файл — *C:\Recovery\file.exe*. Во второй строке, каждый файл, в котором есть подходящий хеш SHA-1, всегда будет исключен, несмотря на имя обнаружения.



Чтобы убедиться, что все угрозы обнаружены, мы рекомендуем создавать исключения из обнаружения только тогда, когда это абсолютно необходимо.

Чтобы добавить файлы и папки в список исключений, выберите **Расширенные параметры** (клавиша F5) > **Модуль обнаружения** > **Исключения** > **Исключения из обнаружения** > **Изменить**.

Чтобы исключить объект (по названию обнаружения или хешу) из очистки, нажмите **Добавить**.

Для потенциально нежелательных и потенциально опасных приложений также можно создать исключение по имени обнаружения.

- В окне предупреждения, которое сообщает об обнаружении (щелкните **Показать расширенные параметры** и выберите **Исключить из обнаружения**).

- Из контекстного меню «Файлы журнала» с помощью Мастера создания исключения из обнаружения.

- Щелкнув **Инструменты** > **Карантин**, после чего щелкнув правой кнопкой мыши находящийся на карантине файл и выбрав в контекстном меню команду **Восстановить и исключить из сканирования**.

Критерии объектов исключения из обнаружения

- **Путь**. Ограничение исключения из обнаружения для определенного пути (или любого другого пути).
- **Имя обнаружения**: если рядом с исключаемым файлом указано имя обнаружения, файл исключается только для этого обнаружения, а не полностью. Если этот файл впоследствии окажется зараженным другой вредоносной программой, он будет обнаружен.
- **Хеш**: файл исключается на основании указанного хеша SHA-1 независимо от типа, расположения, имени или расширения.

Элементы управления

- **Добавить**: добавление новой записи для исключения объектов из очистки.
- **Изменить**: изменение выделенных записей.
- **Удалить**: удаление выбранных записей (чтобы выбрать несколько записей, щелкайте их, удерживая нажатой клавишу CTRL).
- **Импорт/Экспорт**: выполнять импорт и экспорт исключений из обнаружения удобно, если нужно создать резервную копию текущих исключений для использования в будущем. Экспорт параметров также удобен для пользователей в неуправляемых средах, если необходимо использовать предпочитаемую конфигурацию на нескольких компьютерах. С этой целью можно легко импортировать TXT-файл для переноса нужных параметров.
  Отображение образца формата для файла импорта/экспорта

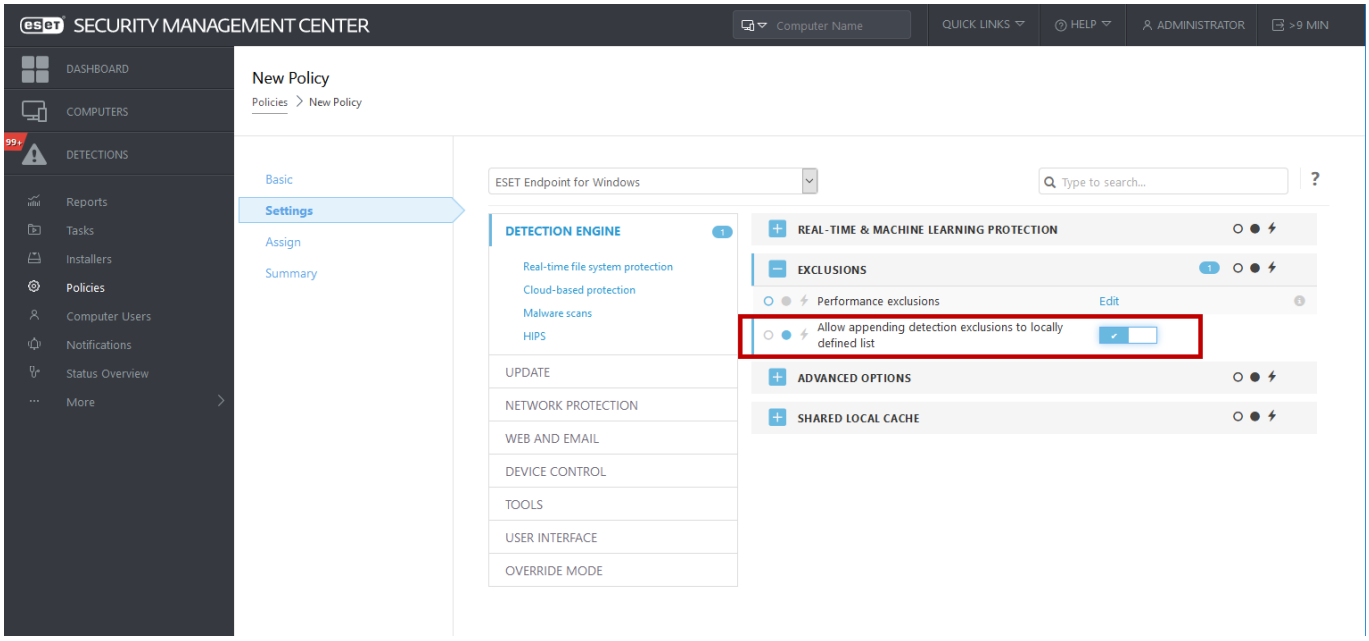
```
# {"product":"endpoint","version":"7.2.2055","path":"Settings.ExclusionsManagement.D
etectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}

4c59cd02-357c-4b20-a0ac-
ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,,
```

Настройка исключений из обнаружения в ESET PROTECT

ESMC версии 7.1 и ESET PROTECT версии 8.0 включает новый мастер управления исключениями обнаружения— создание исключения из обнаружения и применение его к большему количеству компьютеров/групп.

Возможные исключения из обнаружения из ESET PROTECT

При наличии локального списка исключений обнаружения, администратор должен применить политику с помощью **Разрешать добавление исключения из обнаружения к локально заданному списку**. После этого, добавление исключение из обнаружения из ESET PROTECT будет работать, как и ожидалось.

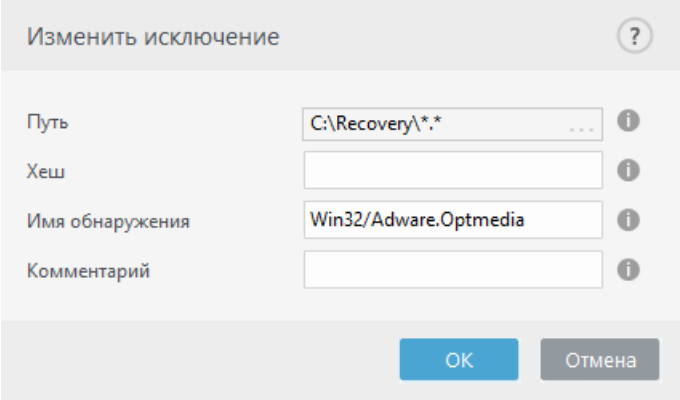


Добавление или изменение исключений из обнаружения

Исключить обнаружение

Следует указать действительное имя для обнаружения ESET. Чтобы определить имя обнаружения, перейдите в раздел Файлы журнала и выберите элемент **Обнаружения** в раскрывающемся меню «Файлы журнала». Этот параметр полезен при обнаружении образца ложного срабатывания в ESET Endpoint Security. Добавлять в исключения реальные заражения крайне опасно. Рекомендуем исключать только затронутые файлы или каталоги, щелкнув элемент **...** в поле **Маска пути**, либо делать это только на ограниченный период времени. Исключения также применяются к потенциально нежелательным, потенциально опасным и подозрительным приложениям.

См. также Формат исключения пути.

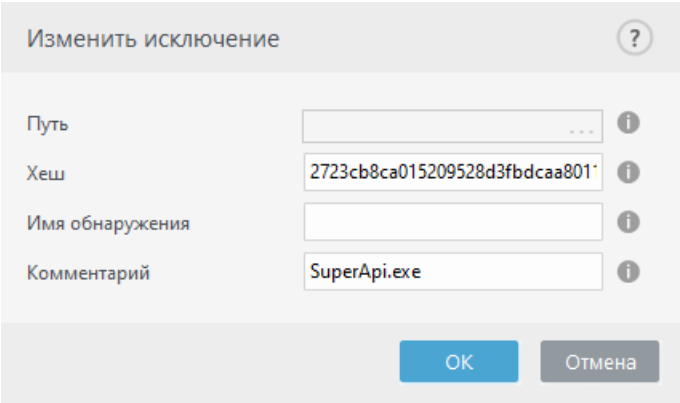


См. также Пример исключения из обнаружения, который приведен ниже.

Исключить хеш

Файл исключается на основании указанного хеша SHA-1 независимо от типа, расположения,

имени или расширения.



Чтобы исключить определенное обнаружение по имени, введите правильное имя обнаружения:
Win32/Adware.Optmedia
Также для исключения обнаружения с помощью окна предупреждения ESET Endpoint Security можно воспользоваться приведенным далее форматом:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Элементы управления

- **Добавить**: команда, исключающая объекты из сканирования.
- **Изменить**: изменение выделенных записей.
- **Удалить**: удаление выбранных записей (чтобы выбрать несколько записей, щелкайте их, удерживая нажатой клавишу CTRL).

Создание исключения из обнаружения мастера

Исключение из обнаружения также можно создать из контекстного меню Файлы журнала (недоступно для обнаружения вредоносных программ):

1. В главном окне программы щелкните **Инструменты** > **Файлы журнала**.
2. Щелкните правой кнопкой мыши обнаружение в разделе **Журнал обнаружений**.
3. Выберите **Создать исключение**.

Чтобы исключить одно или несколько обнаружений на основе **критерии исключения**, щелкните элемент **Изменить критерии**:

- **Точные файлы**: исключение каждого файла по хешу SHA-1.
- **Обнаружение**: исключение каждого файла по имени обнаружения.

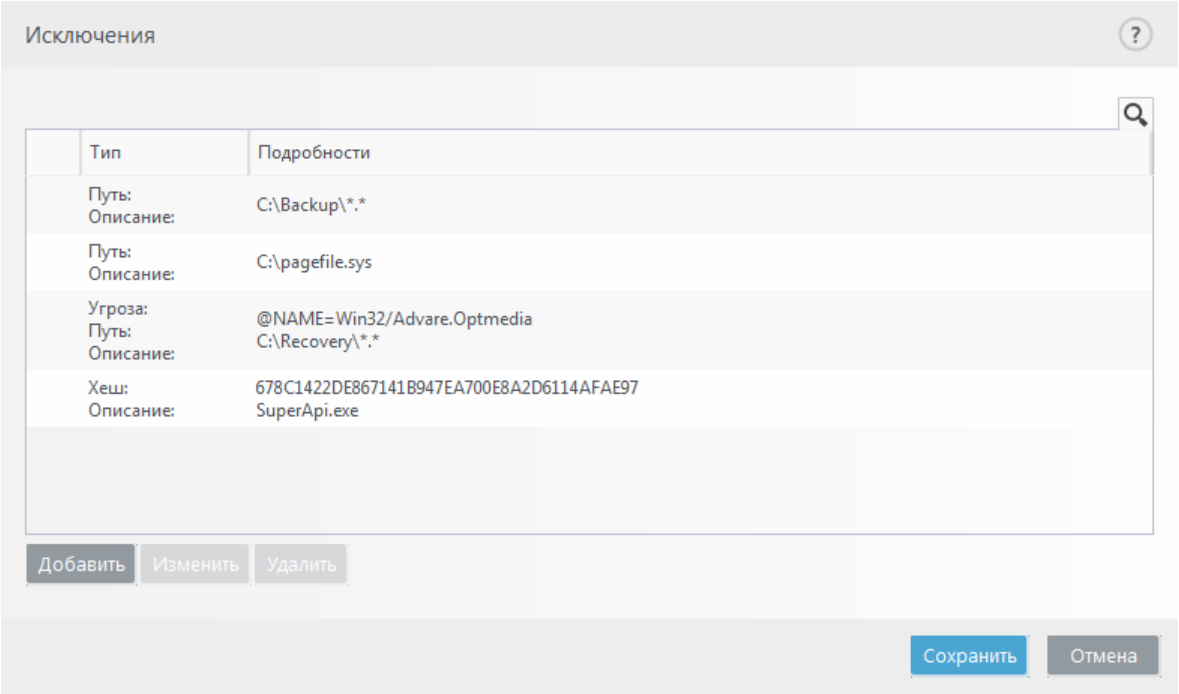
• **Путь + обнаружение**: исключение каждого файла по имени и пути обнаружения, включая имя файла (например, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Рекомендуемая опция выбирается предварительно в зависимости от типа обнаружения.

Кроме того, перед нажатием на элемент **Создать исключение** вы можете добавить **комментарий**.

Исключения (версия 7.1 или более ранняя)

Исключения в версии 7.1 и более ранних версиях включают в себя следующее: Исключения для быстродействия и Исключения из обнаружения, которые объединены.



Исключения для процессов

Функция исключений для процессов позволяет исключать процессы приложений из Защиты файловой системы в реальном времени. Некоторые методики, используемые при резервном копировании и призванные повысить его скорость, улучшить целостность процессов и доступность служб, вызывают конфликт с защитой от вредоносных программ на уровне файлов. Аналогичные проблемы могут возникать при попытках динамической миграции виртуальных машин. Единственный действенный способ избежать таких проблем — отключить антивирусное ПО. При исключении отдельных процессов (например, отвечающих за резервное копирование) все операции с файлами таких процессов игнорируются и считаются безопасными, что снижает отрицательное влияние на процесс резервного копирования. Создавать исключения следует с осторожностью — добавленное в исключение средство резервного копирования может получить доступ к зараженным файлам, не выдав при этом оповещения, поэтому расширенные разрешения доступны только для модуля защиты в реальном времени.

Исключения для процессов позволяют снизить риск возникновения конфликтов и повысить производительность исключенных приложений, что положительно сказывается на производительности и стабильности операционной системы в целом. Исключение для процесса или приложения предполагает исключение и для его исполняемого файла (*.exe*).

Добавить исполняемые файлы в список исключаемых процессов можно с помощью команды **Расширенные параметры** (F5) > **Модуль обнаружения** > **Защита файловой системы в режиме реального времени** > **Исключения для процессов**.

Эта функция предназначена для добавления в исключения средств резервного копирования. Исключение из сканирования процессов, выполняемых средством резервного копирования, обеспечивает стабильность системы и способствует лучшей производительности резервного копирования, не замедляя его.

Щелкните **Изменить**, чтобы открыть окно управления **Исключения для процессов**, в котором можно добавить исключения и выбрать исполняемые файлы (например *Backup-tool.exe*), которые будут исключены из сканирования.
Если файл *.exe* добавлен в перечень исключений, ESET Endpoint Security не выполняет мониторинг его действий, как и не сканируются любые операции с файлами, выполняемые этим процессом.

Если исполняемый файл не выбран с помощью функции обзора, необходимо указать полный путь к файлу, иначе исключение не будет работать правильно, а система HIPS может выдавать сообщения об ошибке.

Для существующих процессов также доступны функции **изменения** и **удаления** из исключений.

Защита доступа в Интернет не принимает во внимание такие исключения. Если вы добавили в исключение исполняемый файл своего веб-браузера, скачиваемые файлы по-прежнему будут сканироваться. Это позволит обнаружить зараженные файлы. Это разъяснение дано в познавательных целях, и мы не рекомендуем добавлять в исключение веб-браузер.

Добавление или изменение исключений процессов

В этом диалоговом окне можно **добавлять** процессы, исключаемые из модуля обнаружения. Исключения для процессов позволяют снизить риск возникновения конфликтов и повысить производительность исключенных приложений, что положительно сказывается на производительности и стабильности операционной системы в целом. Исключение для процесса или приложения предполагает исключение и для его исполняемого файла (*.exe*).

Выберите путь к файлу исключенного приложения, щелкнув ... (например, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводите имя приложения.
Если файл *.exe* добавлен в перечень исключений, ESET Endpoint Security не выполняет мониторинг его действий, как и не сканируются любые операции с файлами, выполняемые этим процессом.

Если исполняемый файл не выбран с помощью функции обзора, необходимо указать полный путь к файлу, иначе исключение не будет работать правильно, а система HIPS может выдавать сообщения об ошибке.

Для существующих процессов также доступны функции **изменения** и **удаления** из исключений.

Исключения системы HIPS

С помощью исключений можно исключать процессы из глубокой поведенческой проверки системы HIPS.

Чтобы исключить объект, щелкните **Добавить** и введите путь к объекту или выделите его в древовидной структуре. Выбранные записи также можно **изменять** и **удалить**.

Ознакомьтесь с главой Исключения.

ThreatSense параметры

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.

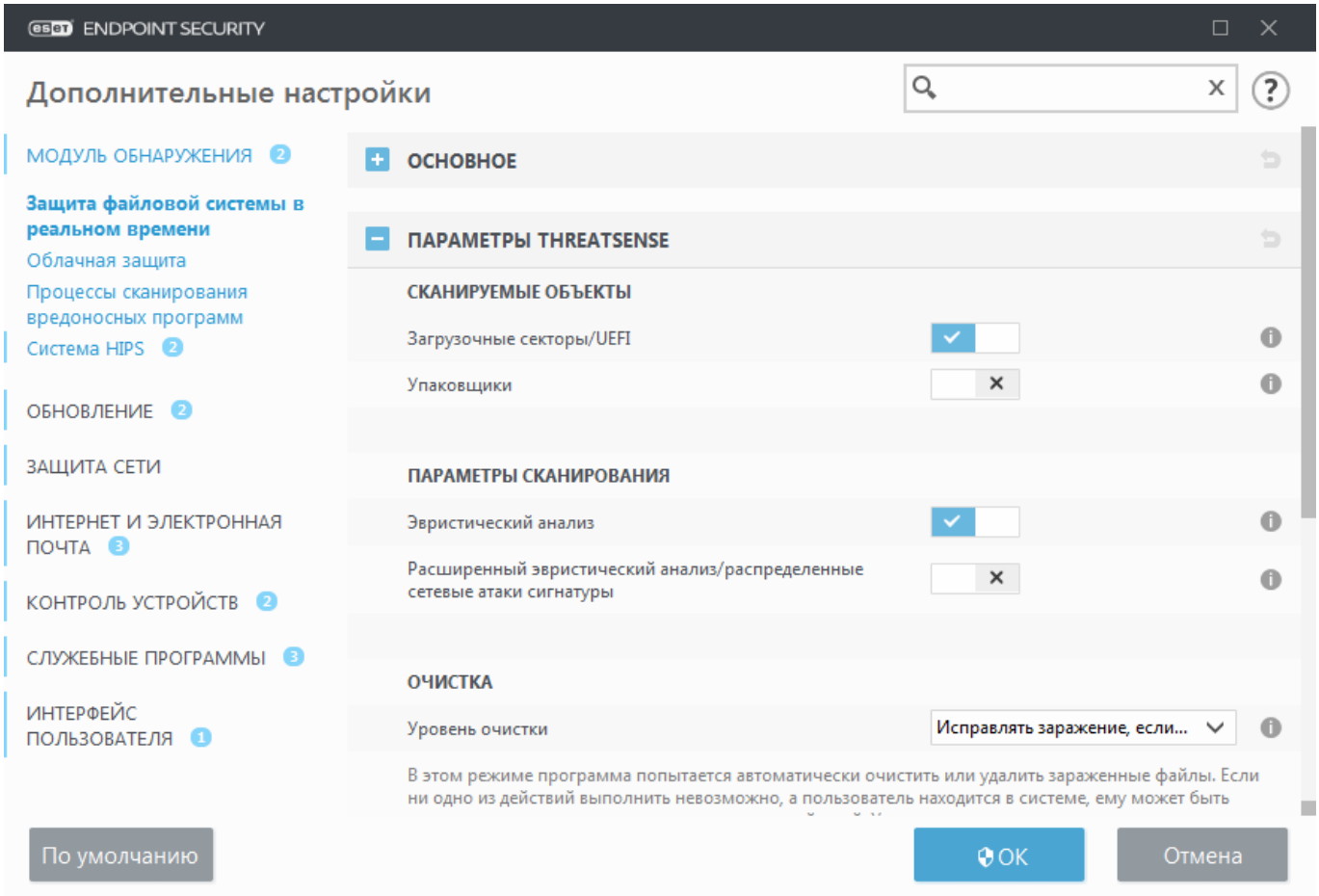
Для модуля ThreatSense можно настроить несколько параметров сканирования:

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

Чтобы открыть окно параметров, щелкните **Параметры ThreatSense** в окне расширенных параметров 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 при запуске
- 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. Загрузочные секторы сканируются на наличие вредоносных программ в основной загрузочной записи. Дополнительные сведения о UEFI см. в глоссарии.

Почтовые файлы. Программа поддерживает расширения 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. Тип архивов (SFX), содержимое которых может

извлекаться автоматически.

Программы сжатия исполняемых файлов: в отличие от стандартных типов архивов, программы сжатия исполняемых файлов после запуска распаковываются в памяти. Благодаря эмуляции кода модуль сканирования распознает не только стандартные статические упаковщики (UPX, yoda, ASPack, FSG 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).

Очистка

Параметры очистки определяют поведение ESET Endpoint Security при очистке объектов.

Исключения

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

Другое

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

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

Запускать фоновое сканирование с низким приоритетом: каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь работает с ресурсоемкими программами, можно активировать фоновое сканирование с низким

приоритетом и высвободить тем самым ресурсы для других приложений.

Журнал всех объектов. Журнал проверки отображает все отсканированные файлы в самораспаковывающихся архивах, даже незараженные (может создавать большое количество данных журнала сканирования и увеличивать размер его файла).

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.

Максимальное время сканирования объекта (с): определяет максимальное значение времени сканирования файлов в объекте контейнера (например, архив RAR/ZIP или электронная почта с несколькими вложениями). Эта настройка не применяется к отдельным файлам. Если пользователь укажет собственное значение и указанное время истечет, сканирование будет остановлено как можно скорее, вне зависимости от того, завершено ли сканирование каждого файла в объекте контейнера.

Если речь идет об архиве с большими файлами, сканирование будет прекращено не раньше, чем произойдет извлечение файла из архива (например, когда пользовательская переменная задается в 3 секунды, но извлечение файла занимает 5 секунд). Остальные файлы в архиве не будут сканироваться по истечении этого времени.
Чтобы ограничить время сканирования, в том числе архивов большего размера, используйте параметры **Максимальный размер объекта** и **Максимальный размер файла в архиве** (не рекомендуется в связи с возможными проблемами безопасности).
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.

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

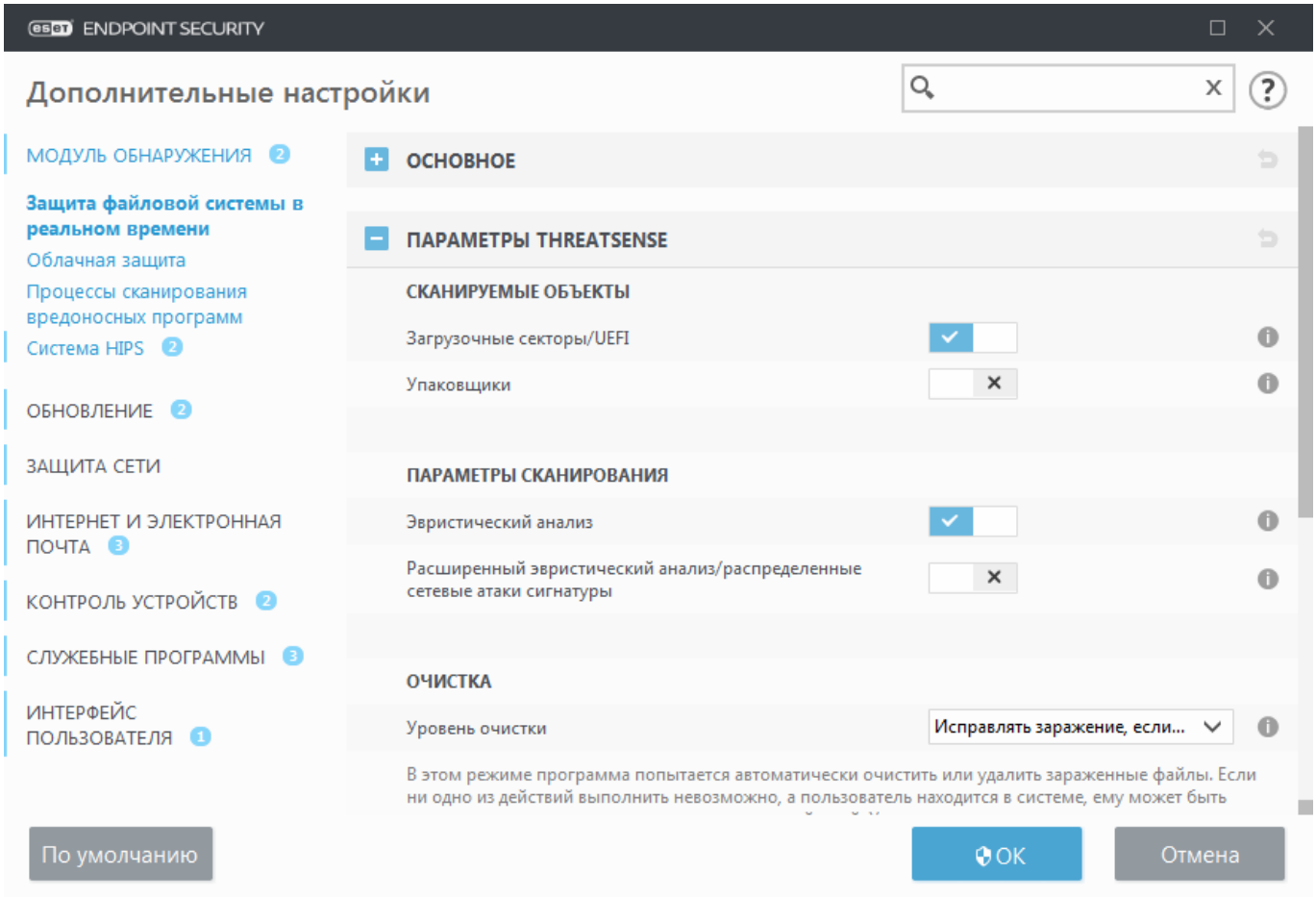
Уровни очистки

Чтобы получить доступ к настройкам уровня очистки для нужного модуля защиты, разверните **Параметры ThreatSense** (например, **Защита файловой системы в реальном времени**) и нажмите **Очистка**.

Защита в реальном времени и другие модули защиты имеют следующие уровни исправления (то есть очистки).

Исправление в ESET Endpoint Security 8

Уровень очистки	Описание
Всегда исправлять обнаружения	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, с системными файлами), если обнаружение не удается исправить, обнаруженный объект оставляется в исходном расположении. Функция **Всегда исправлять обнаружения** является рекомендуемой настройкой по умолчанию в управляемой среде.
Исправлять обнаружения, если это безопасно, в другом случае оставить	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, системные файлы или архивы, которые содержат и чистые, и зараженные файлы), если обнаружение не удается исправить, обнаруженный объект остается в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае спрашивать	Пытаться исправлять обнаружения при очистке объектов. В некоторых случаях, если ни одно из действий выполнить невозможно, конечный пользователь получает интерактивное предупреждение, в котором следует выбрать действие по исправлению (например, удалить или проигнорировать). Этот параметр рекомендуется в большинстве случаев.
Всегда спрашивать у конечного пользователя	Конечному пользователю отображается интерактивное окно при очистке объектов, и он должен выбрать действие по исправлению (например, удалить или пропустить). Этот уровень предназначен для более опытных пользователей, которые знают, какие действия следует предпринять в случае обнаружения.



Исключенные из сканирования расширения файлов

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.

> ℹ Не стоить путать с другими типами Исключений.

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.

> ✓ Для добавления в список нового расширения нажмите **Добавить**. Введите расширение в пустое поле (например, `tmp`) и нажмите кнопку **OK**. Выбрав вариант **Добавить несколько значений**, можно добавить несколько расширений имен файлов, разделив их символом перевода строки, запятой или точкой с запятой (например, выберите **Точка с запятой** из раскрывающегося меню в качестве разделителя и введите `edb;eml;tmp`). Можно использовать специальный символ «?» (вопросительный знак). Вопросительный знак представляет любой символ (например, `?db`).

> Чтобы расширения файлов отображались в операционной системе Windows, снимите флажок **Скрывать расширения для зарегистрированных типов файлов**, выбрав **Панель управления** > **Свойства папки** > **Вид** и примените это изменение.

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.

Сеть

С помощью раздела **Сеть** вы можете быстро перейти к следующим компонентам и настройкам меню «**Расширенные параметры**»:

- **Файервол**. Здесь можно настроить режим фильтрации для файервола ESET ***. Доступ к дополнительным настройкам можно получить, щелкнув значок шестеренки ⚙ > **Настроить** рядом с элементом **Файервол** или нажав клавишу **F5**, которая вызывает меню **Расширенные параметры**.

- **Защита от сетевых атак (IDS)**: анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который определяется как «вредоносный», будет заблокирован. ESET Endpoint Security будет информировать при подключении к незащищенной беспроводной сети или сети со слабой защитой.

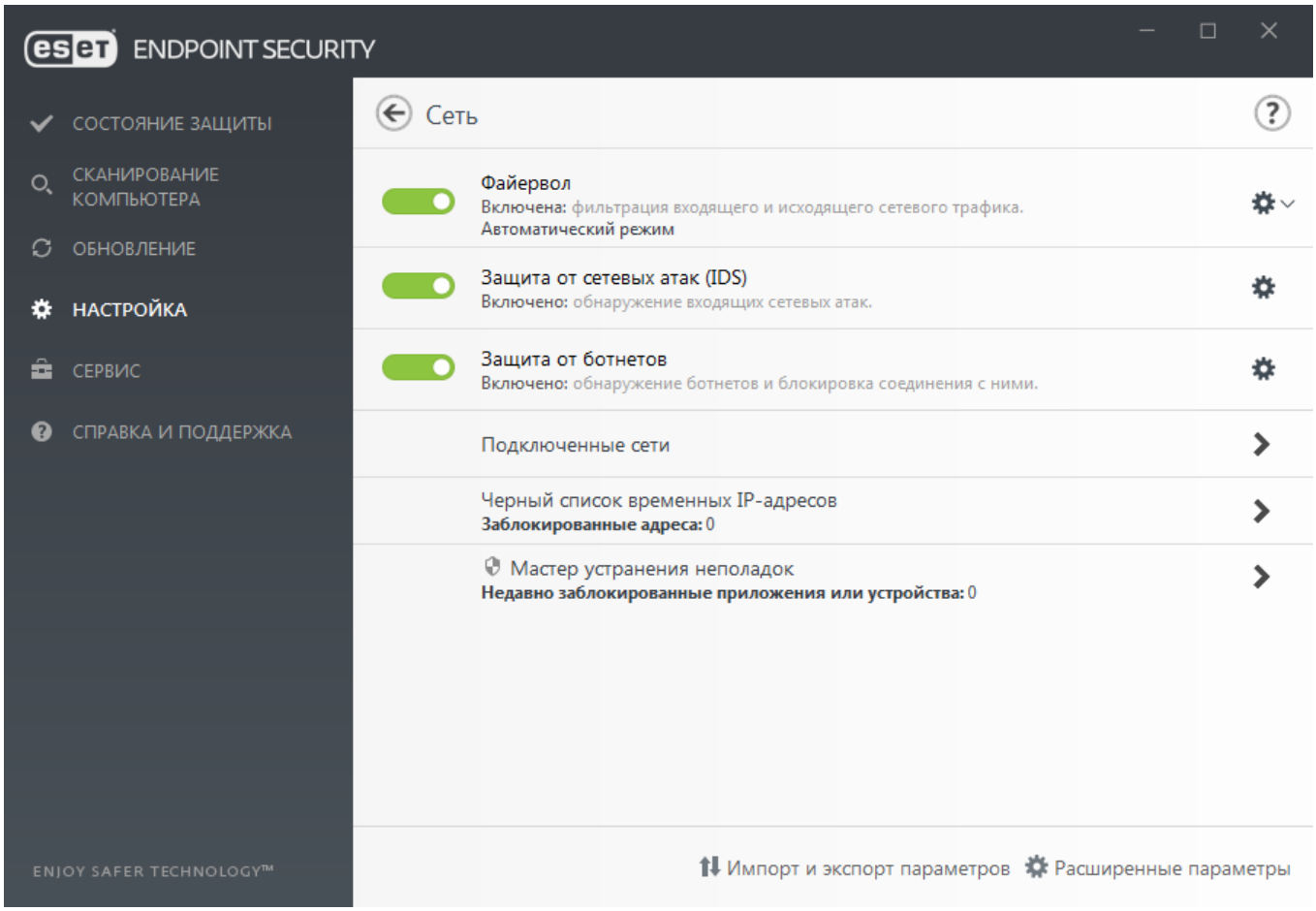
- **Защита от ботнетов**: быстро и точно определяет вредоносные программы в системе. Защиту от ботнетов можно на некоторое время отключить. Для этого щелкните элемент (не рекомендуется).

- **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. В этом окне вы также

можете увидеть **Сетевые адаптеры** в нижнем правом углу. Можно просмотреть каждый сетевой адаптер и его профиль файервола и доверенную зону. Более подробную информацию см. в разделе Сетевые адаптеры.

• **Временный черный список 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**: открывается окно «Файервол» в меню дополнительных настроек, в котором можно определить, каким образом файервол будет обрабатывать сетевой обмен данными.

• **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

блокированию всего сетевого трафика. В этом режиме файервол отключает все функции фильтрации и разрешает все входящие и исходящие соединения. Чтобы повторно включить файервол, когда для фильтрации сетевого трафика включен этот режим, щелкните **Включить файервол**.

• **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.

файервол;

Файервол контролирует весь входящий и исходящий сетевой трафик, разрешая или запрещая (на основе заданных правил фильтрации) те или иные сетевые подключения. Он обеспечивает защиту от атак с удаленных компьютеров и позволяет блокировать некоторые потенциально опасные службы.

Основные сведения

Включить файервол

рекомендуется оставить эту функцию включенной, чтобы обеспечить защиту системы. При включенном файерволе сетевой трафик сканируется в обоих направлениях.

Оценить также правила файервола Windows

В автоматическом режиме разрешать также входящий трафик, разрешенный правилами файервола Windows и не заблокированный явным образом правилами ESET.

> Правила брандмауэра Windows, настроенные с помощью групповой политики (GPO), не оцениваются.

Режим фильтрации

Поведение файервола зависит от выбранного режима фильтрации. От него также зависит степень участия пользователя в процессе.

Для файервола ESET Endpoint Security доступны следующие режимы фильтрации:

Режим фильтрации	Описание
Автоматический режим	Автоматический режим — режим по умолчанию. Этот режим подходит для пользователей, которым нравится простота и удобство использования персонального файервола, а также отсутствие необходимости создавать правила. В режиме по умолчанию можно создавать пользовательские правила, однако это не необходимо. В **автоматическом режиме** разрешен весь исходящий трафик системы и блокируется большая часть входящего трафика — кроме некоторого трафика из доверенной зоны (как указано в разделе IDS и расширенные параметры/Разрешенные службы) и ответов на недавний исходящий трафик.
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 соответствуют 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, но его не следует использовать длительное время. Участие пользователя не требуется, потому что ESET Endpoint Security сохраняет правила согласно предварительно настроенным параметрам. Чтобы избежать рисков, режим обучения рекомендуется использовать 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.

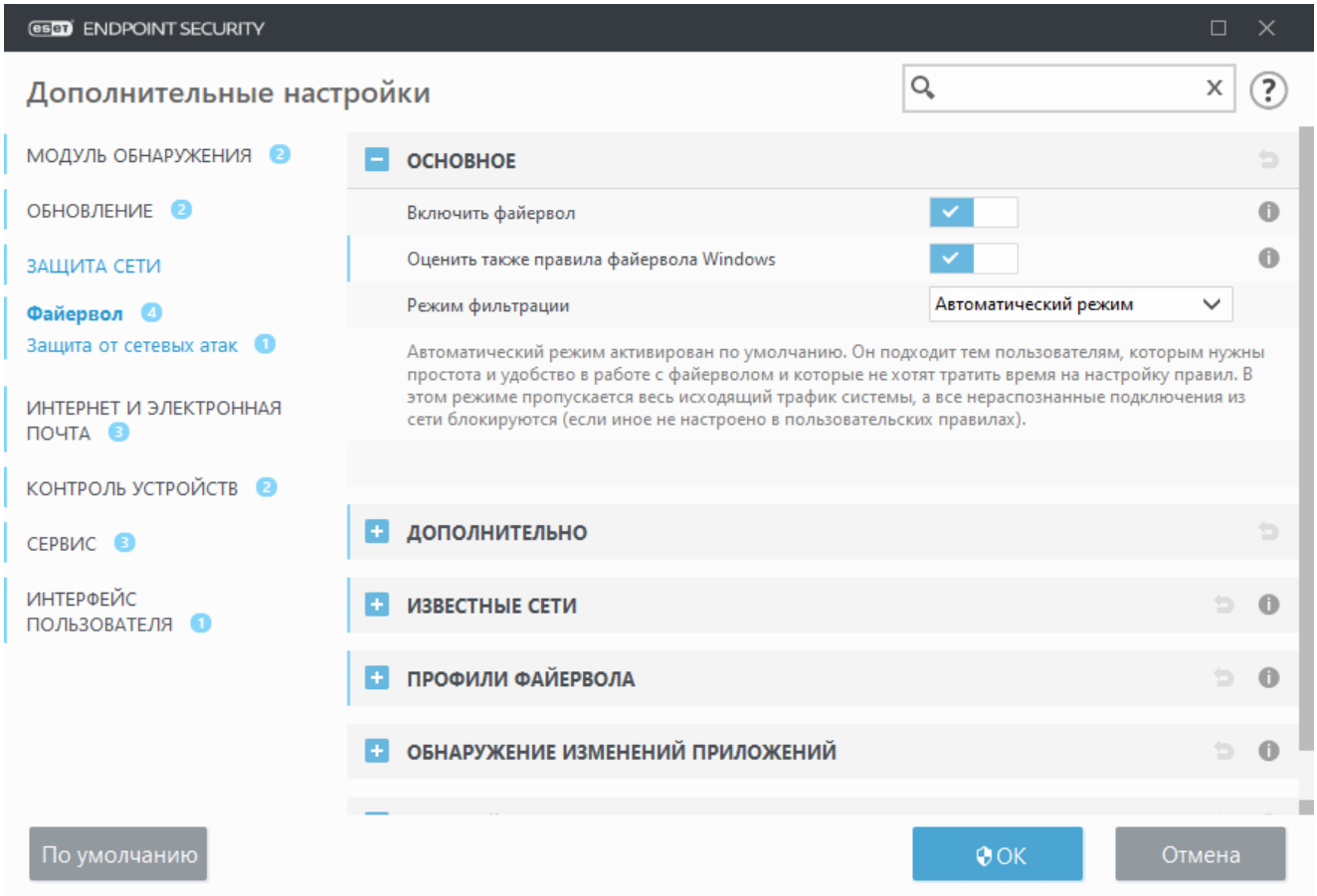
Дополнительно

Правила

В разделе настройки правил можно просмотреть все правила, которые применяются к трафику, создаваемому отдельными приложениями в пределах доверенных зон и сети Интернет.

Зоны

Зона — это набор сетевых адресов, объединенных в логическую группу.



Вы можете создать правило IDS, когда ботнет атакует ваш компьютер. Исключение можно изменить в разделе **Расширенные параметры** (клавиша F5) > **Защита сети** > **Защита от сетевых атак** > **Правила IDS**, щелкнув **Изменить**.

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 файервола.

Последовательно выберите **Расширенные параметры** (F5) > **Файервол** > **Основная информация** > **Режим фильтрации** и в раскрывающемся меню выберите пункт **Режим обучения**, чтобы активировать **параметры режима обучения**. В этом разделе представлены следующие параметры.

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

Режим задан после завершения режима обучения: определите режим фильтрации, который будет восстановлен файерволом программы ESET Endpoint Security по завершении периода режима обучения. См. дополнительные сведения о режимах фильтрации. Чтобы после завершения режима обучения изменить режим фильтрации файервола на Спросить пользователя, нужны права администратора.

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 используются 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.

Защита от сетевых атак

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 подключаться к

опасным серверам.Дополнительные сведения о защите от ботнетов см. в глоссарии.

Правила IDS: Позволяет настраивать расширенные параметры фильтрации для обнаружения различных типов атак, которые могут быть предприняты, чтобы навредить компьютеру.

Расширенные параметры фильтрации

В разделах «Файервол» и «Защита от сетевых атак» можно настроить расширенные параметры фильтрации для обнаружения нескольких типов атак и уязвимостей, которые злоумышленники могут применить против вашего компьютера.

> В некоторых случаях уведомление о заблокированном соединении не отображается. См. раздел Ведение журнала и создание правил и исключений на основе журнала, чтобы узнать, как просматривать заблокированные соединения в журнале файервола.

> Доступность отдельных параметров в разделах «Расширенные параметры» (**F5**) > **Защита сети** > **Файервол** и «Расширенные параметры» (**F5**) > **Защита сети** > **Защита от сетевых атак** зависит от типа или версии модуля файервола, а также от версии операционной системы.

Разрешенные службы

Параметры в этой группе предназначены для облегчения настройки доступа к службам этого компьютера из доверенной зоны. С помощью многих из них можно включить или отключить предопределенные правила файервола.

- **Разрешить общий доступ к файлам и принтерам в доверенной зоне**: позволяет открыть доступ к файлам и принтерам общего доступа с удаленных компьютеров, расположенных в доверенной зоне.
- **Разрешить UPNP для системных служб в доверенной зоне**: разрешает протоколы UPnP входящих и исходящих запросов для системных служб. Технология UPnP (Universal Plug and Play, также известная как Microsoft Network Discovery) используется в Windows Vista и более поздних версиях операционной системы.
- **Разрешить входящие соединения RPC в доверенной зоне**: позволяет устанавливать TCP-соединения из доверенной зоны, предоставляя доступ к программе сопоставления портов MS RPC и службам RPC/DCOM.
- **Разрешить удаленный рабочий стол в доверенной зоне**: позволяет подключаться по протоколу удаленного рабочего стола Microsoft (RDP) и предоставляет компьютерам в доверенной зоне доступ к вашему компьютеру с помощью программы, которая использует протокол RDP (например, программы для подключения к удаленному рабочему столу). Узнайте, как разрешить RDP-соединения за пределами доверенной зоны.
- **Разрешить вход в многоадресные группы по IGMP**: разрешает входящие и исходящие многоадресные потоки IGMP и входящие многоадресные потоки UDP, например потоковую передачу видеоданных, созданных программами, которые используют протокол IGMP (протокол управления группами Интернета).
- **Разрешить соединенные мостом подключения**: выберите этот параметр, чтобы избежать прерывания соединенных мостом подключений. Сетевой мост подключает виртуальную машину к сети с помощью адаптера Ethernet главного компьютера. При использовании сетевых мостов виртуальная машина может получать доступ к другим устройствам в сети и наоборот, как если бы это был физический компьютер в сети.

• **Разрешить автоматическое обнаружение веб-служб (WSD) для системных служб в доверенной зоне**: разрешает входящие запросы обнаружения веб-служб из доверенных зон через файервол. WSD — это протокол, используемый для обнаружения служб в локальной сети.

• **Использовать разрешение групповых адресов в доверенной зоне (LLMNR)**: LLMNR (Link-local Multicast Name Resolution) — это протокол на основе пакетов DNS, который разрешает и узлам IPv4, и узлам IPv6 выполнять разрешение имен для узлов в той же локальной ссылке без необходимости в DNS-сервере или настройке клиента DNS. Этот параметр разрешает входящие многоадресные DNS-запросы из доверенной зоны через файервол.
• **Поддержка домашних групп Windows**: включает поддержку домашних групп для Windows 7 и более поздних версий операционной системы. Домашняя группа может использовать общий доступ к файлам и принтерам в домашней сети. Для настройки домашней группы воспользуйтесь меню **Пуск** > **Панель управления** > **Сеть и Интернет** > **Домашняя группа**.

Обнаружение вторжения

• **Протокол SMB**: обнаруживает и блокирует разные проблемы с безопасностью в протоколе SMB (подробности указаны ниже).

• **Обнаружение атаки в виде нестандартной задачи сервера при проверке подлинности**: обеспечивает защиту от атаки, использующей нестандартную задачу во время аутентификации, чтобы получить учетные данные пользователя.

• **Обнаружение попытки обхода IDS при открытии именованного канала**: обнаружение известных методов обхода именованных каналов MSRPCS в протоколе SMB.

• **Обнаружение общих уязвимостей и слабых мест** (CVE): применяемые методы обнаружения различных атак, червей, брешей в системе безопасности и эксплойтов в протоколе SMB. Более подробные сведения об идентификаторах CVE приводятся на веб-сайте CVE по адресу cve.mitre.org.

• **Протокол RPC**: обнаруживает и блокирует различные идентификаторы CVE в системе удаленного вызова процедур, разработанной для среды распределенных вычислений (DCE).
• **Протокол RDP**: обнаруживает и блокирует различные идентификаторы CVE в протоколе RDP (см. выше в этом разделе).
• **Обнаружение подделки записей кэша ARP**: обнаружение подделки записей кэша ARP, предпринятой с помощью атаки «злоумышленник в середине», или обнаружение сканирования сетевого коммутатора. Протокол ARP (протокол разрешения адреса) используется сетевым приложением или устройством для определения адреса Ethernet.
• **Обнаружение сканирования портов TCP/UPD**: обнаружение ПО сканирования портов, т. е. приложения, предназначенного для выявления открытых портов на узле путем отправления клиентских запросов на диапазон адресов портов и поиска активных портов для использования уязвимости службы. Дополнительную информацию об этом типе атаки см. в глоссарии.
• **Блокировать небезопасный адрес после обнаружения атаки**: IP-адреса, которые были обнаружены в качестве источников атак, будут добавлены в «черный» список, чтобы на некоторое время предотвратить подключение.
• **Показывать уведомление при обнаружении атаки**: включает уведомления на панели

задач в правом нижнем углу экрана.
• **Показывать уведомление при обнаружении атаки, использующей бреши в системе безопасности**: показывает уведомления, если обнаруживается атака, использующая бреши в системе безопасности, или если опасный объект пытается войти в систему через брешь.

Проверка пакетов

• **Разрешить входящее подключение к общим ресурсам администратора по протоколу SMB** : общие ресурсы администратора — это общие сетевые ресурсы по умолчанию, которые совместно используют разделы жесткого диска (*C$*, *D$*, ...) в системе вместе с системной папкой (*ADMIN$*). Отключение соединения с общими ресурсами администратора должны уменьшить возможные последствия угроз безопасности. Например, червь Conficker выполняет атаки перебором по словарю, чтобы подключиться к общим ресурсам администратора.

• **Запретить старые (неподдерживаемые) диалекты SMB**: запрет сеансов SMB, использующих старый диалект SMB, который не поддерживается IDS. Современные операционные системы Windows поддерживают старые диалекты SMB благодаря обратной совместимости со старыми операционными системами, такими как Windows 95. Злоумышленник может использовать старый диалект в сеансе SMB, чтобы избежать контроля трафика. Запретите старые диалекты SMB, если вашему компьютеру не нужно обмениваться файлами (или вообще осуществлять обмен данными SMB) с компьютером под управлением ОС Windows старой версии.

• **Запретить сеансы SMB без расширенной безопасности**: расширенная безопасность может быть использована во время согласования сеанса SMB, чтобы обеспечить более безопасный механизм аутентификации, чем аутентификация LAN Manager Challenge/Response (LM). Схема LM считается слабой и не рекомендуется для использования.

• **Запретить открытие исполняемых файлов на сервере за пределами доверенной зоны в протоколе SMB**: разрывает соединение при попытке запуска исполняемого файла (.exe, .dll и др.) из общей папки на сервере, который не относится к доверенной зоне файервола. Обратите внимание, что копирование исполняемых файлов из надежных источников может быть допустимо. С другой стороны, это обнаружение должно уменьшить риски нежелательного открытия файла на вредоносном сервере (например, если пользователь открыл файл, щелкнув гиперссылку на общий вредоносный исполняемый файл).

• **Запретить аутентификацию NTLM в протоколе SMB при подключении к серверу в доверенной зоне или за ее пределами**: протоколы, которые используют схемы аутентификации NTLM (обе версии), могут подвергаться атакам с попыткой пересылки учетных данных (известны как атаки SMB Relay, если речь идет о протоколе SMB). Если запретить аутентификацию NTLM с использованием сервера, который находится за пределами доверенной зоны, это поможет снизить риски пересылки учетных данных вредоносным сервером, который находится за пределами доверенной зоны. Кроме того, можно запретить аутентификацию NTLM с использованием сервера из доверенной зоны.

• **Разрешить подключение к службе диспетчера учетных записей безопасности**: для получения дополнительных сведений об этой службе см. раздел [MS-SAMR].

• **Разрешить подключение к службе локальной системы безопасности**: для получения

дополнительных сведений об этой службе см. разделы [MS-LSAD] и [MS-LSAT].

- **Разрешить подключение к службе удаленного управления реестром**: для получения дополнительных сведений об этой службе см. раздел [MS-RRP].

- **Разрешить подключение к службе диспетчера служб**: для получения дополнительных сведений об этой службе см. раздел [MS-SCMR].

- **Разрешить подключение к службе сервера**: для получения дополнительных сведений об этой службе см. раздел [MS-SRVS].

- **Разрешить подключение к другим службам** – MSRPC — это реализация Microsoft механизма DCE RPC. Кроме того, MSRPC может использовать именованные каналы, перенесенные в протокол SMB (протокол общего доступа к файлам сети) для транспорта (транспорт ncacn_np). Службы MSRPC предоставляют интерфейсы для удаленного доступа к операционной системе Windows и удаленного управления ею. За последние годы обнаружено несколько уязвимостей, которые используются в среде системы Windows MSRPC (червь Conficker, червь Sasser и др.). Отключите обмен данными со службами MSRPC, которые не нужно предоставлять для уменьшения последствий угроз безопасности (например, удаленное выполнение кода или атаки типа «Отказ в обслуживании»).

Правила IDS

В некоторых случаях система обнаружения вторжения (Intrusion Detection Service, IDS) может расценить передачу информации между маршрутизаторами или другими внутренними сетевыми устройствами как потенциальную атаку. Например, вы можете добавить известный безопасный адрес в адреса, исключенные из системы обнаружения вторжений, чтобы обойти IDS.

> i Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> - Создание правил IDS на рабочих станциях клиента в ESET Endpoint Security (8.x)
> - Создание правил IDS для рабочих станций клиента в ESET PROTECT (8.x)

Столбцы

- **Обнаружение**: тип обнаружения.

- **Приложение**: выберите путь к файлу исключенного приложения, щелкнув ... (например, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводите имя приложения.

- **Удаленный IP-адрес**. Список удаленных адресов, диапазонов или подсетей (IPv4 или IPv6). Для разделения адресов используйте запятую.

- **Блокировать**. Каждый системный процесс имеет свое поведение по умолчанию и назначенное действие (блокировать или разрешить). Для изменения поведения ESET Endpoint Security по умолчанию вы можете разрешить или заблокировать его запуск из раскрывающегося меню.

- **Уведомить**. Выберите Да, чтобы отображать уведомления на рабочем столе на своем компьютере. Выберите Нет, чтобы отключить уведомления. Доступные значения: По

умолчанию, Да, Нет.

• **Записать в журнал**. Выберите **Да**, чтобы записывать события в файлы журнала ESET Endpoint Security. Выберите **Нет**, чтобы отключить запись. Доступные значения: **По умолчанию**, **Да**, **Нет**.

Вкладка «Исключения» отображается в том случае, если администратор создал исключения IDS в веб-консоли ESET PROTECT. Исключения IDS могут содержать только разрешающие правила и оцениваются перед правилами IDS.

Управление правилами IDS

• **Добавить**: нажмите для создания нового правило IDS.
• **Изменить**: нажмите для изменения существующего правила IDS.

• **Удалить**: выберите и щелкните для удаления правила IDS из списка исключений.

• **Вверх/Поднять/Опустить/Вниз**: позволяет настроить уровень приоритета правил (исключения обрабатываются сверху вниз).

Чтобы отображать уведомление и выполнять запись в журнал при каждом возникновении события:
1.Щелкните**Добавить**, чтобы добавить новое правило IDS.
2.Выберите нужное предупреждение в раскрывающемся меню **Обнаружение**.
3.Щелкните **...** и выберите путь к файлу приложения, к которому будет применено уведомление.
4.Оставьте значение **По умолчанию** в раскрывающемся меню**Блокировать**. Это позволит унаследовать действие по умолчанию, примененное ESET Endpoint Security.
5.Выберите в раскрывающихся меню **Уведомить** и**Записать в журнал** значения **Да**.
6.Щелкните **OK**, чтобы сохранить это уведомление.

Чтобы удалить повторяющиеся уведомления о типе обнаружения, который вы не рассматриваете как угрозу:
1.Щелкните**Добавить**, чтобы добавить новое исключение IDS.
2.Выберите нужное предупреждение в раскрывающемся меню **Обнаружение**, например **Сеанс SMB без расширений безопасности**. **атака сканирования портов TCP**.
3.Выберите **В** в раскрывающемся меню с направлениями для входящего подключения.
4.Выберите для раскрывающегося меню **Уведомить** значение **Нет**.
5.Выберите для раскрывающегося меню **Записать в журнал** значение **Да**.
6.Оставьте значение **Приложение** пустым.
7.Если входящий трафик поступает не с определенного IP-адреса, оставьте значение **Удаленные IP-адреса** пустым.
8.Щелкните **OK**, чтобы сохранить это уведомление.

Блокировка возможной угрозы

Такая ситуация может произойти, когда, например, приложение на компьютере пытается передать вредоносный трафик на другой компьютер в сети, используя брешь в системе безопасности, или когда кто-нибудь пытается сканировать порты в сети.

Угроза: имя угрозы.

Источник: сетевой адрес источника.

Объект: сетевой адрес целевого объекта.

Прекратить блокировку: для возможной угрозы создается правило IDS, которое разрешает передачу данных.

Продолжать блокировать: блокировка обнаруженной угрозы. Чтобы создать для этой угрозы правило IDS, которое блокирует передачу данных, установите флажок **Не уведомлять меня снова**.

> Отображаемая в этом окне информация зависит от типа обнаруженной угрозы. Для получения дополнительных сведений об угрозах и других связанных терминах см. раздел о типах удаленных атак или типах обнаруженных угроз.

Устранение неполадок защиты сети

Мастер устранения неполадок помогает устранить проблемы с подключениями, вызванные файерволом ESET. Выберите в раскрывающемся меню период времени, в течение которого связь была заблокирована. Список недавно заблокированных подключений отображает общие данные о типе приложения или устройства, репутации и общем числе приложений и устройств, заблокированных в течение такого периода времени. Нажмите кнопку **Подробности**, чтобы просмотреть подробные сведения о заблокированном подключении. Затем разблокируйте приложение или устройство, с которым возникли проблемы подключения.

После нажатия кнопки **Разблокировать** ранее заблокированное подключение будет разрешено. Если все же возникают проблемы с приложением или ваше устройство не работает надлежащим образом, щелкните **Приложение все еще не работает**, чтобы разрешить все подключения, ранее заблокированные для такого устройства. Если это не поможет, перезагрузите компьютер.

Щелкните **Показать изменения**, чтобы посмотреть правила, созданные с помощью мастера. Кроме того, это можно сделать, выбрав пункты **Расширенные параметры** > **Защита сети** > **Файервол** > **Дополнительно** > **Правила**.

Нажмите кнопку **Разблокировать еще , чтобы устранить проблемы с подключением для другого устройства или приложения**.

Подключенные сети

К разделу «**Подключенная сеть**» можно перейти из главного окна программы ESET Endpoint Security. Для этого выберите **Настройка** > **Сеть** > **Подключенные сети**.

Отображение сетей, к которым подключены сетевые адаптеры. После нажатия ссылки, расположенной под именем сети, вам будет предложено выбрать тип защиты (максимальная или разрешенная) для сети, к которой вы подключены с помощью сетевого адаптера. Другой вариант — щелкнуть значок шестеренки, чтобы изменить выбранный вариант в разделе

«**Расширенные параметры**». Этим параметром определяется возможность доступа других компьютеров сети к вашему устройству.

Вы можете подключиться к трем типам сетевых расположений:

- **Общедоступная сеть**: этот тип сетевого расположения предназначен для общественных мест и не является доверенным. Ваше устройство не будет видимо в сети, и вы не сможете видеть другие устройства, подключенные к этой сети. Для общедоступных сетей функция сетевого обнаружения по умолчанию отключена.

- **Домашняя или офисная сеть**: в отличие от общедоступной сети подключенные к частной сети компьютеры могут совместно использовать ресурсы через соединение LAN. Вариант **Домашняя или офисная сеть** следует выбирать, если вы доверяете устройствам, подключенным к сети.

- **Доменная сеть**: этот тип сетевого расположения контролируется сетевым администратором, и вы не можете выбирать или менять этот тип сети. Сеть определяется как доменная, когда локальный компьютер является частью Active Directory Domain Services. Локальный компьютер может проходить аутентификацию на контроллере домена через одно из его сетевых подключений.

Выбор сетевого расположения помогает обеспечить надлежащий уровень безопасности компьютера.

Щелкните **Сетевые адаптеры** в правом нижнем углу окна, чтобы просмотреть все сетевые адаптеры, а также назначенные им профили файервола и доверенных зон. Дополнительные сведения см. в разделе Сетевые адаптеры.

> i Когда выбран вариант **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).

Известные сети

Если вы часто подключаете компьютер к сетям общего пользования или другим сетям, помимо рабочей сети, рекомендуем вам проверять надежность новых сетей, к которым выполняется подключение. Выполнив определение сетей, ESET Endpoint Security может распознать доверенные (домашние или рабочие) сети, используя различные параметры сети, заданные в конфигурации **Сетевая идентификация**. При подключении к сети компьютерам часто назначаются IP-адреса, похожие на адреса 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.

> 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.

Редактор известных сетей

Настройку известных сетей можно выполнить вручную, выбрав **Расширенные параметры** > **Защита сети** > **Файервол** > **Известные сети** и щелкнув **Изменить** рядом с параметром **Известные сети**.

Столбцы

Имя: имя известной сети.

Тип защиты. Показывает заданную для сети настройку: **Домашняя или офисная сеть**, **Сеть общего пользования** или **Использовать параметр Windows**.

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

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 расположены на таких вкладках:

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).

Предупреждать о слабом шифровании Wi-Fi. ESET Endpoint Security сообщит о подключении к незащищенной беспроводной сети или сети со слабой защитой.

Профиль файервола. Позволяет выбрать профиль файервола, применяемый при подключении к этой сети.

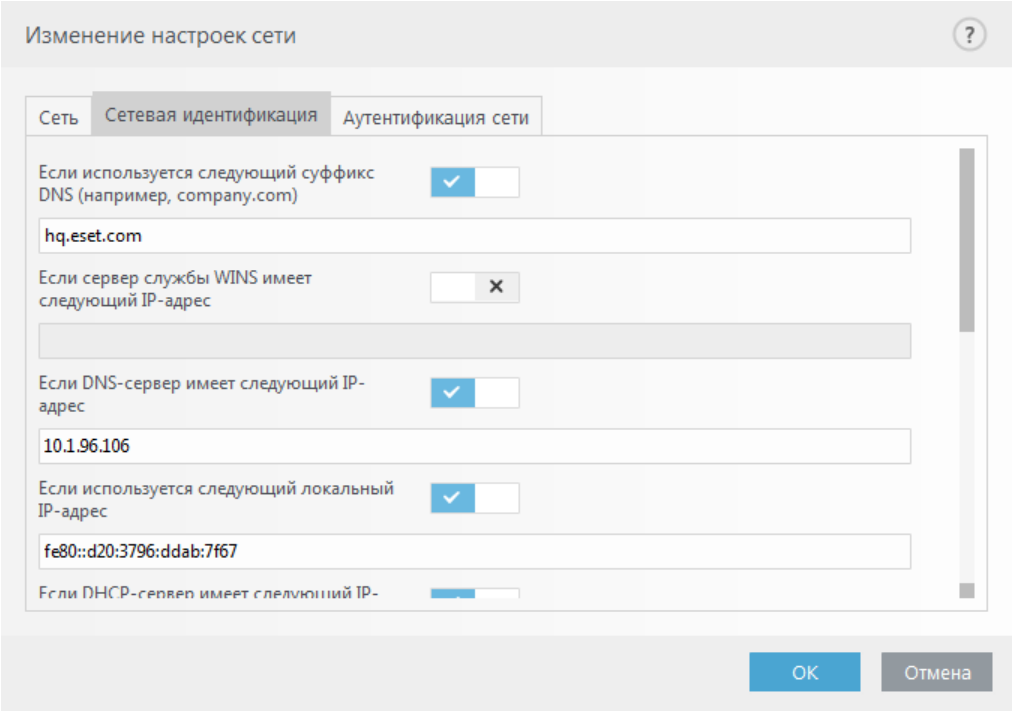
Профиль обновления. Позволяет выбрать профиль обновления, применяемый при подключении к этой сети.

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.

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.



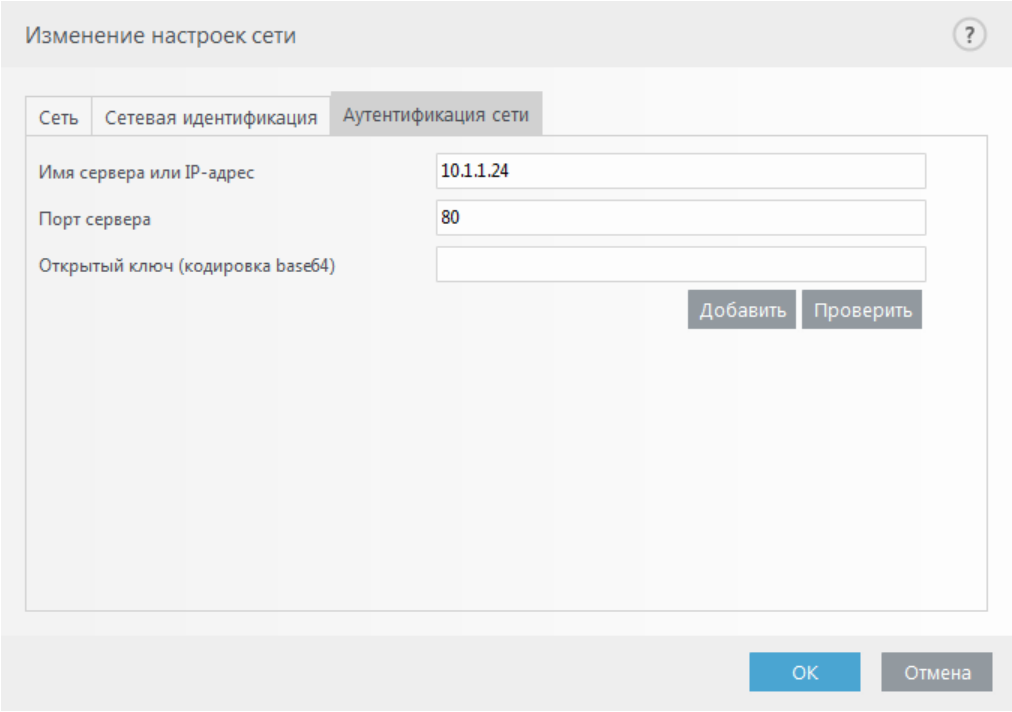
Аутентификация сети

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).



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.

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 файерволе.

Профили файервола

Глобальный профиль по умолчанию. Если в настройках сети и адаптера не указан профиль, применяется глобальный профиль по умолчанию.

Список профилей. 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.

Профили, назначаемые сетевым адаптерам. Когда настроенный для определенной сети сетевой адаптер подключен к этой сети, для него можно задать параметры использования профиля.

Кроме того, можно указать конкретный профиль, который будет использоваться для определенной сети, для чего следует выбрать элементы **Расширенные параметры** (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 со списком **Профили, назначаемыми сетевым адаптерам**, выберите профиль из раскрывающегося меню **Профиль файервола по умолчанию** и затем нажмите **OK**.

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

Профили, назначаемые сетевым адаптерам

Переключая профили, можно быстро изменять поведение файервола. 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 файервола 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. Сетевой адаптер может использовать профиль файервола, настроенный для известной подключенной сети. Если для этой сети нет настроенных профилей или настройки сетевого адаптера не предусматривают использование профиля сети, используется профиль адаптера по умолчанию.

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.

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

Обнаружение изменения приложений

Функция отслеживания изменений в приложениях выводит уведомление, если измененное приложение, для которого предназначено правило файервола, устанавливает соединение. Она нужна, чтобы правила, предназначенные для одного приложения, не нарушало другое приложение, временно или окончательно заменяя исполняемый файл исходного приложения исполняемым файлом другого приложения или злонамеренно изменяя исполняемый файл исходного приложения.

Обратите внимание, что эта функция не предназначена для обнаружения изменений во всех приложениях. Она создана, чтобы не нарушались существующие правила файервола, и отслеживаются только приложения, для которых эти правила предназначены.

Включить отслеживание изменений приложений: если выбран этот параметр, программа будет отслеживать изменения в приложениях (обновления, заражения и другие изменения). При попытке измененного приложения установить соединение пользователь получит уведомление от файервола.

Разрешить изменения в подписанных (доверенных) приложениях: не уведомлять, если после изменения действительная цифровая подпись приложения остается неизменной.

Список приложений, исключенных из проверки: добавление и удаление приложений, при изменении которых не выводятся уведомления.

Приложения, исключенные из проверки

Файервол в продукте ESET Endpoint Security выявляет изменения в приложениях, к которым применяются правила (см. раздел Обнаружение изменений приложений).

В определенных случаях приходится отключать эту функцию для некоторых приложений, если нужно исключить их из проверки файерволом.

Добавить: открывает окно, в котором можно выбрать приложение и добавить его в список

приложений, исключенных из обнаружения изменений. Вы можете выбрать из списка запущенных приложений с открытой передачей данных по сети, для которых существует правило файервола, или добавить конкретное приложение.

Изменить: открывает окно, в котором можно изменить расположение приложения из списка приложений, исключенных из обнаружения изменений. Вы можете выбрать из списка запущенных приложений с открытой передачей данных по сети, для которых существует правило файервола, или изменить расположение вручную.

Удалить: удаление записей из списка приложений, исключенных из проверки.

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 файервола можно задать действия, которые выполняются при установке сетевых соединений различных типов. Чтобы настроить правило фильтрации, откройте окно **Расширенные параметры** (клавиша F5) > **Защита сети** >**Файервол** > **Дополнительно**. Некоторые предопределенные правила связаны с флажками из **разрешенных служб** (Разрешенные службы и параметры) и не могут быть отключены напрямую. Для их отключения необходимо использовать 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 исходящим 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. Файервол дает пользователю возможность обнаружить и разорвать такие подключения.

Список правил файервола

Список правил файервола можно найти в разделе **Расширенные параметры** (F5) > **Защита сети** > **Файервол** > **Основная информация**, щелкнув **Изменить** возле элемента **Правила**.

Столбцы

Имя: имя правила.

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

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

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

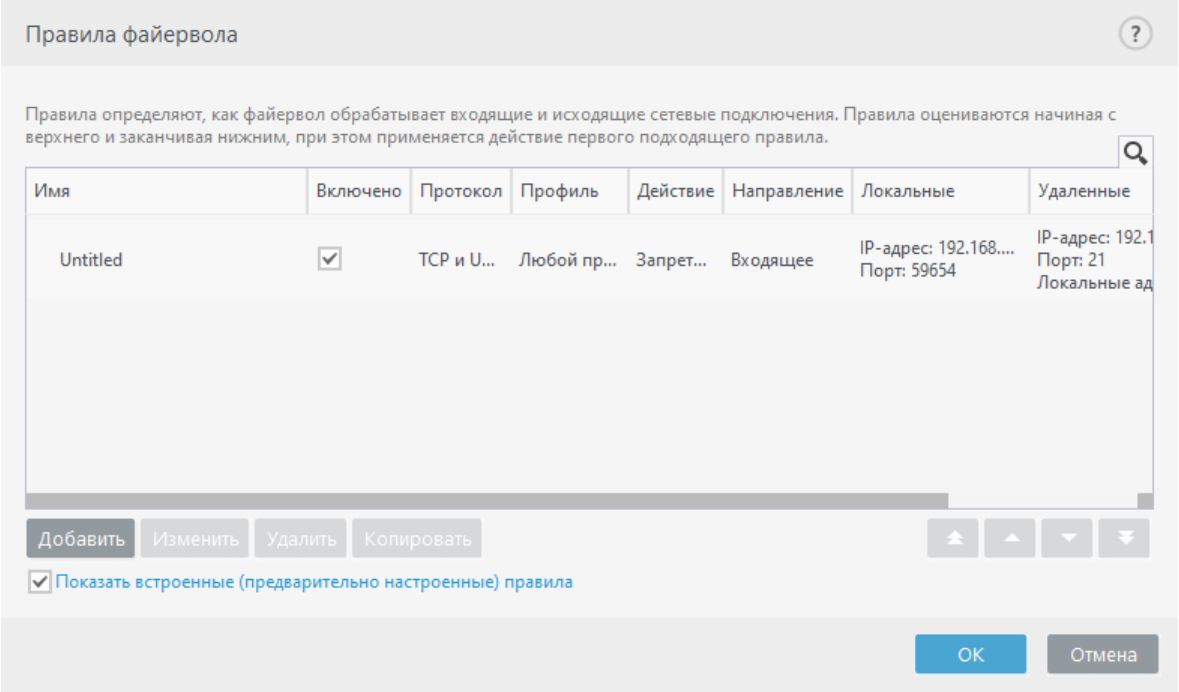
Действие: сведения о состоянии подключения (блокировать/разрешать/спрашивать).

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

Локальный: удаленный адрес, диапазон адресов или подсеть в формате IPv4 или IPv6 и порт локального компьютера.

Удаленный: удаленный адрес, диапазон адресов или подсеть в формате IPv4 или IPv6 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).

Щелкните значок поиска в верхней правой части экрана, чтобы искать правила по имени, протоколу или порту.

Добавление и изменение правил файервола

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.

> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> • Создание и изменение правил файервола в ESET Endpoint Security
> • Создание и изменение правил файервола для рабочих станций клиента в ESET Security Management Center

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.

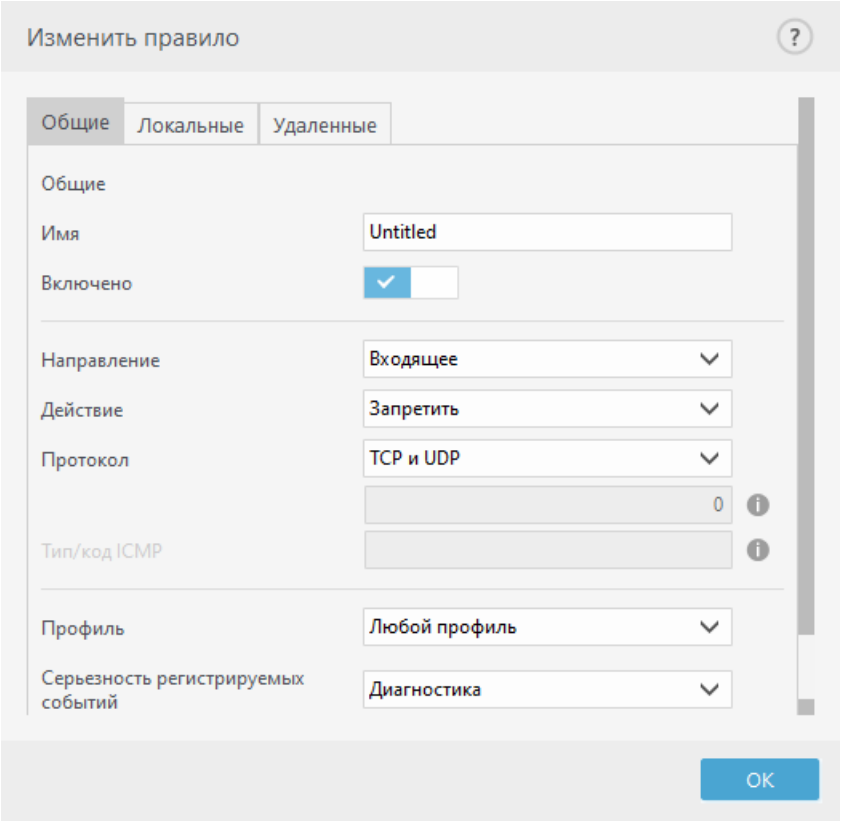
При создании нового правила необходимо ввести его имя в поле **Имя**. Направление подключения, к которому применяется правило, выбирается в раскрывающемся списке **Направление**, а действие, которое должно выполняться, когда подключение удовлетворяет параметрам правила, — в раскрывающемся списке **Действие**.

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

Если включить параметр **Серьезность регистрируемых событий**, действия, связанные с этим правилом, будут записываться в журнал. Уведомить пользователя: вывод сообщения в случае применения правила.



Журналы файервола со статусом **Предупреждение** могут собираться решением ESET Security Management Center.

Мы создаем новое правило, разрешающее веб-браузеру Firefox доступ к веб-сайтам в сети Internet и локальной сети. В данном примере необходимо настроить следующие параметры.
1.На вкладке **Общие** включите исходящие подключения по протоколам TCP и UDP.
2.Перейдите на вкладку **Локальный**.
3.Выберите путь к файлу используемого вами веб-браузера, щелкнув **...** (например, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводите имя приложения.
4.На вкладке **Удаленный** включите порты 80 и 443, если следует разрешить стандартные действия, связанные с посещением веб-страниц.

Обратите внимание, что возможности изменения предварительно заданных правил ограничены.

Правило файервола — локальный

Укажите имя локального приложения, а также локальные порты, к которым будет применяться правило.

Порт: номер локального порта (или номера нескольких портов). Если номера не указаны, правило будет применяться ко всем портам. Добавьте один порт связи или укажите их диапазон.

IP-адрес: возможность добавить один или несколько удаленных адресов, диапазон адресов или подсеть, к которым применяется правило. Если номер не указан, правило будет применяться ко всем подключениям.

Зоны: список добавленных зон.

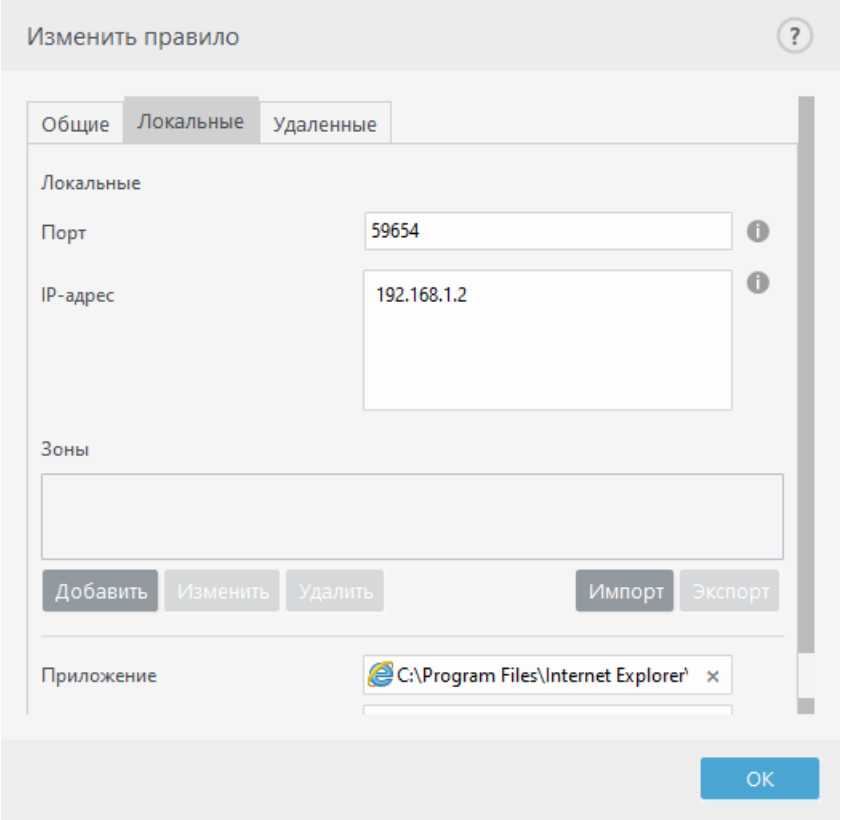
Добавить: добавление созданной зоны из раскрывающегося меню. Для создания зоны используется вкладка Настройка зоны.

Удалить: удаление зон из списка.

Приложение: имя приложения, к которому применяется правило. Добавьте расположение приложения, к которому нужно применить правило.

Служба: в раскрывающемся меню отображаются имена системных служб.

> ✔ Рекомендуется создать правило для зеркала, предоставляющего обновления через порт 2221, с помощью службы EHttpSrv, которую можно найти в раскрывающемся меню.



Правило файервола — удаленный

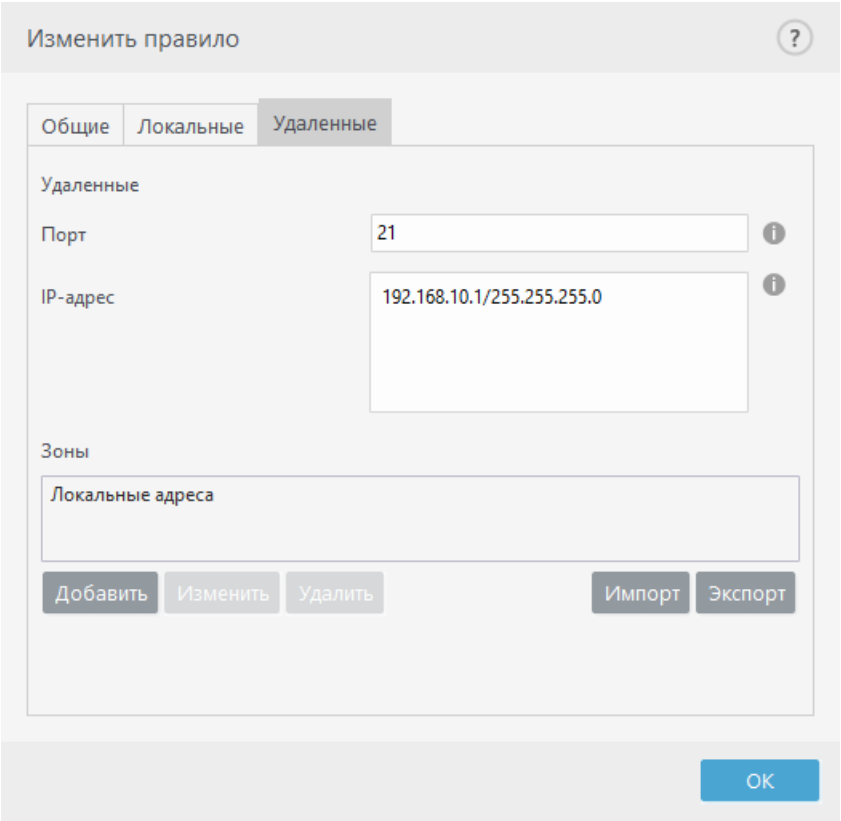
Порт: номер удаленного порта или номера нескольких портов. Если номера не указаны, правило будет применяться ко всем портам. Добавьте один порт связи или укажите их диапазон.

IP-адрес: возможность добавить удаленный адрес, диапазон адресов или подсеть. Адрес, диапазон адресов, подсеть или удаленная зона, к которым применяется правило. Если значение не указано, правило будет применяться ко всем подключениям.

Зоны: список добавленных зон.

Добавить: добавление зоны, выбранной в раскрывающемся меню. Для создания зоны используется вкладка Настройка зоны.

Удалить: удаление зон из списка.



Временный черный список IP-адресов

Чтобы просмотреть список IP-адресов, которые были обнаружены как источники атак и добавлены в черный список для блокировки соединений в течение определенного периода времени, в ESET Endpoint Security выберите **Настройка** > **Защита сети** > **Временный черный список IP-адресов**. Временно блокируемые IP-адреса блокируются на 1 час.

Столбцы

IP-адрес. Отображение IP-адреса, который был заблокирован.

Причина блокирования: отображение типа атаки, которая была предотвращена с адреса (например, атака сканирования портов TCP).

Время ожидания: отображение времени и даты, когда адрес будет удален из «черного» списка.

Элементы управления

Удалить. Щелкните, чтобы удалить IP-адрес из черного списка до того, как истечет срок действия списка.

Удалить все. Щелкните, чтобы немедленно удалить все адреса из черного списка.

Добавить исключение. Щелкните, чтобы добавить исключение файервола в фильтрацию IDS.

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 Разрешенные службы и 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 офисная, 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**.

Настройка зон

Зона — это коллекция сетевых адресов, которая представляет собой одну логическую группу IP-адресов. Зонами удобно пользоваться, когда один и тот же набор адресов необходимо использовать в нескольких правилах. Каждому адресу в группе назначаются одинаковые правила, определенные для всей группы в целом. Пример такой группы — **доверенная зона**. Доверенная зона — это группа сетевых адресов, которые никак не блокируются файерволом. Зоны можно настроить в меню **Расширенные параметры** > **Защита сети** > **Файервол** > **Дополнительно**. Для этого рядом с элементом **Зоны** щелкните **Изменить**. Чтобы добавить новую зону, щелкните **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. См. также Зоны файервола.

Зоны файервола

Дополнительные сведения о зонах см. в разделе Настройка зон.

Столбцы

Имя: имя группы удаленных компьютеров.

IP-адреса: относящиеся к зоне удаленные IP-адреса.

Элементы управления

При **добавлении** или **изменении** зоны доступны такие поля.

Имя: имя группы удаленных компьютеров.

Описание: общее описание группы.

Адрес удаленного компьютера (IPv4, IPv6, диапазон, маска): добавление удаленного адреса, диапазона адресов или подсети.

Удалить: удаление зоны из списка.

> Учтите, что заранее определенные зоны удалить невозможно.

Журнал файервола

Файервол 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 **Защита сети** в раскрывающемся меню **Журнал**. Чтобы включить ведение журнала в файерволе, 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 файервола 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.

> Сообщение об использовании уязвимости в системе безопасности записывается даже в том случае, если конкретная уязвимость уже исправлена, так как попытка использования обнаруживается и блокируется на сетевом уровне до возникновения фактического использования.

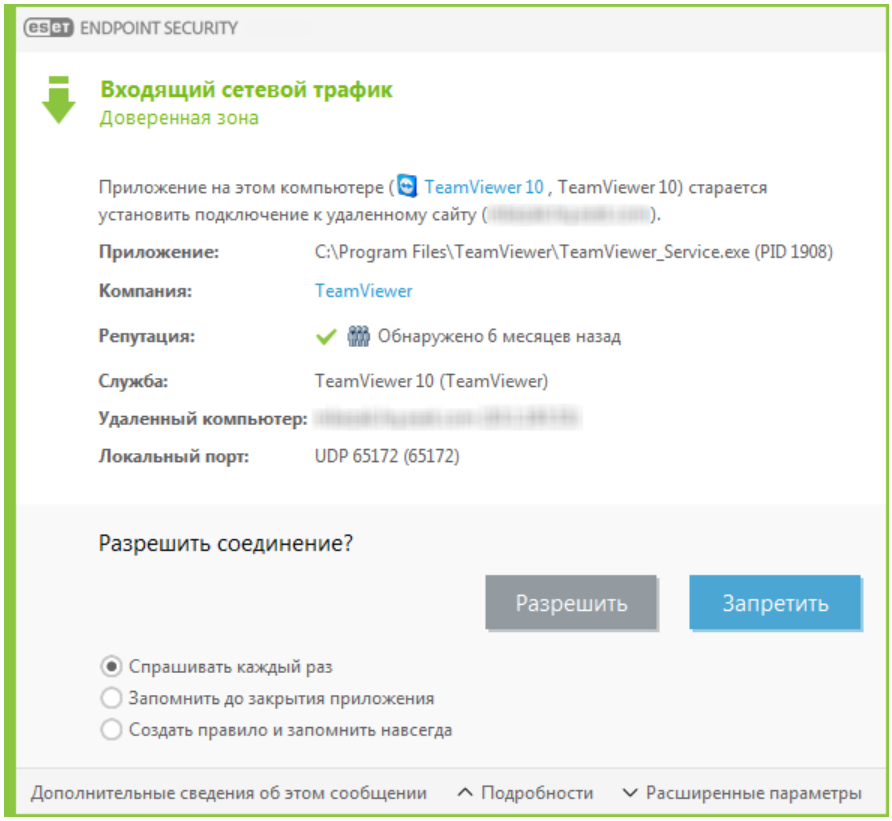
Установка соединения: обнаружение

Файервол обнаруживает каждое из новых сетевых соединений. Активный режим персонального файервола определяет, какие действия должны выполняться для нового

правила. Если активирован **автоматический режим** или **режим на основе политики**, файервол 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 файервола. Если персональный файервол 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 файервола 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, файервол 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, файервол является эффективным средством противодействия разнообразным атакам с применением вредоносного кода.

Решение проблем с файерволом ESET

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

Для решения проблем с файерволом ESET см. следующие темы:

- Мастер устранения неполадок
- Ведение журнала и создание правил и исключений на основе журнала
- Создание исключений на основе уведомлений файервола
- Расширенное ведение журналов для защиты сети
- Решение проблем с фильтрацией протоколов

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**.

> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> • Add a firewall exception using the Troubleshooting wizard **(Добавление исключения файервола с помощью мастера устранения неполадок)**

Ведение журнала и создание правил и исключений на основе журнала

По умолчанию файервол ESET не вносит в журнал все блокируемые соединения. Если вы хотите видеть, что было заблокировано файерволом, включите ведение журнала в разделе **Диагностика** > **Расширенные параметры** > **Инструменты** > **Диагностика**. Если в журнале есть элемент, который файерволу не следует блокировать, можно создать правило или правило 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.

> 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.

Создание правил на основе журнала

В новой версии ESET Endpoint Security можно создавать правила на основе журнала. В главном меню последовательно выберите **Инструменты** > **Файлы журнала**. В раскрывающемся меню выберите пункт **Защита сети**, 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**;
- включите **Показывать уведомление при обнаружении атак, использующие бреши в системе безопасности** в меню **Расширенные параметры** (F5) > **Защита сети** > **Защита от сетевых атак** > **Расширенные параметры** > **Обнаружение вторжений**.

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).

> 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.

Расширенное ведение журналов для защиты сети

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

1. Перейдите в раздел **Расширенные параметры** > **Сервис** > **Диагностика** и выберите параметр **Включить расширенное ведение журналов для защиты сети**.

2. Попробуйте воспроизвести текущую проблему.

3. Отключите функцию «Расширенное ведение журналов для защиты сети».

4. Файл журнала PCAP, созданный с помощью функции «Расширенное ведение журналов для защиты сети», можно найти в папке, где создаются дампы памяти для диагностики: *C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics*

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 удается использовать какие-либо функции устройства в сети (например, не удается 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»

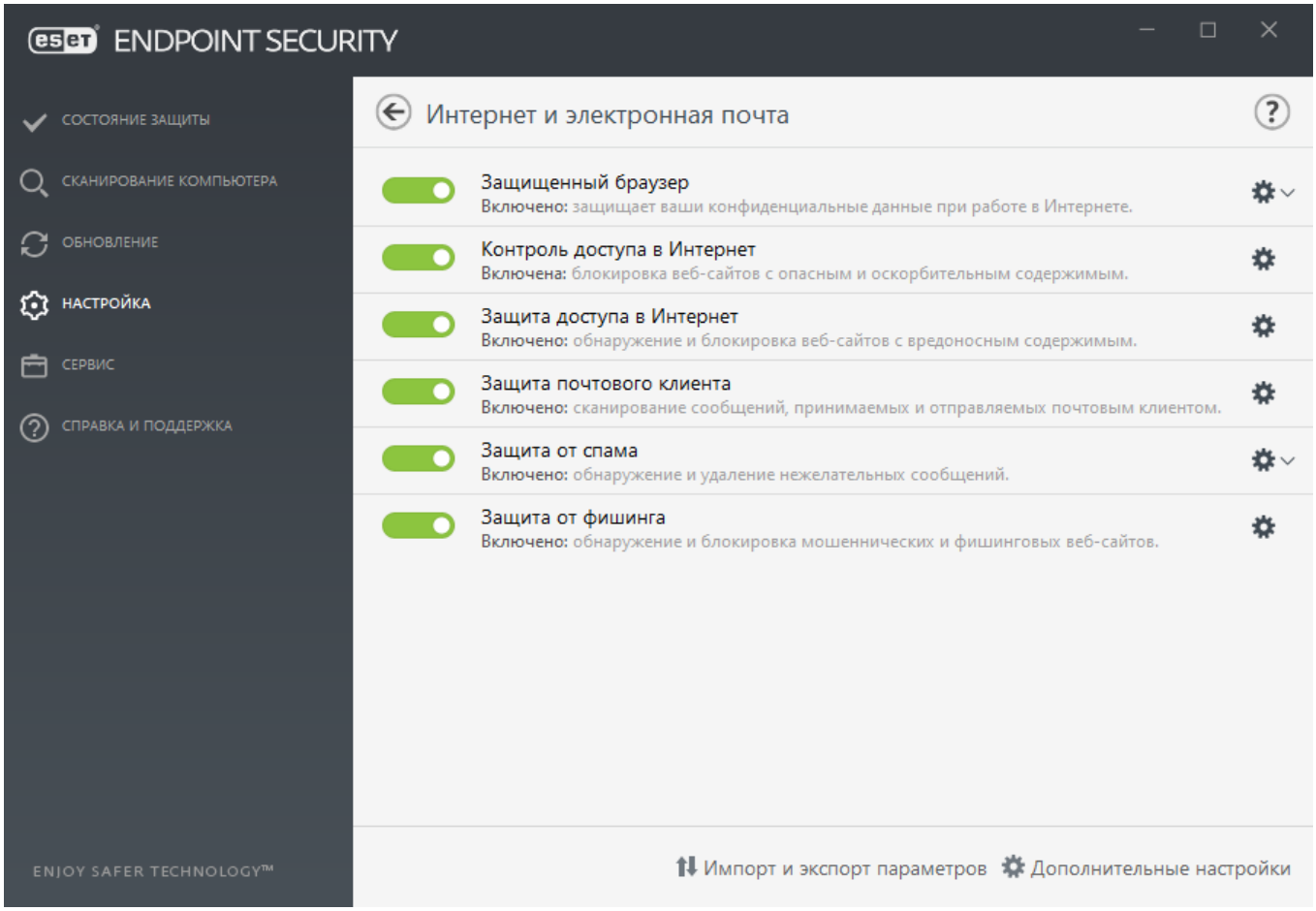
При включении фильтрации протоколов SSL программа ESET Endpoint Security выполняет фильтрацию протокола SSL так, что установленные программы доверяют ее действиям (происходит импорт сертификата в их хранилище сертификатов). Для некоторых приложений это невозможно, если они запущены. Например, для браузеров 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.

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.



Защищенный браузер: Защищает ваши конфиденциальные данные при работе в Интернете.

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 также стал и основным средством распространения вредоносного кода. Поэтому крайне важно уделить особое внимание **защите доступа в Интернет**.

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

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

Если щелкнуть значок шестеренки рядом с элементом Защита от спама, доступны следующие опции.

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

Белый список/**Черный список**/**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.

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

Фильтрация протоколов

Защита протоколов приложений от вирусов обеспечивается модулем сканирования ThreatSense, в котором объединены все современные методы сканирования для выявления вредоносных программ. Функция фильтрации протоколов работает автоматически, независимо от используемых клиентом веб-браузера и электронной почты. Для редактирования настроек зашифрованных (SSL) параметров выберите **Расширенные параметры** (F5) > **Интернет и электронная почта** > **SSL/TLS**.

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.

IPv4-адреса и маска:
- *192.168.0.10*: добавление IP-адреса отдельного компьютера, для которого должно быть применено правило.
- *192.168.0.1* до *192.168.0.99*: введите начальный и конечный IP-адреса, чтобы задать диапазон IP-адресов (или несколько компьютеров), к которым следует применить правило.
- Подсеть (группа компьютеров), заданная IP-адресом и маской. Например, *255.255.255.0* — это маска сети для префикса *192.168.1.0/24*, который означает диапазон адресов от *192.168.1.1* до 192.168.1.254.

IPv6-адрес и маска:
- *2001:718:1c01:16:214:22ff:fec9:ca5* — IPv6-адрес отдельного компьютера, для которого нужно применить правило.
- *2002:c0a8:6301:1::1/64* — IPv6-адрес с длиной префикса 64 бита, т. е. от *2002:c0a8:6301:0001:0000:0000:0000:0000* до *2002:c0a8:6301:0001:ffff:ffff:ffff:ffff.*

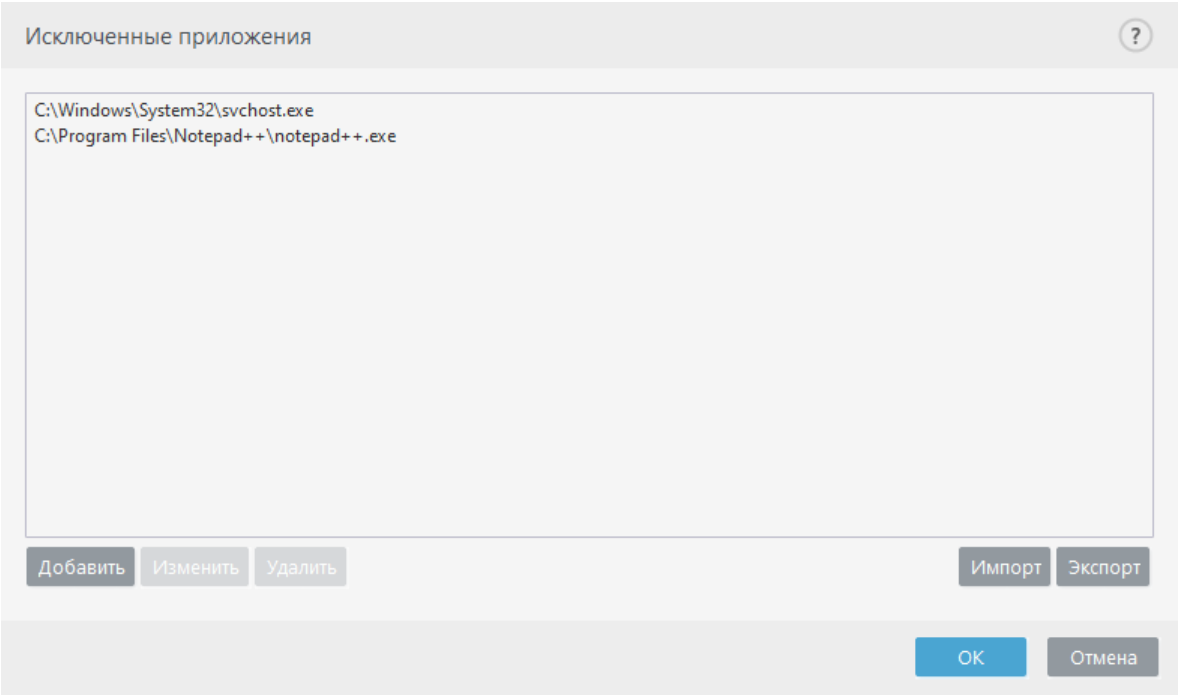
Исключенные приложения

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.



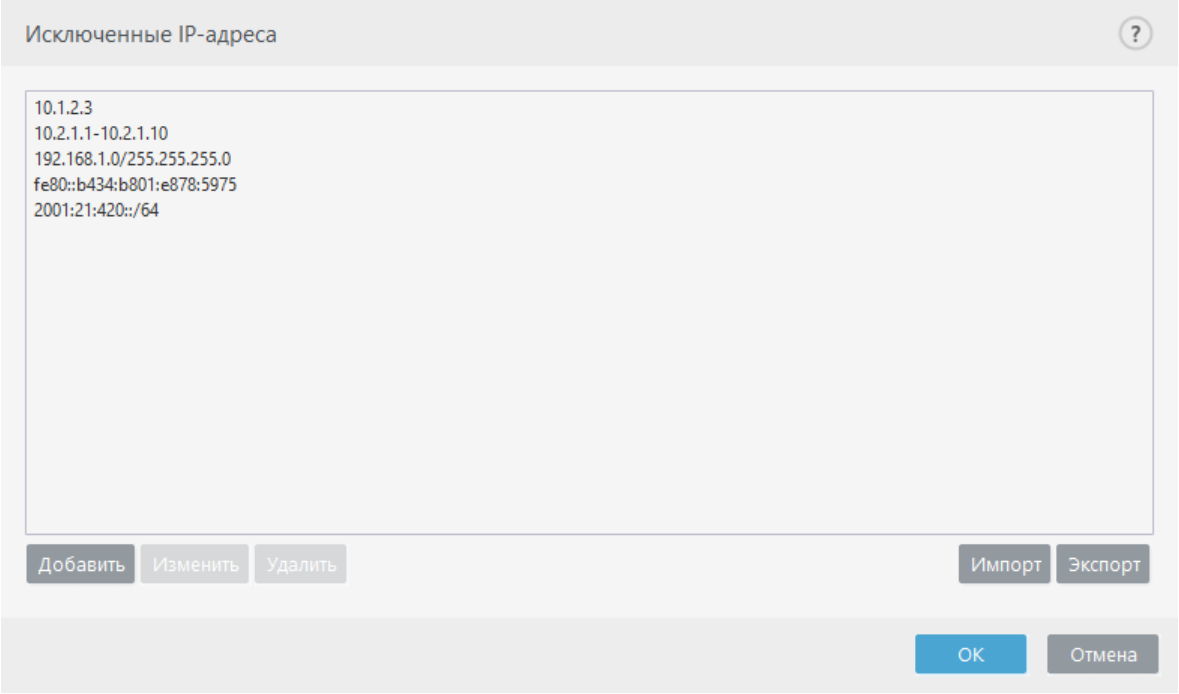
Исключенные IP-адреса

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.



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. Фильтрация протокола включена по умолчанию. Ее можно отключить в разделе **Расширенные параметры** > **Интернет и электронная почта** > **SSL/TLS** или с помощью политики. Если фильтрация протоколов отключена, программа не сканирует обмен данными по протоколу SSL.

режим фильтрации протоколов SSL/TLS доступен со следующими параметрами:

Режим фильтрации	Описание
Автоматический режим	Автоматический режим: используемый по умолчанию режим, в котором сканируются только соответствующие приложения, такие как веб-браузеры и почтовые клиенты.
Интерактивный режим	При выполнении входа на новый защищенный SSL--сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора действия. Этот режим позволяет создавать список сертификатов SSL и приложений, исключаемых из сканирования.
Режим политики	Выберите этот вариант, чтобы сканировать все защищенные SSL-соединения, кроме тех, которые защищены исключенными из проверки сертификатами. Если устанавливается новое соединение, использующее неизвестный заверенный сертификат, пользователь не получит уведомления, а само соединение автоматически будет фильтроваться. При доступе к серверу с ненадежным сертификатом, который помечен пользователем как доверенный (добавлен в список доверенных сертификатов), соединение с этим сервером разрешается, а содержимое канала связи фильтруется.

Список приложений, отфильтрованных с помощью SSL/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: когда этот параметр включен, соединение с доверенными доменами будет исключено из проверки. 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.

> Адреса не будут отфильтрованы, если включен параметр **Исключить соединение с доверенными доменами** и домен считается надежным.

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 не удается установить доверие сертификата: в некоторых случаях сертификат невозможно проверить с помощью хранилища сертификатов доверенных корневых центров сертификации (TRCA). Это значит, что сертификат подписан кем-либо (например, администратором 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 срок действия сертификата** (установлен по умолчанию), пользователю будет предложено выбрать действие, которое следует предпринять во время установки зашифрованного соединения. Можно выбрать вариант **Блокировать подключения, использующие данный сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтом, использующим непроверенный сертификат.

Если сертификат поврежден: это значит, что сертификат был неправильно подписан или поврежден. В этом случае мы рекомендуем оставить выбранным параметр **Блокировать подключения, использующие данный сертификат**. Если выбран параметр **Запрашивать срок действия сертификата**, пользователю будет предложено выбрать действие, которое следует предпринять при установке зашифрованного соединения.

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
- Уведомления касательно сертификатов в продуктах ESET
- При посещении веб-страниц отображается «Зашифрованный сетевой трафик: ненадежный сертификат»

Сертификаты

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

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

используется красный цвет. Если же сертификат есть в этом списке, окно будет оформлено зеленым цветом.

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

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

Зашифрованный сетевой трафик

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 непроверяемый или недействительный сертификат, а продукт ESET Endpoint Security настроен на выдачу запросов пользователю в таких случаях (по умолчанию запросы отображаются для непроверяемых сертификатов, а для недействительных — нет), появится диалоговое окно с запросом на **разрешение** или **блокирование** подключения. Если сертификата нет в Trusted Root Certification Authorities store (TRCA), то он считается ненадежным.

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**.

> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> - Уведомления касательно сертификатов в продуктах ESET
> - При посещении веб-страниц отображается «Зашифрованный сетевой трафик: ненадежный сертификат»

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

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 щелкните **Удалить**.

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

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 фильтрованных приложений.

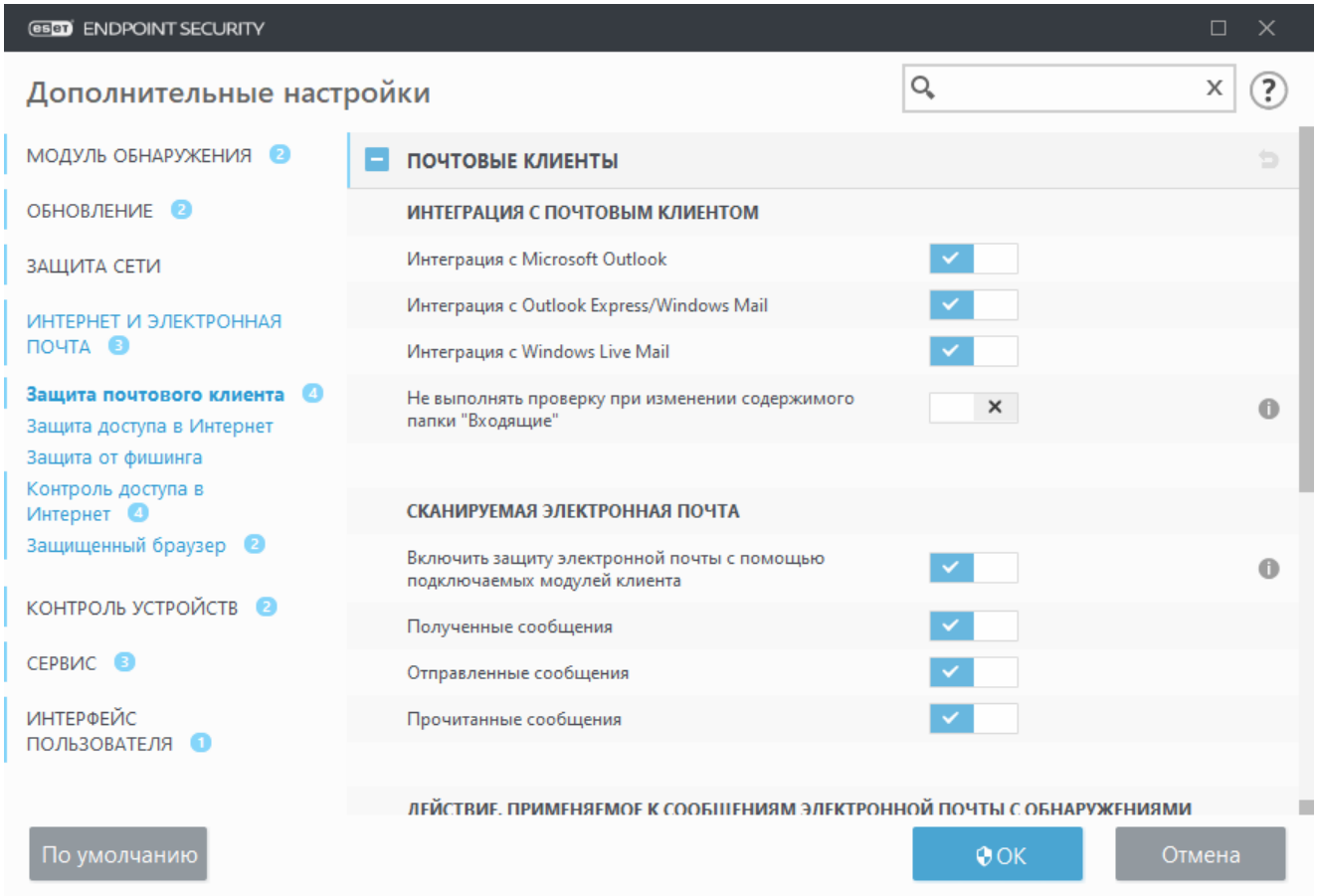
Изменить: выберите сертификат, который нужно настроить, и нажмите кнопку **Изменить**.

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

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

Защита почтового клиента

Интеграция ESET Endpoint Security с почтовым клиентом увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, в ESET Endpoint Security можно настроить интеграцию. При этом панель инструментов ESET Endpoint Security вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты. Параметры интеграции доступны в разделе **Настройка > Расширенные параметры** (клавиша F5) > **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 Windows Live Mail. 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.

Включите параметр **Не выполнять проверку при изменении содержимого папки «Входящие»**, если при извлечении сообщения электронной почты наблюдается замедление работы системы.

Сканируемая электронная почта

Включить защиту электронной почты с помощью подключаемых модулей клиента: если этот параметр отключен, защита электронной почты с помощью подключаемых модулей клиента выключена.

Полученные сообщения — если этот параметр включен, программа отмечает полученные сообщения электронной почты.

Отправленные сообщения — если этот параметр включен, программа отмечает отправленные сообщения электронной почты.

Прочитанные сообщения — если этот параметр включен, программа отмечает прочитанные сообщения электронной почты.

> Рекомендуем оставить параметр **Включить защиту электронной почты с помощью подключаемых модулей клиента** включенным. Даже если интеграция отключена или не работает, передача данных по электронной почте остается защищенной модулем Фильтрация протоколов (для протоколов IMAP/IMAPS, POP3/POP3S).

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 (действие по умолчанию). Зараженные сообщения будут автоматически перемещаться в указанную папку.

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

Повторить сканирование после обновления — если этот параметр включен, после обновления модуля обнаружения выполняется повторное сканирование зараженных сообщений электронной почты.

Принять результаты сканирования из других модулей — если этот параметр включен, вместо повторного сканирования модуль защиты электронной почты будет использовать результаты сканирования, полученные от других модулей защиты.

Протоколы электронной почты

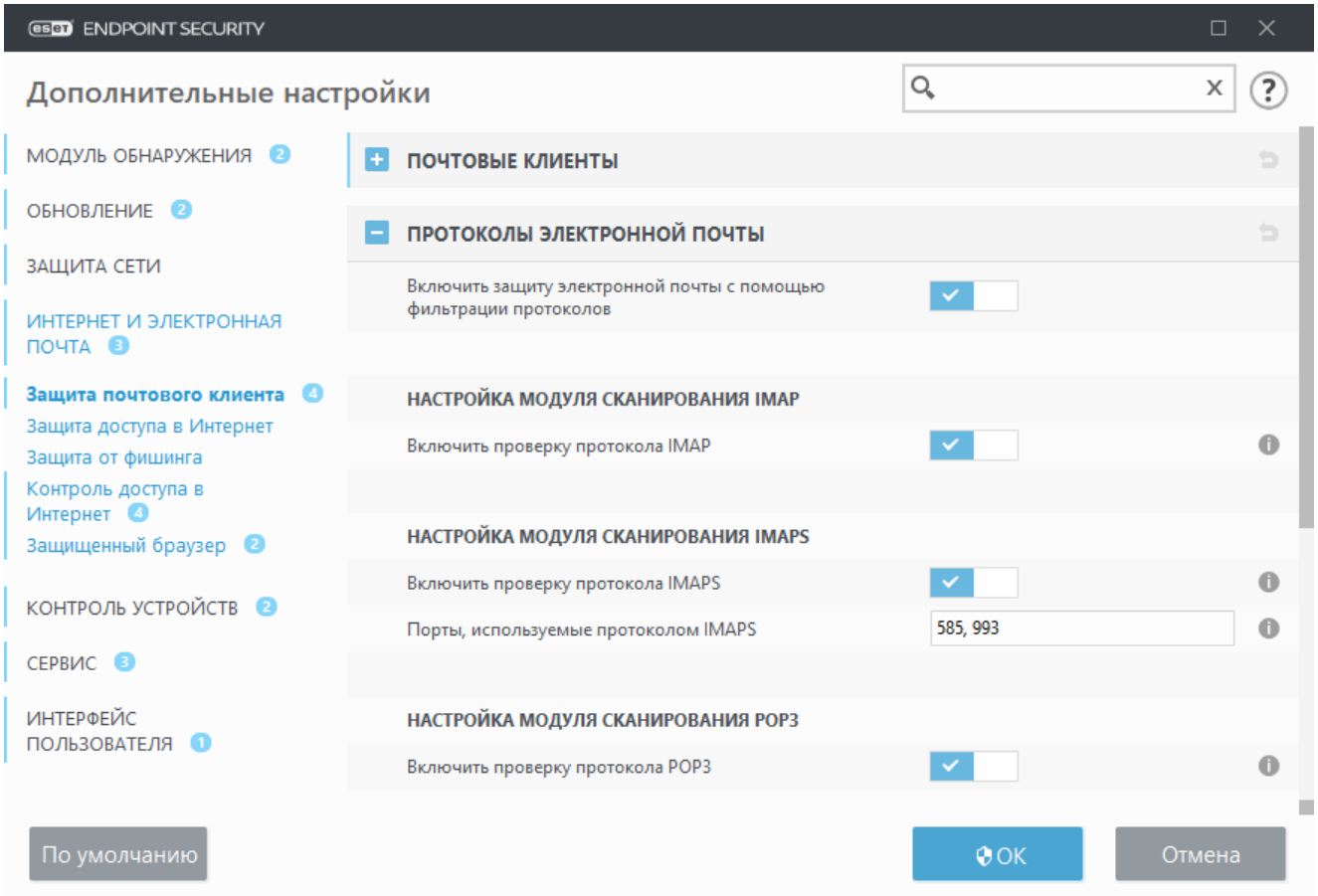
IMAP и POP3 — это самые популярные протоколы в мире. Они используются для обмена данными по электронной почте с помощью приложения почтового клиента. Протокол IMAP — это интернет-протокол для получения электронной почты, который имеет определенные преимущества перед POP3. Например, сразу несколько клиентов могут одновременно подключаться к одному и тому же почтовому ящику и получать сведения о состоянии сообщения, в частности сведения о том, что сообщение было прочитано, удалено или на него был дан ответ. Модуль защиты, обеспечивающий такой контроль, автоматически запускается при запуске системы и остается активным в памяти.

ESET Endpoint Security обеспечивает защиту этих протоколов независимо от используемого почтового клиента и без необходимости перенастраивать почтовый клиент. По умолчанию сканируются все данные, передаваемые по протоколам POP3 и IMAP, независимо от используемых по умолчанию номеров портов POP3/IMAP.
Данные, передаваемые по протоколу MAPI, не сканируются, но связь с сервером Microsoft Exchange может сканировать модуль интеграции в почтовых клиентах, таких как Microsoft Outlook.

Рекомендуем оставить параметр **Включить защиту электронной почты с помощью фильтрации протоколов** включенным. Чтобы настроить проверку протоколов IMAP/IMAPS и POP3/POP3S, последовательно выберите элементы Расширенные параметры > **Интернет и электронная почта** > **Защита почтового клиента** > **Протоколы электронной почты**.

ESET Endpoint Security также поддерживает сканирование протоколов IMAPS (585, 993) и POP3S (995), 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. При необходимости можно добавить и другие порты. Номера портов следует разделять запятой.

Шифрованные соединения сканируются по умолчанию. Чтобы просмотреть настройки модуля сканирования, перейдите к пункту SSL/TLS в разделе «Расширенные параметры», щелкните **Интернет и электронная почта** > **SSL/TLS**, и активируйте параметр**Включить фильтрацию протоколов SSL/TLS**.



Оповещения и предупреждения для сообщений электронной почты

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

После проверки к сообщению электронной почты может быть прикреплено уведомление с результатами сканирования. Вы можете выбрать **Добавлять уведомление к полученным и прочитанным сообщениям электронной почты** или **Добавлять уведомление к отправленным сообщениям**. Обратите внимание, что в некоторых случаях уведомления могут отсутствовать в проблемных HTML-сообщениях или в сообщениях, поврежденных вредоносными программами. Уведомления могут быть добавлены к входящим и прочитанным сообщениям или к исходящим сообщениям (или и к тем, и к другим). Доступны указанные ниже варианты.

- **Никогда**: уведомления не будут добавляться.
- **При обнаружении**: будут отмечены только сообщения, содержащие вредоносные программы (по умолчанию).
- **Для всей электронной почты при сканировании**: программа будет добавлять уведомления ко всем сканируемым сообщениям электронной почты.

Изменять тему отправленных сообщений электронной почты: снимите этот флажок, если вы не желаете, 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.

Текст для добавления в тему обнаруженных сообщений электронной почты. Этот шаблон можно изменить, если нужно отредактировать формат префикса, добавляемого к зараженному сообщению. Эта функция заменяет тему сообщения Hello на формат [обнаружение %DETECTIONNAME%] Hello. Переменной %DETECTIONNAME% обозначается обнаружение.

Интеграция с почтовыми клиентами

В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, Почта Windows и Windows Live Mail. 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.

Панель инструментов Microsoft Outlook

Защита Microsoft Outlook работает в виде подключаемого модуля. После установки ESET Endpoint Security эта панель инструментов, в которой присутствуют возможности для защиты от вирусов испама, добавляется в Microsoft Outlook.

Спам: позволяет пометить выбранные сообщения как спам. «Отпечаток» помеченного сообщения будет отправлен на центральный сервер, на котором хранятся сигнатуры спама. Если на сервер поступает несколько аналогичных «отпечатков» от разных пользователей, такое сообщение в дальнейшем будет классифицироваться как спам.

Не спам: позволяет пометить выбранные сообщения как не являющиеся спамом.

Адрес отправителя спама («черный» список, список рассылающих спам адресов): добавляет новый адрес отправителя в «черный список». Все сообщения, полученные с внесенных в список адресов, будут автоматически классифицироваться как спам.

> ⚠ Остерегайтесь подделки адреса отправителя, направленной на то, чтобы заставить получателя прочесть сообщение и ответить на него.

Доверенные адреса («белый» список, список доверенных адресов): добавляет новый адрес отправителя в «белый» список. Все сообщения, полученные с адресов из «белого» списка, никогда не будут автоматически классифицироваться как спам.

ESET Endpoint Security: если щелкнуть этот значок, откроется главное окно ESET Endpoint Security.

Повторное сканирование сообщения: позволяет запустить проверку электронной почты вручную. Можно указать сообщения, которые будут проверяться, и активировать повторное сканирование полученных сообщений. Для получения дополнительных сведений см. раздел Защита почтового клиента.

Настройки модуля сканирования: на экран выводятся параметры защиты почтового клиента.

Настройка модуля антиспама: на экран выводятся параметры защиты от спама.

Адресные книги: открывается окно защиты от спама, содержащее списки исключенных, доверенных адресов и адресов отправителей спама.

Панель инструментов Outlook Express и Почты Windows

Защита для Outlook Express и Почты Windows функционирует в качестве подключаемого модуля. После установки ESET Endpoint Security эта панель инструментов, в которой присутствуют возможности для защиты от вирусов испама, добавляется в Outlook Express или Почту Windows.

Спам: позволяет пометить выбранные сообщения как спам. «Отпечаток» помеченного сообщения будет отправлен на центральный сервер, на котором хранятся сигнатуры спама. Если на сервер поступает несколько аналогичных «отпечатков» от разных пользователей, такое сообщение в дальнейшем будет классифицироваться как спам.

Не спам: позволяет пометить выбранные сообщения как не являющиеся спамом.

Адрес отправителя спама: добавляет новый адрес отправителя в «черный список». Все сообщения, полученные с внесенных в список адресов, будут автоматически классифицироваться как спам.

Остерегайтесь подделки адреса отправителя, направленной на то, чтобы заставить получателя прочесть сообщение и ответить на него.

Доверенный адрес: добавляет новый адрес отправителя в «белый» список. Все сообщения, полученные с адресов из «белого» списка, никогда не будут автоматически классифицироваться как спам.

ESET Endpoint Security: если щелкнуть этот значок, откроется главное окно ESET Endpoint Security.

Повторное сканирование сообщения: позволяет запустить проверку электронной почты вручную. Можно указать сообщения, которые будут проверяться, и активировать повторное сканирование полученных сообщений. Для получения дополнительных сведений см. раздел Защита почтового клиента.

Настройки модуля сканирования: на экран выводятся параметры защиты почтового клиента.

Настройка модуля антиспама: на экран выводятся параметры защиты от спама.

Интерфейс

Настроить вид: позволяет изменить внешний вид панели инструментов в почтовом клиенте. Для того чтобы настроить внешний вид независимо от параметров почтового клиента, снимите этот флажок.

Показывать надписи: отображение описаний значков.

Текст справа: описания размещаются не снизу, а справа от значков.

Большие значки: отображение в меню значков крупного размера.

Окно подтверждения

Это уведомление предназначено для подтверждения того, что пользователю действительно нужно выполнить выбранное действие, и для предотвращения тем самым возможных ошибок.

Кроме того, в окне также есть возможность отключить подтверждения.

Повторно сканировать сообщения

Панель инструментов ESET Endpoint Security, интегрированная в почтовые клиенты, дает пользователю возможность указать ряд параметров для проверки электронной почты. Параметром **Повторно сканировать сообщения** предлагается два описанных далее режиме сканирования.

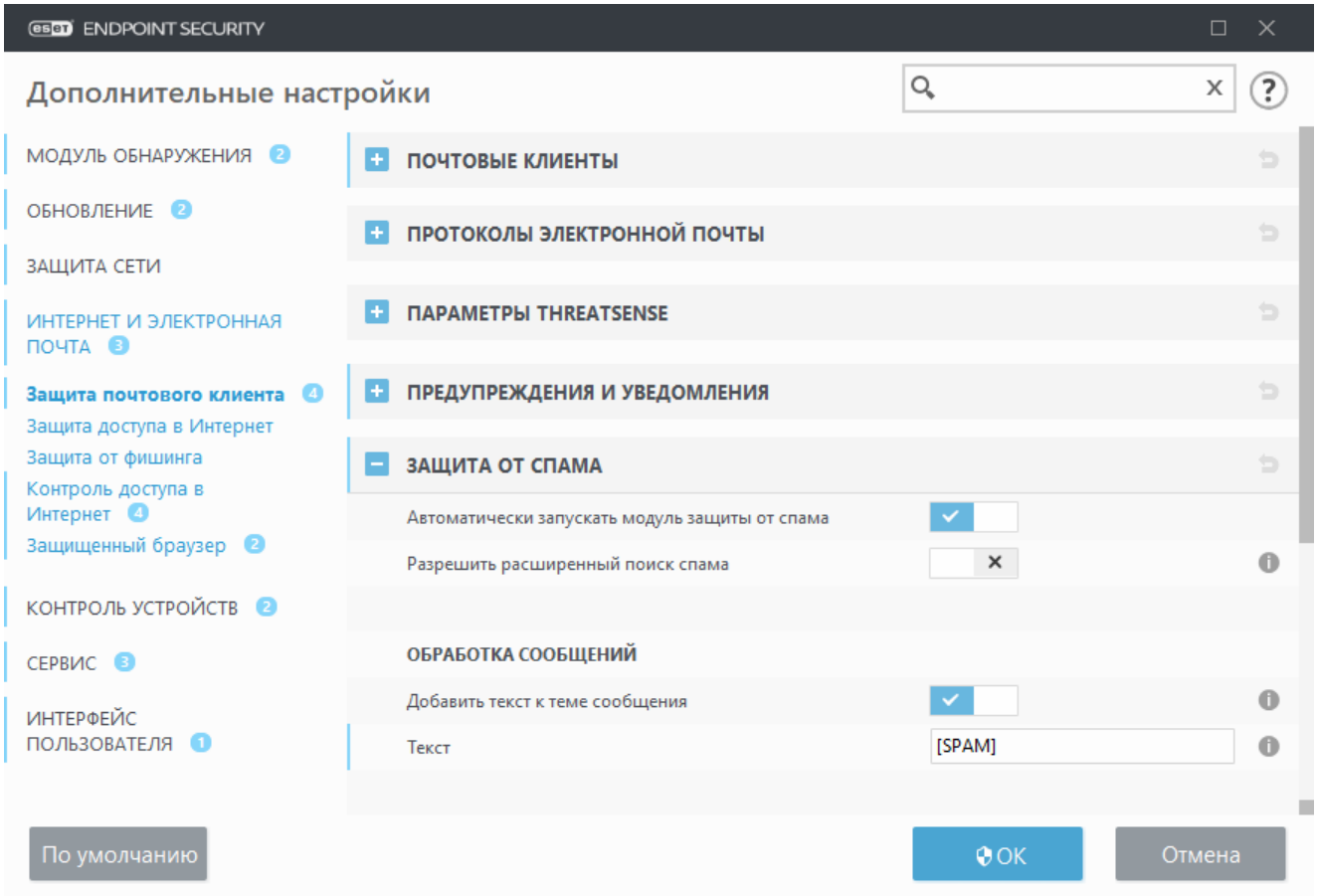
Все сообщения в текущей папке: сканируются сообщения в отображаемой сейчас папке.

Только выбранные сообщения: сканируются только помеченные пользователем сообщения.

Флажок **Повторно сканировать уже сканированные сообщения** дает пользователю возможность выполнить еще одно сканирование сообщений, которые уже были просканированы ранее.

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 50 %. 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.



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 папку: выбор папки, в которую будут перемещаться обнаруженные зараженные сообщения электронной почты.

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.

> 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 считает 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.

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

Адресные книги модуля защиты от спама

В модуле защиты от спама ESET Endpoint Security можно конфигурировать различные параметры адресных списков.

Адресные книги

Разрешить списки адресов пользователя: установите этот флажок, чтобы активировать адресную книгу, созданную пользователем в собственном почтовом клиенте.

Разрешить глобальные списки адресов: задайте этот параметр, чтобы активировать глобальную адресную книгу, доступную для всех пользователей, в качестве службы каталогов

в пределах рабочей станции с электронной почтой. В глобальном списке адресов содержатся сведения для всех пользователей электронной почты, групп рассылки и ресурсов.

«Белый» список пользователя: список контактов, в котором можно добавлять, изменять и удалять адреса, которые пользователь считает безопасными и допустимыми для обмена сообщениями.

«Черный» список пользователя: список контактов, в котором можно добавлять, изменять и удалять адреса, которые пользователь считает опасными и недопустимыми для обмена сообщениями.

Список исключений пользователя: этот список контактов содержит адреса электронной почты, которые могут быть подделаны и использованы для отправки спама. См. также список исключений.

Глобальные белый список/черный список/список исключений: с помощью этих списков ко всем пользователям ESET Endpoint Security на этой рабочей станции применяются политики защиты от спама. Когда ESET Endpoint Security управляется дистанционно, политика ESET PROTECT/ESMC/ECA будет применяться ко всем назначенным рабочим станциям.

Добавлять в "белый" список пользователя автоматически

Добавлять адреса из адресной книги: добавление адресов из списка контактов в «белый» список.

Добавлять адреса получателей из исходящих сообщений: добавление адресов получателей из отправленных сообщений в «белый» список.

Добавлять адреса из сообщений, повторно классифицированных как НЕ спам: добавление адресов отправителей из сообщений, повторно классифицированных как НЕ спам, в «белый» список.

Автоматически добавлять в список исключений пользователя

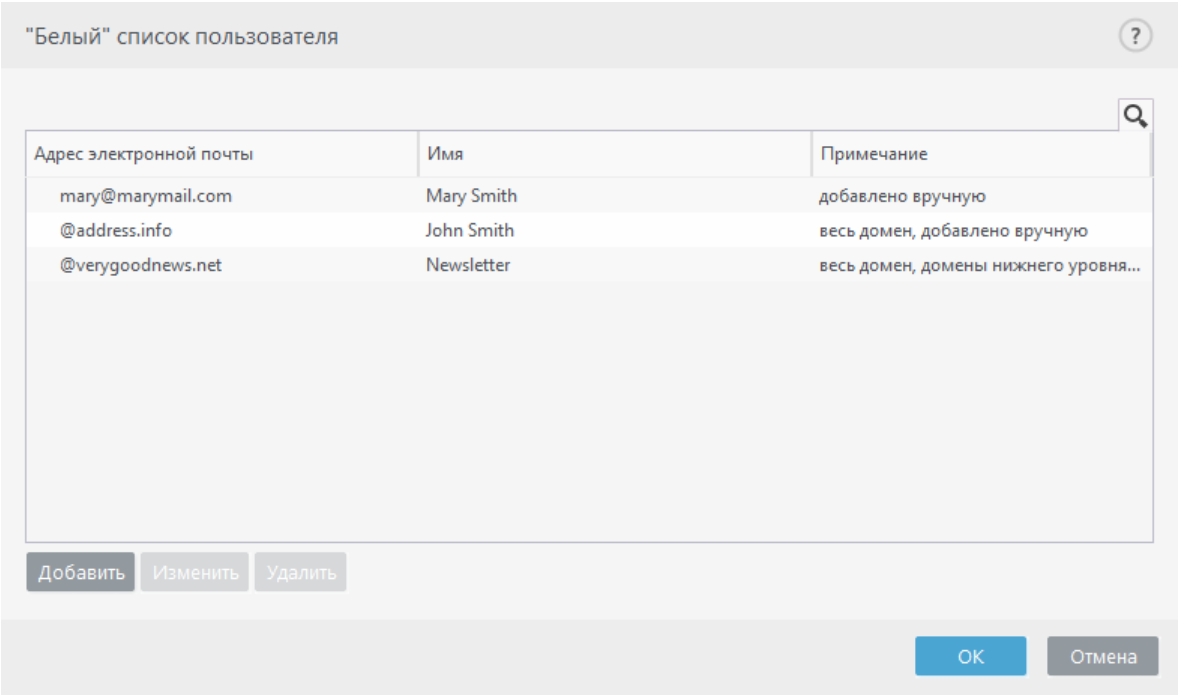
Добавлять адреса из собственных учетных записей: добавление адресов из существующих учетных записей почтового клиента в список исключений.

«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 **Расширенные параметры** > **Интернет и электронная почта** > **Защита почтового клиента** > **Адресные книги модуля защиты от спама** при помощи кнопок «**Добавить**», «**Изменить**» 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.

Добавление или изменение адреса в черном списке, белом списке или исключениях

В этом окне можно добавлять и изменять записи белого и черного списков. Откройте главное окно программы ESET Endpoint Security и выберите **Расширенные параметры** > **Интернет и электронная почта** > **Защита почтового клиента** > **Адресные книги модуля защиты от спама**.

Адрес электронной почты: адрес электронной почты, который следует добавить или изменить.

Имя: имя записи.

Весь домен: установите этот флажок, чтобы применить запись ко всему домену контакта (не только к адресу, указанному в поле Адрес электронной почты, а ко всем адресам электронной

почты в домене *address.info*).

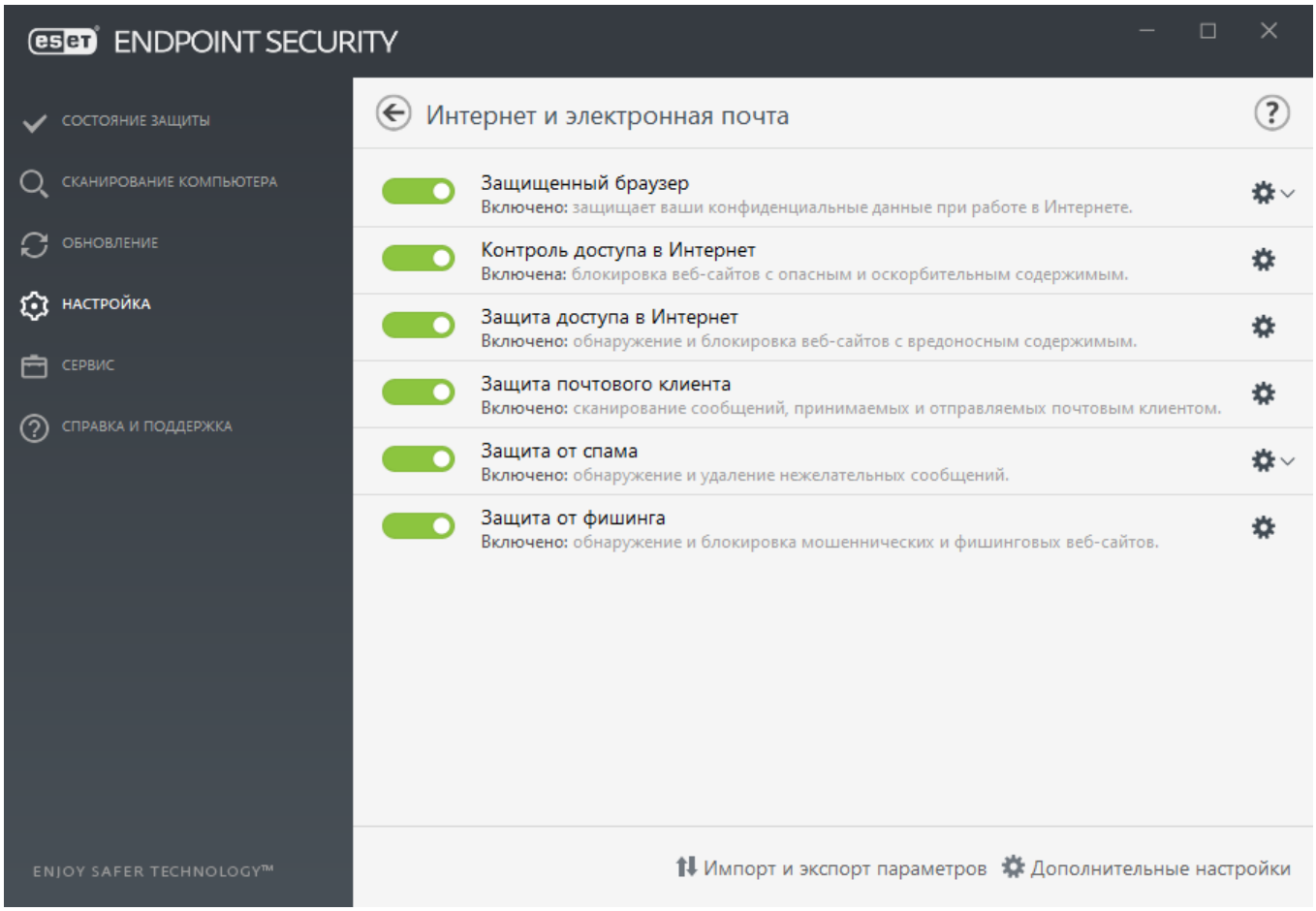
Домены нижнего уровня: установите этот флажок, чтобы запись применялась к доменам нижнего уровня контакта (*address.info* представляет домен, а *my.address.info* — поддомен).

Защита доступа в Интернет

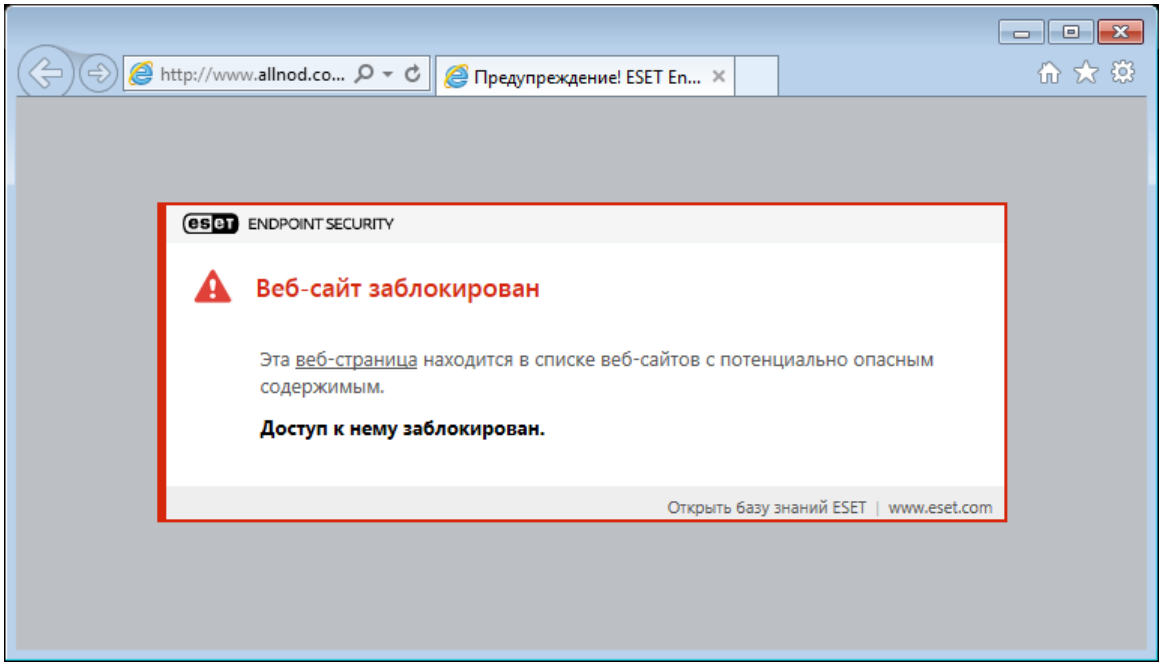
Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основной средой распространения вредоносного кода. Защита доступа в Интернет работает путем отслеживания соединений между веб-браузерами и удаленными серверами в соответствии с правилами протоколов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

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

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



Защита веб-доступа будет отображать следующее сообщение в браузере, когда веб-сайт заблокирован:



Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
- Разблокирование безопасного веб-сайта на отдельной рабочей станции в ESET Endpoint Security
- Разблокирование безопасного веб-сайта на конечной точке с помощью ESET Security Management Center

---

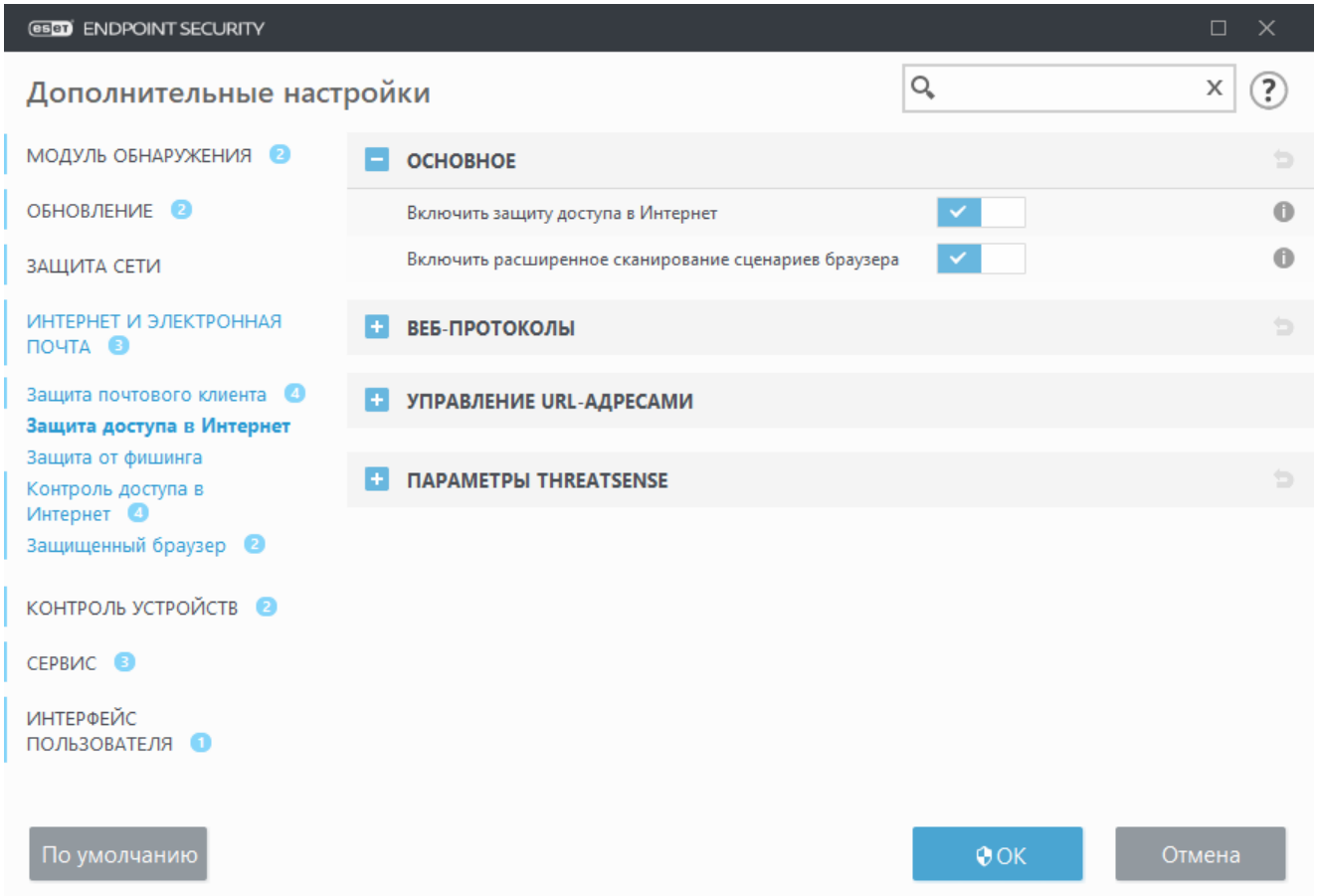
В разделе **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в Интернет** доступны указанные ниже варианты.

- **Базовый** — чтобы включить или отключить эту функцию в расширенных параметрах.

- **Веб-протоколы**. Возможность настройки отслеживания в стандартных протоколах, которые используются в большинстве браузеров.

- **Управление URL-адресами**. Здесь можно задавать URL-адреса, которые следует блокировать, разрешать или исключать из проверки.

- **Параметры ThreatSense** — расширенная настройка модуля антивирусного сканирования. Дает возможность настраивать определенные параметры, например тип сканируемых объектов (сообщения электронной почты, архивы и т. д.), методы обнаружения для защиты доступа в Интернет и т. д.



Расширенные параметры настройки защиты доступа в Интернет

В разделе **Расширенные параметры** (F5) > **Интернет и электронная почта** > **Защита доступа в Интернет** > **Базовый**доступны указанные ниже варианты.

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

Включить расширенное сканирование сценариев браузера: когда этот параметр включен, все исполняемые в интернет-браузерах программы JavaScript будут проверяться модулем обнаружения.

> Настоятельно рекомендуется не отключать защиту доступа в Интернет.

Веб-протоколы

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

Настройка модуля сканирования HTTP

HTTP-трафик отслеживается для всех портов и приложений.

Настройка модуля сканирования HTTPS

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 (443, 0-65535), которые указаны в списке **Порты, используемые протоколом HTTPS**, вне зависимости от версии операционной системы.

Шифрованные соединения сканируются по умолчанию. Чтобы просмотреть настройки модуля сканирования, перейдите к пункту SSL/TLS в разделе «Расширенные параметры», щелкните **Интернет и электронная почта** > **SSL/TLS**, и активируйте параметр**Включить фильтрацию протоколов SSL/TLS**.

Управление URL-адресами

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

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

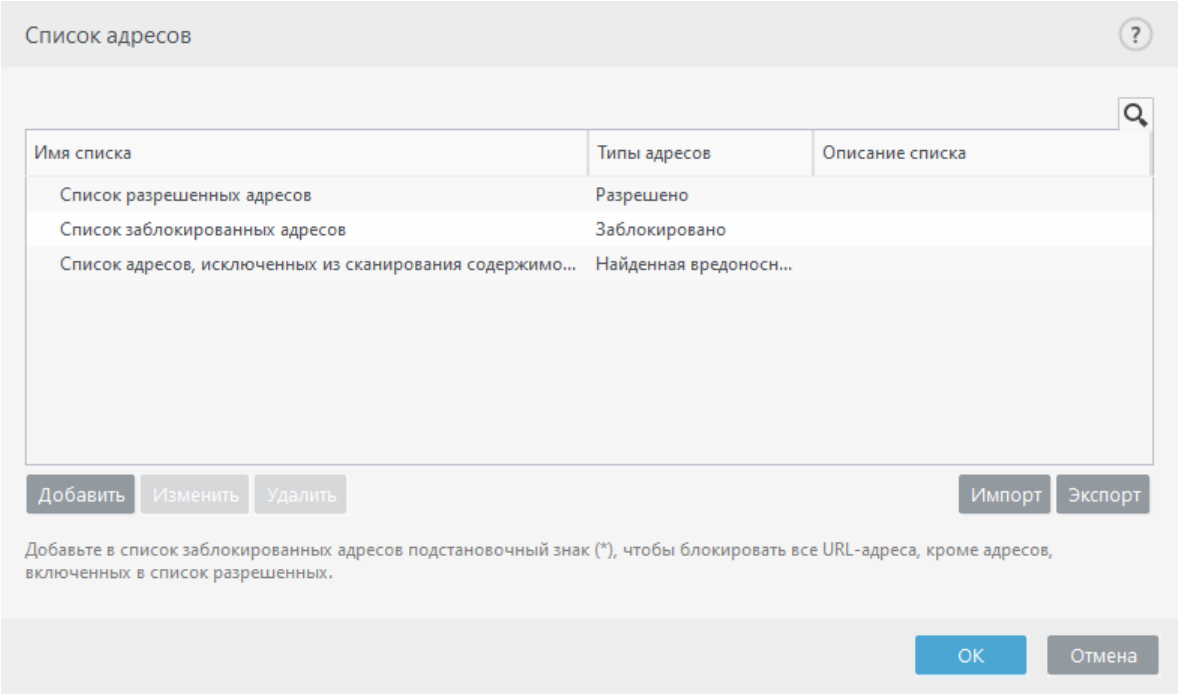
Посещение веб-сайтов, добавленных в **список заблокированных адресов** невозможно, кроме случаев, когда их адреса также добавлены в **список разрешенных адресов**. Веб-сайты из **списка адресов, для которых отключено сканирование содержимого**, загружаются без проверки на вредоносный код.

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

В списках можно использовать такие специальные символы, как «*» (звездочка) и «?» (вопросительный знак). Символ звездочки заменяет любую последовательность символов, а вопросительный знак — любой символ. Особое внимание следует уделить указанию адресов, исключенных из проверки, поскольку в этот список должны входить только доверенные и надежные адреса. Точно так же нужно убедиться в том, что символы шаблона * и ? 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**.

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

> Адреса не будут отфильтрованы, если параметр **Интернет и электронная почта** > **SSL/TLS** > **Исключить соединение с доверенными доменами** включен и домен считается надежным.



Элементы управления

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 эту установку для добавления или удаления адресов.

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

Список URL-адресов

В этом разделе можно указать списки HTTP-адресов, которые будут блокироваться, разрешаться или исключаться из проверки.

По умолчанию доступны следующие три списка.

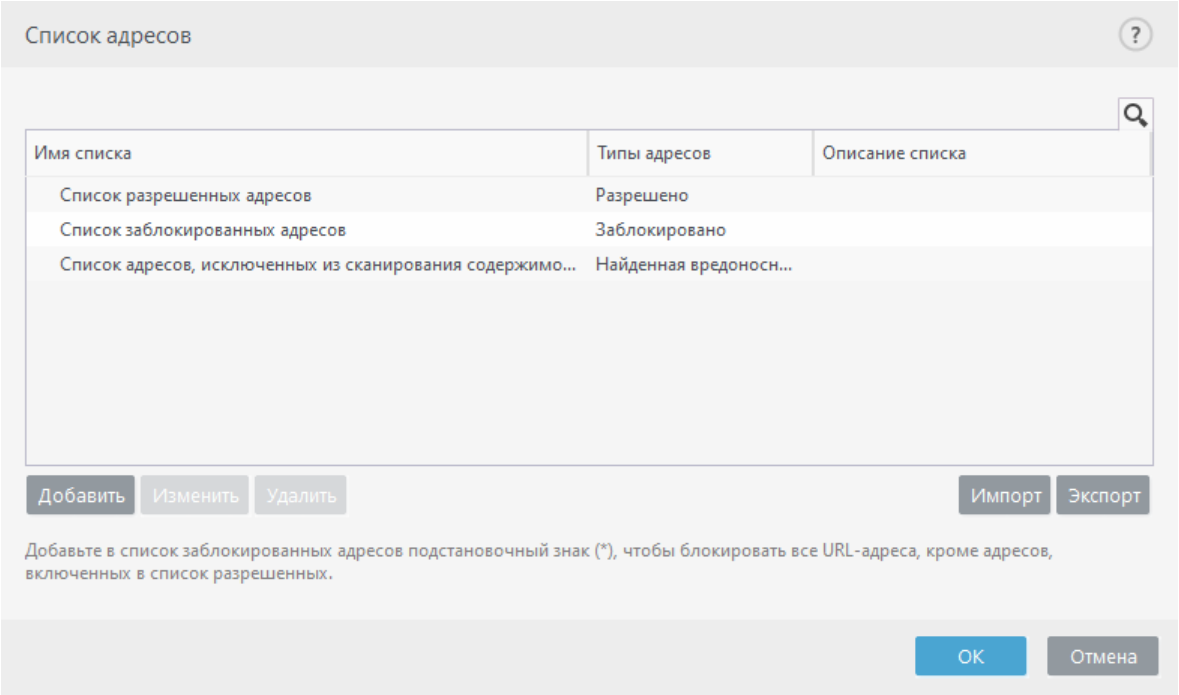
- **Список адресов, исключенных из сканирования содержимого**. Для всех добавленных в этот список адресов проверка на наличие вредоносного кода выполняться не будет.

- **Список разрешенных адресов**. Если установлен флажок «Предоставить доступ только к разрешенным HTTP-адресам», а в списке заблокированных адресов указан символ

звездочки («*» — блокировать все адреса без исключений), пользователю будет предоставлен доступ только к разрешенным адресам. Адреса в этом списке остаются доступными, даже если они включены в список заблокированных адресов.

• **Список заблокированных адресов**. Пользователь не сможет получить доступ к адресам из этого списка, если они не включены в список разрешенных адресов.

Чтобы создать новый список, нажмите кнопку **Добавить**. Для удаления выделенных списков нажмите кнопку **Удалить**.



Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
• Разблокирование безопасного веб-сайта на отдельной рабочей станции в ESET Endpoint Security
• Разблокирование безопасного веб-сайта на конечной точке с помощью ESET Security Management Center

Дополнительные сведения см. в разделе Управление URL-адресами.

Создание списка URL-адресов

В этом разделе можно указать списки URL-адресов и масок, которые будут блокироваться, разрешаться или исключаться из проверки.

При создании списка можно настроить следующие параметры.

Тип списка адресов. Доступны три типа списков:

• **Список адресов, для которых отключена проверка**. Все добавленные в этот список адреса не будут проверятся на наличие вредоносного кода.
• **Заблокировано**. Пользователь не сможет получить доступ к адресам из этого списка.
• **Разрешенные**. Если в настройках политики предусмотрено использование этой функции, а в список добавлено значение подстановочного знака (*), вы сможете получить

доступ к адресам в этом списке, даже если они заблокированы.

Имя списка. Здесь указывается имя списка. При изменении одного из трех предварительно заданных списков это поле будет недоступно.

Описание списка. Поле для короткого описания списка (необязательно). При изменении одного из трех предварительно заданных списков это поле будет недоступно.

Список активен. Щелкните ползунок, чтобы активировать список.

Уведомлять о применении. Щелкните ползунок, чтобы получать уведомления об использовании этого списка при оценке посещенного HTTP-сайта. Например, если веб-сайт будет заблокирован или разрешен (включен в список заблокированных или разрешенных адресов), на рабочем столе отобразится соответствующее уведомление. Уведомление будет содержать имя списка, в котором указан веб-сайт.

Серьезность регистрируемых событий. Выберите уровень серьезности в раскрывающемся меню. Записи с уровнем детализации «Предупреждение» могут собираться средством ESMC или ESET PROTECT.

Элементы управления

Добавить. Добавление нового URL-адреса в список (несколько адресов следует указывать через запятую).

Изменить. Изменение существующего адреса в списке. Удалять можно только адреса, добавленные посредством команды **Добавить**.

Удалить: удаление существующих адресов из списка. Доступно только для адресов, созданных с помощью команды **Добавить**.

Импорт. Импорт файла с URL-адресами (в качестве разделителя следует использовать разрыв строки, например текстовый файл с кодировкой UTF-8).

Как добавить маску URL-адреса

Прежде чем вводить нужный адрес или маску домена ознакомьтесь с указаниями в этом диалоговом окне.

ESET Endpoint Security позволяет пользователям блокировать доступ к указанным веб-узлам и предотвращать отображение их содержимого в веб-браузере. Пользователь может указать адреса, которые необходимо исключить из проверки. Если полное имя удаленного сервера неизвестно или пользователь хочет указать группу удаленных серверов, то для идентификации такой группы можно использовать так называемые маски. Эти маски обозначаются символами ? и *.

- Используйте «?», чтобы заменить любой символ.
- Используйте «*», чтобы заменить текстовую строку.

Например, маска *.c?m применяется ко всем адресам, у которых последняя часть начинается с буквы «c», заканчивается буквой «m» и содержит любой символ между ними (.com, .cam и т. д.).

Начальная последовательность «*.» перед именем домена интерпретируется особым образом. Прежде всего, в данном случае подстановочный знак * не соответствует символу косой черты («/»). Смысл этого исключения — избежать обхода маски. Например, маска **.domain.com* не будет соответствовать *http://anydomain.com/anypath#.domain.com* (такой суффикс можно присоединить к любому URL-адресу, не влияя на загрузку). Вторая особенность заключается в том, что в этом случае «*.» соответствует пустой строке. Это позволяет обозначить одной маской целый домен, включая возможные поддомены. Например, маска **.domain.com* соответствует *http://domain.com*. Использовать маску **domain.com* было бы неверно, поскольку она также совпала бы с *http://anotherdomain.com*.

Защита от фишинга

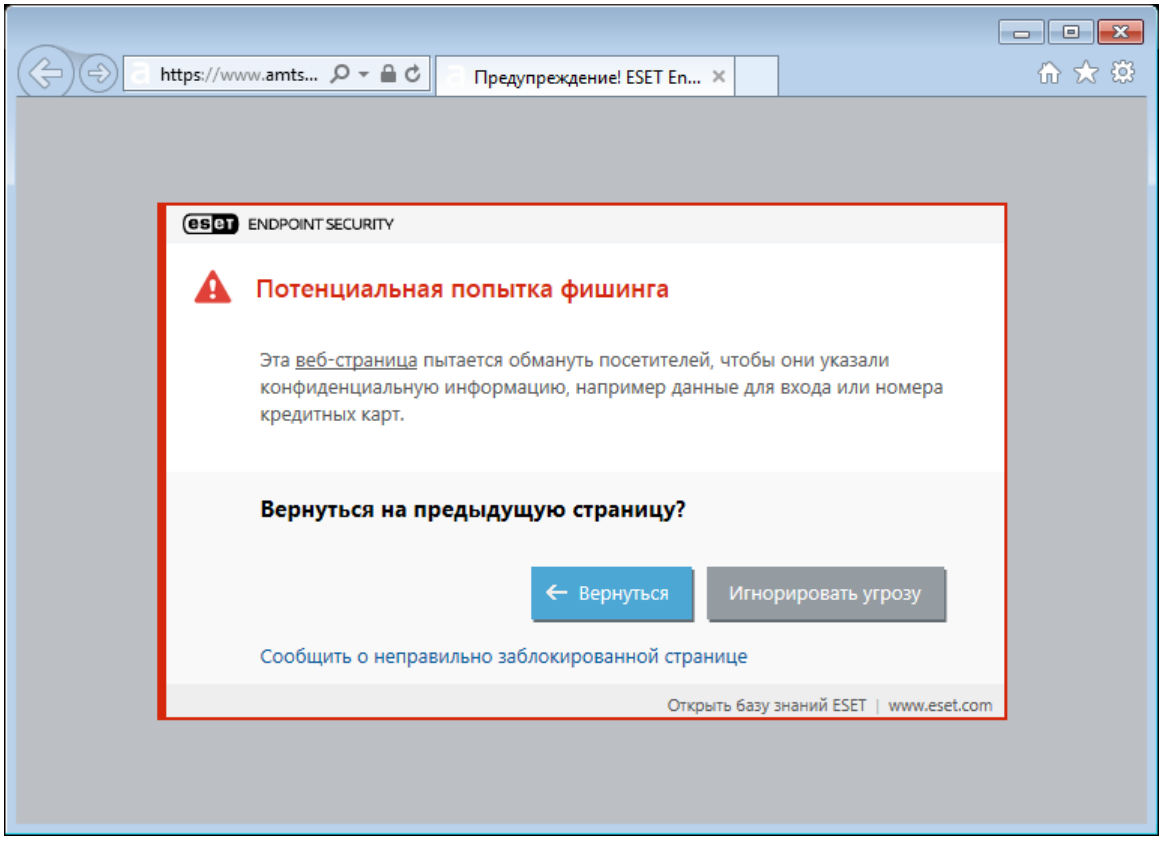
Термин «фишинг» обозначает преступную деятельность, в рамках которой используется социальная инженерия (манипулирование пользователями, направленное на получение конфиденциальной информации). Фишинг часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов, 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).



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.

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.).

Расширенные параметры защищенного

браузера

Эти параметры доступны в разделе **Расширенные параметры** (F5) > **Интернет и электронная почта** > **Защищенный браузер**.

Основные сведения

Включить Защищенный браузер: после включения функции, и вы можете открыть окно Защищенные веб-сайты.

Перенаправление на веб-сайты

Включить перенаправление на защищенные веб-сайты : если этот параметр включен, веб-сайты из списка защищенных сайтов и внутреннего списка интернет-банкинга будут перенаправляться в защищенный браузер.

Защищенные веб-сайты: список сайтов, для которых можно выбирать, в каком браузере (обычном или защищенном) они будут открываться. На рамке браузера будет отображаться логотип ESET, указывающий, что активен защищенный режим просмотра.

Защищенные страницы интернет-банкинга и платежей: отключено по умолчанию. В дополнение к списку в разделе Защищенные веб-сайты веб-сайты во внутреннем списке ESET будут перенаправляться в браузер, защищенный ESET. Веб-сайты, определяемые ESET, регулярно обновляются.

Защищенный браузер

Включить расширенную защиту памяти: если этот параметр включен, память защищенного браузера будет защищена от исследования другими процессами.

Включить защиту клавиатуры: если этот параметр включен, информация, вводимая с помощью клавиатуры в защищенный браузер, будет скрыта от других приложений. Это повышает защиту от клавиатурных шпионов.

Конфигурировать интерактивные оповещения Защищенного браузера: позволяет открыть окно Интерактивные предупреждения.

Защищенные веб-сайты

ESET Endpoint Security содержит встроенный список предварительно заданных веб-сайтов, при попытке открытия которых будет открываться защищенный браузер. Вы можете добавлять другие веб-сайты или редактировать этот список с помощью настроек программы.

Список **Защищенные веб-сайты** можно просматривать и изменять с помощью команды **Расширенные параметры** (F5) > **Интернет и электронная почта** > **Защищенный браузер** > **Основная информация** > **Защищенные веб-сайты** > **Изменить**.

Окно содержит такие разделы.

Столбцы

Веб-сайт: защищенный веб-сайт.

Защищенный браузер: в защищенном режиме просмотра вдоль границы окна браузера будет отображаться логотип ESET.

Обычный браузер: выберите этот параметр, чтобы продолжить работу в используемом по умолчанию веб-браузере (например, для выполнения банковских операций).

Элементы управления

Добавить: добавление веб-сайта в список известных веб-сайтов.

Изменить: изменение выбранных записей.

Удалить. Удаление выбранных записей.

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 содержимым, а также к ресурсам, посещение которых может отрицательно сказаться на эффективности работы.

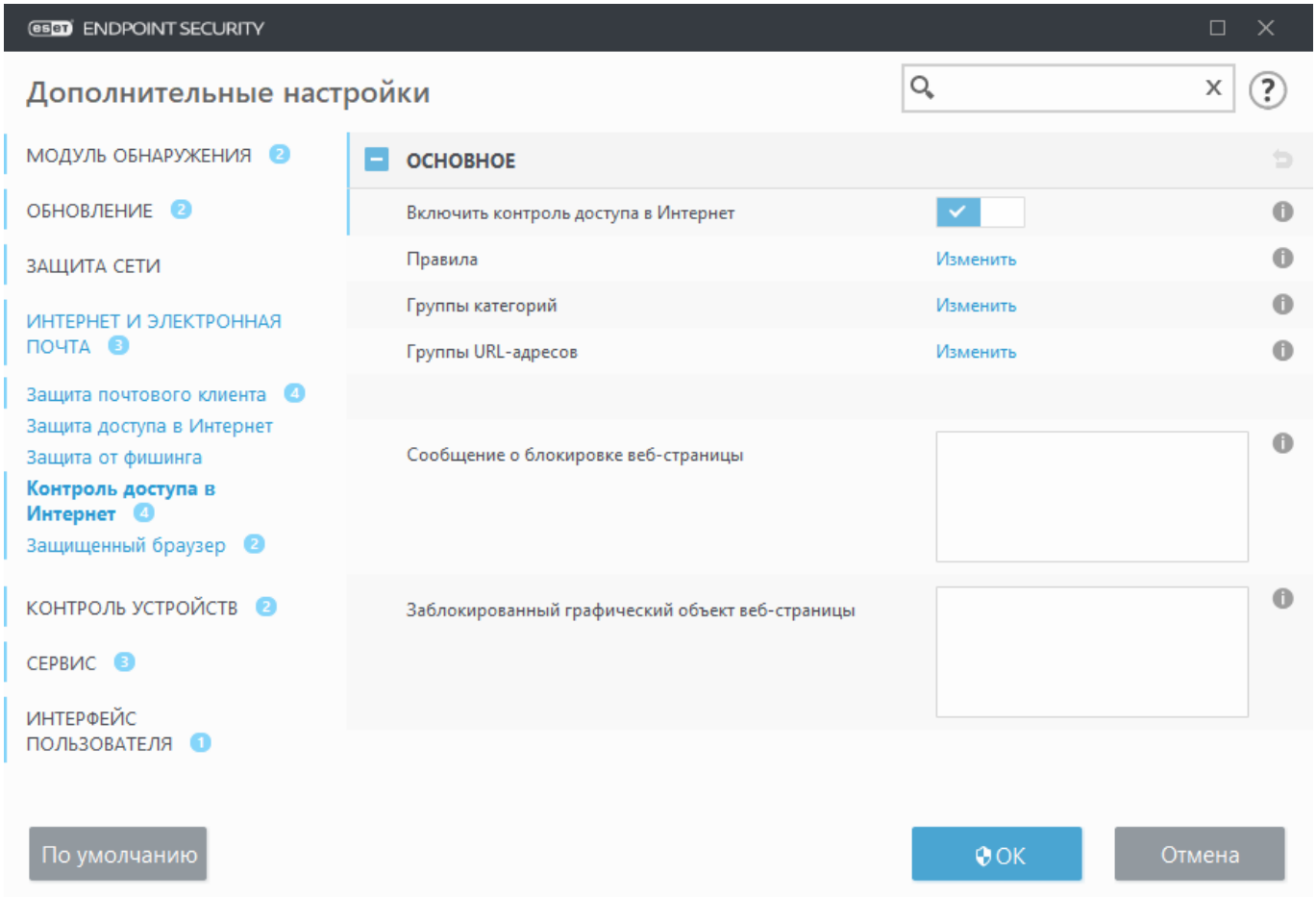
Функция контроля доступа в Интернет позволяет блокировать веб-страницы, которые могут содержать потенциально нежелательные материалы. Кроме того, работодатели или системные администраторы могут запрещать доступ к более чем 27 предварительно заданным категориям веб-сайтов, включая более 140 подкатегорий.

Контроль доступа в Интернет по умолчанию отключен. Чтобы включить его, выполните следующие действия.

1. Нажмите клавишу **F5** для входа в меню **Расширенные параметры**, а затем разверните пункты **Интернет и электронная почта** > **Контроль доступа в Интернет**.

2. Выберите **Включить контроль доступа в Интернет**, чтобы активировать контроль доступа в Интернет в ESET Endpoint Security.

3. Чтобы настроить доступ к определенным веб-страницам, щелкните **Изменить** рядом с элементом **Правила** для перехода в окно Редактор правил для контроля доступа в Интернет.

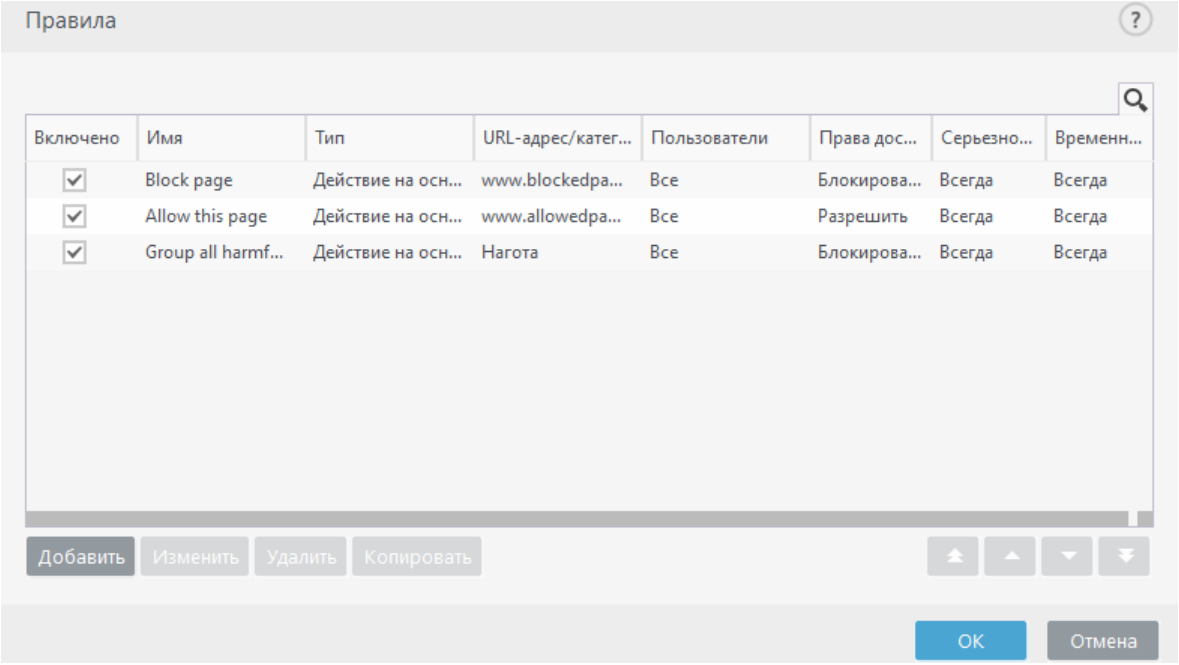


Поля **Сообщение о блокировке веб-страницы** и **Заблокированный графический объект веб-страницы** позволяют с легкостью настроить сообщение, которое отображается при блокировке веб-сайта.

> Если вы хотите заблокировать все веб-страницы и оставить доступными только некоторые, используйте управление URL-адресами.

Правила контроля доступа в Интернет

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



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.

Нажмите **Добавить** или **Изменить** для настройки правила. Нажмите **Копировать**, чтобы создать новое правило с предопределенными опциями, использованными для другого выбранного правила. Нажав и выбрав **Ctrl**, можно выбрать несколько правил и удалить все выбранные правила. Флажок **Включено** используется для применения или отключения правила; это полезно, если вы не хотите удалять правило навсегда, поскольку, возможно, вы сможете его использовать в будущем.

Порядок сортировки правил определяет их приоритет. Правила с наивысшим приоритетом находятся вверху списка. Чтобы изменить приоритет правила, выберите его и нажмите кнопку со стрелкой для повышения или понижения приоритета правила. Нажмите кнопку с двойной стрелкой, чтобы переместить правило в начало или конец списка.

Ознакомьтесь с дополнительными сведениями о создании правил.

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.

Имя

Чтобы упростить идентификацию правила, введите его описание в поле **Имя**.

Включено

Чтобы включить или отключить это правило, воспользуйтесь переключателем **Включено**. Это

может быть полезно в том случае, если вы не хотите безвозвратно удалять правило.

Действие

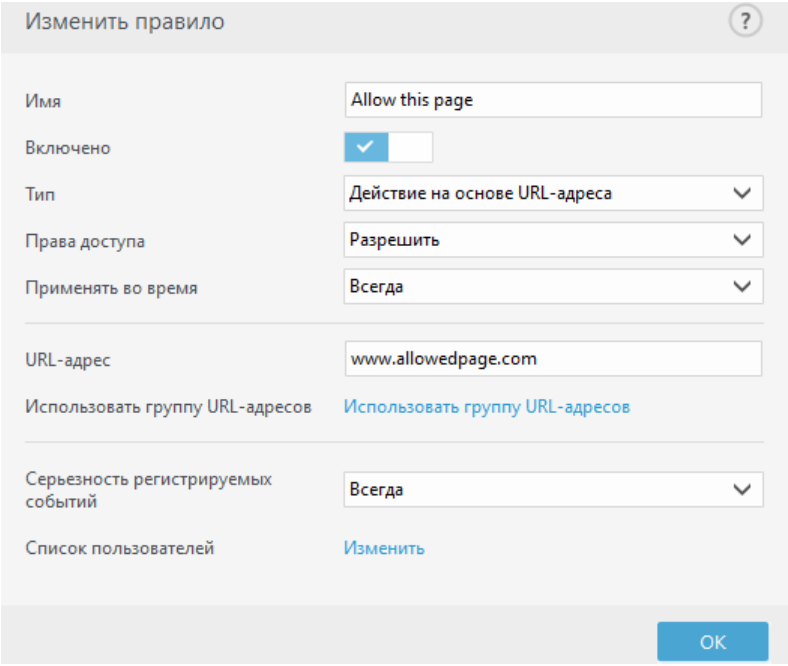
Выберите **Действие на основе URL-адреса** или **Действие на основе категории**.

Действие на основе URL-адреса

Если правила управляют доступом к определенному веб-сайту, укажите адрес веб-сайта в поле **URL-адрес**.

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.

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



Действие на основе категории

Выбрав эту функцию, укажите категорию веб-сайтов для действия в раскрывающемся меню.

Категория URL-адресов или **Группа пользователей**. Если будет обнаружена такая категория веб-сайтов или группы категорий, доступ будет разрешен, заблокирован или будет показано предупреждение.

Права доступа

- **Разрешить**: доступ к URL-адресу или категории будет открыт.
- **Предупредить**: будет показано предупреждение об URL-адресе или категории.
- **Всегда предупреждать**: предупреждение пользователя о URL-адресе/категории. Вы можете перейти на веб-сайт, но администратор получит уведомление.
- **Блокировать**: URL-адрес или категория будет блокироваться.

Применять во время

Позволяет применять созданное правило в определенное время. В раскрывающемся меню выберите созданный временной интервал.

- См. дополнительные сведения о временных интервалах.

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.

> Уровень серьезности регистрируемых событий можно настроить для каждого списка. Журналы со статусом **Предупреждение** могут собираться ESET Security Management Center.

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.

Группы категорий

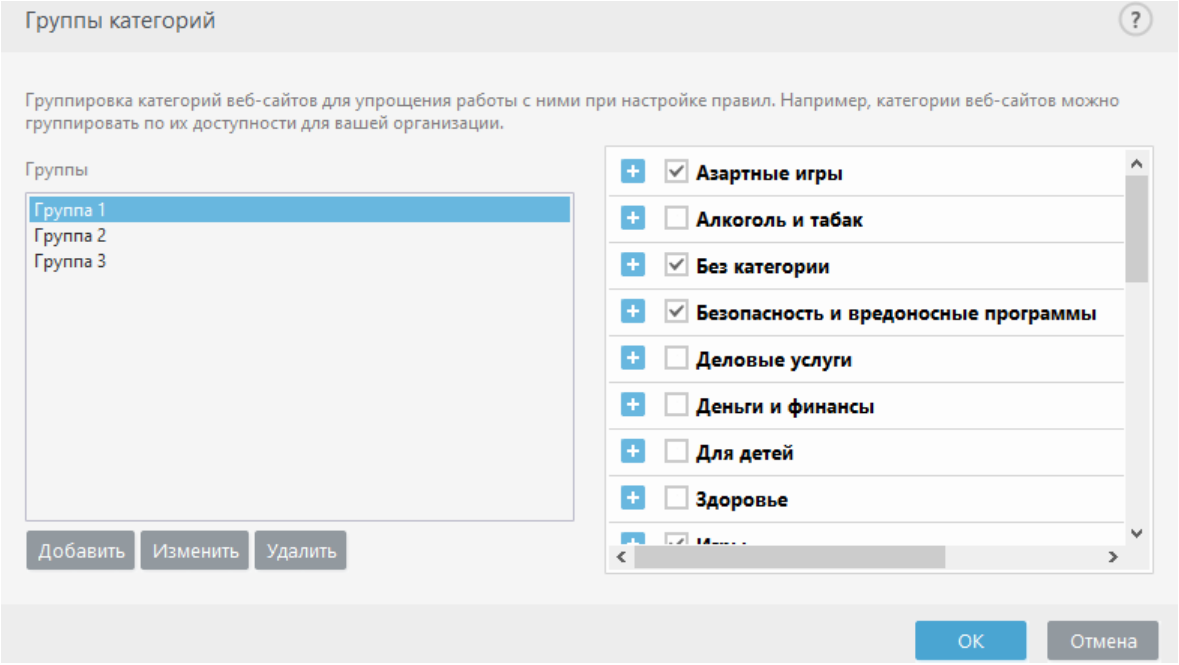
Окно «Группы категорий» разделено на две части. В левой части окна содержится список групп категорий.

- **Добавить**: нажмите для создания новой группы категорий.

• **Изменить**: используется для изменения существующей группы категорий.
• **Удалить**: выберите и щелкните, чтобы удалить существующую группу категорий из списка.

В правой части окна 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, а также приемлемые категории. 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 пользователям могут приходить уведомления 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.

> 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.

Группы URL-адресов

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

Создание группы URL-адресов

Чтобы создать группу URL-адресов, нажмите кнопку **Добавить** и введите имя новой группы URL-адресов.

Группа URL-адресов может пригодиться в том случае, если администратору нужно создать правило для нескольких веб-страниц (заблокированных или разрешенных).

Добавление URL-адресов в список группы URL-адресов — вручную

Чтобы добавить новый URL-адрес в список, выберите группу URL-адресов и нажмите кнопку **Добавить** в нижней правой части окна.

В списке URL-адресов нельзя использовать специальные символы «*» (звездочка) и «?» (вопросительный знак).

Указывать полное имя домена с http:// или https:// необязательно.

При добавлении домена в группу все содержимое, расположенное в нем и во всех поддоменах (например, *sub.examplepage.com*), будет заблокировано или разрешено в зависимости от выбранного вами действия на основе URL-адреса.

Если между двумя правилами возникнет противоречие, т. е. одно правило будет блокировать какой-либо домен, а второе — разрешать этот же домен, то соответствующий домен или IP-адрес все равно будет заблокирован. Дополнительные сведения о создании правил см. в разделе «Действие на основе URL-адреса».

Добавление URL-адресов в список группы URL-адресов — импорт с помощью .txt файла

Нажмите кнопку **Импорт**, чтобы импортировать файл со списком URL-адресов (в качестве разделителя используется разрыв строки, например файл .txt с кодировкой UTF-8). В списке URL-адресов нельзя использовать специальные символы «*» (звездочка) и «?» (вопросительный знак).

Использование групп URL-адресов для контроля доступа в Интернет

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 **OK**.

> 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.

Настройка сообщений о блокировке веб-страницы

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

Это используемое по умолчанию сообщение и дизайн уведомления в браузере, когда пользователь пытается перейти на заблокированный веб-сайт:

Использование

Давайте заблокируем категорию веб-сайта «Оружие».

Примером сообщения о блокировке веб-страницы может быть:

```
Веб-
страница %URL_OR_CATEGORY% заблокирована, поскольку содержит неприемлемое или вредоносное содержимое.
Для получения более подробной информации обратитесь к администратору.
```

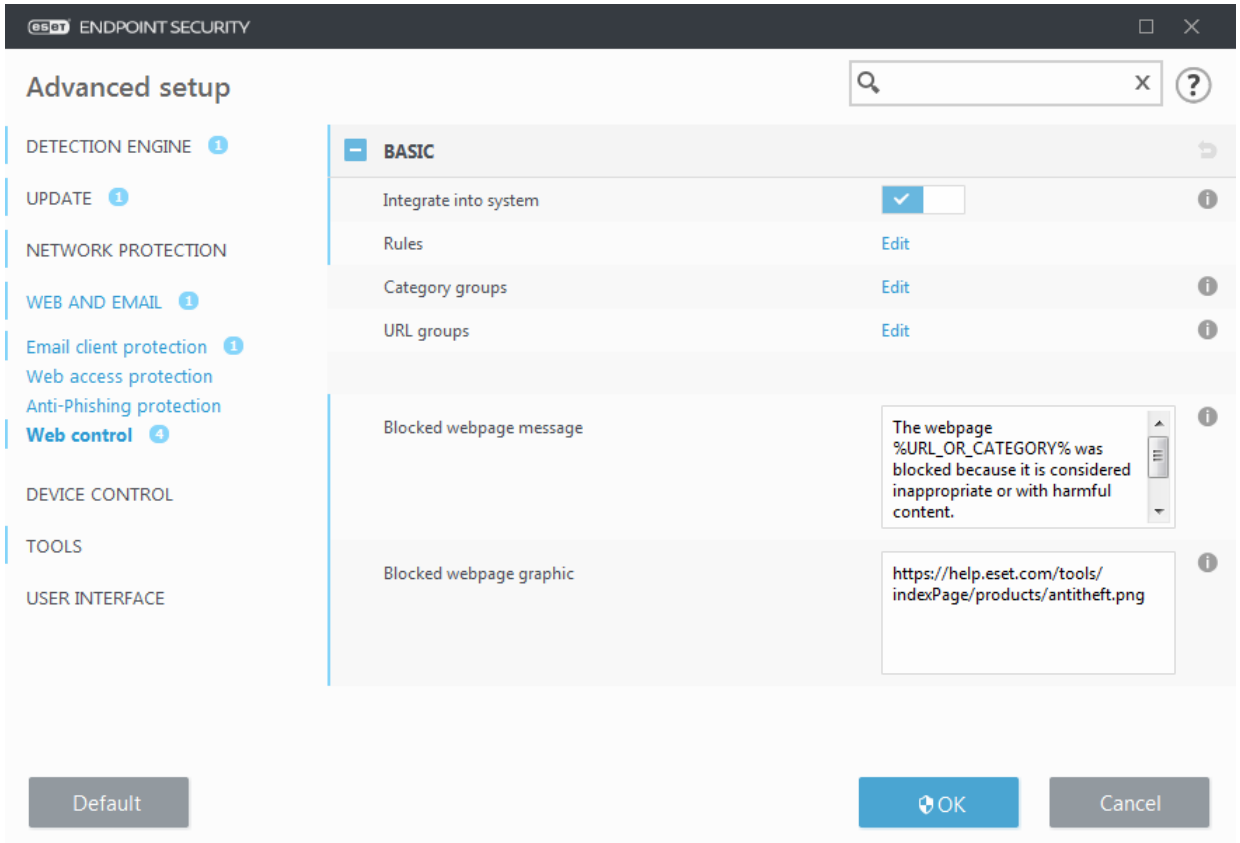
Переменная	Описание
%CATEGORY%	Заблокированная категория контроля доступа в интернет.
%URL_OR_CATEGORY%	Заблокирован веб-сайт или категория контроля доступа в интернет (зависит от правила блокировки контроля доступа в интернет).
%STR_GOBACK%	Значение кнопки «Назад»
%product_name%	Название продукта ESET (ESET Endpoint Security)
%product_version%	Версия продукта ESET.

Примером заблокированных графических материалов веб-страницы может быть:

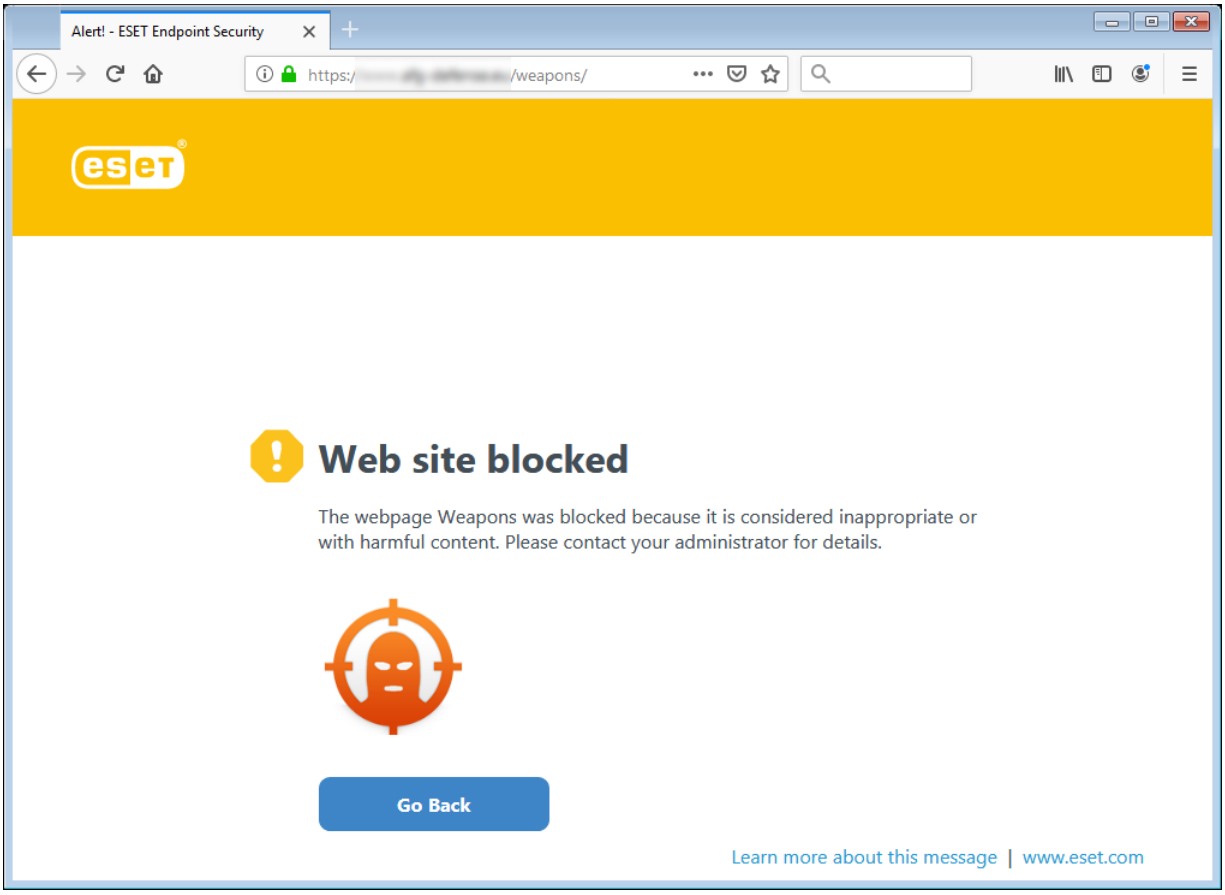
```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

Размер изображения (ширина/высота) будет масштабироваться автоматически, если размер слишком велик.

Конфигурация в ESET Endpoint Security будет выглядеть следующим образом:



Настраиваемое уведомление в браузере при попытке пользователя получить доступ к заблокированному веб-сайту, будет выглядеть следующим образом:



Обновление программы

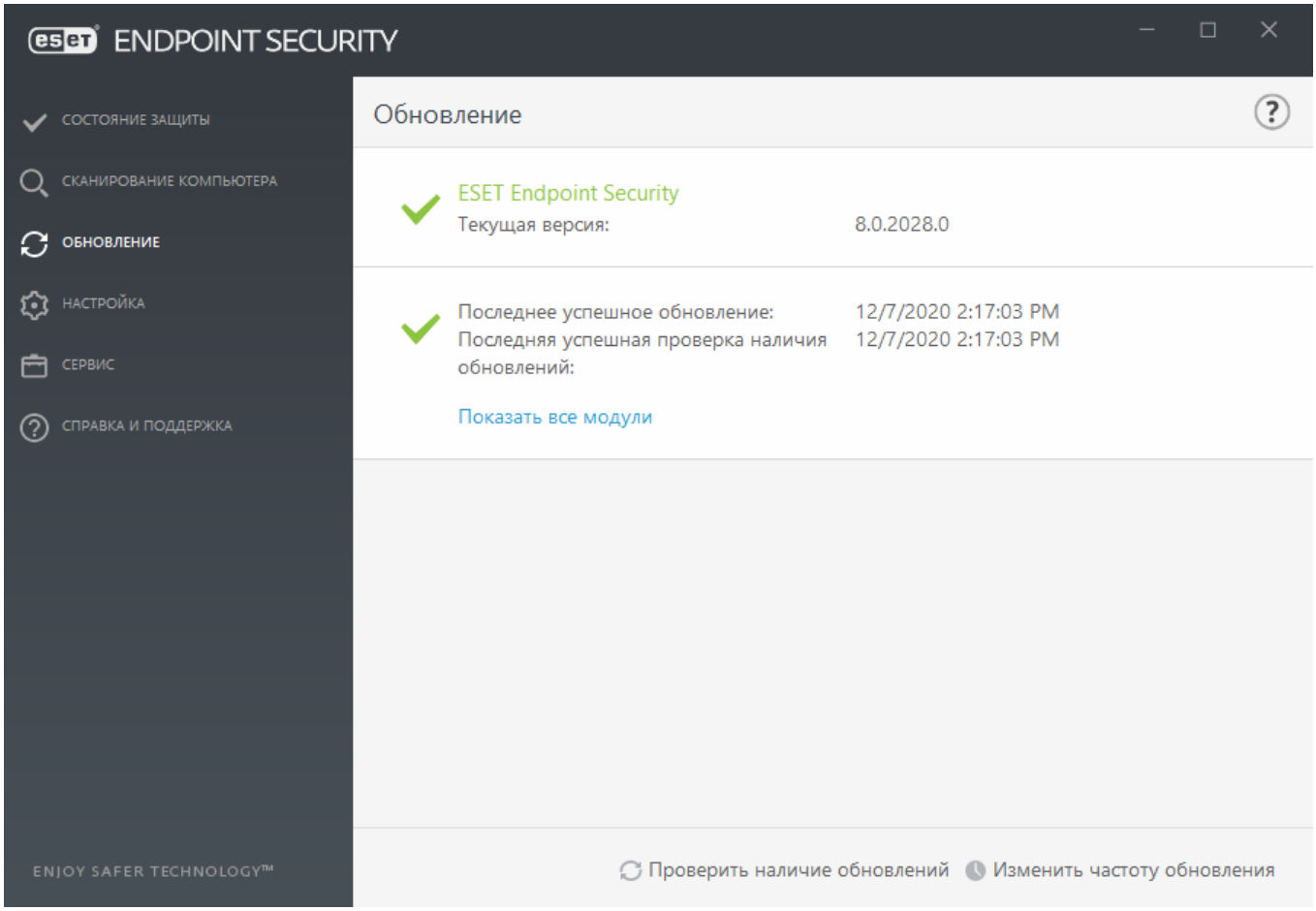
Регулярное обновление ESET Endpoint Security — лучший способ добиться максимального уровня безопасности компьютера. Модуль обновления поддерживает актуальность программы двумя способами: обновляет модуль обнаружения и обновляет компоненты системы. Обновления по умолчанию выполняются автоматически после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

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 файла офлайн-лицензии (не вводя имя пользователя и пароль) и попробовать выполнить обновление, отобразится красный текст **Модули не обновлены**. Он означает, что загружать обновления можно только с зеркала.

> Лицензионный ключ предоставляет компания ESET после приобретения ESET Endpoint Security.



Текущая версия: номер сборки ESET Endpoint Security.

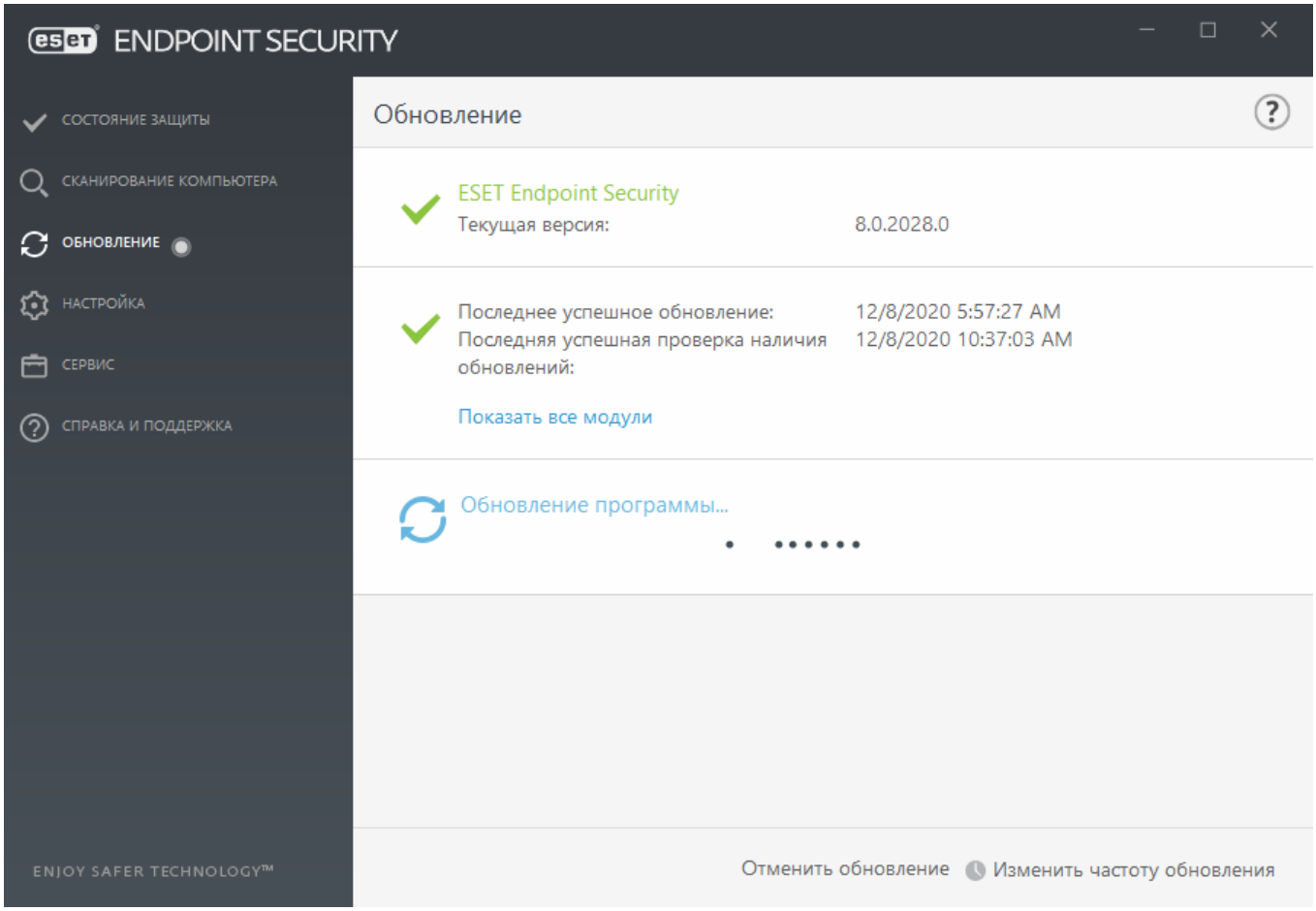
Последнее успешное обновление: дата и время последнего обновления. Следует убедиться, что в этом поле указана недавняя дата, поскольку это значит, что версия модуля обнаружения актуальна.

Последняя успешная проверка на наличие обновлений. Дата и время последней успешной 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**.

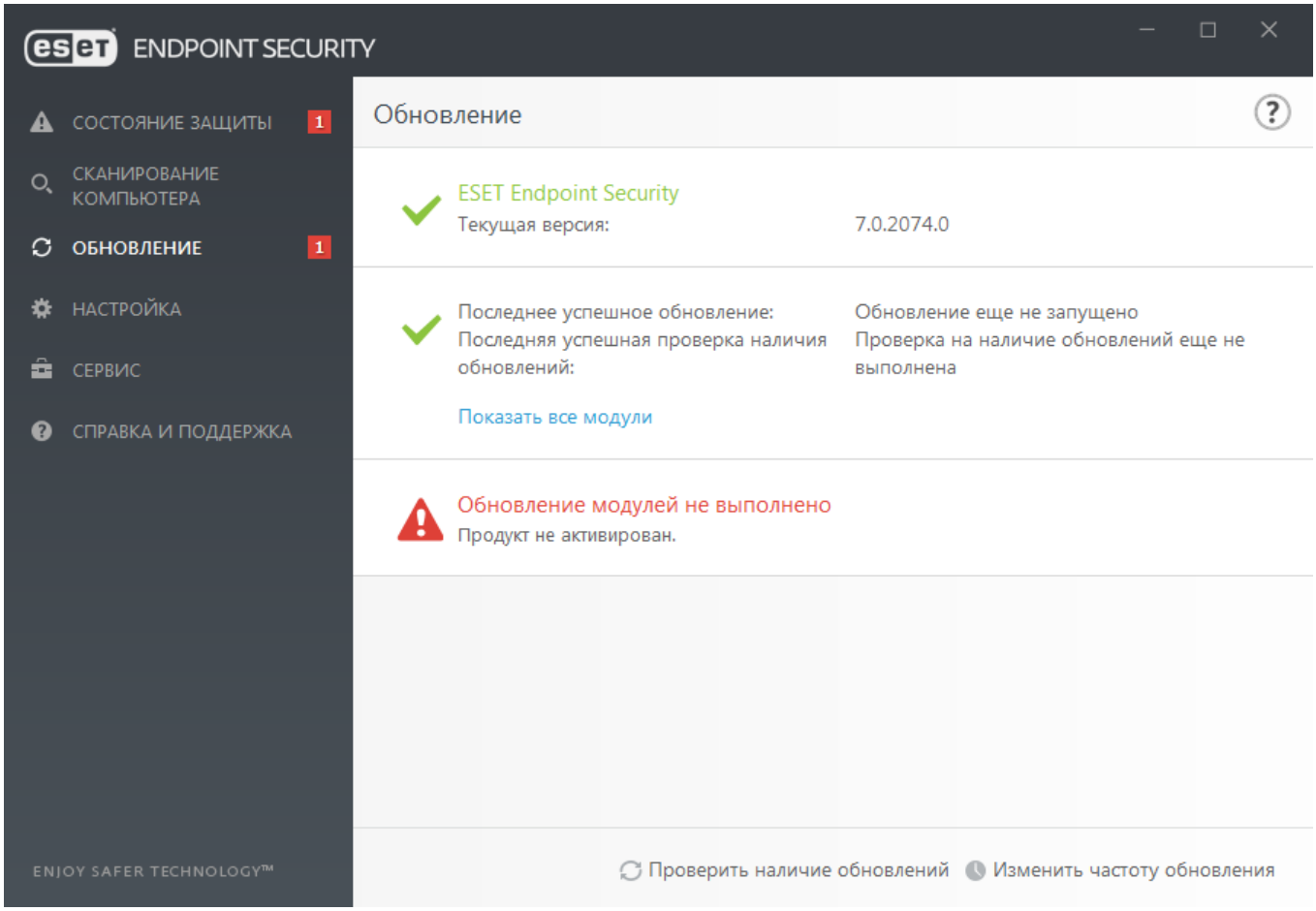


> Как правило, модули обновляются несколько раз в день. Если это не происходит, значит программа устарела. При этом повышается риск заражения. Необходимо обновить модули как можно скорее.

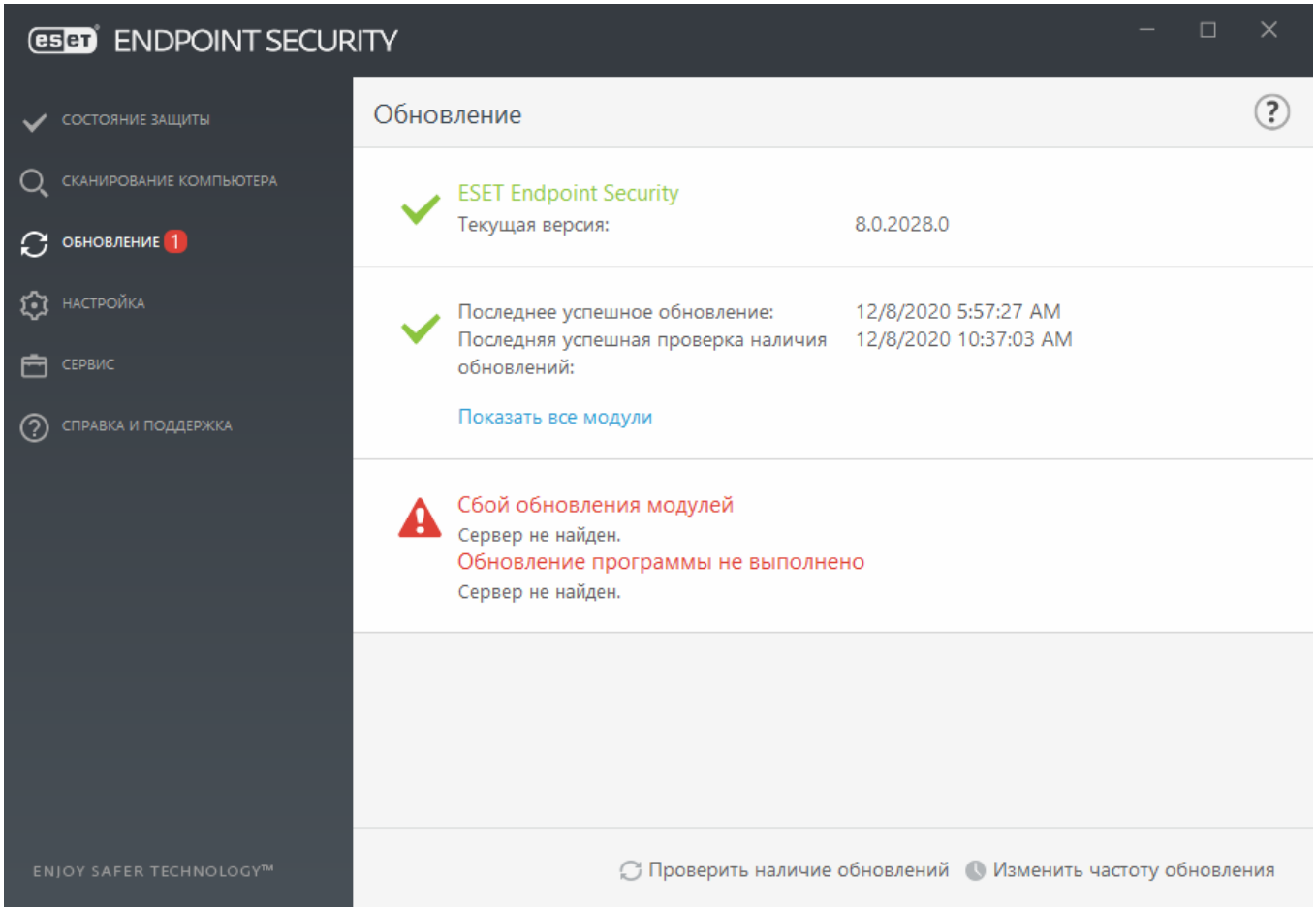
Модуль обнаружения устарел: эта ошибка появляется после нескольких неудачных попыток обновить модули. Рекомендуется проверить настройки обновления. Наиболее частая причина этой ошибки — неправильно введенные данные для аутентификации или неверно настроенные параметры подключения.

Предыдущее уведомление связано с двумя указанными ниже сообщениями об ошибках при обновлении (**Обновление модулей 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** > **Изменить лицензию** 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.



Дополнительные сведения можно найти в этой статье базы знаний ESET.

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.

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 HTTPS).

Основные сведения

Текущий профиль обновления отображается в раскрывающемся меню **Выбрать профиль обновления по умолчанию**.

Чтобы создать профиль, см. сведения в разделе Профили.

Автоматическое переключение профилей: назначение профиля обновления в соответствии с известными сетями в файерволе. Автоматическое переключение профилей позволяет менять профиль для определенной сети в зависимости от настроек в планировщике. Дополнительные сведения приведены в справке.

Настроить уведомления об обновлении: щелкните Изменить, чтобы выбрать, какие

уведомления приложения будут отображаться. Можно выбрать, нужно ли их показывать на рабочем столе и/или отправлять по электронной почте.

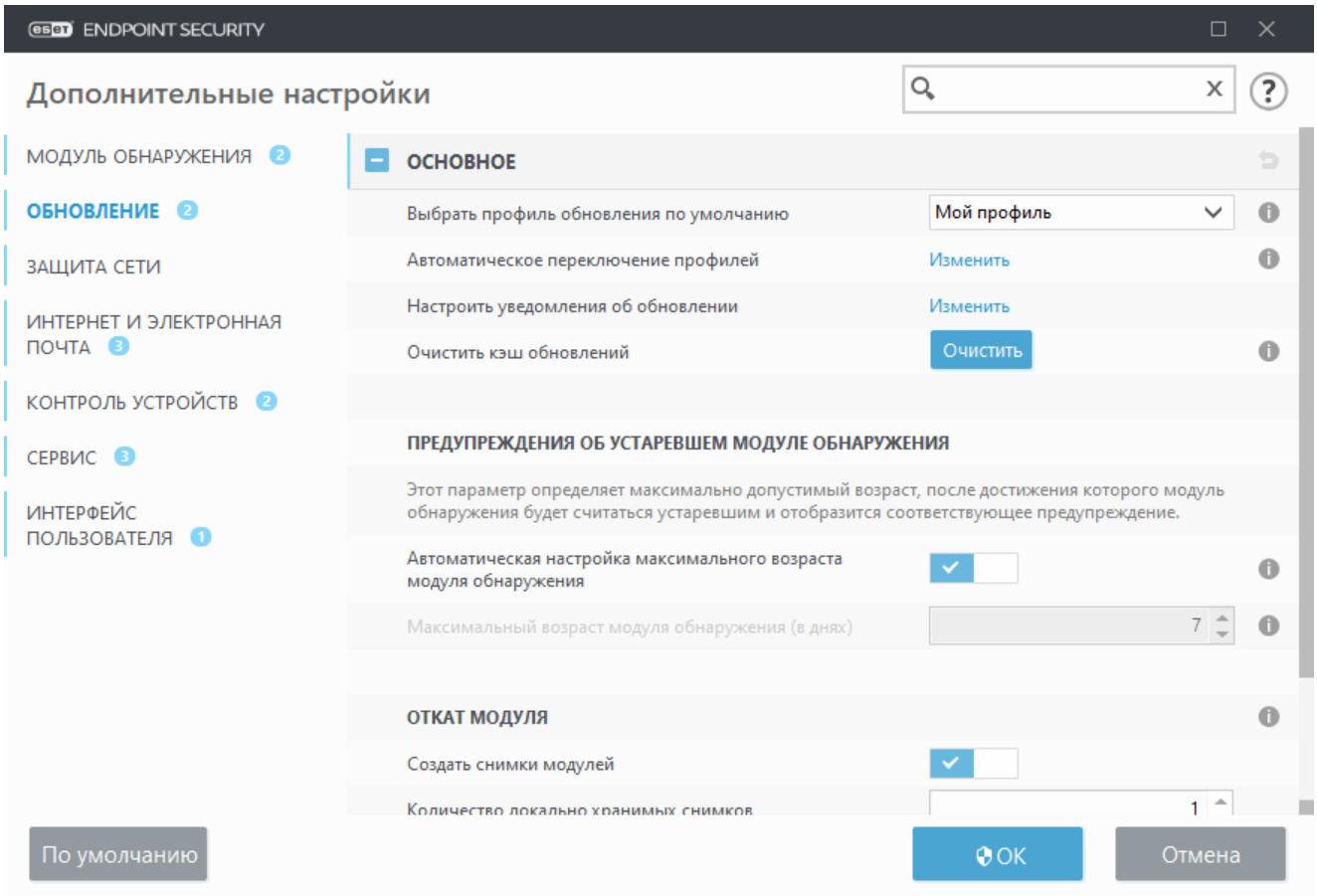
Если во время загрузки обновлений модуля обнаружения возникли проблемы, рядом с параметром **Очистить кэш обновлений** щелкните **Очистить**, чтобы удалить временные файлы обновлений (очистить кэш).

Предупреждения об устаревшем модуле обнаружения

Автоматически задавать максимальный возраст модуля обнаружения. Позволяет задать максимальное время (в днях), по истечении которого модуль обнаружения будет считаться устаревшим. Значение по умолчанию для параметра **Максимальный возраст модуля обнаружения (в днях)** — 7.

Откат модуля

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.



Профили

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 **Выберите профиль, который нужно изменить** отображается текущий профиль. По умолчанию для него задано значение **Мой профиль**.

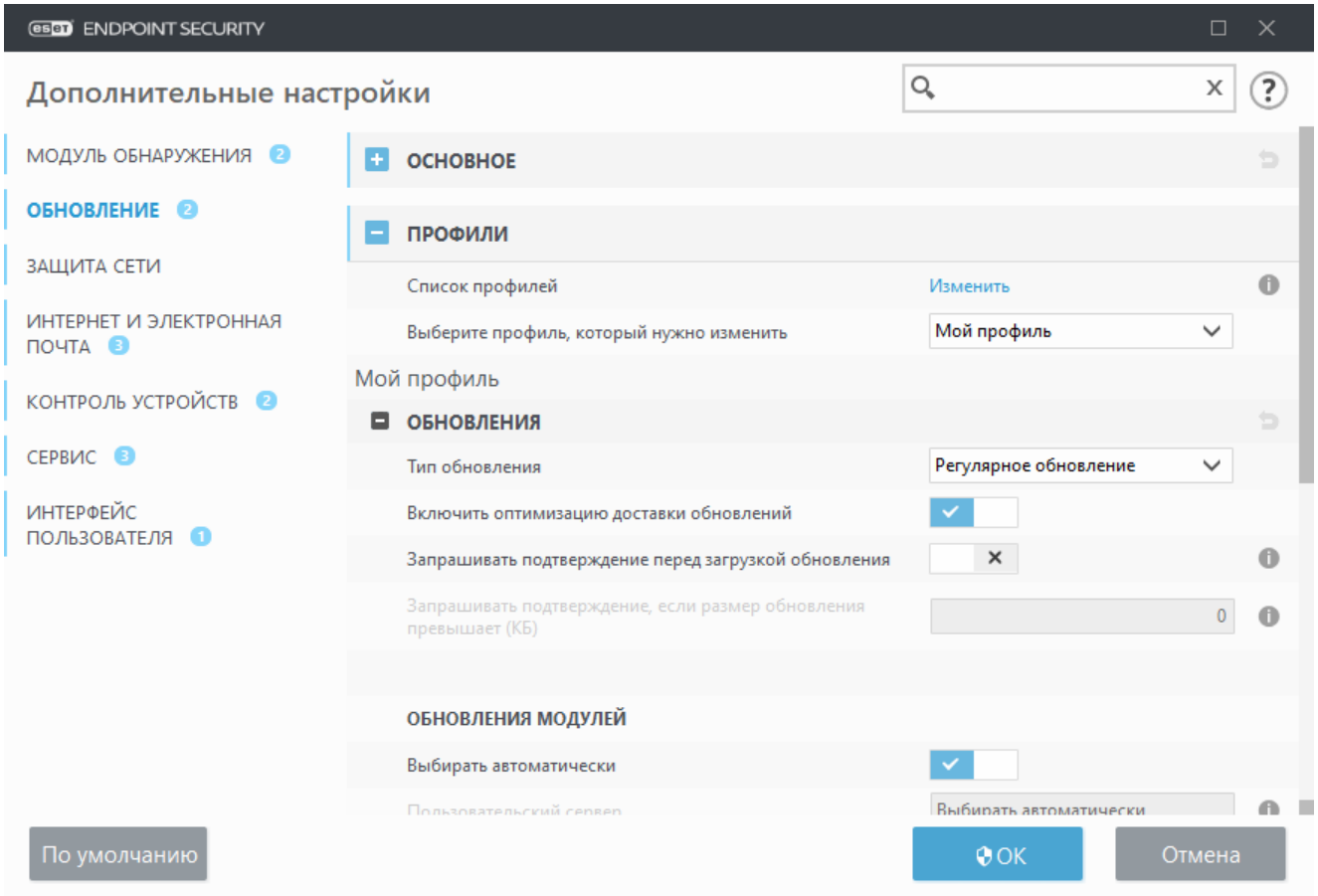
Чтобы создать профиль, рядом с элементом **Список профилей** щелкните **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**.

Обновления

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).

Включить оптимизацию доставки обновлений. Если опция включена, файлы обновлений можно загрузить с CDN (сеть доставки контента). Отключение этого параметра может привести к прерываниям загрузки и замедлению работы при перегрузке выделенных серверов обновления ESET. Отключение полезно, когда доступ к файерволу ограничен только для IP-адреса сервера обновления ESET, или если подключение к службам не работает CDN.

Запрашивать подтверждение перед загрузкой обновления. Программа отобразит уведомление, где можно подтвердить или отменить скачивание файла обновления. Если размер файла обновления больше значения, указанного в параметре Запрашивать подтверждение, если размер обновления превышает (КБ), на экран будет выводиться диалоговое окно для подтверждения. Если для размера файла обновления задано значение 0 КБ, программа всегда будет отображать диалоговое окно для подтверждения.



Обновления модулей

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

Включить более частые обновления сигнатур обнаружения. Сигнатуры обнаружения будут обновляться чаще. Если отключить этот параметр, качество обнаружения может ухудшиться.

Разрешить обновление модуля со съемных носителей: позволяет выполнить обновление со съемного носителя, если он содержит созданное зеркало. Если установлен флажок Автоматически, обновление будет выполняться в фоновом режиме. Если нужно показывать диалоговые окна обновления, выберите Всегда спрашивать.

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

> Номер порта сервера HTTP, указанный в примерах выше, зависит от того, какой порт использует ваш сервер HTTP/HTTPS.

Обновление компонентов программы

См. раздел Режим обновления.

Параметры подключения

См. раздел Параметры подключения.

Зеркало обновлений

См. раздел Зеркало обновлений.

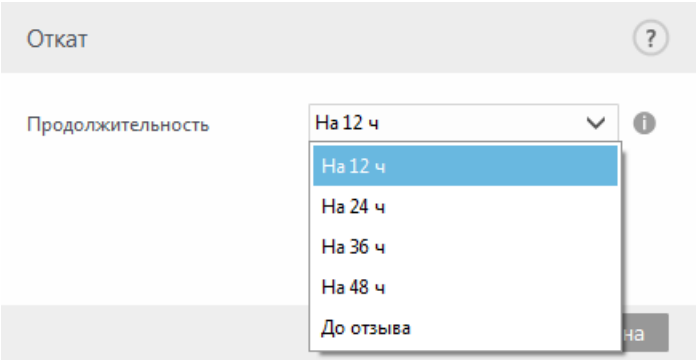
Откат обновления

Если вы подозреваете, что последнее обновление модуля обнаружения или новые модули программы повреждены или работают нестабильно, вы можете выполнить откат до предыдущей версии и временно отключить обновления. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени.

Программа ESET Endpoint Security создает снимки модуля обнаружения и модулей программы. Эти снимки используются функцией отката. Для создания снимков базы данных вирусов оставьте флажок **Создать снимки модулей** установленным. Когда флажок **Создать снимки модулей** установлен, первый снимок создается при первом обновлении. Следующий снимок создается через 48 часов. В поле **Количество локально хранимых снимков** указывается количество хранимых снимков модуля обнаружения.

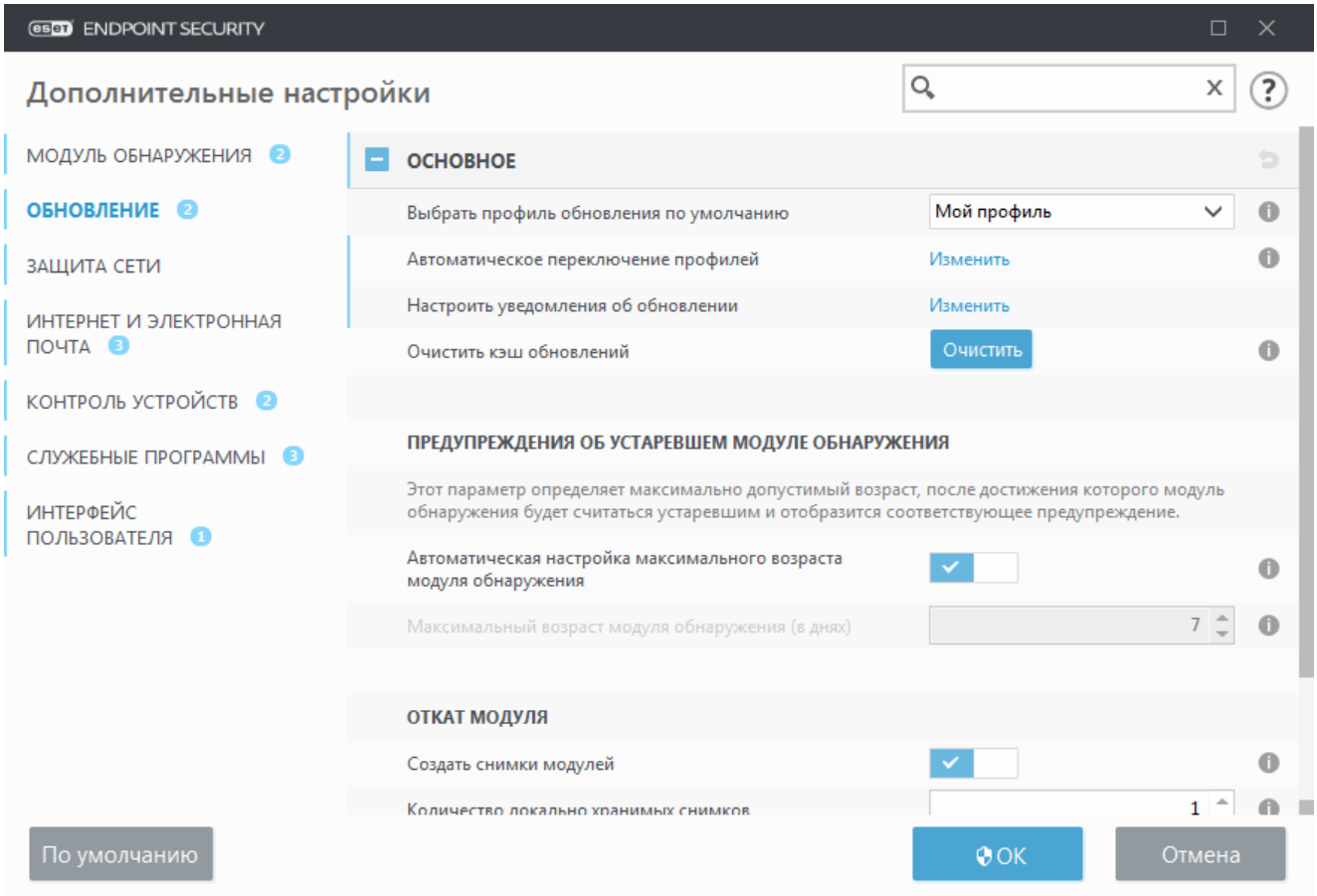
> Когда достигается максимальное количество снимков (например, три), самый старый снимок заменяется новым снимком каждые 48 часов. ESET Endpoint Security откатывает версии обновления модуля обнаружения и модуля программы до самого старого снимка.

В раскрывающемся меню **Длительность** нужно выбрать промежуток времени, если был нажат элемент **Откат** (**Расширенные параметры** (F5) > **Обновление** > **Основное** > **Откат модуля**).



Выберите вариант **До отзыва**, чтобы отложить регулярные обновления на неопределенный период, пока функция обновления не будет восстановлена вручную. Поскольку это подвергает систему опасности, не рекомендуется использовать этот параметр.

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



Предположим, последней версии модуля обнаружения присвоен номер 22700. Версии 22698 и 22696 хранятся в качестве снимков модуля обнаружения. Обратите внимание, что версия 22697 недоступна. В этом примере компьютер был выключен во время обновления 22697, и более новая версия обновления стала доступна до того, как была загружена версия 22697. Если в поле **Количество локально хранимых снимков** установлено значение 2 и пользователь щелкнет **Откат**, модуль обнаружения (включая модули программы) вернется к версии 22696. Это может занять некоторое время. Чтобы проверить, произведен ли откат до предыдущей версии модуля обнаружения, откройте окно Обновление.

Обновление компонентов программы

Раздел **Обновление компонентов программы** 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 раскрывающемся меню **Режим обновления** доступны три параметра:

- **Запрашивать подтверждение перед обновлением**. Это вариант по умолчанию для неуправляемых конечных точек. Пользователю будет предлагаться подтвердить обновление компонентов программы или отказаться от него, когда такое обновление становится доступно.

• **Автообновление**. Обновления компонентов программы будут загружаться и устанавливаться автоматически. Обратите внимание на то, что может потребоваться перезагрузка компьютера.

• **Никогда не обновлять**. Обновление компонентов программы выполняться не будет. Этот вариант подходит для серверной установки, поскольку серверы обычно перезапускаются только при техническом обслуживании.

По умолчанию обновления компонентов программы загружаются с серверов репозитория ESET. В больших или автономных средах трафик можно распределить, чтобы использовать внутреннее кэширование файлов компонентов программы.

Определение пользовательского сервера для обновления компонентов программы

1.Задайте путь к обновлению компонентов программы в поле **Пользовательский сервер**.
Можно использовать ссылку HTTP(S), путь общей сетевой папки SMB, путь на локальном диске или съемном носителе. В случае сетевых дисков используйте путь UNC вместо буквы подключенного диска.

2.Не заполняйте поля **Имя пользователя** и **Пароль**, если они не обязательны.
Если необходимо, задайте здесь соответствующие учетные данные для аутентификации HTTP на пользовательском веб-сервере.

3.Подтвердите изменения и проверьте наличие обновления компонентов программы, выполнив стандартное обновление ESET Endpoint Security.

> 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.

Параметры подключения

Для доступа к параметрам настройки прокси-сервера для конкретного профиля обновлений щелкните элемент **Обновление** в дереве **Расширенные параметры** (F5), а затем щелкните элемент **Профили** > **Обновления** > **Параметры подключения**.

Прокси-сервер

Откройте раскрывающееся меню **Режим прокси-сервера** и выберите один из трех перечисленных далее вариантов.

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

Выберите вариант **Использовать общие параметры прокси-сервера**, чтобы использовать параметры конфигурации прокси-сервера, уже заданные в разделе дерева расширенных параметров **Сервис** > **Прокси-сервер**.

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

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

• Для обновления ESET Endpoint Security используется прокси-сервер, отличный от указанного в разделе Сервис > **Прокси-сервер**. При такой конфигурации нужно указать параметры нового прокси-сервера: адрес **прокси-сервера**, **порт передачи данных** (по умолчанию 3128), а также **имя пользователя** и **пароль** для прокси-сервера (если необходимо).
• Общие параметры прокси-сервера не заданы глобально, однако ESET Endpoint Security будет подключаться к прокси-серверу для получения обновлений.
• Компьютер подключается к Интернету через прокси-сервер. Параметры берутся из Internet Explorer в процессе установки программы, но при их изменении (например, при смене поставщика услуг Интернета) нужно убедиться в том, что указанные в этом окне параметры прокси-сервера верны. Если этого не сделать, программа не сможет подключаться к серверам обновлений.

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

Использовать прямое подключение, если прокси-сервер недоступен: прокси-сервер не будет использоваться при обновлении, если он недоступен.

Общие ресурсы Windows

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.

> ⚠ 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.

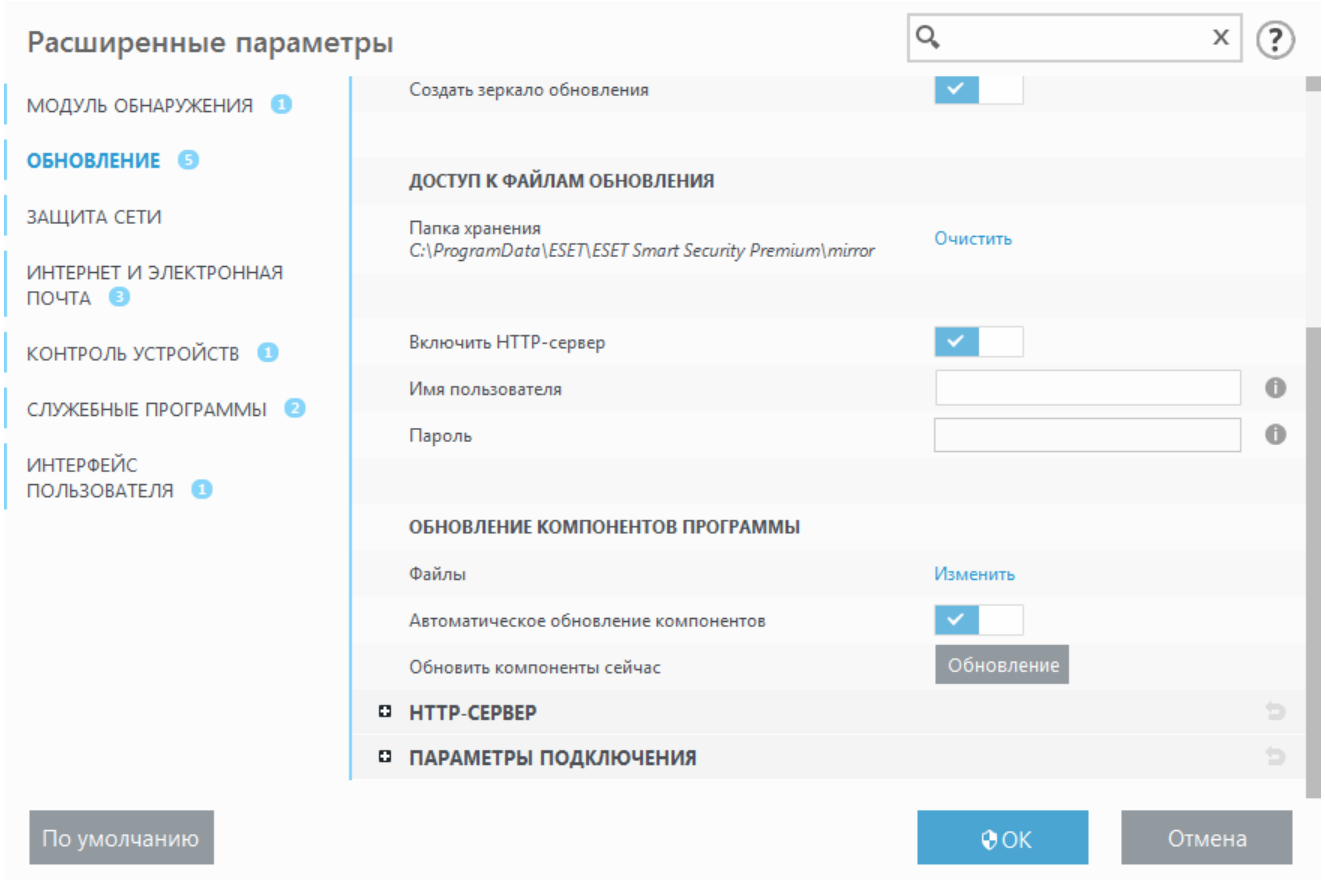
Выберите параметр **Отключиться** от сервера после завершения обновления для принудительного отключения, если подключение к серверу остается активным даже после загрузки обновлений.

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.

> ℹ Чтобы свести к минимуму интернет-трафик в сетях, в которых используется ESET PROTECT для управления большим количеством клиентов, рекомендуется использовать прокси-сервер Apache HTTP, а не настраивать клиент как зеркало. Прокси-сервер Apache HTTP можно установить вместе с ESET PROTECT с помощью комплексного установщика или как отдельный компонент. Дополнительные сведения и описание различий между прокси-сервером Apache HTTP, средством «Зеркало» и прямым подключением можно найти на странице онлайн-справки ESET PROTECT.

Настроить локальный сервер зеркала можно в расширенных параметрах в разделе **Обновление**. Чтобы попасть в этот раздел, нажмите клавишу **F5** (откроется меню «Расширенные параметры»), щелкните **Обновление** > **Профили** и разверните элемент **Зеркало обновлений**.



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

Доступ к файлам обновления

Включить HTTP-сервер. Если этот параметр активирован, файлы обновлений будут доступны по протоколу HTTP без необходимости указывать учетные данные.

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.

Обновление компонентов программы

Файлы: при настройке зеркала можно указать предпочитаемые языки обновлений. Выбранные

языки должны поддерживаться сервером зеркала, который настроил пользователь.

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.

HTTP-сервер и SSL для зеркала

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**.

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.

> Данные для аутентификации, такие как **имя пользователя** и **пароль**, предназначены только для доступа к зеркальному HTTP-серверу. Заполнять эти поля необходимо только в том случае, если требуются имя пользователя и пароль.

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.

> **Самозаверяющие сертификаты для зеркала HTTPS**
> Если вы используете зеркальный сервер HTTPS, необходимо импортировать его сертификат в хранилище доверенных корневых сертификатов на всех клиентских компьютерах. См. раздел Установка доверенного корневого сертификата в Windows.

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 **Расширенные параметры** > **Обновление** > **Профили** > **Зеркало обновлений** 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**.

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.

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.

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 обновлений** 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 **Расширенные параметры** (F5) и последовательно щелкните элементы **Обновление** > **Профили** > **Обновления** > **Обновления модулей**.

- Отключите 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 **Расширенные параметры** > **Обновление** > **Профили** > **Зеркало обновлений** необходимо настроить доступ к зеркалу, сняв флажок **Включить HTTP-сервер**. Этот параметр 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 **Расширенные параметры** (F5) и щелкните **Обновление** > **Профили** > **Обновления** > **Параметры подключения** > **Общие ресурсы Windows** > **Подключаться к локальной сети как**. Этот параметр аналогичен используемому для обновления и описан в разделе Подключение к локальной сети.

Чтобы получить доступ к папке зеркала, это нужно сделать в той же учетной записи, что и для входа в компьютер, на котором создано зеркало. В случае, если компьютер находится в домене, следует использовать имя пользователя в формате «ДОМЕН\имя_пользователя». Если компьютер не находится в домене, следует использовать «IP-адрес_сервера\имя_пользователя» или «ИМЯ_КОМПЬЮТЕРА\имя_пользователя».

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

1. Откройте в ESET Endpoint Security меню **Расширенные параметры** и щелкните **Обновление** > **Профили** > **Обновления**.

2. Рядом с элементом **Обновления модулей** снимите флажок **Выбирать автоматически** и добавьте новый сервер в поле **Сервер обновлений** , используя формат *UNC*\ПУТЬ.

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

Создание зеркала с помощью средства «Зеркало»
Средство «Зеркало» создает структуру папок, которая отличается от создаваемой в зеркале Endpoint. Каждая папка содержит файлы обновления для группы продуктов. Укажите полный путь к надлежащей папке в параметрах обновления продукта, использующего зеркало.
Например, чтобы обновить ESET PROTECT из зеркала, задайте следующее значение параметра Сервер обновлений (подставив корневой адрес вашего HTTP-сервера):
`http://your_server_address/mirror/eset_upd/era6`

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.

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.

ESET Endpoint Security ошибка при подключении при загрузке файлов обновлений: обычно происходит при указании неправильных данных сервера обновлений (сетевого пути к папке зеркала), с которого рабочие станции загружают обновления.

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**

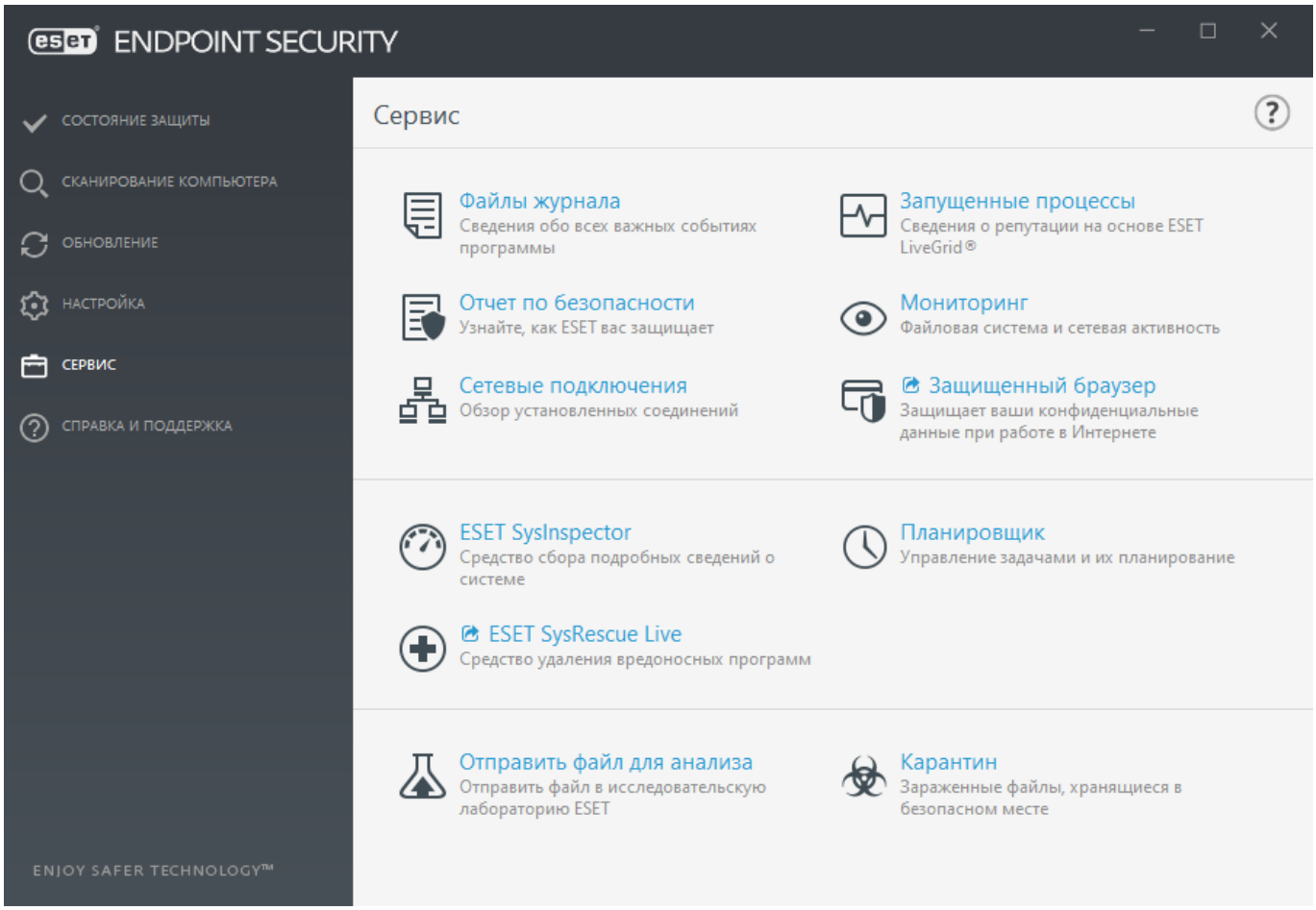
Каждую задачу обновления можно изменить в соответствии с конкретными требованиями. Кроме задач по умолчанию можно создать другие задачи обновления с пользовательскими настройками. Дополнительную информацию о создании и настройке задач обновления см. в разделе Планировщик.

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
- Отчет по безопасности (для неуправляемых конечных точек)
- Запущенные процессы (если использование системы ESET LiveGrid® включено в ESET Endpoint Security)
- Мониторинг
- Планировщик
- Сетевые подключения (если Файервол включен в программе ESET Endpoint Security)
- Защищенный браузер (отключен в ESET Endpoint Security по умолчанию)
- ESET SysInspector
- ESET SysRescue Live: перенаправляет на веб-сайт ESET SysRescue Live, с которого можно загрузить образ ESET SysRescue Live с расширением .iso для компакт- или DVD-диска.
- Карантин
- Отправка образца на анализ. Возможность отправить подозрительный файл на анализ в исследовательскую лабораторию ESET (может быть недоступна в зависимости от конфигурации ESET LiveGrid®).



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**. Этот журнал содержит подробную информацию об угрозах и 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. Неочищенные заражения всегда отмечены красным текстом на розовом фоне, очищенные заражения — желтым текстом на белом фоне. Неочищенные потенциально опасные приложения (PUA) отмечены желтым текстом на белом фоне.

- **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 при подключении к ESET Enterprise Inspector. Протокол отображает сведения о причине и исходном модуле, заблокировавшем файл, а также о приложении и пользователе, которые инициировали исполнение файла. Более подробная информация приведена в онлайн-руководстве пользователя ESET Enterprise Inspector.

- **Отправленные файлы**. Содержит записи о файлах, отправленных в ESET LiveGrid® или ESET Dynamic Threat Defense для анализа.

- **Журналы аудита**. Каждый журнал содержит такие сведения, как дата и время внесения изменения, тип изменения, описание, источник и пользователь. Дополнительные сведения см. в разделе Журналы аудита.

- **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.

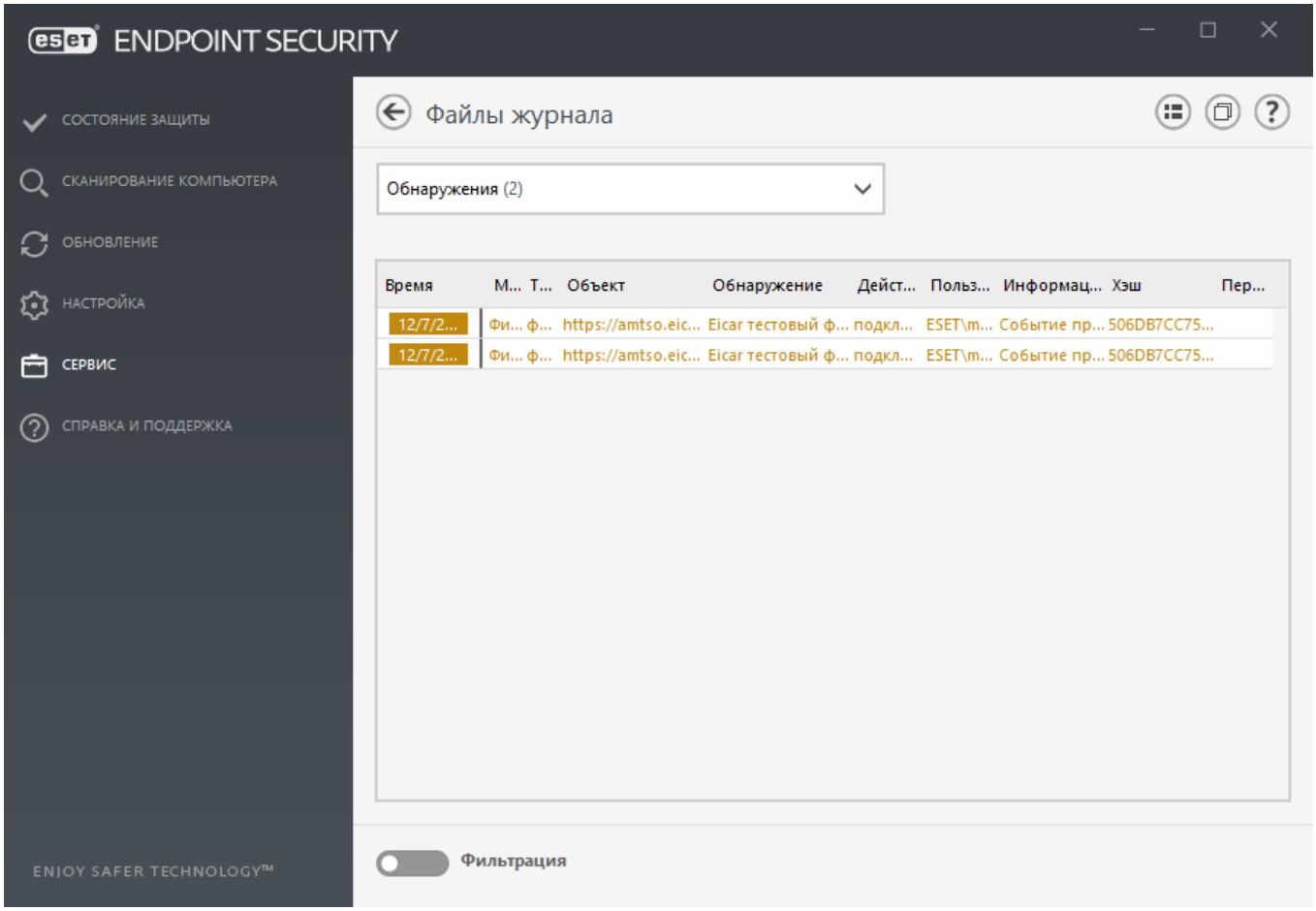
• **Защита сети** – В журнале файервола отображаются сведения обо всех удаленных атаках, обнаруженных модулем защиты от сетевых атак или файерволом. В нем находится информация обо всех атаках, которые были направлены на компьютер пользователя. В столбце Событие отображаются обнаруженные атаки. В столбце 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. Если правило не совпадает с подключенным устройством, запись о нем в журнале не создается. Также здесь отображаются такие сведения, как тип устройства, серийный номер, имя производителя и размер носителя (при его наличии).



Выделите содержимое любого журнала и нажмите клавиши `Ctrl + C`**, чтобы скопировать его в буфер обмена**. Удерживайте клавиши `Ctrl + Shift`, чтобы выделить несколько записей.

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

Щелкните правой кнопкой мыши определенную запись, чтобы открыть 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.).
- **Фильтр**: при выборе этого параметра на экран выводится окно Фильтрация журнала, 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.
- **Найти/Найти далее/Найти ранее**: щелкнув этот параметр, в окне «Фильтрация журнала» можно определить критерии фильтрации, чтобы выделить определенную запись.
- **Создать исключение**: создание нового Исключения из обнаружения с помощью мастера (Недоступно для обнаружения вредоносных программ).

Фильтрация журнала

Чтобы указать критерии фильтрации, выберите **Сервис** > **Файлы журнала** и щелкните **Фильтрация**.

С помощью функции фильтрации журналов можно найти нужную информацию среди множества записей. Эта функция позволяет сузить круг, если вы ищете записи журнала по типу события, состоянию или периоду времени. Можно отфильтровать записи журнала по определенным параметрам поиска. В окне «Файлы журналов» отобразятся только записи, которые соответствуют этим параметрам.

В поле **Найти текст** введите ключевое слово для поиска. Используйте раскрывающееся меню **Искать в столбцах**, чтобы уточнить условия поиска. Выберите одну или несколько записей в раскрывающемся меню **Типы записей журнала**. Задайте **период времени**, результаты за

который нужно вывести на экран. Можете также использовать другие параметры поиска, например **Только слова целиком** или **С учетом регистра**.

Найти текст

Введите строку (слово целиком или частично). Появятся только записи, в которых содержится эта строка. Остальные записи будут опущены.

Искать в столбцах

Выберите, какие столбцы будут учитываться при поиске. Для использования в поиске можно отметить один столбец или сразу несколько.

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,

Период времени, с

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

• **Не указано** (по умолчанию). Поиск по периоду времени не выполняется, а ведется в журнале целиком.
• **Прошлый день**
• **Прошлая неделя**
• **Прошлый месяц**
• **Период времени**. Можно указать определенный период времени (начало и конец периода), чтобы отфильтровать записи по нему.

Только слова целиком

Установите этот флажок, если для получения более точных результатов нужно искать определенные слова целиком.

С учетом регистра

Включите этот параметр, если при фильтрации должен учитываться регистр букв. После настройки параметров поиска или фильтрации нажмите кнопку **OK**, чтобы отобразились отфильтрованные записи журнала, или нажмите кнопку Найти, чтобы начать поиск. Поиск в файлах журнала ведется сверху вниз, начиная с текущей позиции (выделенной записи). Поиск прекращается, когда находится первая соответствующая его критериям запись. Чтобы найти следующую запись, нажмите клавишу **F3**. Чтобы уточнить критерии поиска, щелкните правой кнопкой мыши и выберите пункт **Найти**.

Настройка ведения журнала

Настройку ведения журнала ESET Endpoint Security можно открыть из главного окна программы. Выберите **Настройки** > **Дополнительные настройки** > **Служебные программы** > **Файлы журнала**. Этот раздел используется для настройки управления журналами. Программа автоматически удаляет старые файлы журналов, чтобы сэкономить дисковое пространство. Для файлов журнала можно задать параметры, указанные ниже.

Минимальная степень детализации журнала: настройка минимального уровня детализации записей о событиях.

- **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 файерволаи т. п.).

> i Если выбрать уровень детализации «**Диагностика**», в журнал будут записываться сведения обо всех заблокированных подключениях.

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

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

Щелкните **Оптимизировать**, чтобы начать дефрагментацию файлов журналов. Все пустые записи журналов удаляются для улучшения производительности и скорости обработки журналов. Такое улучшение особенно заметно, если в журналах содержится большое количество записей.

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

- **Целевой каталог**: каталог, в котором будут храниться файлы журналов (только для текстового формата и формата CSV). Вы можете скопировать путь или выбрать другой каталог, щелкнув **Отменить выбор**. Каждый раздел журнала сохраняется в отдельный файл с предварительно заданным именем (например, в файл *virlog.txt* сохраняется раздел **Обнаруженные угрозы** файла журнала, если для хранения файлов журнала вы используете текстовый формат файлов).

• **Тип**: если выбрать формат **Текст**, журналы будут сохраняться в текстовый файл, данные в котором будут разделены табуляцией. То же касается формата **CSV**. Если выбрать **Событие**, журналы будут сохраняться не в файл, а в журнал событий Windows (его можно просмотреть на панели управления в средстве просмотра событий).

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

Включить отслеживание изменений конфигурации в журнале аудита: информирует вас о каждом изменении конфигурации. Дополнительные сведения см. в разделе Журналы аудита.

> i Для более быстрого решения проблем специалисты ESET иногда могут запрашивать у пользователей журналы с их компьютеров. ESET Log Collector облегчает сбор необходимой информации. Дополнительные сведения о ESET Log Collector см. в статье базы знаний ESET.

Журналы аудита

В среде предприятия, как правило, имеется несколько пользователей с правами доступа, которые дают возможность настраивать конечные точки. Поскольку изменение конфигурации продукта может значительно повлиять на его работу, крайне важно, чтобы администраторы могли отслеживать изменения, внесенные пользователями, и на основе этой информации быстро выявлять и устранять проблемы, а также предотвращать их повторение в будущем.

Журнал аудита — это новый тип ведения журнала, представленный в ESET Endpoint Security версии 7.1, который помогает определить причину проблемы. В журнал аудита заносятся изменения в конфигурации или состоянии защиты и записываются моментальные снимки для последующего изучения.

Чтобы просмотреть **журнал аудита**, в главном меню последовательно выберите **Инструменты**, **Файлы журнала** и в раскрывающемся списке выберите **Журналы аудита**.

Журнал аудита содержит такую информацию:

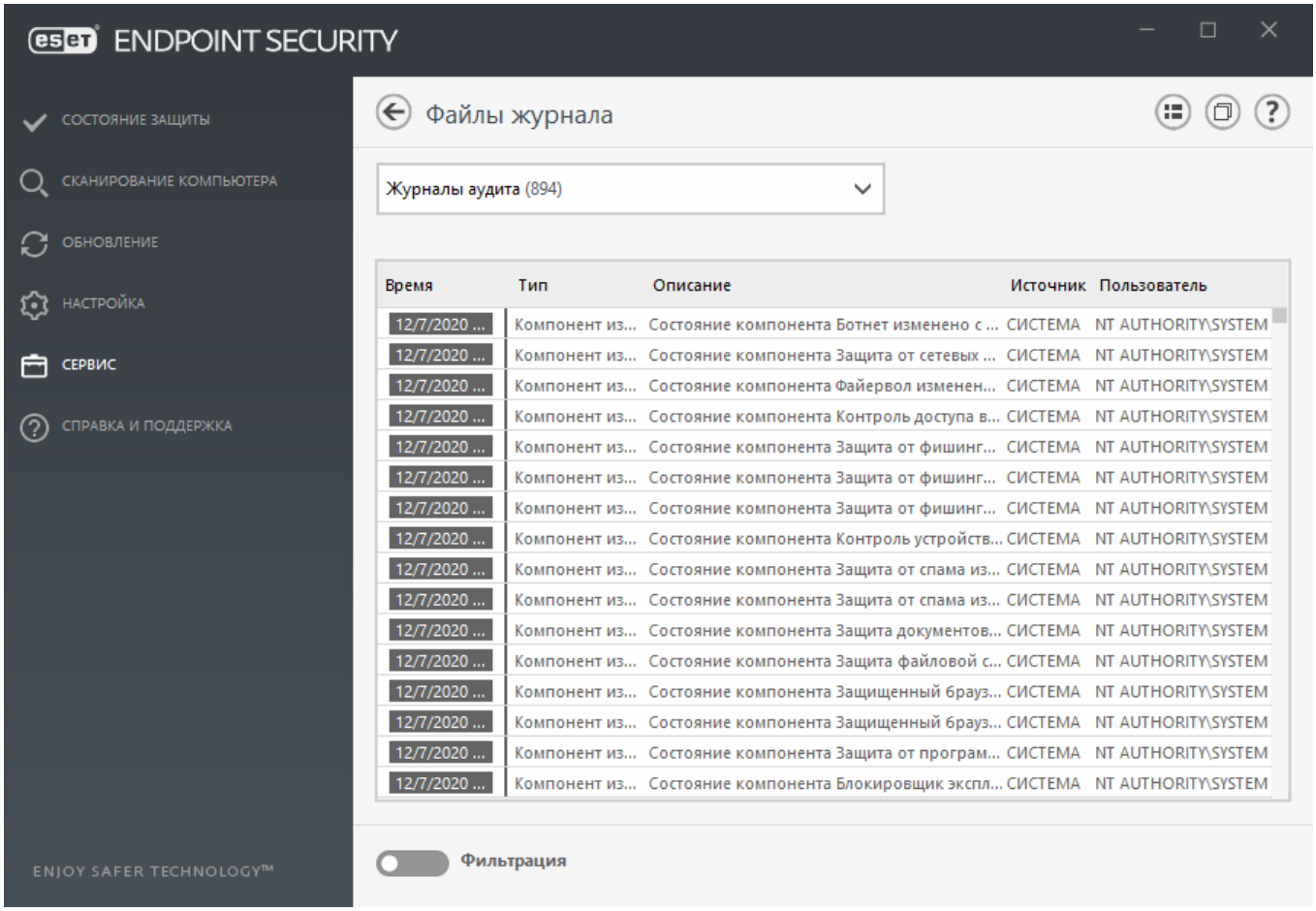
• Время: когда произошло изменение.

• Тип: какой тип параметра или компонента был изменен.

• Описание: что именно было изменено и какая часть параметров была изменена, а также количество измененных параметров.

• Источник: где находится источник изменения.

• Пользователь: кто внес изменение.



В окне «Файлы журнала» щелкните правой кнопкой мыши любой тип в разделе **Параметры изменены** журнала аудита и выберите в контекстном меню пункт **Показать изменения**, чтобы просмотреть подробные сведения о внесенном изменении. Кроме того, вы можете отменить изменение параметров, выбрав в контекстном меню пункт **Восстановить** (недоступен для продуктов под управлением ESMC или ESET PROTECT). Если вы выберете в контекстном меню пункт **Удалить все**, будет создан журнал с информацией об этом действии.

Если в разделе **Расширенные параметры** > **Сервис** > **Файлы журнала** включен параметр **Автоматически оптимизировать файлы журнала**, дефрагментация журналов аудита будет выполняться автоматически, как и в случае других журналов.

Если в разделе **Расширенные параметры** > **Сервис** > **Файлы журнала** включен параметр **Автоматически удалять записи старше, чем (дн.)**, записи в журнале, созданные раньше, чем указанное количество дней назад, будут автоматически удаляться.

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.

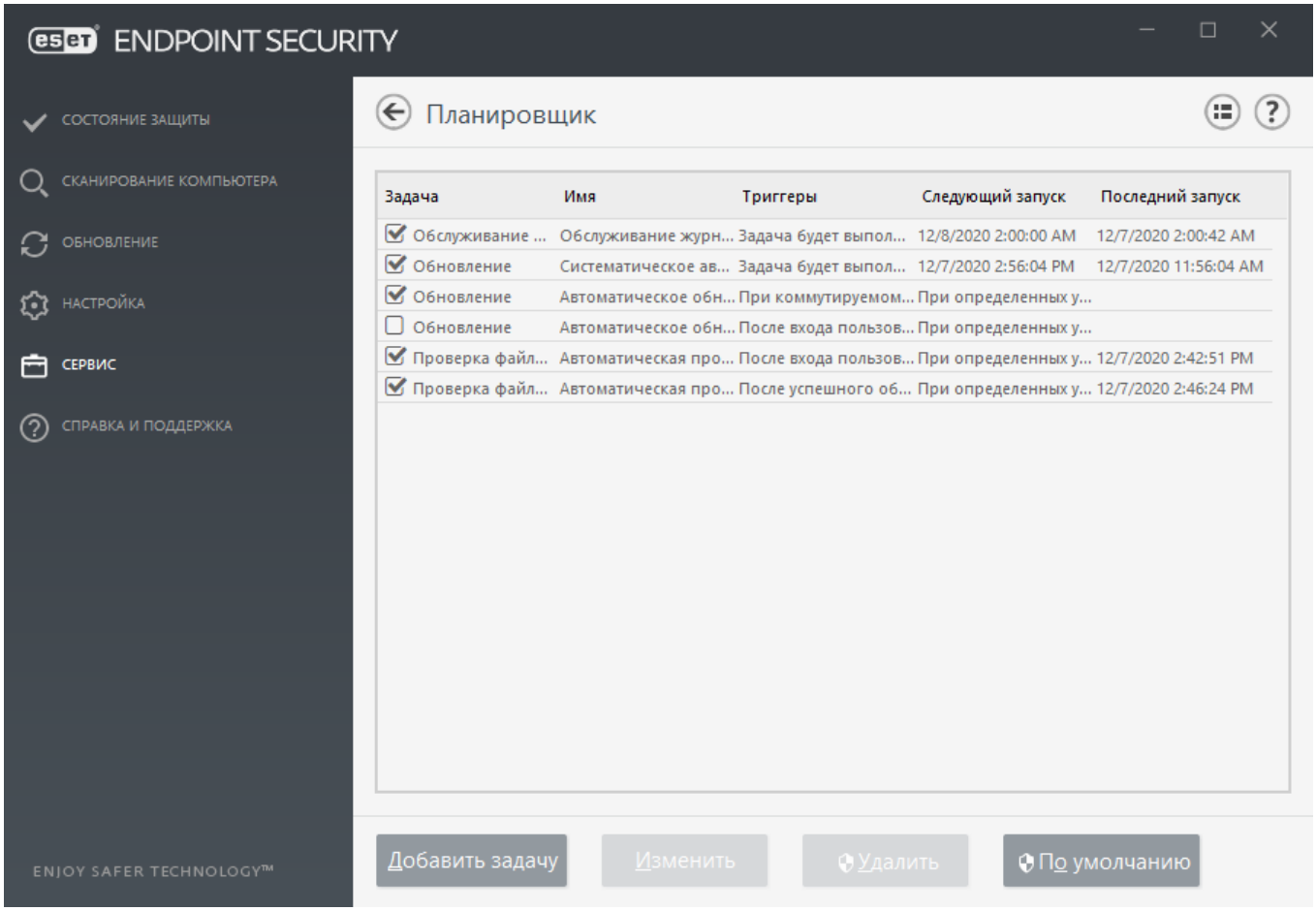
Планировщик предназначен для планирования выполнения следующих задач: обновление

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 снимок состояния компьютера**: создание снимка состояния компьютера в ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого их них.

   • **Сканирование компьютера по требованию**: сканирование файлов и папок на компьютере.

   • **Обновление**: планирование задачи обновления, в рамках которой обновляется модуль обнаружения и программные модули.

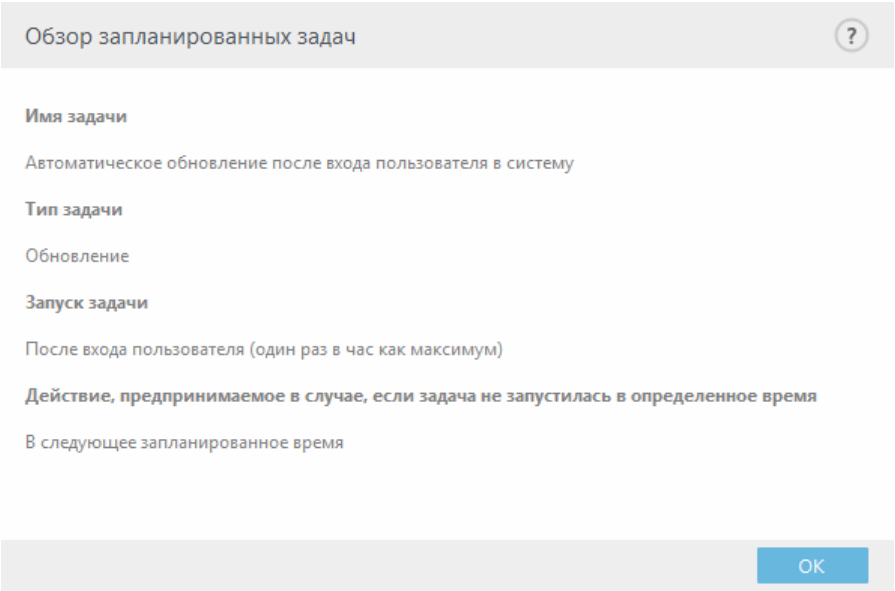
4. Активируйте кнопку **Включено** при необходимости активировать задачу (это можно сделать позже, установив/сняв флажок в списке запланированных задач), нажмите кнопку **Далее** и выберите один из режимов времени выполнения:

- **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.

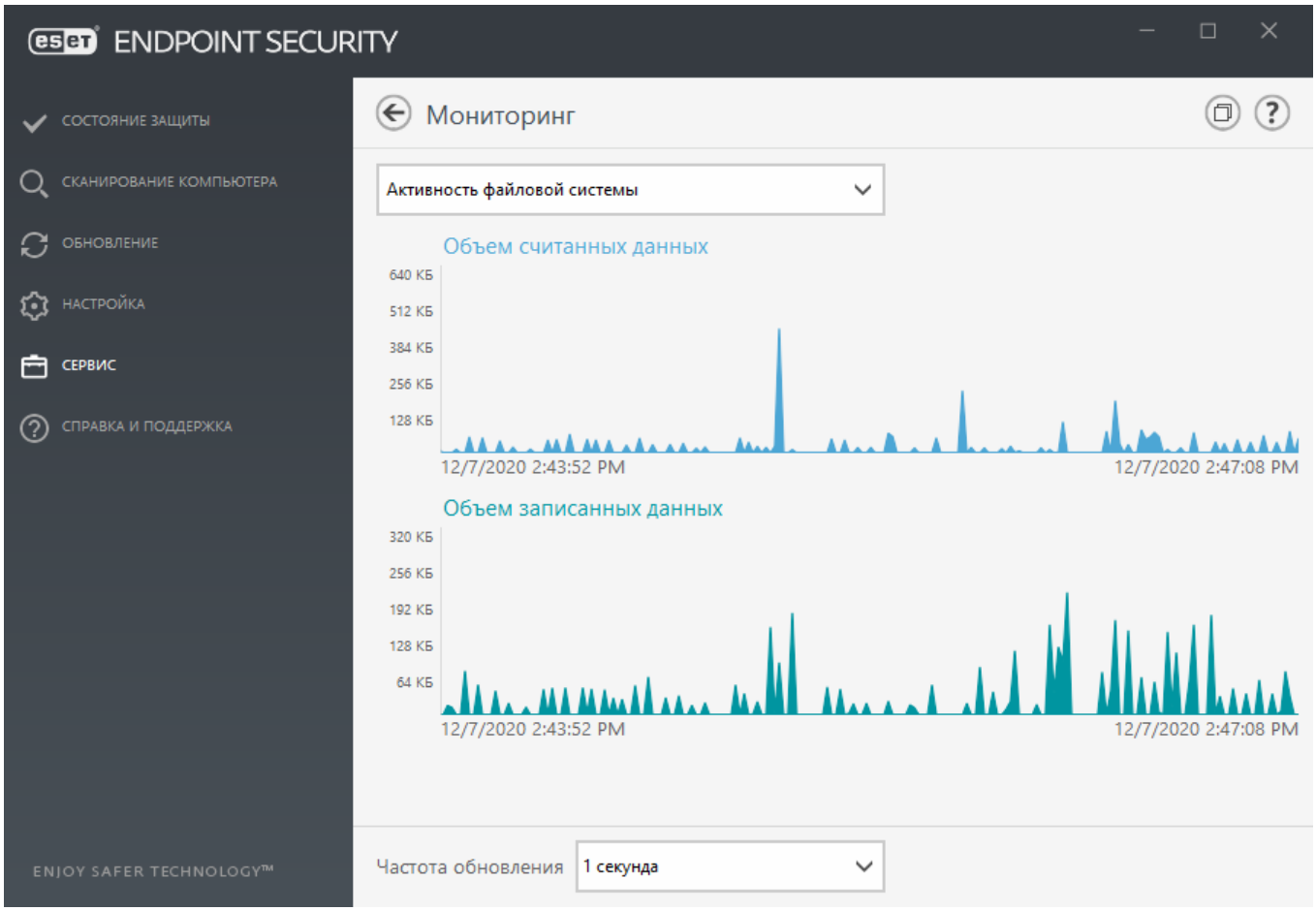
- **В следующее запланированное время**
- **Как можно скорее**
- **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** (интервал можно указать с помощью параметра **Время с момента последнего запуска**).

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



Мониторинг

Чтобы просмотреть текущую **активность файловой системы** в графическом виде, выберите **Служебные программы** > **Мониторинг**. 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 (бирюзовый цвет) данных. Оба значения измеряются в КБ (килобайтах)/МБ/ГБ. Если навести указатель мыши на прочитанные или записанные данные в условных обозначениях под графиком, на нем 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 (бирюзовый цвет) данных.

ESET SysInspector

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

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.

- **Показать**: 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**. Удаление выбранного журнала.
- **Удалить все**: удаление всех журналов.

- **Экспорт**: экспорт журнала в файл или архив в формате XML.

Защита на основе облака

Технология ESET LiveGrid® (основанная на передовой системе своевременного обнаружения ESET ThreatSense.Net) использует данные от пользователей ESET со всего мира и отправляет их в вирусную лабораторию ESET. 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.

Доступны три варианта:

Вариант 1. Включить систему репутации ESET LiveGrid®

Система репутации ESET LiveGrid® основана на белом и черном списке, которые хранятся в облаке.

Проверите репутацию запущенных процессов и файлов непосредственно в интерфейсе программы или в контекстном меню, благодаря чему становится доступна дополнительная информация из ESET LiveGrid®.

Вариант 2. Включить систему обратной связи ESET LiveGrid®

Система обратной связи ESET LiveGrid®, дополняющая систему репутации ESET LiveGrid®, собирает информацию о компьютерах пользователей, 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.

Вариант 3. Не включать ESET LiveGrid®

Функциональность программного обеспечения при этом не ограничивается, но в некоторых случаях ESET Endpoint Security может быстрее реагировать на новые угрозы, чем обновление модулей обнаружения, когда система ESET LiveGrid® включена.

> Дополнительную информацию о ESET LiveGrid® см. в глоссарии.
> См. наши иллюстрированные инструкции на английском и еще нескольких языках по включению и отключению ESET LiveGrid® в ESET Endpoint Security.

Настройка облачной защиты в окне расширенных

параметров

Чтобы получить доступ к параметрам ESET LiveGrid®, нажмите **F5** для перехода в раздел «Расширенные параметры» и разверните **Модуль обнаружения** > «**Облачная защита**».

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.

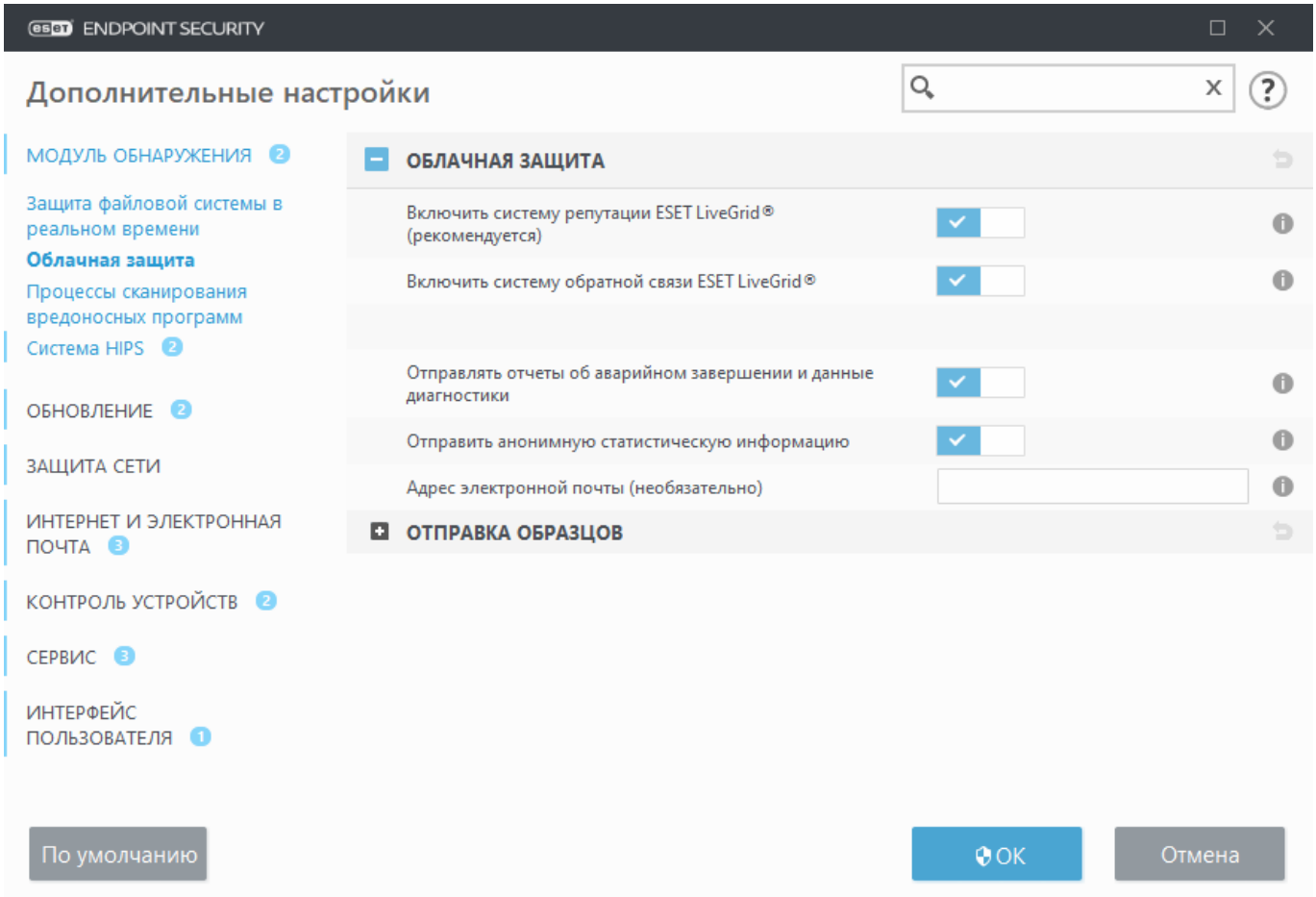
Включение средства ESET LiveGrid® системы отзывов — отправляет соответствующие данные образцов (описанные в разделе **Отправка образцов**) вместе с отчетами о сбоях и статистическими данными в исследовательскую лабораторию ESET для дальнейшего анализа.

Включить ESET Dynamic Threat Defense (не отображается в ESET Endpoint Security). ESET Dynamic Threat Defense — это платная служба, предоставляемая компанией ESET. С ее помощью добавляется уровень защиты, предназначенный специально для уменьшения воздействия от новых видов угроз. Подозрительные файлы автоматически передаются в облако ESET. В облаке они анализируются с помощью наших передовых модулей обнаружения вредоносных программ. Пользователь, который предоставил образец, получит отчет о поведении, содержащий сводные сведения о поведении образца.

Отправлять отчеты об аварийном завершении и данные диагностики: отправка относящихся к ESET LiveGrid® диагностических данных, таких как отчеты об аварийных завершениях и дампы памяти модулей. Рекомендуем не выключать этот параметр, чтобы помочь ESET выявлять проблемы, совершенствовать продукты и улучшать защиту конечных пользователей.

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).

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.



Отправка образцов

Отправка образцов вручную — включение опции отправки образцов в ESET вручную из контекстного меню, карантина или раздела Инструменты > Отправка образца на анализ.

Автоматическая отправка обнаруженных образцов

Укажите, какие образцы будут отправляться в компанию ESET для анализа и совершенствования механизмов обнаружения. Доступны следующие варианты:

- **Все обнаруженные образцы**: все объекты, обнаруженные модулем обнаружения (в том числе потенциально нежелательные приложения, если в настройках модуля сканирования включен соответствующий параметр).
- **Все образцы, кроме документов**: все обнаруженные объекты, кроме **документов** (см. ниже).
- **Не отправлять**: обнаруженные объекты не будут отправляться в компанию ESET.

Автоматическая отправка подозрительных образцов

Эти образцы также будут отправлены в компанию ESET в том случае, если модуль обнаружения их не обнаружит. Например, образцы, которые почти попали под обнаружение, признаны подозрительными одним из модулей защиты ESET Endpoint Security или демонстрируют неоднозначное поведение.

- **Исполняемые файлы**: включает такие файлы, как .exe, .dll, .sys.

- **Архивы**: включает такие типы файлов, как .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

- **Сценарии**: включает такие типы файлов, как .bat, .cmd, .hta, .js, .vbs, .ps1.

- **Другое**: включает такие типы файлов, как .jar, .reg, .msi, .sfw, .lnk.

- **Возможный спам**: эта функция позволяет отправлять потенциальный спам (целиком или частично) и вложения в ESET для анализа. Включив ее, вы поможете точнее обнаруживать спам — для себя и для всего мира.

- **Документы**: включает документы Microsoft Office и PDF с активным содержимым и без него.
  Развернуть список всех включаемых типов файлов документов

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Исключения

Фильтр исключений позволяет исключить из отправки определенные файлы или папки (например, может понадобиться исключить файлы, которые могут содержать конфиденциальную информацию, такую 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.

> ✔ Чтобы исключить файлы, загруженные с адреса download.domain.com, откройте **Расширенные параметры** > **Облачная защита** > **Отправка образцов** > **Исключения** и добавьте исключение .download.domain.com.

ESET Dynamic Threat Defense

Чтобы включить службу ESET Dynamic Threat Defense на клиентском компьютере с помощью веб-консоли ESET PROTECT, воспользуйтесь информацией в разделе Настройка EDTD для ESET Endpoint Security.

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.

Фильтр «Исключение» для защиты на

основе облака

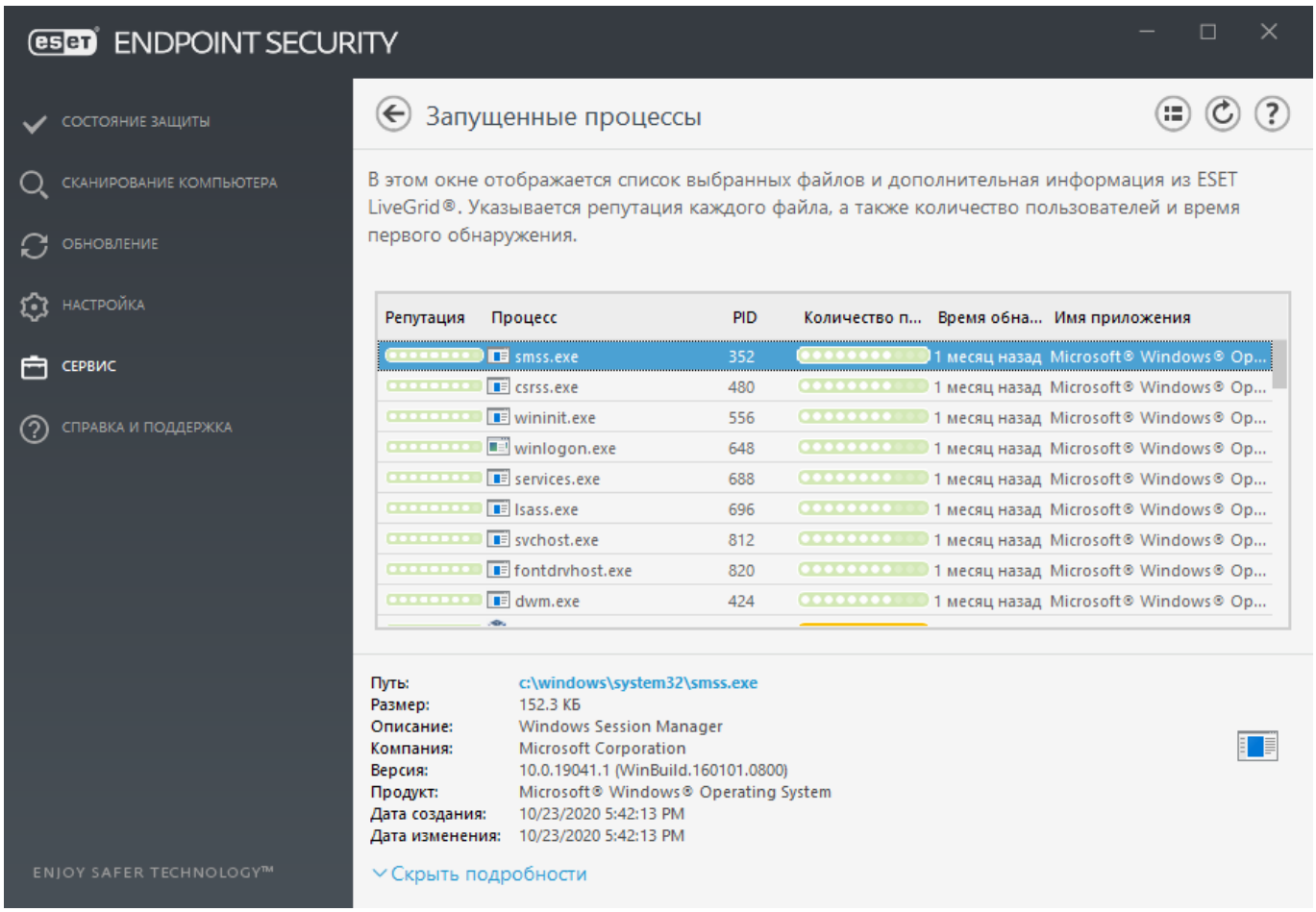
Фильтр «Исключение» позволяет исключить из отправки образцов определенные файлы или папки. Перечисленные в этом списке файлы никогда не будут передаваться в ESET на анализ, даже если они содержат подозрительный код. Файлы распространенных типов (DOC и т. п.) исключаются по умолчанию.

> С помощью этой функции можно исключить файлы, в которых может присутствовать конфиденциальная информация, например документы и электронные таблицы.

> Чтобы исключить файлы, загруженные с адреса download.domain.com, откройте **Расширенные параметры** > **Облачная защита** > **Отправка образцов** > **Исключения** и добавьте исключение .download.domain.com.

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®.



Репутация. В большинстве случаев ESET Endpoint Security и технология ESET LiveGrid® определяют для объектов (файлов, процессов, разделов 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 репутации: от 9 — наилучшая репутация (зеленый), до 0 — наихудшая репутация (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.

> Известные приложения, помеченные зеленым, 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®.

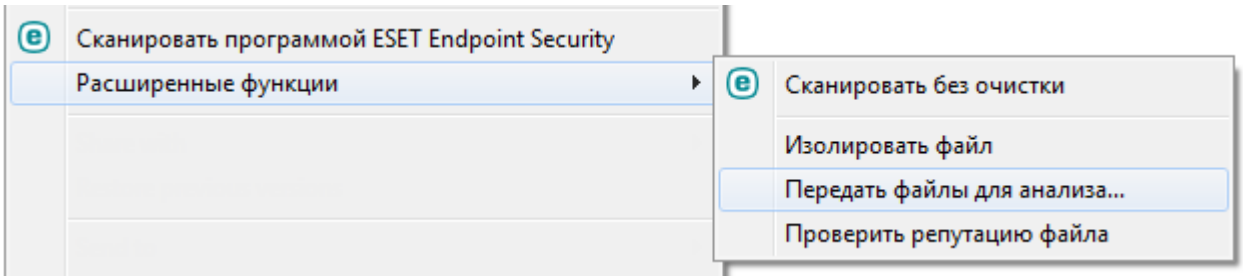
> Если для приложения выбран уровень безопасности Неизвестно (оранжевый), оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в безопасности файла, воспользуйтесь функцией отправки на анализ, чтобы отправить файл в вирусную лабораторию ESET. Если 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.

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®**.



Отчет по безопасности

Эта функция позволяет получить обзор статистики для следующих категорий:

Заблокированные веб-страницы: отображает количество заблокированных веб-страниц (URL-адрес внесен в «черный» список потенциально нежелательных приложений, фишинговый сайт, взломанный маршрутизатор, IP-адрес или сертификат).

Обнаружены зараженные объекты электронной почты: отображается количество обнаруженных зараженных объектов электронной почты.

Веб-страницы, заблокированные в контроле доступа в Интернет: отображается количество заблокированных веб-страниц в Контроле доступа в интернет.

Обнаружено потенциально нежелательное приложение: отображается количество потенциально нежелательных приложений.

Обнаружен спам в электронной почте: отображается количество обнаруженного спама в электронной почте.

Проверка документов выполнена: отображается количество просканированных объектов документов.

Просканировано приложений. Отображается количество просканированных исполняемых объектов.

Просканировано других объектов. Отображается количество других просканированных объектов.

Просканировано объектов на веб-страницах. Отображается количество просканированных объектов на веб-страницах.

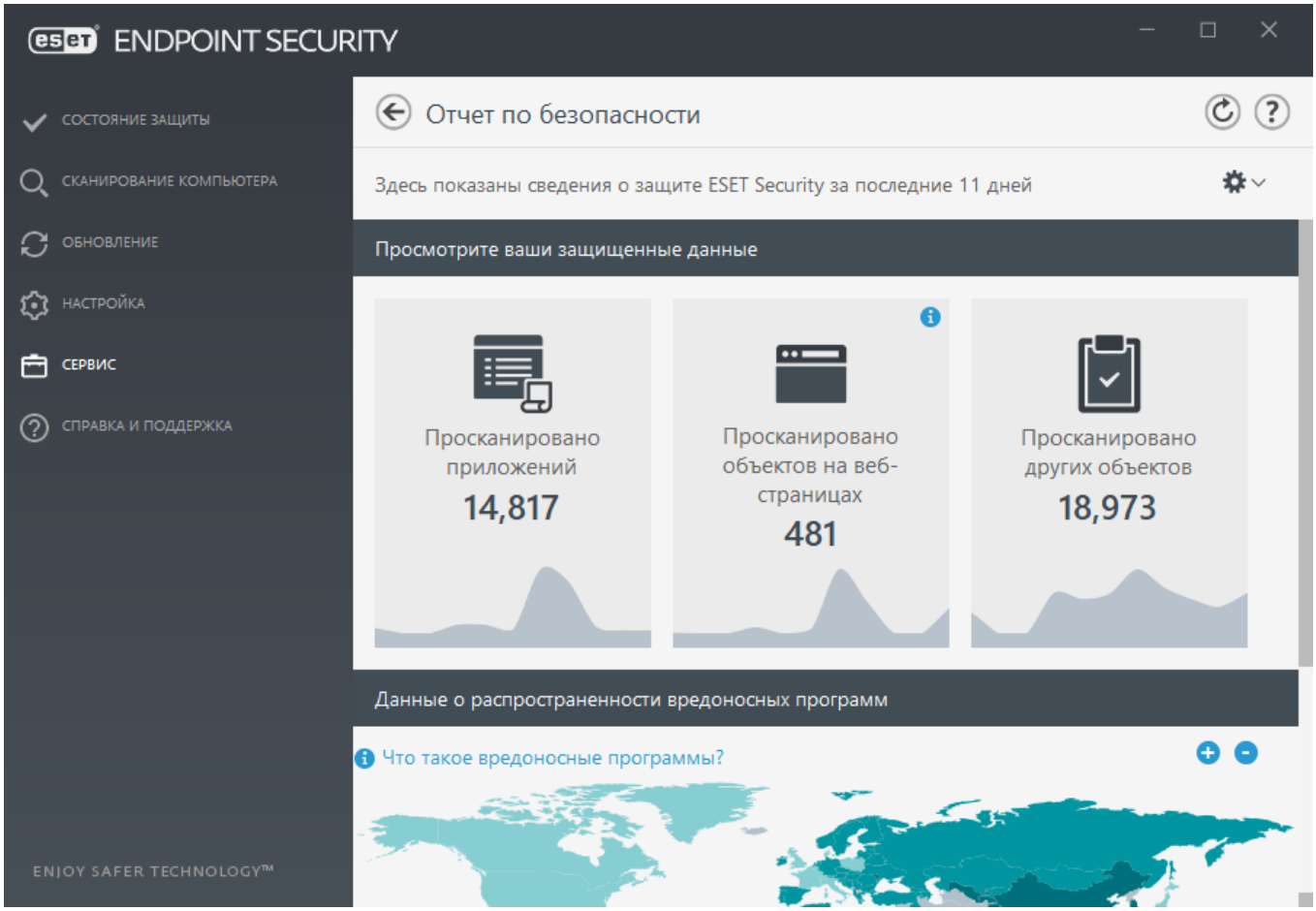
Просканировано объектов электронной почты: отображается количество просканированных объектов электронной почты.

Порядок расположения этих категорий определяется их числовыми значениями — от большего к меньшему. Категории с нулевыми значениями не отображаются. Щелкните "**Больше**", чтобы

развернуть и отобразить скрытые категории.

Под категориями показана карта с фактической ситуацией с вирусами в мире. Наличие вирусов в каждой стране обозначено с помощью цвета: чем темнее цвет, тем больше вирусов. Страны, по которым нет данных, показаны серым цветом. Если навести указатель мыши на страну, отобразятся данные о ней. Можно выбрать определенный континент, чтобы автоматически увеличить масштаб.

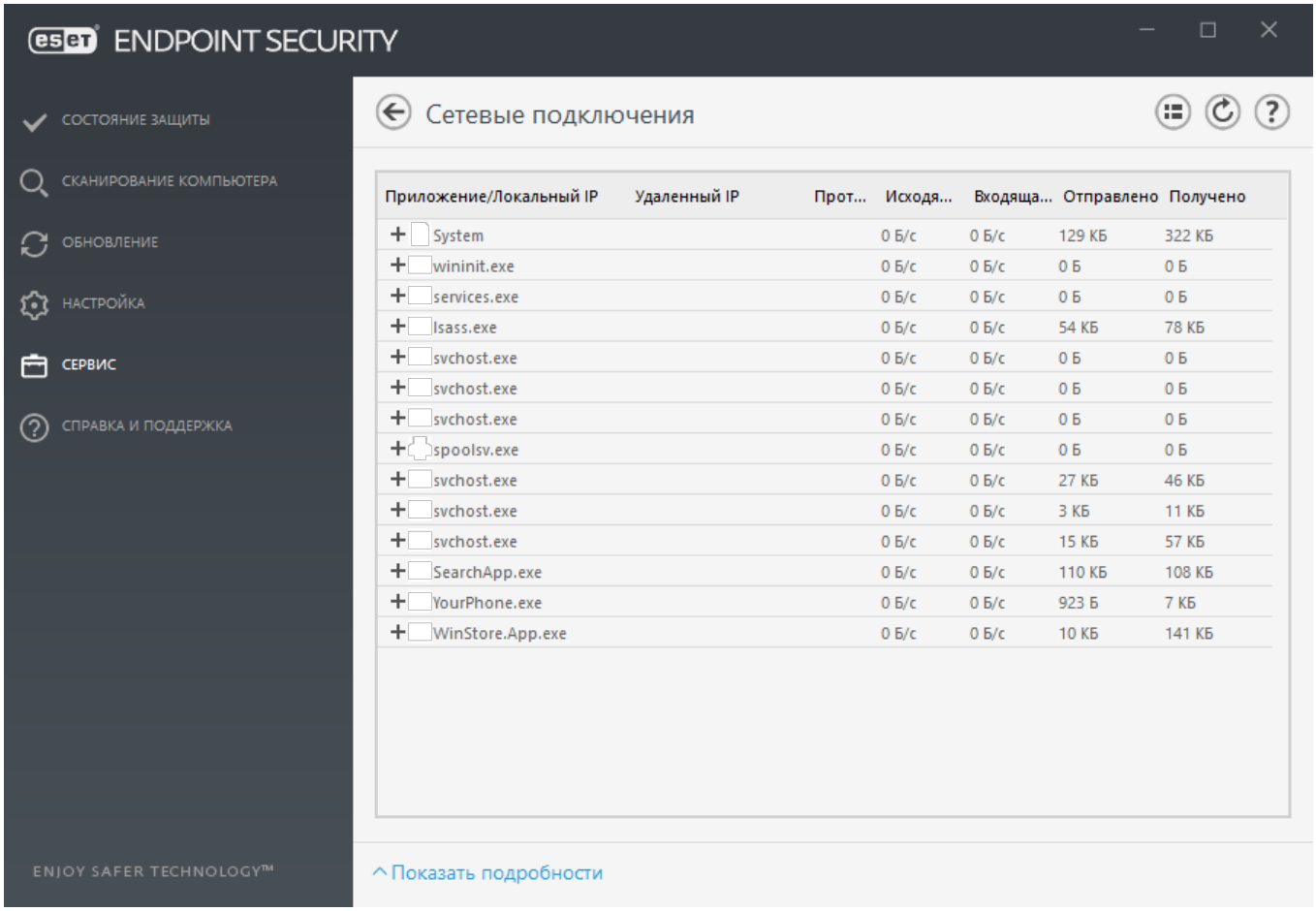
В правом верхнем углу щелкните значок шестеренки ⚙, чтобы **включить или выключить уведомления отчета по безопасности** или выбрать, за какой период нужно отобразить данные: за последние 30 дней или с момента активации продукта. Если установка ESET Endpoint Security выполнялась меньше 30 дней назад, вы сможете выбрать только количество дней с момента установки. По умолчанию выбран период 30 дней.



Элемент **Сбросить данные** позволяет очистить статистику и удалить существующие данные отчета по безопасности. Это действие нужно подтвердить, если только флажок **Запрашивать подтверждение перед сбросом статистики** не снят в меню **Расширенные параметры** > **Интерфейс** > **Предупреждения и окна сообщений** > **Подтверждения**.

Сетевые подключения

В разделе «Сетевые подключения» отображается список активных и отложенных соединений. Это позволяет управлять всеми приложениями, которые устанавливают исходящие соединения.



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 файервол использует предопределенное 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 файервол использует предопределенное правило. Описание параметров см. в разделе Правила и зоны.

ESET SysRescue Live

ESET SysRescue Live — это бесплатная служебная программа, которая позволяет создать загрузочный восстановительный CD/DVD- или USB-диск. Вы можете запустить зараженный компьютер с помощью такого носителя, просканировать его на наличие вредоносных программ и очистить зараженные файлы.

Основное преимущество служебной программы ESET SysRescue Live заключается в том, что она выполняется независимо от основной операционной системы, но имеет прямой доступ к диску и файловой системе. Это позволяет удалять угрозы, которые в обычных условиях устранить невозможно (например, при запущенной операционной системе и т. д.).

- Онлайн-справка по ESET SysRescue Live

Отправка образцов на анализ

При обнаружении подозрительного файла на компьютере или подозрительного сайта в Интернете его можно отправить на анализ в исследовательскую лабораторию ESET (может быть недоступно в зависимости от конфигурации ESET LiveGrid®).

Вы можете отправлять только образцы, которые соответствуют по крайней мере одному из следующих критериев:
• Программа ESET не обнаруживает образец.
• Образец ошибочно обнаруживается как угроза.
• Мы не принимаем личные файлы (которые вы хотите просканировать на наличие вредоносных программ с помощью ESET) в качестве образцов (вирусная лаборатория ESET не проводит сканирование по запросу пользователей).
• В теме письма должна быть описана проблема, а текст должен содержать как можно более полную информацию о файле (например, снимок экрана или адрес веб-сайта, с которого он был загружен).

Вы можете отправить образец файла или сайта в ESET для анализа одним из следующих способов.

1. С помощью диалогового окна отправки образца в разделе **Сервис** > **Отправка образца на анализ**.

2. Файл также можно отправить по электронной почте. Если этот способ для вас удобнее, заархивируйте файлы с помощью WinRAR/ZIP, защитите архив паролем «infected» и отправьте его по адресу samples@eset.com.

3. Чтобы сообщить о спаме, ложном обнаружении спама или неправильной категоризации веб-сайтов модулем «Контроль доступа в интернет», см. эту статью базы знаний ESET.

Откройте раздел **Выбрать образец для анализа** и 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. Этот адрес отправляется в ESET вместе с подозрительными файлами и может использоваться для запроса дополнительной информации, необходимой для анализа. Указывать адрес электронной почты необязательно. Чтобы не указывать его, выберите **Отправить анонимно**.

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.
Если образец окажется вредоносным приложением или веб-сайтом, его обнаружение будет добавлено при следующем обновлении программы ESET.

Выбор образца для анализа — подозрительный файл

Обнаруженные признаки и симптомы заражения вредоносной программой: введите описание поведения подозрительного файла на вашем компьютере.

Источник файла (URL-адрес или поставщик): укажите источник файла и опишите, как он попал на ваш компьютер.

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут идентифицировать подозрительный файл.

> ℹ Хотя только первый параметр (**Обнаруженные признаки и симптомы заражения вредоносной программой**) является обязательным, дополнительная информация также помогает идентифицировать образцы в лаборатории.

Выбор образца для анализа — подозрительный сайт

В раскрывающемся меню **Проблема с сайтом** выберите одно из следующих значений.

- **Зараженный**: веб-сайт содержит вирусы или другие вредоносные программы, которые распространяются различными способами.
- **Фишинг**: часто используется для получения доступа к конфиденциальным сведениям, таким как номера банковских счетов, PIN-коды и т. п. Дополнительную информацию об этом типе атаки см. в глоссарии.
- **Мошеннический**: мошеннический веб-сайт, созданный для быстрого получения прибыли.
- Выберите **Другое**, если вышеуказанные параметры не соответствуют сайту, который вы собираетесь отправить.

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут проанализировать подозрительный сайт.

Выбор образца для анализа — ложно обнаруженный файл

Мы просим отправлять файлы, которые обнаруживаются как зараженные, но при этом не являются таковыми, чтобы мы могли улучшить наш модуль защиты от вирусов и шпионских программ и обеспечить защиту другим пользователям. Ложное обнаружение возможно, когда шаблон файла совпадает с таким же шаблоном, присутствующим в модуле обнаружения.

Имя и версия приложения: имя программы и ее версия (например, номер, псевдоним или

кодовое название).

Источник файла (URL-адрес или поставщик): укажите источник файла и опишите, как он попал на ваш компьютер.

Цель приложения: это общее описание приложения, его типа (например, браузер, проигрыватель мультимедиа и т. п.) и функциональности.

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут в обработке подозрительного файла.

> i Первые три параметра нужно указать, чтобы идентифицировать нормальные приложения и отличить их от вредоносного кода. Предоставление дополнительной информации в значительной степени помогает лаборатории в процессе идентификации и обработки образцов.

Выбор образца для анализа — ложно обнаруженный сайт

Мы просим отправлять нам сведения о сайтах, которые определены как зараженные, мошеннические или фишинговые, но таковыми не являются. Ложное обнаружение возможно, когда шаблон файла совпадает с таким же шаблоном, присутствующим в модуле обнаружения. Отправьте нам сведения об этом веб-сайте, чтобы мы могли улучшить наш модуль защиты от вирусов и фишинга и обеспечить защиту других пользователей.

Примечания и дополнительная информация: здесь можно ввести дополнительную информацию или описание, которые помогут в обработке подозрительного веб-сайта.

Выбор образца для анализа — другое

Этот вариант следует использовать, если файл невозможно отнести к категории **Подозрительный файл** или **Ложное срабатывание**.

Причина отправки файла: введите подробное описание и причину отправки файла.

Оповещения

Чтобы настроить способ сообщения о событиях в ESET Endpoint Security, перейдите в раздел **Расширенные параметры** (F5) > **Сервис** > **Уведомления**. В этом окне можно настроить следующие типы уведомлений:

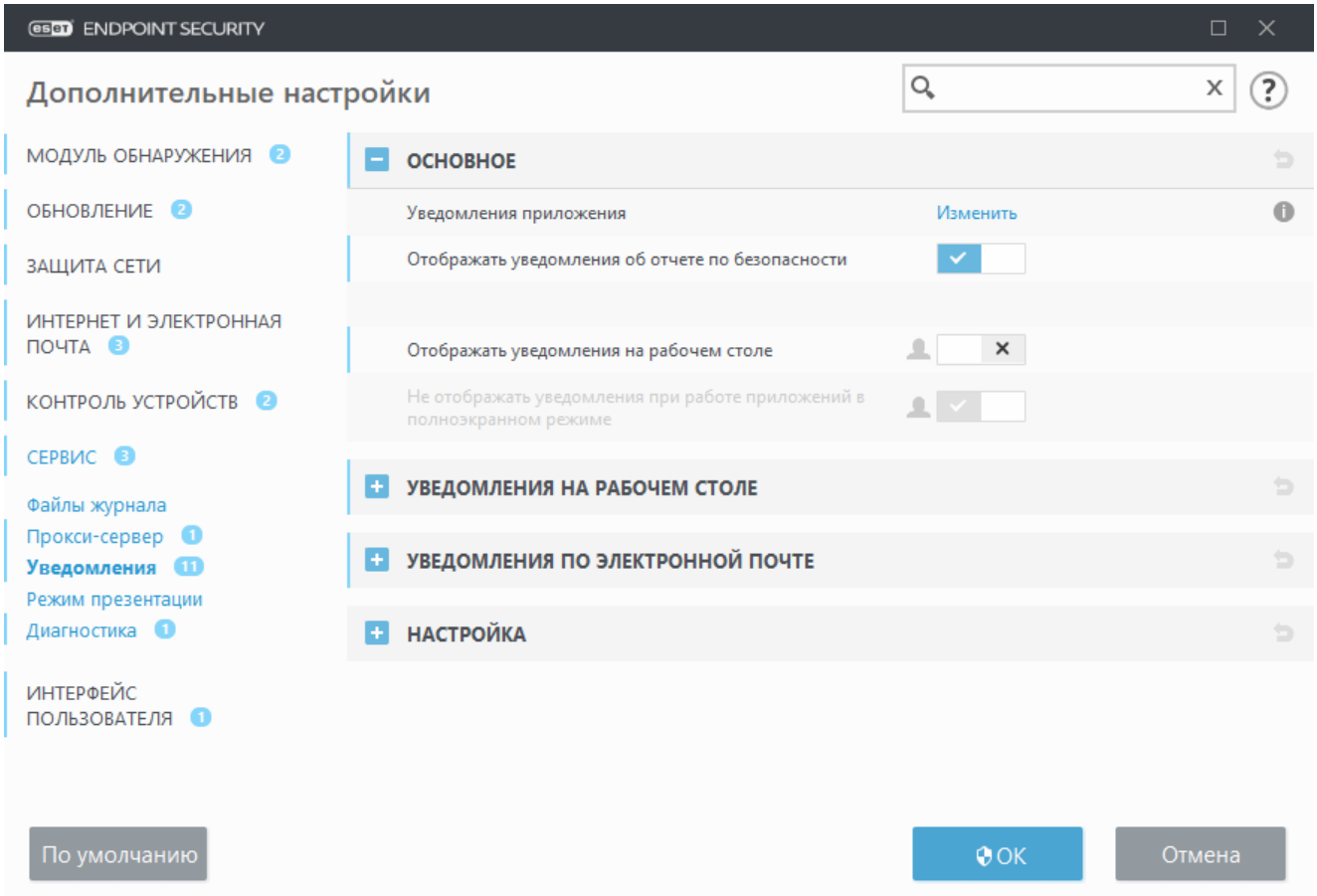
- **Уведомления приложения**: отображать непосредственно в главном окне программы.
- **Уведомления на рабочем столе**: уведомление на рабочем столе отображается в виде небольшого всплывающего окна возле панели задач.
- **Уведомления по электронной почте**: уведомления отправляются на указанный адрес электронной почты.

• **Настройка уведомлений**: добавьте произвольное сообщение к, например, уведомлению на рабочем столе.

В разделе **Основная информация** используйте соответствующие переключатели для настройки нижеприведенных параметров.

Переключатель	По умолчанию	Описание
Отображать уведомления на рабочем столе	✓	Если отключить этот параметр, всплывающие уведомления возле панели задач будут скрыты. Рекомендуем не выключать этот параметр, чтобы продукт мог сообщать вам о событиях.
Не отображать уведомления при...	✓	Оставьте параметр **Не отображать уведомления при работе приложений в полноэкранном режиме** включенным, чтобы скрывать все неинтерактивные уведомления.
Отображать уведомления об отчете по безопасности	×	Включите, чтобы получать уведомление при создании новой версии отчета по безопасности (такая возможность доступна, только если управление не осуществляется с помощью ESET Security Management Center).
Отображать уведомление об успешном обновлении	×	Включите, чтобы получить уведомление при обновлении продуктом своих компонентов и модулей обнаружения.
Отправлять уведомления о событиях по электронной почте	×	Включите, чтобы активировать уведомления по электронной почте.

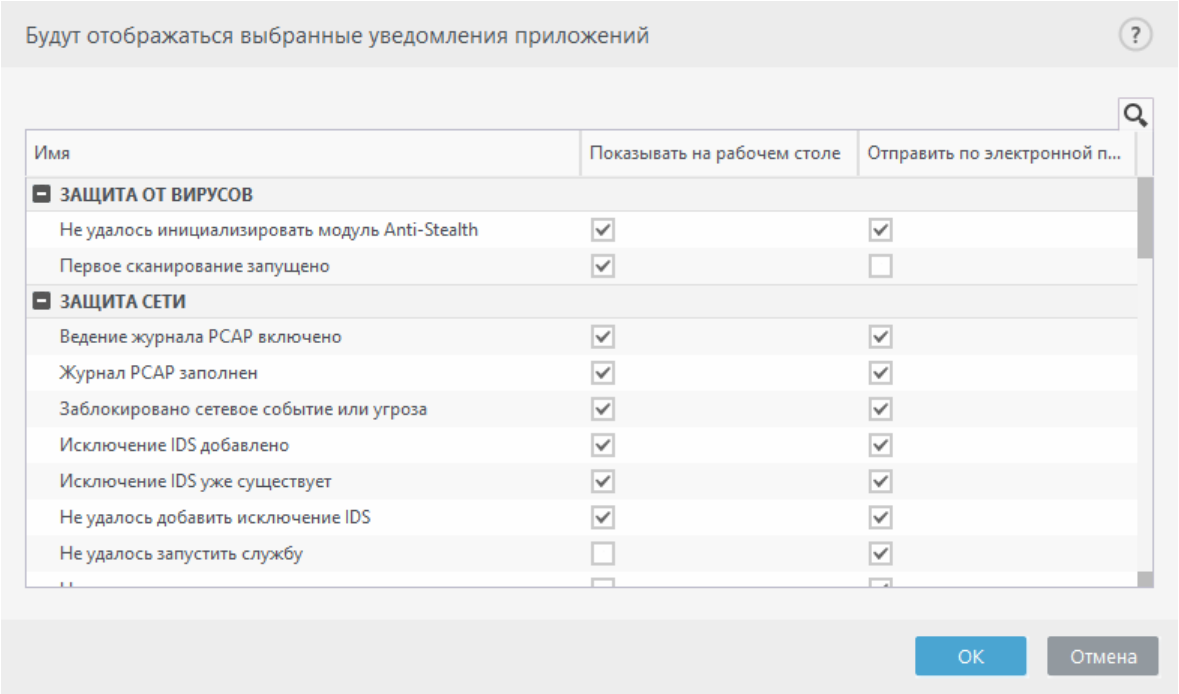
Чтобы включить или отключить определенные уведомления приложения, щелкните элемент **Изменить** рядом с элементом **Уведомления приложения**.



Уведомления приложения

Чтобы изменить видимость уведомлений приложения (отображаются в нижнем правом углу экрана), перейдите в раздел **Сервис** > **Уведомления** > **Основная информация** > **Уведомления приложения** в дереве «Расширенные параметры» ESET Endpoint Security.

Список уведомлений делится на три столбца. В первом столбце имена уведомлений сортируются по категориям. Чтобы изменить то, как продукт уведомляет о новых событиях в приложении, установите флажки в соответствующих столбцах **Показывать на рабочем столе** и **Отправить по электронной почте**.



Чтобы задать общие параметры для уведомлений на рабочем столе (например, время отображения сообщения или минимальную детализацию отображаемых событий), см. Уведомления на рабочем столе в разделе **Расширенные параметры** > **Сервис** > **Уведомления**.

Чтобы задать формат сообщения электронной почты и настроить параметры сервера SMTP, см. Уведомления по электронной почте в разделе **Расширенные параметры** > **Сервис** > **Уведомления**.

> Если вы хотите настроить уведомления **Файл проанализирован** и **Файл не проанализирован** при использовании ESET Dynamic Threat Defense, для параметра Проактивная защита нужно задать значение **Заблокировать исполнение до получения результата анализа**.

Уведомления на рабочем столе

Уведомление на рабочем столе отображается в виде небольшого всплывающего окна возле панели задач. По умолчанию оно отображается в течение 10 секунд, затем медленно исчезает. Это основной способ, с помощью которого программа ESET Endpoint Security сообщает пользователю об обновлении программы, подключении новых устройств, завершении задач сканирования на наличие вирусов и об обнаружении новых угроз.

В разделе **Уведомления на рабочем столе** можно настроить работу всплывающих уведомлений. Можно задать следующие атрибуты.

Продолжительность: время, в течение которого отображается уведомление. Значение должно быть в диапазоне от 3 до 30 секунд.

Прозрачность: прозрачность уведомления в процентах. Поддерживается диапазон от 0 (нет прозрачности) до 80 (очень высокая прозрачность).

Минимальная детализация отображаемых событий: в раскрывающемся меню можно

выбрать начальный уровень серьезности уведомлений, которые следует отображать:

- **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 Antistealth работает неправильно).

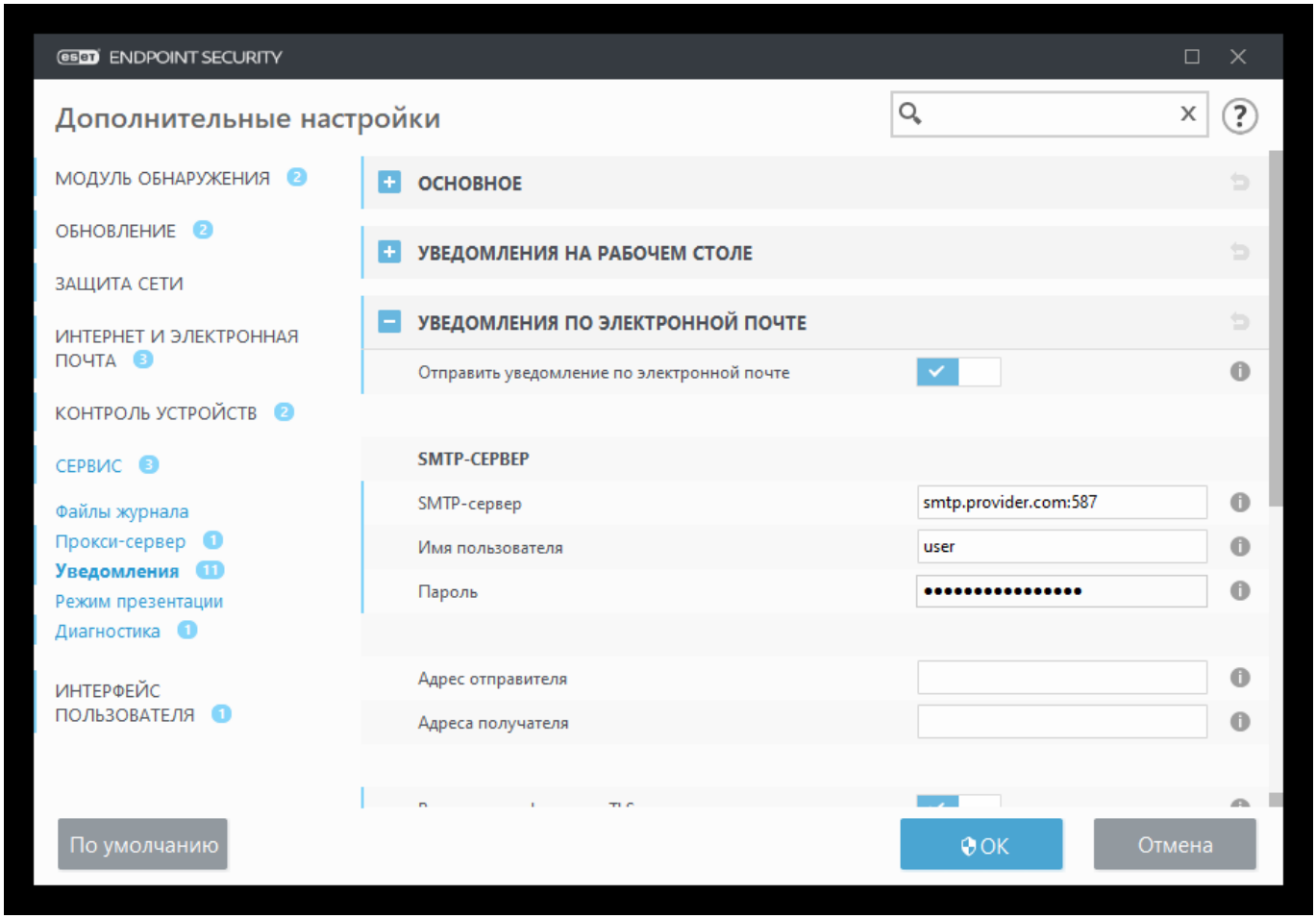
- **Ошибки**: записываются ошибки (не активирована защита документов) и критические ошибки.

- **Критические ошибки**: записываются только критические ошибки (ошибки запуска защиты от вирусов или уведомления о наличии вируса в системе).

В многопользовательских системах отображать уведомления на экране следующего пользователя: введите полные имена учетных записей пользователей, которым нужно разрешить получать уведомления на рабочем столе. Например, если для работы на компьютере вы используете учетную запись, отличную от учетной записи администратора, но хотите получать информацию о новых событиях продукта.

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** в разделе **Основная информация**.



SMTP-сервер

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

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 (;).

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

Настройки электронной почты

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 Antistealth 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).

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.

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.

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 угрозе 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: преобразование сообщения электронной почты в кодировку символов ANSI, основанную на региональных настройках Windows (например, windows-1250, Unicode (UTF-8), ACSII 7-bit, или японский (ISO-2022-JP)). В результате, "á" будет изменен на "a", а неизвестный символ на "?".

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.

• **%TimeStamp%** — дата и время события.

• **%Scanner%** — задействованный модуль.

- **%ComputerName%** — имя компьютера, на котором появилось оповещение.
- **%ProgramName%** — программа, создавшая оповещение.
- **%InfectedObject%** — имя зараженного файла, сообщения и т. п.
- **%VirusName%** — идентифицирующие данные заражения.
- **%Action%** — действие, предпринимаемое в случае заражения.
- **%ErrorDescription%** — описание события, не имеющего отношения к вирусам.

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

Настройка уведомлений

В этом окне можно настроить, какая информация содержится в оповещениях.

Текст оповещения по умолчанию: текст, который по умолчанию отображается в нижней части уведомления.

Угрозы

Чтобы оповещения о вредоносных программах оставались на экране, пока их не закроют вручную, установите флажок **Не закрывать автоматически оповещения о вредоносных программах**.

Чтобы воспользоваться текстом, отличным от текста по умолчанию, отключите параметр **Использовать текст по умолчанию** и в поле **Текст оповещения об угрозе** введите собственный текст.

Карантин

Главная функция карантина — безопасное хранение обнаруженных объектов (например, вредоносных программ, зараженных файлов или потенциально нежелательных приложений).

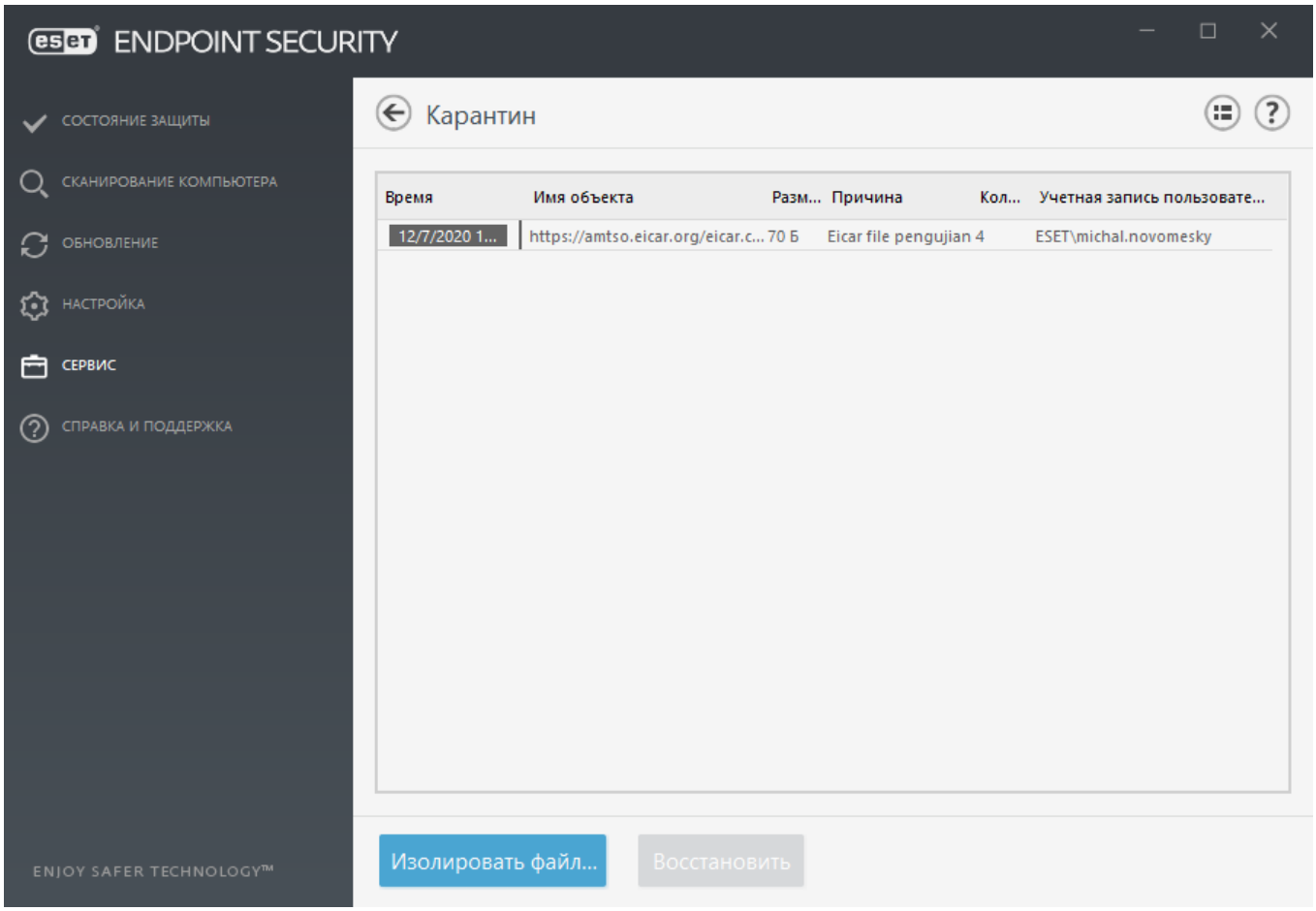
Карантин можно открыть из главного окна программы ESET Endpoint Security, щелкнув элемент **Сервис** > **Карантин**.

Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, содержащей такие сведения:

- дату и время помещения файла на карантин;
- путь к исходному расположению файла;
- его размер в байтах;
- причину помещения файла на карантин (например, объект добавлен пользователем);

• количество обнаружений (например, повторяющиеся обнаружения одного и того же файла или архив, содержащий несколько заражений).

- Я управляю карантином на клиентских рабочих станциях удаленно



Помещение файлов на карантин

Программа ESET Endpoint Security автоматически помещает удаленные файлы на карантин (если пользователь не отключил эту функцию в окне предупреждения).

Дополнительные файлы следует помещать на карантин, если:

a.их нельзя вылечить;

b.их нельзя безопасно удалить;

c.они отнесены программой ESET Endpoint Security к зараженным по ошибке;

d.файл с подозрительной активностью, но не определяется модулем сканирования.

Чтобы поместить файл на карантин, можно использовать несколько приведенных ниже вариантов.

a.Используйте функцию перетаскивания, чтобы вручную отправить файл на карантин. Для этого щелкните файл, переместите указатель мыши в отмеченную область, удерживая нажатой кнопку мыши, после чего отпустите кнопку мыши. После этого приложение перейдет на передний план.

b.Щелкните **Переместить в карантин** в главном окне программы.

c.Для этого также можно воспользоваться контекстным меню, нажав правой кнопкой мыши в окне **Карантин** и выбрав пункт **Карантин**

Восстановление из карантина

Файлы, помещенные на карантин, можно также восстановить в исходное расположение.

• Для этого щелните правой кнопкой мыши файл, помещенный на карантин, и в контекстном меню нажмите кнопку **Восстановить**.

• Если файл помечен как потенциально нежелательное приложение, параметр **Восстановить и исключить из сканирования** включен. См. также Исключения.

• Контекстное меню содержит также функцию **Восстановить в**, которая позволяет восстановить файл в расположение, отличное от исходного.

• Функция восстановления недоступна в некоторых случаях, например, для файлов, расположенных в сетевой папке, доступной только для чтения.

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 выбрать и удалить несколько элементов одновременно. Удаленные элементы безвозвратно удаляются с вашего устройства и из карантина.

Отправка файла из карантина

Если на карантин помещен файл, который не распознан программой, или файл неверно квалифицирован как зараженный (например, в результате ошибки эвристического метода кода) и изолирован, передайте образец в исследовательскую лабораторию ESET для проведения анализа. Чтобы отправить файл, щелкните его правой кнопкой мыши и в контекстном меню выберите пункт **Передать на анализ**.

> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> • Управление карантином в ESET PROTECT (8.x)
> • Продукт ESET уведомил меня об обнаружении. Что мне делать?

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.

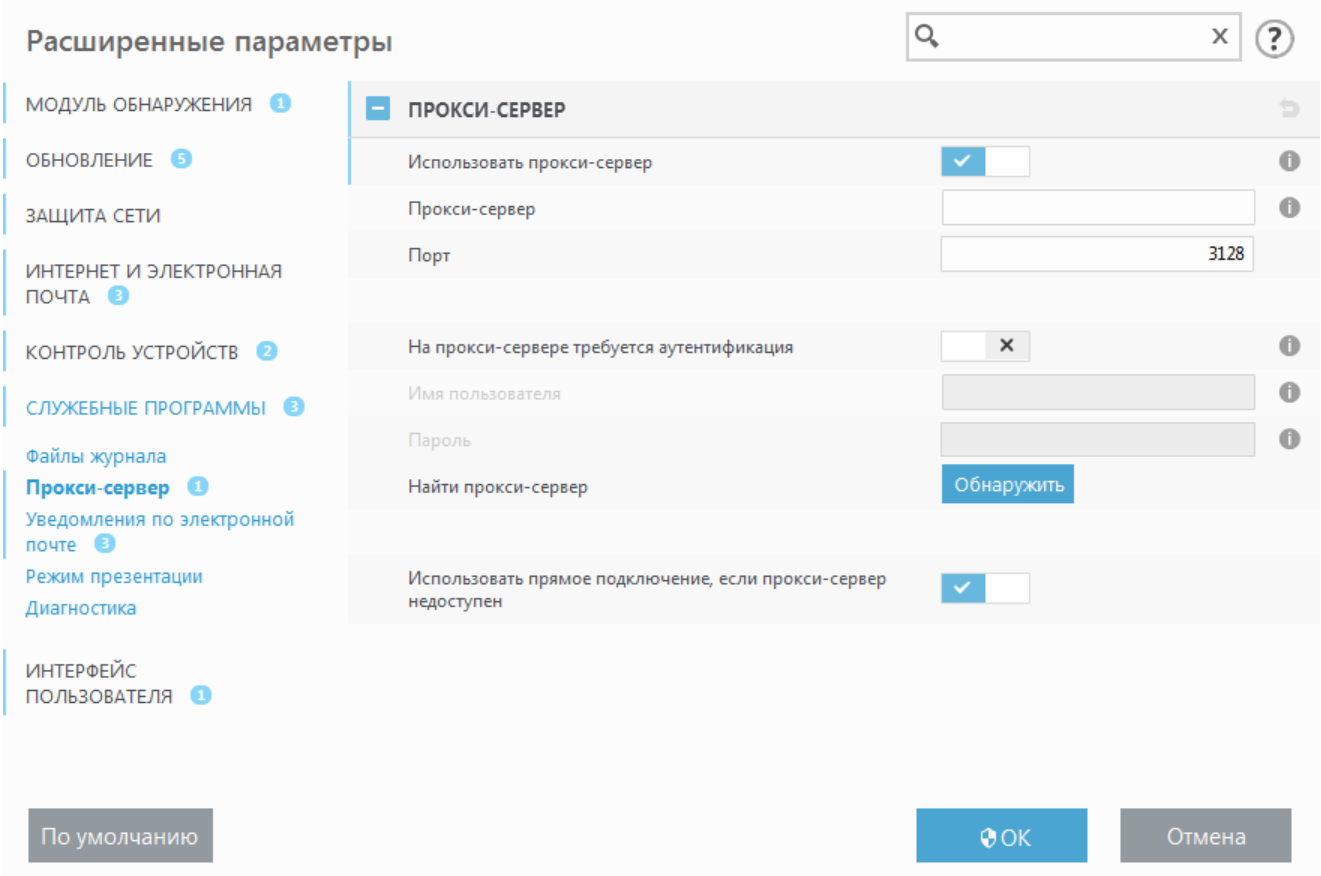
Для настройки параметров прокси-сервера на этом уровне установите флажок **Использовать прокси-сервер**, а затем введите адрес прокси-сервера в поле **Прокси-сервер**, а также укажите номер его **порта** в соответствующем поле.

Если для обмена данными с прокси-сервером требуется аутентификация, установите флажок **Прокси-сервер требует аутентификации**, а затем заполните поля **Имя пользователя** и **Пароль**. Нажмите кнопку **Найти прокси-сервер**, чтобы автоматически определить параметры прокси-сервера и подставить их. Будут скопированы параметры подключения к Интернету, указанные в Internet Explorer или Google Chrome.

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

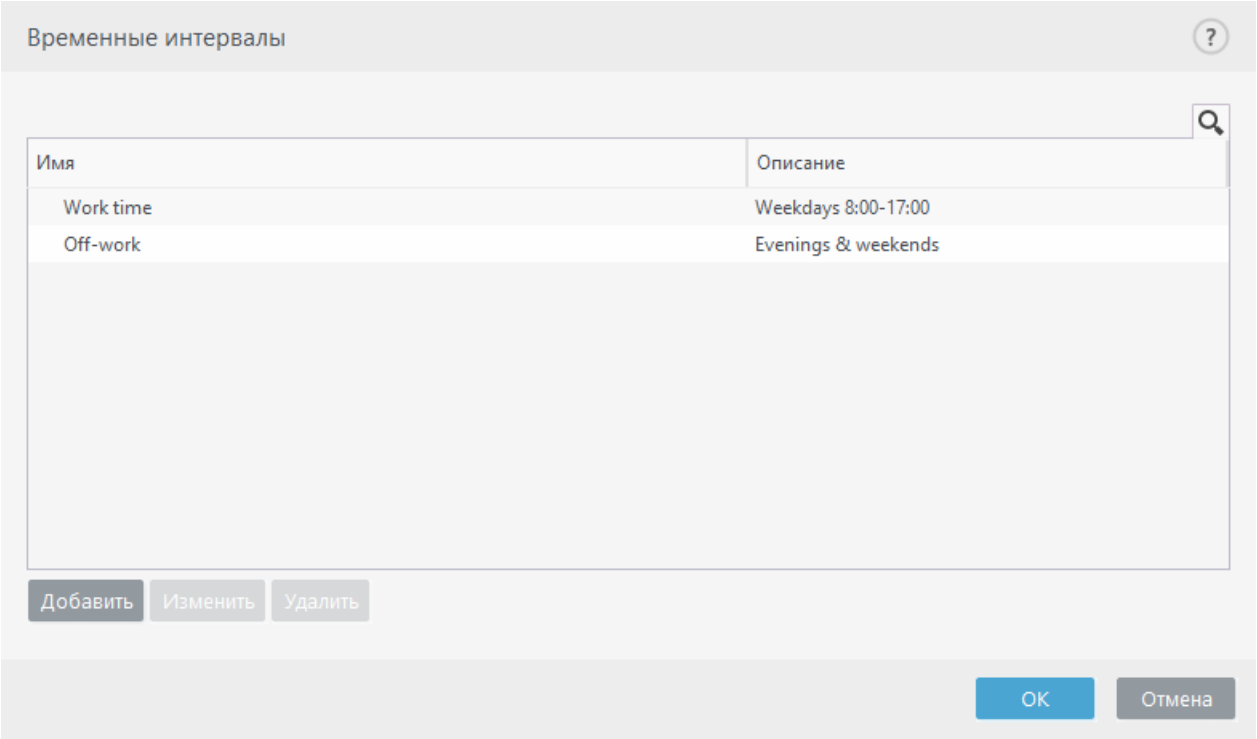
Использовать прямое подключение, если прокси-сервер недоступен: если в ESET Endpoint Security настроено подключение через прокси-сервер, а он недоступен, ESET Endpoint Security будет обходить прокси-сервер и подключаться к серверам ESET напрямую.

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.



Временные интервалы

Можно создавать временные интервалы, а затем назначать правила для **Контроля устройств** и **контроля доступа в Интернет**. Параметр **Временные интервалы** можно найти, если перейти в раздел **Расширенные параметры** > **Инструменты**. Это дает возможность определить часто используемые временные интервалы (например, время работы, выходные и другое) и легко использовать их без переопределения диапазонов времени для каждого правила. Временной интервал применим к любому правилу соответствующего типа, который поддерживает управление по времени.



Чтобы создать временной интервал, выполните следующие действия:

1. Щелкните **Изменить** > **Добавить**.
2. Введите имя и **описание** временного интервала и нажмите **Добавить**.
3. Укажите день и время начала и окончания для временного интервала или выберите **Весь день**.
4. Нажмите **OK**, чтобы подтвердить.

Один временной интервал может быть определен с одним или несколькими диапазонами времени с учетом дня и времени суток. Когда временной интервал будет создан, он будет отображаться в раскрывающемся меню **Применять во время** в окне редактора правил для контроля устройств или в окне редактора правил для контроля доступа в Интернет.

Центр обновления Microsoft Windows®

Функция обновления Windows является важной составляющей защиты пользователей от вредоносных программ. По этой причине обновления Microsoft Windows следует устанавливать

сразу после их появления. Программное обеспечение ESET 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 **OK**. После проверки статуса сервера обновлений на экран будет выведено окно «Обновления системы», поэтому данные об обновлении системы могут быть недоступны непосредственно после сохранения изменений.

Проверка лицензии с интервалом

Программе ESET Endpoint Security необходимо подключаться к серверам ESET автоматически. Чтобы изменить этот параметр, перейдите в раздел **Расширенные параметры (F5)** > **Сервис** > **Лицензия**. По умолчанию для параметра **Проверка с интервалом** установлено значение **Автоматически**, и сервер лицензий ESET проверяет продукт несколько раз в час. Если сетевой трафик станет слишком большим, измените значение на **Ограничено**, чтобы уменьшить нагрузку. Если выбрано значение **Ограничено**, ESET Endpoint Security связывается с сервером лицензий только раз в сутки или после перезагрузки компьютера.

> Если для параметра **Проверка с интервалом** установлено значение **Ограничено**, на применение в параметрах ESET Endpoint Security связанных с лицензией изменений, внесенных с помощью ESET Business Account/ESET MSP Administrator, может уйти до одного дня.

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 Окна предупреждений и сообщений и Уведомления можно изменить поведение предупреждений об обнаружениях и системных уведомлений. 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.

См. также раздел Как свернуть ESET Endpoint Security интерфейс (полезен для управляемых сред).

Элементы интерфейса пользователя

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 запущен, но отображаются только уведомления.

Вручную. Графический интерфейс пользователя не запускается автоматически после входа. Любой пользователь может запустить его вручную.

Скрытый. Ни уведомления, ни предупреждения не отображаются. Графический интерфейс может запустить только администратор. Этот режим может быть полезным в управляемых средах или ситуациях, когда нужно экономить ресурсы системы.

> 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 Security Management Center, применив соответствующую политика.

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: возможность интеграции элементов управления ESET Endpoint Security в контекстное меню.

Состояния

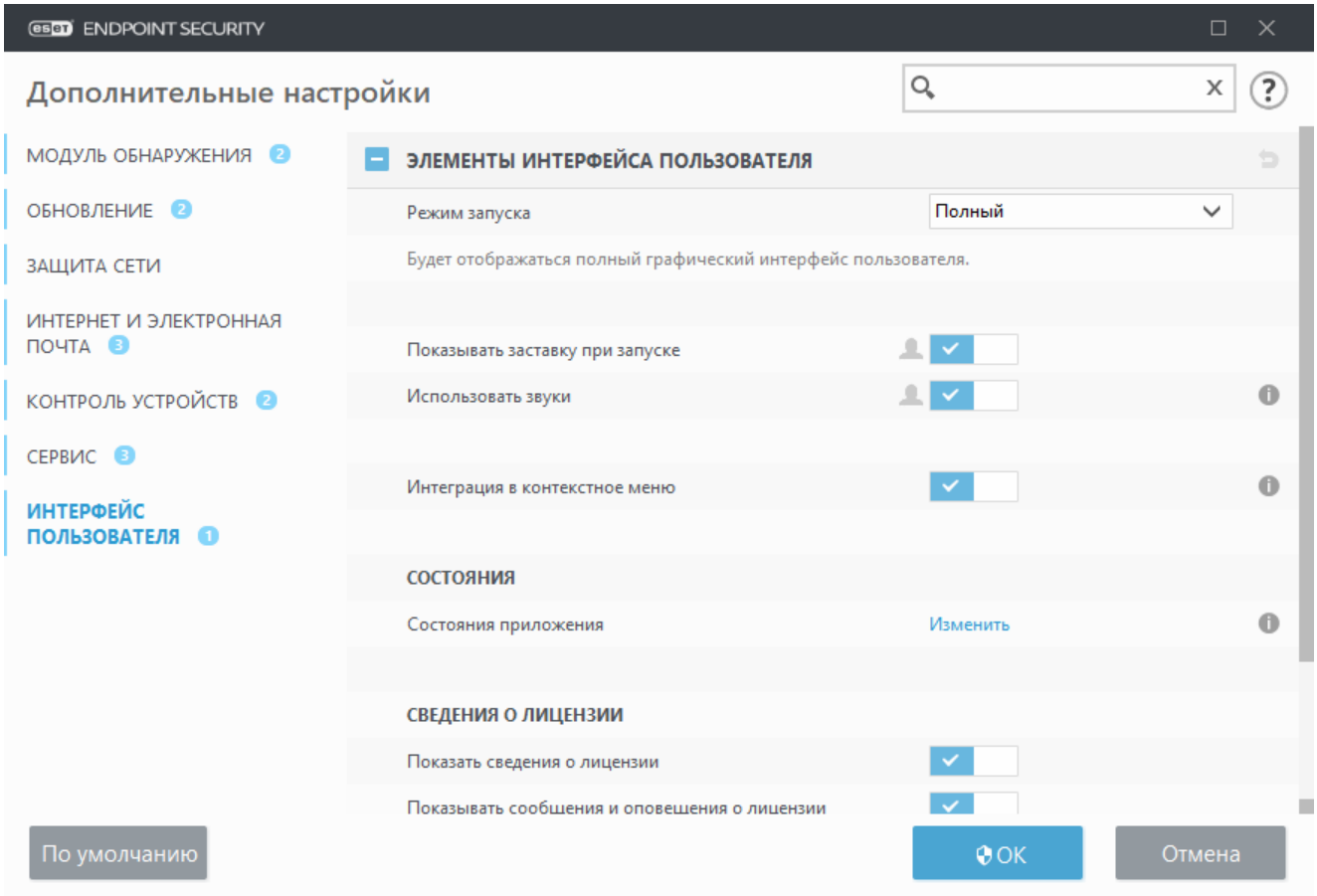
Состояния приложения. Чтобы включить или выключить отображение состояний в области главного меню **Состояние защиты**, щелкните элемент **Изменить**.

Информация о лицензии

Показать сведения о лицензии. Если этот параметр отключен, дата истечения срока действия лицензии не будет отображаться в окнах **Состояние защиты** и **Справка и поддержка**.

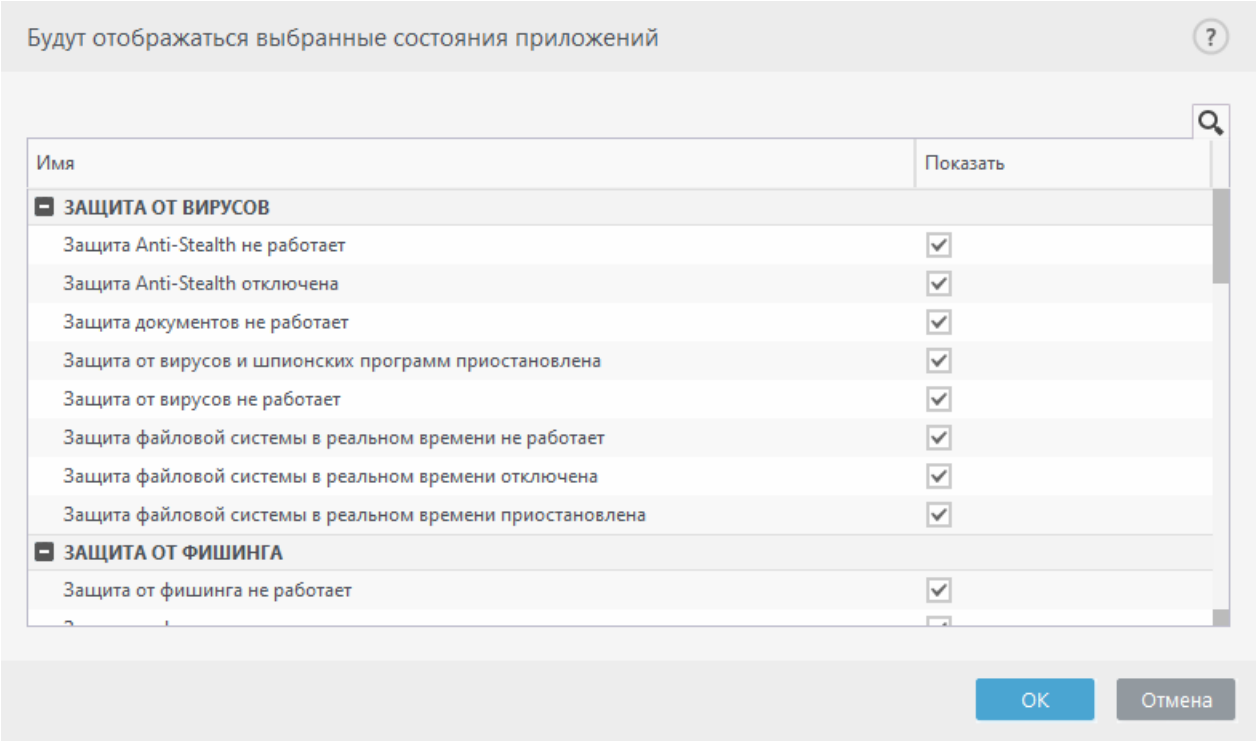
Показывать сообщения и оповещения о лицензии: если этот параметр отключен, уведомления и сообщения будут отображаться только по истечении срока действия лицензии.

> Настройки сведений о лицензии применяются, но являются недоступными, если продукт ESET Endpoint Security активирован с помощью лицензии MSP.



Состояния приложения

Чтобы настроить состояния приложения на первой панели ESET Endpoint Security, перейдите в раздел **Интерфейс** > **Элементы интерфейса** > **Состояния приложения** в дереве «Расширенные параметры» ESET Endpoint Security.



Включение или отключение отображения состояния для приложений. Например, при временном отключении защиты от вирусов и шпионских программ или при включении режима презентации. Кроме того, состояние приложения будет отображаться, если продукт не активирован или срок действия лицензии истек. Эту настройку можно изменить с помощью политикESET Security Management Center .

Настройка доступа

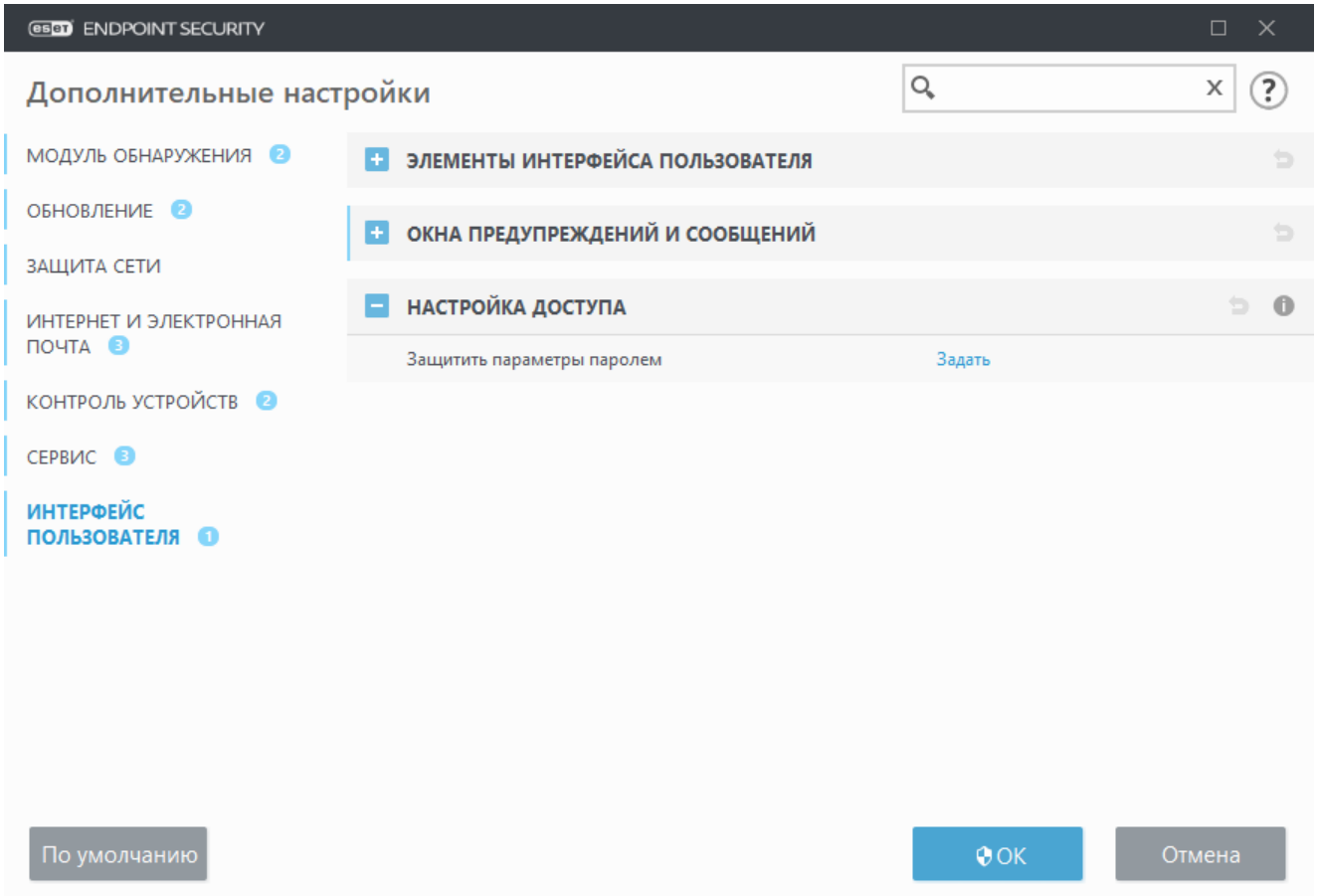
Для обеспечения максимальной безопасности системы важно правильно настроить ESET Endpoint Security. Неквалифицированное изменение параметров может привести к потере важных данных. Во избежание несанкционированного изменения параметры ESET Endpoint Security можно защитить паролем.

Управляемые среды

Администратор может создать политику защиты параметров паролем для ESET Endpoint Security на подключенных клиентских компьютерах. Указания по созданию новой политики см. в разделе Защищенные паролем параметры.

Неуправляемый

Настройки парольной защиты можно найти в меню **Расширенные параметры** (**F5**) в разделе **Интерфейс** > **Настройка доступа**.



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

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

Пароль для доступа к расширенным параметрам

Для защиты параметров настройки ESET Endpoint Security от несанкционированного изменения необходимо установить новый пароль.

Управляемые среды

Администратор может создать политику защиты параметров паролем для ESET Endpoint Security на подключенных клиентских компьютерах. Указания по созданию новой политики см. в разделе Защищенные паролем параметры.

Неуправляемый

Если нужно изменить существующий пароль, выполните следующие действия.

1. Введите старый пароль в поле **Старый пароль**.
2. Введите новый пароль в поля **Новый пароль** и **Подтвердите пароль**.

3. Нажмите кнопку **OK**.

Теперь для внесения каких-либо изменений в ESET Endpoint Security нужно будет указать этот пароль.

Если вы забудете пароль, доступ к дополнительным параметрам можно восстановить.

- Восстановление с помощью метода «Восстановить пароль» (версия 7.1 и более поздние версии)
- Восстановление с помощью средства разблокировки ESET (версия 7.0 и более поздние версии)

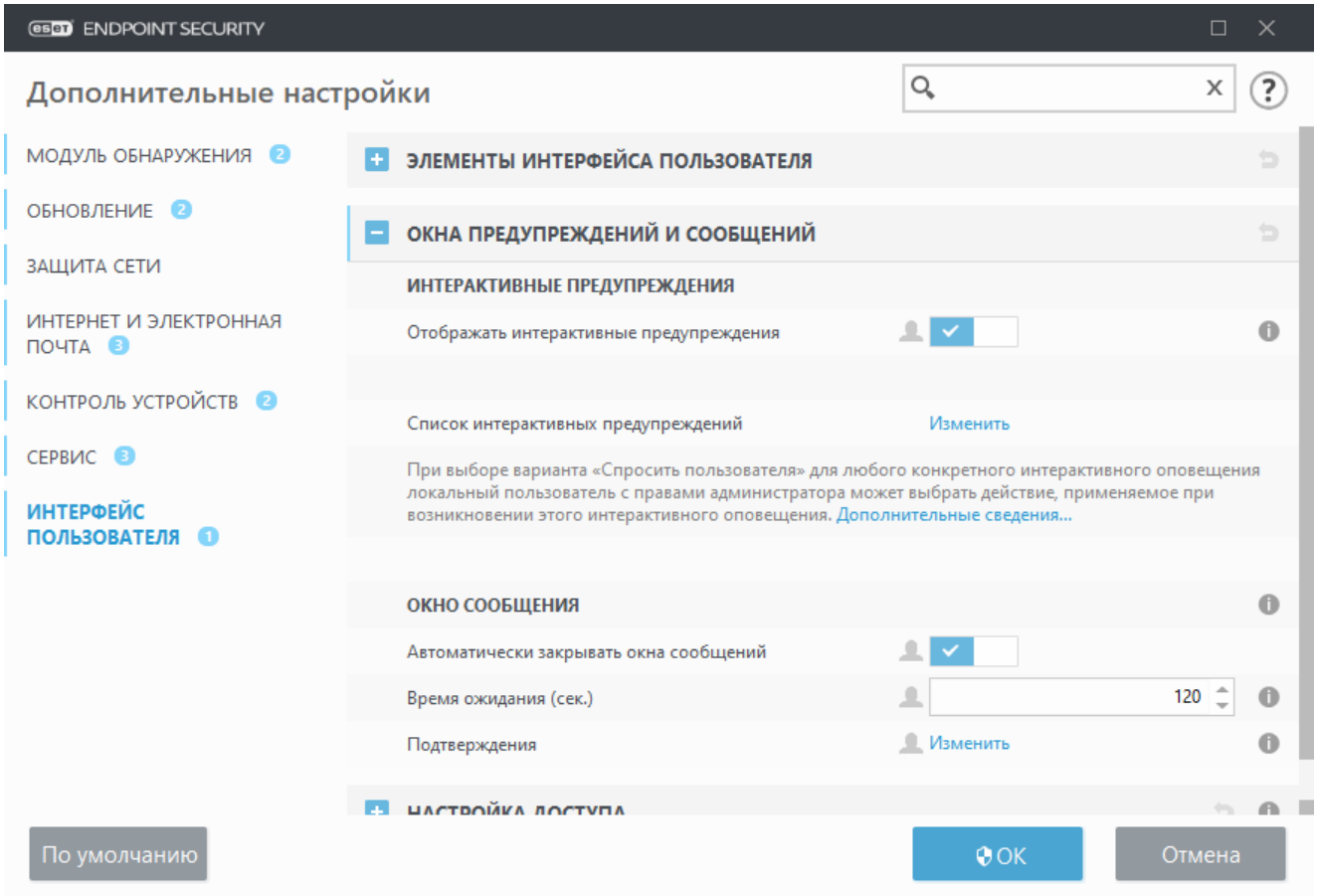
Щелкните здесь, если забыли лицензионный ключ, выданный ESET, дату окончания срока действия своей лицензии или другую информацию о лицензии на ESET Endpoint Security.

Окна предупреждений и сообщений

Нужны сведения о распространенных предупреждениях и уведомлениях?

- Угроза найдена
- Адрес заблокирован
- Программа не активирована
- Доступно обновление
- Данные обновления не согласованы
- Устранение ошибки «Обновление модулей не выполнено»
- «Файл поврежден» или «Не удалось переименовать файл»
- Сертификат веб-сайта отозван
- Сетевая угроза заблокирована

Раздел **Окна предупреждений и сообщений** в разделе **Пользовательский интерфейс** позволяет конфигурировать способ обработки обнаружений ESET Endpoint Security, при которых требуется принятие решения пользователем (например, потенциальные поддельные веб-сайты).



Интерактивные предупреждения

Окна интерактивных предупреждений отображаются при новом обнаружении или если требуется вмешательство пользователя.

Отображать интерактивные предупреждения

ESET Endpoint Security версия 7.2 и более поздние версии:

- Для неуправляемых пользователей мы рекомендуем оставить эту опцию по умолчанию (включенной).
- Для управляемых пользователей, оставьте этот параметр включенным и выберите заранее определенные действия для пользователей в Список интерактивных предупреждений.

Отключение функции **Отображать интерактивные предупреждения** приведет к скрытию всех окон предупреждений и диалоговых окон браузера. Предопределенное действие по умолчанию будет выбрано автоматически (например, "потенциальный поддельный веб-сайт" будет заблокирован).

ESET Endpoint Security версия 7.1 и более ранние версии:

Этот параметр имеет название **Отображать предупреждения**. Настроить заранее определенные действия для определенных окон интерактивных предупреждений невозможно.

Уведомления на рабочем столе

Уведомления на рабочем столе и всплывающие подсказки предназначены только для информирования и не требуют участия пользователя. Раздел **Уведомления на рабочем столе** был перемещен в раздел «Расширенные параметры» > **Сервис** > **Уведомления** (версия 7.1 и более поздние версии).

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.

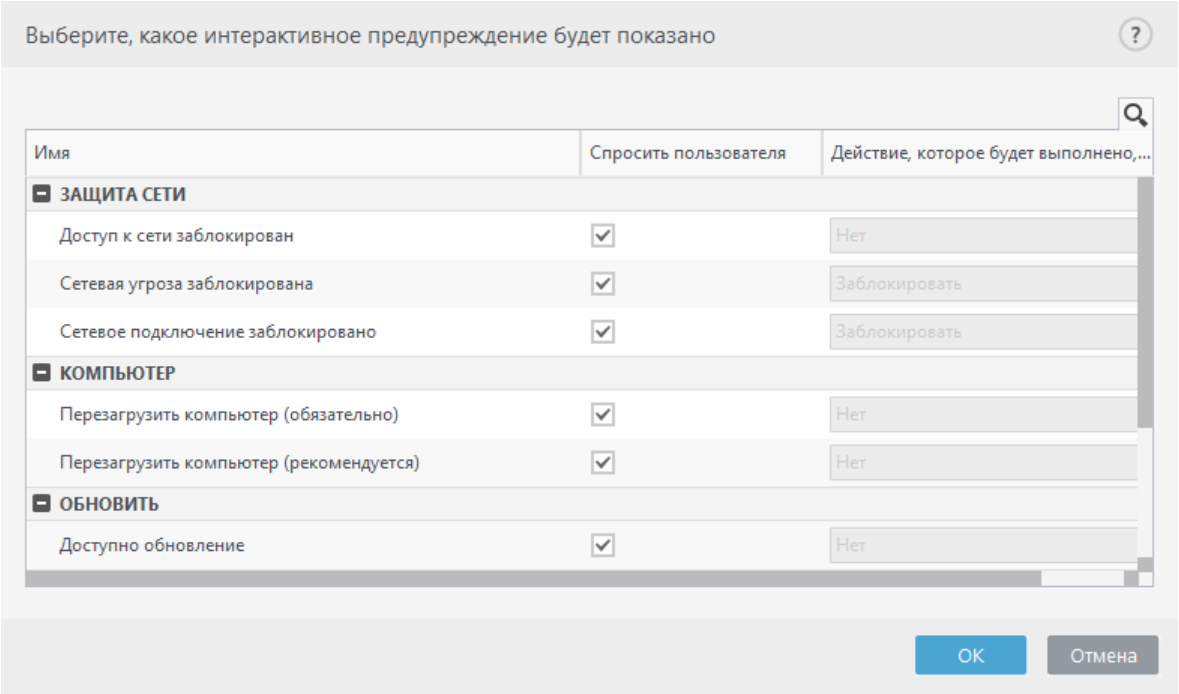
Подтверждения: отображение списка подтверждений, для которых можно настроить параметры отображения.

Интерактивные предупреждения

В данном разделе описаны несколько окон интерактивных предупреждений, которые ESET Endpoint Security будут отображаться перед выполнением каких-либо действий.

Чтобы настроить поведение для настраиваемых интерактивных предупреждений, перейдите по ссылке **Интерфейс** > **Окна предупреждений и сообщений** > **Список интерактивных предупреждений** ESET Endpoint Security Расширенное дерево настроек и щелкните **Изменить**.

> Полезно для управляемых сред, где администратор может отменить выбор **Спросить пользователя** и выбрать заранее определенное действие, применяемое при отображении окон интерактивных предупреждений.
> См. также состояния приложения продукта.



Дополнительные сведения о конкретном окне интерактивного предупреждения см. в следующих разделах справки:

Съемные носители

- Обнаружено новое устройство

Защищенный браузер

- Разрешить продолжение в браузере по умолчанию

Защита сети

- Доступ к сети заблокировано отображается при запуске клиентской задачи **Изолирование компьютера от сети** этой рабочей станции из ESET PROTECT.
- Сетевое подключение заблокировано
- Сетевая угроза заблокирована

Предупреждения веб-браузера

- Обнаружено потенциально нежелательное содержимое
- Веб-сайт заблокирован из-за фишинга

Компьютер

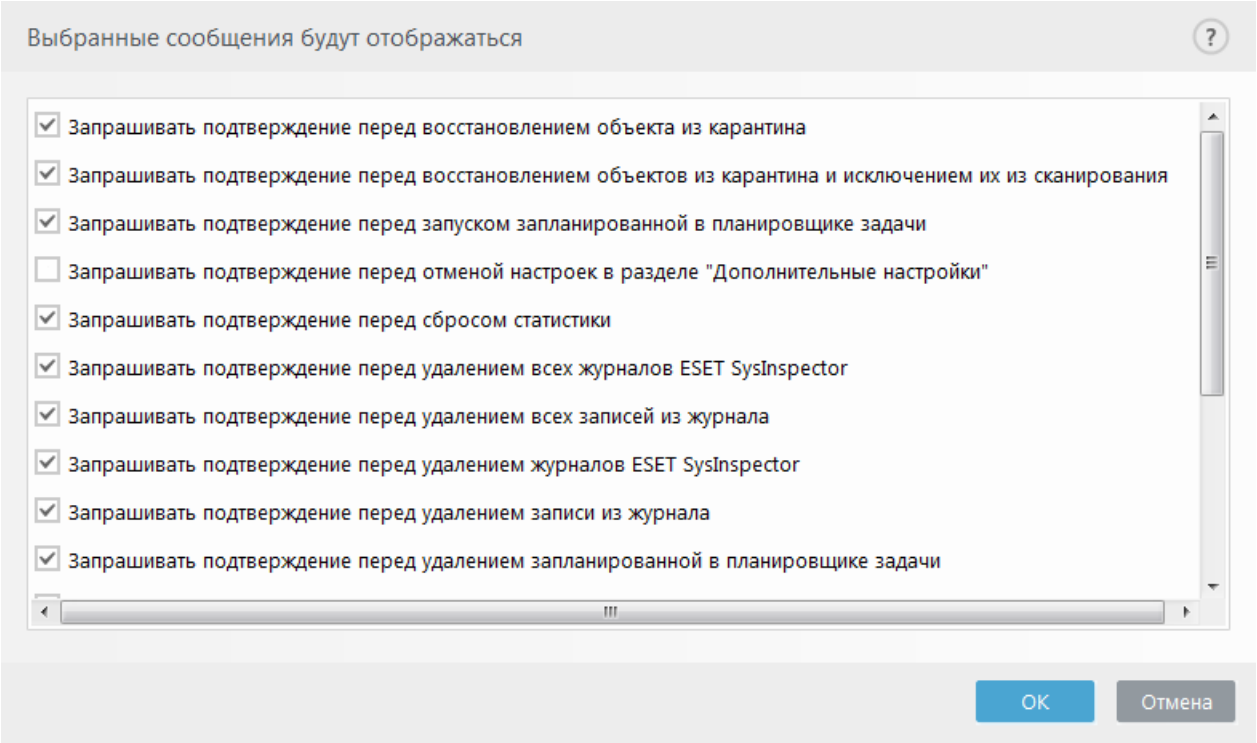
Наличие этих предупреждений изменит интерфейс на оранжевый:

- Перезагрузить компьютер (обязательно)
- Перезагрузить компьютер (рекомендуется)

> Интерактивные предупреждения не содержат модуль обнаружения, HIPS или интерактивные окна файервола, так как их поведение можно настроить отдельно в конкретной функции.

Подтверждения

Чтобы настроить подтверждения, перейдите в раздел **Интерфейс** > **Окна предупреждений и сообщений** > **Сообщение подтверждения** ESET Endpoint Security Расширенное дерево настроек и щелкните **Изменить**.



В этом диалоговом окне отображаются подтверждения, выводимые ESET Endpoint Security перед выполнением какого-либо действия. Установите или снимите флажок рядом с каждым типом подтверждения, чтобы включить или отключить его.

Дополнительные сведения о функциях, связанных с подтверждениями:

- Запрашивать подтверждение перед удалением журналов ESET SysInspector
- Запрашивать подтверждение перед удалением всех журналов ESET SysInspector
- Запрашивать подтверждение перед удалением объекта из карантина
- Запрашивать подтверждение перед отменой настроек в разделе "Дополнительные настройки"
- Запрашивать подтверждение, если решено не удалять все найденные угрозы в окне предупреждения
- Запрашивать подтверждение перед удалением записи из журнала
- Запрашивать подтверждение перед удалением запланированной в планировщике задачи
- Запрашивать подтверждение перед удалением всех записей из журнала
- Запрашивать подтверждение перед сбросом статистики
- Запрашивать подтверждение перед восстановлением объекта из карантина
- Запрашивать подтверждение перед восстановлением объектов из карантина и исключением их из сканирования
- Запрашивать подтверждение перед запуском запланированной в планировщике задачи

- Показывать оповещения о результатах работы модуля защиты от спама
- Показывать оповещения о результатах работы модуля защиты от спама для почтовых клиентов
- Показывать диалоговые окна подтверждения продукта для почтовых клиентов Outlook Express и Windows Mail
- Показывать диалоговые окна подтверждения продукта для Windows Live Mail
- Показывать диалоговые окна подтверждения продукта для почтового клиента Outlook

Ошибка «Конфликт дополнительных настроек»

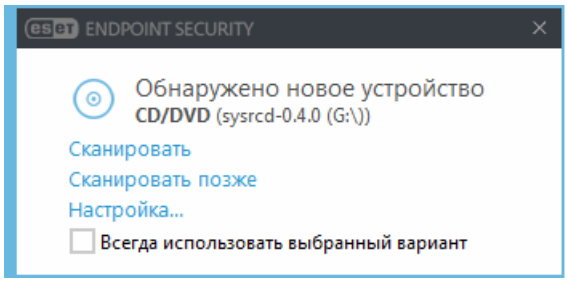
Эта ошибка может возникнуть, если один из компонентов (например, система предотвращения вторжений на узел или файервол) и пользователь создали правила в интерактивном режиме или режиме обучения одновременно.

> Рекомендуется изменить режим фильтрации на **Автоматический режим** по умолчанию, если вы хотите создавать собственные правила. См. дополнительные сведения о режиме обучения файервола ESET. См. дополнительные сведения о системе HIPS и режимах фильтрации HIPS.

Съемные носители

ESET Endpoint Security обеспечивает автоматическое сканирование съемных носителей (компакт- и DVD-дисков, USB-устройств и т. п.) при их подключении к компьютеру. Это может быть удобно, если администратор компьютера хочет предотвратить подключение пользователями съемных носителей с нежелательным содержимым.

Если в ESET Endpoint Security включен параметр **Показать параметры сканирования**, то при подключении съемного носителя отображается следующее диалоговое окно:



Параметры этого диалогового окна:

- **Сканировать сейчас**: запуск сканирования съемного носителя.
- **Сканировать позже**: сканирование съемного носителя будет отложено.
- **Настройка**: вызов раздела **Расширенные параметры**.

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

ESET Endpoint Security 7.2 и более поздние версии

Чтобы получить доступ к настройкам сканирования съемных носителей, откройте Расширенные параметры (**F5**) > **Интерфейс** > **Окна предупреждений и сообщений** > **Интерактивные предупреждения** > **Список интерактивных предупреждений** > **Изменить** > **Обнаружено новое устройство**.

Если параметр **Спросить пользователя** не выбран, выберите нужное действие при вставке съемного носителя в компьютер:

- **Не сканировать**: действия не будут выполняться, окно **Обнаружено новое устройство** открываться не будет.

- **Автоматическое сканирование устройств**: выполняется сканирование подключенного к компьютеру съемного носителя.

- **Показать параметры сканирования**: откроется раздел настроек **Интерактивные предупреждения**.

ESET Endpoint Security версия 7.1 или более ранняя

Чтобы изменить настройки сканирования съемных носителей, последовательно выберите элементы Расширенные параметры (**F5**) > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Съемные носители**.

Действие, которое следует предпринять после подключения съемного носителя: выбор действия по умолчанию, которое выполняется при подключении съемного носителя (компакт-диска, DVD-диска, USB-устройства) к компьютеру. Выберите действие, которое нужно выполнять при подключении съемного носителя к компьютеру.

- **Не сканировать**: действия не будут выполняться, окно **Обнаружено новое устройство** открываться не будет.

- **Автоматическое сканирование устройств**: выполняется сканирование подключенного к компьютеру съемного носителя.

- **Показать параметры сканирования**: переход в раздел, где настраиваются действия со **съемными носителями**.

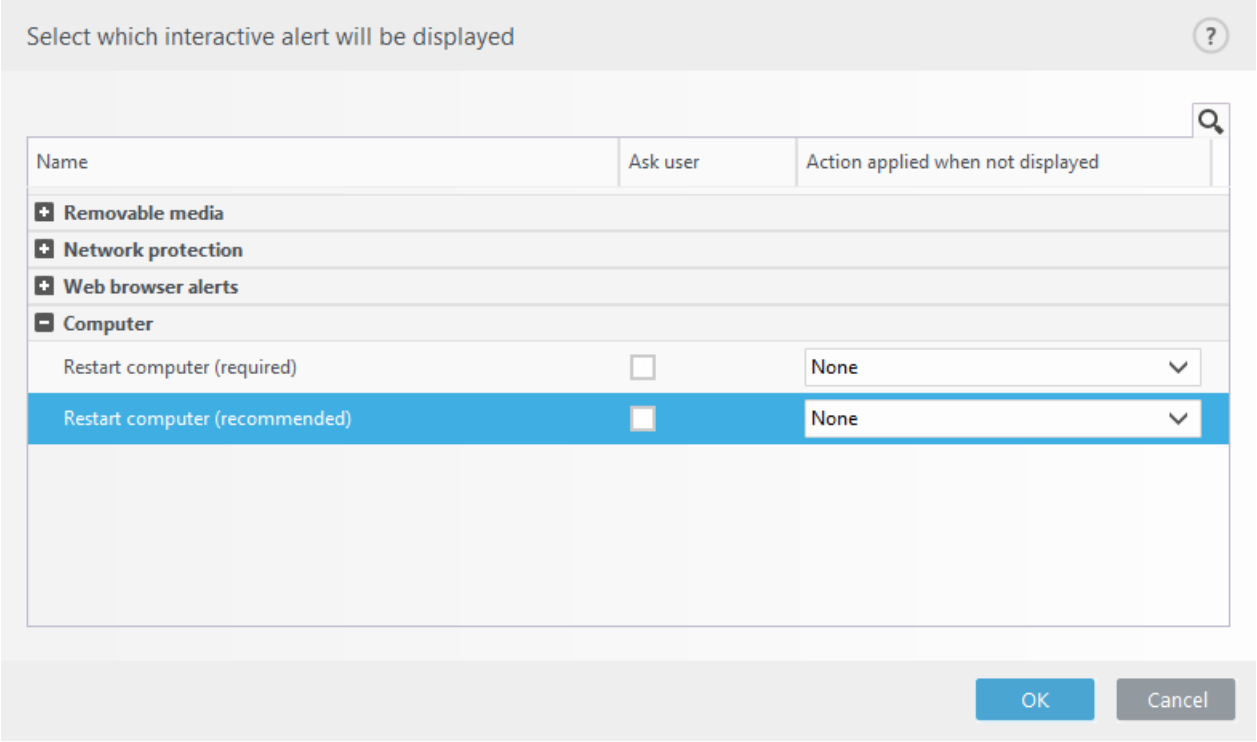
Требуется перезагрузка

Вы можете отключить отображение предупреждений, если компьютеры конечной точки отображают красное предупреждение «Требуется перезагрузка».

Чтобы отключить предупреждения «Необходим перезапуск» или «Рекомендуется перезапуск», выполните приведенные ниже действия.

1. Нажмите клавишу **F5**, чтобы получить доступ к расширенным настройкам и разверните раздел **Предупреждения и окна сообщений**.

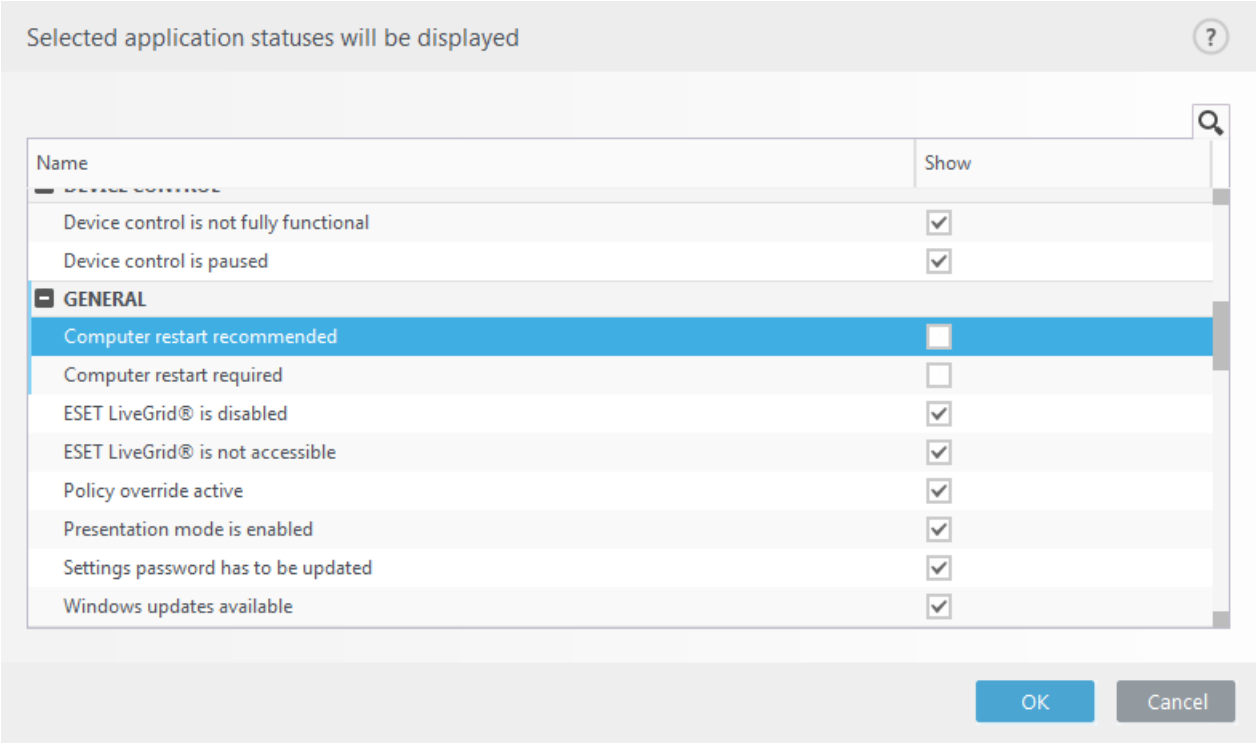
2. Выберите **Изменить** возле пункта **Список интерактивных предупреждений**. В разделе **Компьютер** снимите флажок с пункта **Перезагрузить компьютер (обязательно)** и **Перезагрузить компьютер (рекомендовано)**.



3. Нажмите **OK**, чтобы сохранить изменения в обоих открытых окнах.

4. Предупреждение больше не будет появляться на компьютере конечной точки.

5. (опционально) Чтобы отключить отображение состояния приложения на главном экране программы ESET Endpoint Security, в окне состояний приложений снимите флажок с пункта **Необходима перезагрузка компьютера** и **Рекомендовано перезагрузить компьютер**.



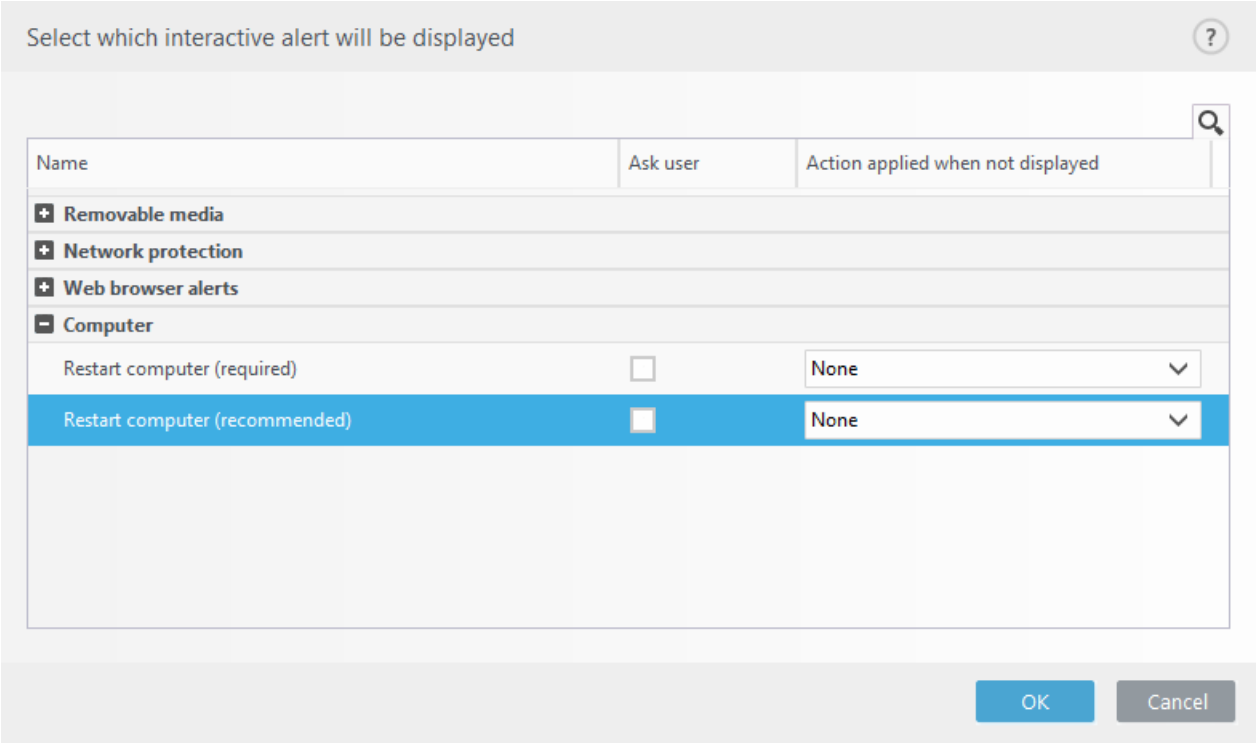
Рекомендуется перезагрузка

Вы можете отключить отображение предупреждений, если компьютеры конечной точки отображают желтое предупреждение «Рекомендуется перезагрузка».

Чтобы отключить предупреждения «Необходим перезапуск» или «Рекомендуется перезапуск», выполните приведенные ниже действия.

1. Нажмите клавишу **F5**, чтобы получить доступ к расширенным настройкам и разверните раздел **Предупреждения и окна сообщений**.

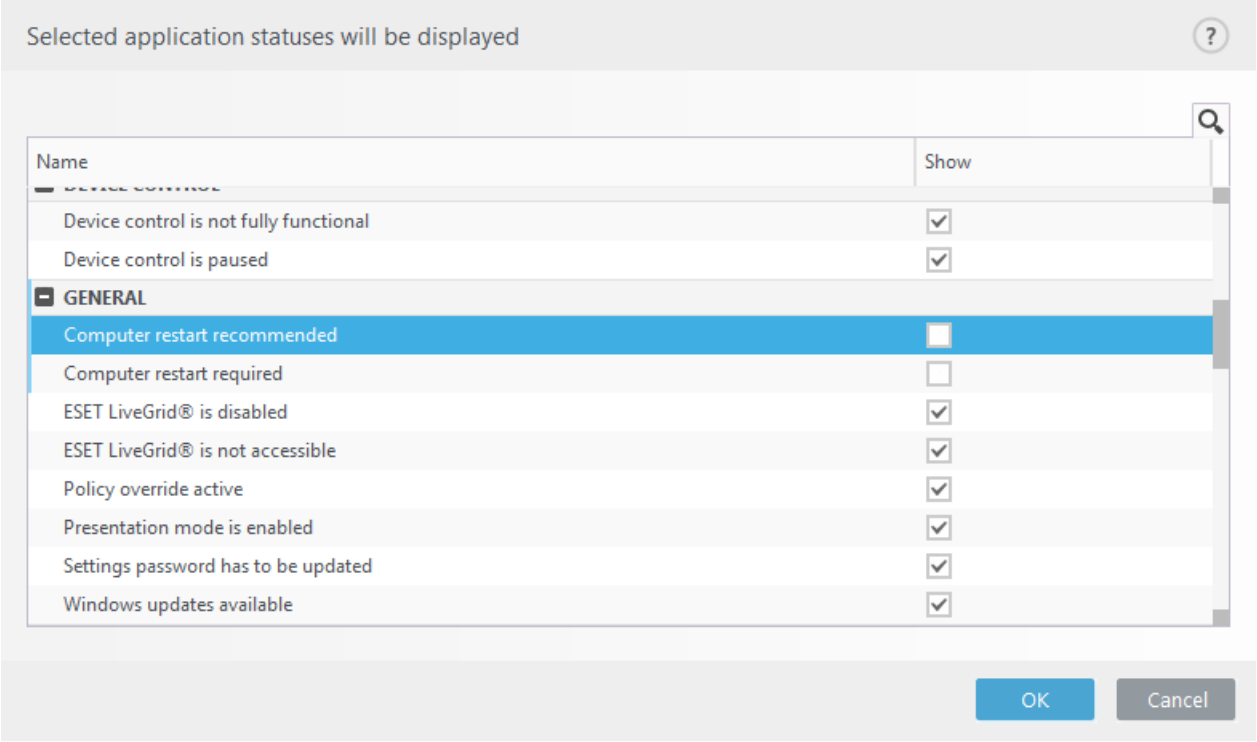
2. Выберите **Изменить** возле пункта **Список интерактивных предупреждений**. В разделе **Компьютер** снимите флажок с пункта **Перезагрузить компьютер (обязательно)** и **Перезагрузить компьютер (рекомендовано)**.



3. Нажмите **OK**, чтобы сохранить изменения в обоих открытых окнах.

4. Предупреждение больше не будет появляться на компьютере конечной точки.

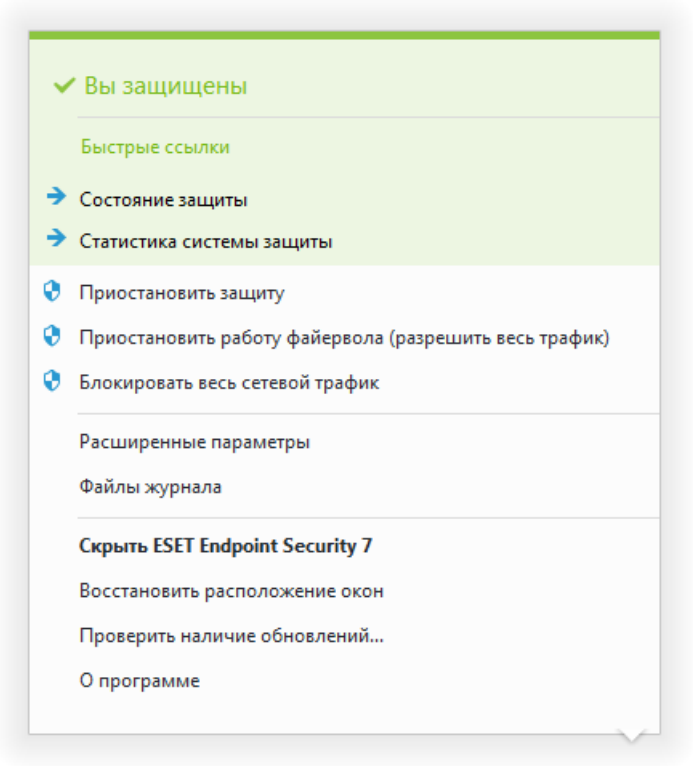
5. (опционально) Чтобы отключить отображение состояния приложения на главном экране программы ESET Endpoint Security, в окне состояний приложений снимите флажок с пункта **Необходима перезагрузка компьютера** и **Рекомендовано перезагрузить компьютер**.



Значок на панели задач

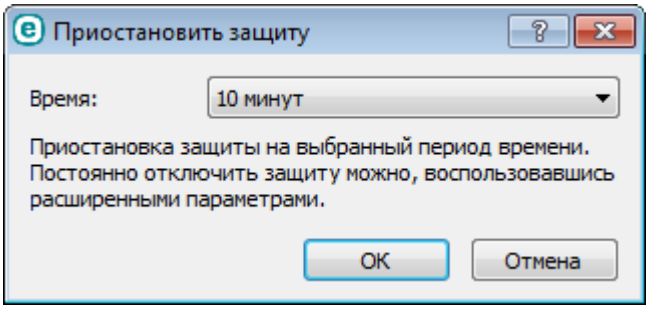
К некоторым наиболее важным функциям и настройкам можно получить доступ, щелкнув правой кнопкой мыши значок на панели задач.

> Чтобы пользователь мог получить доступ к меню значков на панели задач, для режима запуска элементов интерфейса должно быть установлено значение «Полный».



Приостановить защиту. На экран выводится диалоговое окно для подтверждения. В нем можно отключить модуль обнаружения, который контролирует обмен файлами и данными через Интернет и электронную почту, предотвращая тем самым атаки на компьютер.

В раскрывающемся меню **Время** указывается период времени, на который защита будет полностью отключена.



Приостановить работу файервола (разрешить весь трафик): файервол переводится в неактивное состояние. Для получения дополнительных сведений см. раздел Сеть.

Блокировать весь сетевой трафик: файервол 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 настройки**.

Файлы журналов. Файлы журнала содержат информацию обо всех важных событиях программы и предоставляют общие сведения об обнаруженных угрозах.

Открыть ESET Endpoint Security. Если щелкнуть этот значок на панели задач, откроется главное окно программы 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.

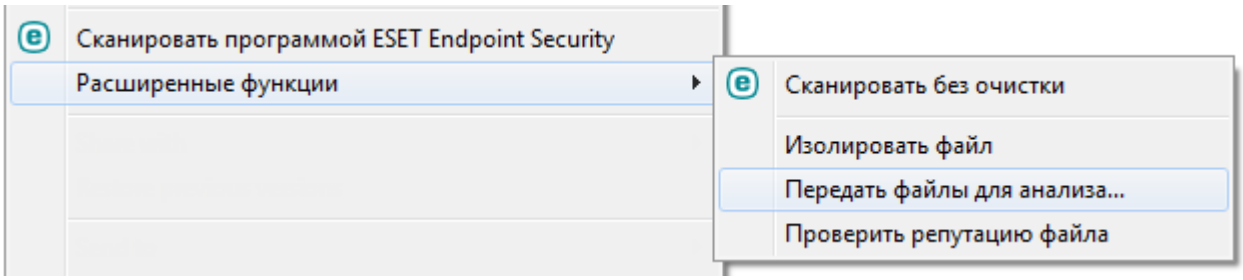
О программе: отображение системной информации, сведений об установленной версии ESET Endpoint Security и модулях программы, а также срока действия лицензии. В нижней части окна представлена информация об операционной системе и системных ресурсах.

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.



Справка и поддержка

В ESET Endpoint Security есть средства для устранения проблем и информация по поддержке, которые помогут решить проблемы, если они возникнут.

Установленный продукт

- **О программе ESET Endpoint Security**: на экран выводится информация о вашей копии программы ESET Endpoint Security.

• **Устранение проблем с продуктом**: щелкните эту ссылку, чтобы найти решения часто встречающихся проблем.

• **Устранение проблем с лицензией**: щелкните эту ссылку, чтобы найти решения проблем с активацией или изменением лицензии.

• **Изменить лицензию**. Щелкните, чтобы открыть окно активации и активировать продукт.

Страница справки – нажмите эту ссылку, чтобы открыть разделы справки ESET Endpoint Security.

Служба технической поддержки

• **Запрос в службу поддержки**: если не удается найти ответ на вопрос, можно обратиться в службу технической поддержки с помощью формы, расположенной на веб-сайте ESET. В зависимости от настроек вашего продукта перед заполнением веб-формы может появиться окно для отправки данных о конфигурации системы.

• **Информация для службы технической поддержки**. В ответ на запрос скопируйте и отправьте информацию (например, название продукта, версию продукта, операционную систему и тип процессора) в службу технической поддержки ESET.

• **ESET Log Collector**: ссылка на статью в базе знаний ESET, откуда можно загрузить программу ESET Log Collector, которая автоматически собирает информацию и журналы с компьютера, чтобы ускорить решение проблем. Дополнительные сведения можно просмотреть в онлайн-руководстве пользователя ESET Log Collectorздесь.

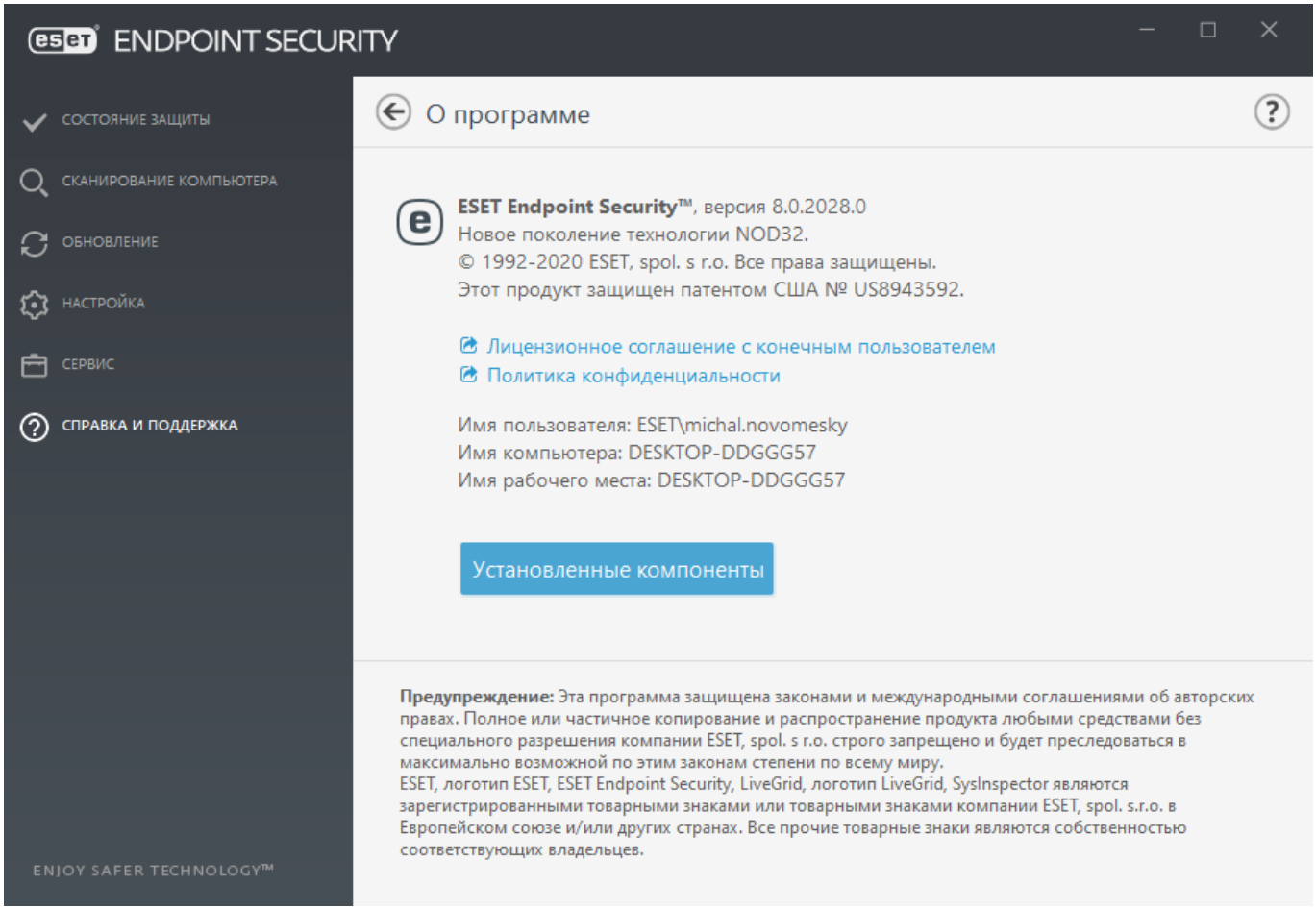
• Включите расширенное ведение журналов, чтобы создать расширенные журналы для всех доступных компонентов и помочь разработчикам в диагностике и решении проблем. Для минимальной степени детализации журнала установлен уровень Диагностика. Расширенное ведение журналов будет автоматически отключено через два часа, если вы не остановите его раньше, щелкнув Остановить расширенное ведение журналов. Когда все журналы будут созданы, отобразится окно уведомления для прямого доступа к папке диагностики, в которой содержатся созданные журналы.

База знаний: в базе знаний ESET содержатся ответы на наиболее часто задаваемые вопросы, а также рекомендуемые решения различных проблем. База знаний регулярно обновляется техническими специалистами ESET, что делает ее самым полезным инструментом для решения разнообразных проблем.

О программе ESET Endpoint Security

В этом окне содержатся сведения об установленной версии ESET Endpoint Security, операционной системе и системных ресурсах вашего компьютера.

Щелкните **Установленные компоненты**, чтобы просмотреть сведения о списке установленных модулей программы и их версиях. Чтобы скопировать информацию о модулях в буфер обмена, используйте команду **Копировать**. Это может быть полезно при устранении проблем или обращении в службу технической поддержки.



Отправка данных о конфигурации системы

Чтобы иметь возможность максимально быстро и эффективно оказывать пользователям помощь, компании ESET требуется информация о конфигурации ESET Endpoint Security, подробные сведения о системе пользователя и запущенных в ней процессах (файл журнала ESET SysInspector) и данные реестра. Компания ESET использует эту информацию только для предоставления клиенту технической поддержки.

При отправке веб-формы будут отправлены и данные о конфигурации системы. Установите флажок **Всегда отправлять эти сведения**, если нужно запомнить это действие для этого процесса. Чтобы отправить форму, не отправляя данные, щелкните элемент **Не отправлять данные**. В этом случае для обращения в службу технической поддержки ESET следует использовать соответствующую онлайн-форму.

Настроить этот параметр можно и по-другому: последовательно щелкните элементы **Расширенные параметры** > **Сервис** > **Диагностика** > **Техническая поддержка**.

> Если вы решили отправить данные о системе, нужно заполнить и отправить веб-форму. В противном случае запрос создан не будет и данные о системе будут потеряны.

Служба технической поддержки

Обратиться в службу технической поддержки

Запрос в службу поддержки: если не удается найти ответ на вопрос, можно обратиться в службу технической поддержки ESET с помощью формы, расположенной на веб-сайте ESET. В зависимости от настроек вашего продукта перед заполнением веб-формы может появиться окно для отправки данных о конфигурации системы.

Получение информации для службы технической поддержки

Информация для службы технической поддержки: в ответ на запрос скопируйте и отправьте информацию в службу технической поддержки ESET (например, сведения о лицензии, имени продукта, версии продукта, операционной системе и компьютере).

ESET Log Collector — ссылка на статью в базе знаний ESET, откуда можно загрузить программу ESET Log Collector, которая автоматически собирает информацию и журналы с компьютера, чтобы ускорить решение проблем. Дополнительные сведения можно просмотреть в онлайн-руководстве пользователя ESET Log Collectorздесь.

Включите **расширенное ведение журналов**, чтобы создать расширенные журналы для всех доступных компонентов и помочь разработчикам в диагностике и решении проблем. Для минимальной степени детализации журнала установлен уровень **Диагностика**. Расширенное ведение журналов будет автоматически отключено через два часа, если вы не остановите его раньше, щелкнув **Остановить расширенное ведение журналов**. Когда все журналы будут созданы, отобразится окно уведомления для прямого доступа к папке диагностики, в которой содержатся созданные журналы.

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 Параметры ThreatSense, где описывается каждый параметр, используемый для настройки сканирования.

Предположим, вам требуется создать собственный профиль сканирования. Хотя конфигурация **Сканировать компьютер** частично подходит, сканировать программы-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 меня **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **OK**, 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.

Сочетания клавиш

Для более удобной навигации в ESET Endpoint Security можно использовать следующие сочетания клавиш:

Сочетания клавиш	Действие выполнено
F1	вызов справки
F5	вызов окна расширенных параметров
Up/Down	переход по элементам в программе
TAB	перемещение курсора по окну
Esc	закрытие активного диалогового окна
Ctrl+U	отображение сведений о лицензии ESET и вашем компьютере (информация для службы технической поддержки)
Ctrl+R	восстановление размеров окна продукта и его положения на экране по умолчанию

Диагностика

Средство диагностики собирает аварийные дампы процессов ESET (например, ekrn). Если происходит аварийное завершение работы приложения, создается соответствующий дамп. С помощью таких дампов разработчики могут отлаживать и исправлять различные проблемы программы ESET Endpoint Security.

Откройте раскрывающееся меню рядом с элементом **Тип дампа** и выберите один из трех доступных вариантов:

- Выберите **Отключить**, чтобы отключить эту функцию.

- **Мини** (по умолчанию) — 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 ограниченный объем включенной в него информации может при анализе 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.

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

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

Создать дамп диагностики: нажмите кнопку **Создать**, чтобы создать в **целевом каталоге** файлы дампа диагностики.

Расширенное ведение журналов

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 журналов для модуля сканирования компьютера: запись всех событий, возникающих в процессе сканирования файлов и папок функцией «Сканирование компьютера» или «Защита файловой системы в реальном времени».

Включение расширенного ведения журнала контроля устройств: запись всех событий, которые происходят в модуле контроля устройств. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем контроля устройств.

Включить расширенное ведение журнала защиты документов: запись всех событий, которые происходят в модуле защиты документов, для диагностики и устранения проблем.

Включить расширенное ведение журнала ядра: запись всех событий, которые происходят в службе ядра ESET (ekrn). Это помогает выявлять и исправлять проблемы. Функция доступна в версии 7.2 и более поздних версиях.

Включить расширенное ведение журнала для лицензирования: запись всего обмена данными между серверами ESET Business Account и решением для активации ESET.

Включить трассировку памяти — Записывать все события, которые помогут разработчикам выявлять утечки памяти.

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 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.

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.

Включение расширенного ведения журналов для защиты файловой системы в реальном времени: запись всех событий, которые происходят в модуле «Защита файловой системы в реальном времени», для диагностики и устранения проблем.

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 контроля доступа в интернет. Это помогает разработчикам выявлять и исправлять проблемы, связанные с модулем родительского контроля.

Расположение файлов журнала

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

Сканер командной строки

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 ESET для командной строки:

```
ecls [OPTIONS..] FILES..
```

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

Параметры

/base-dir=ПАПКА	загрузить модули из ПАПКИ

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

Параметры модуля сканирования

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

/no-sfx	не сканировать самораспаковывающиеся архивы
/rtp	сканировать упаковщики (по умолчанию)
/no-rtp	не сканировать упаковщики
/unsafe	сканировать на наличие потенциально опасных приложений
/no-unsafe	не сканировать на наличие потенциально опасных приложений (по умолчанию)
/unwanted	сканировать на наличие потенциально нежелательных приложений
/no-unwanted	не сканировать на наличие потенциально нежелательных приложений (по умолчанию)
/suspicious	сканировать на наличие подозрительных приложений (по умолчанию)
/no-suspicious	не сканировать на наличие подозрительных приложений
/pattern	использовать сигнатуры (по умолчанию)
/no-pattern	не использовать сигнатуры
/heur	включить эвристический анализ (по умолчанию)
/no-heur	отключить эвристический анализ
/adv-heur	включить расширенную эвристику (по умолчанию)
/no-adv-heur	отключить расширенную эвристику
/ext-exclude=РАСШИРЕНИЯ	исключить из сканирования РАСШИРЕНИЯ файлов, разделенные двоеточием
/clean-mode=РЕЖИМ	использовать РЕЖИМ очистки для зараженных объектов. Доступны указанные ниже варианты. • `none` (по умолчанию) автоматическая очистка не выполняется. • `standard` — 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 без проведения очистки независимо от их типа. • Удаление: приложение ecls.exe удалит без проведения очистки все файлы, кроме важных, таких как системные файлы Windows.
/quarantine	копировать зараженные файлы, если они очищены, в карантин (дополнительно к действию, выполняемому при очистке)
/no-quarantine	не копировать зараженные файлы в карантин

Общие параметры

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

Коды завершения

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

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

ESET CMD

Эта функция включает расширенные команды ecmd. Она позволяет экспортировать и импортировать параметры с помощью командной строки (ecmd.exe). До недавнего времени экспортировать параметры можно было только через графический интерфейс пользователя. Конфигурацию ESET Endpoint Security можно экспортировать в файл с расширением *.xml*.

При включенной функции ESET CMD доступны два метода авторизации:

- **Нет** — без авторизации. Этот метод не рекомендуется, так как он разрешает импортировать любую неподписанную конфигурацию, что представляет собой потенциальный риск.

- **Пароль для расширенной настройки** — пароль требуется для импорта конфигурации из файла с расширением *.xml*. Этот файл должен быть подписан (сведения о подписании файла конфигурации с расширением *.xml* представлены далее). Новую конфигурацию можно импортировать только после того, как будет указан пароль, заданный в разделе Настройка доступа. Если настройка доступа не включена, пароль не совпадает или файл конфигурации в формате *.xml* не подписан, импорт конфигурации выполнен не будет.

После включения ESET CMD можно использовать командную строку для импорта и экспорта конфигураций программы ESET Endpoint Security. Это можно сделать вручную или создать сценарий с целью автоматизации.

Для использования расширенных команд ECMD необходимо запустить их с правами администратора или открыть командную строку Windows (cmd) командой **Запуск от имени администратора**. В противном случае появится сообщение **Error executing command** Кроме того, при экспорте конфигурации должна существовать папка назначения. Команда экспорта работает даже при отключенном параметре ESET CMD.

Расширенные команды ecmd можно выполнить только локально. Выполнение клиентской задачи **Выполнение команды** с использованием ESET PROTECT или ESMC не сработает.

Команда экспорта параметров:
```
ecmd /getcfg c:\config\settings.xml
```

Команда импорта параметров:
```
ecmd /setcfg c:\config\settings.xml
```

Для подписания файла конфигурации в формате XML (*.xml*) выполните следующие действия.

1. Загрузите исполняемый файл XmlSignTool.

2. Откройте командную строку Windows (cmd) с помощью команды **Запуск от имени администратора**.

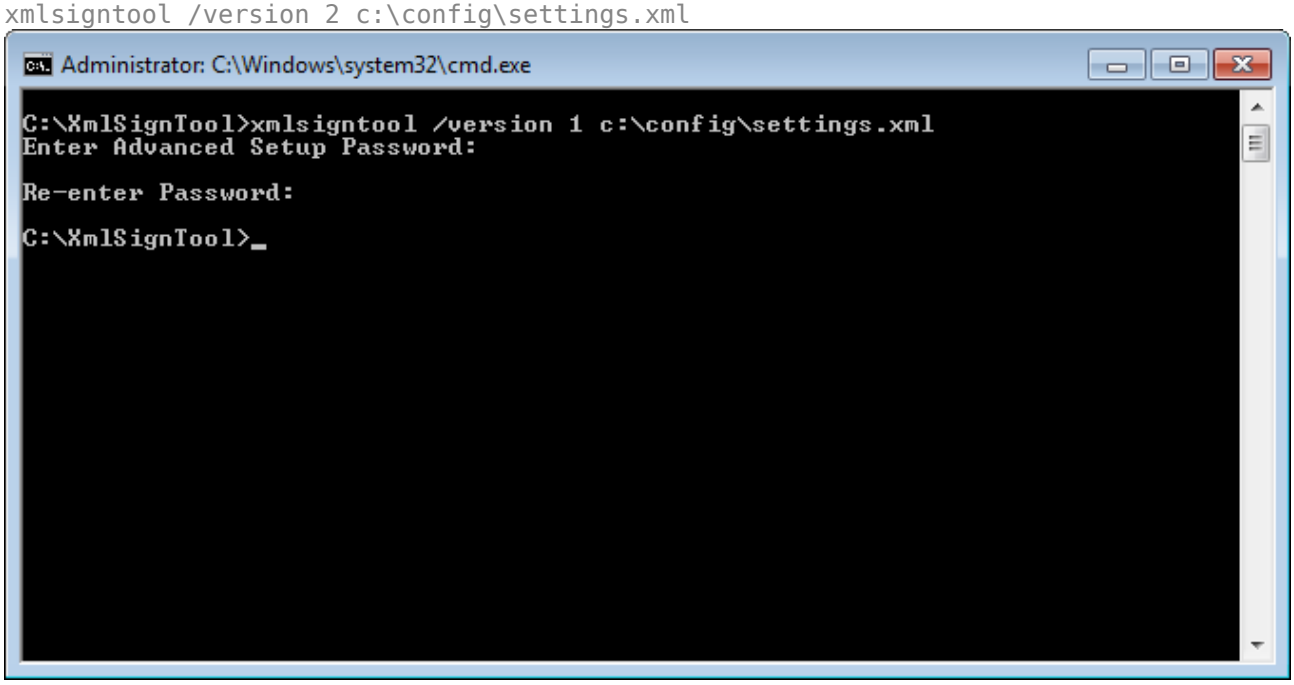
3. Перейдите в расположение файла `xmlsigntool.exe`.

4. Выполните команду для подписания файла конфигурации в формате XML (*.xml*).
Использование: `xmlsigntool /version 1|2 <xml_file_path>`

> Значение параметра `/version` зависит от версии ESET Endpoint Security. Используйте `/version 2` для версии 7 и более новых версий.

5. Введите пароль для дополнительных настроек, а затем введите его еще раз по запросу средства XmlSignTool. Теперь файл конфигурации в формате *XML* подписан и может использоваться для импорта в другом экземпляре ESET Endpoint Security с функцией ESET CMD с помощью метода парольной авторизации.

Команда подписания экспортированного файла конфигурации:
`xmlsigntool /version 2 c:\config\settings.xml`



> Если пароль в разделе Настройка доступа изменится и потребуется импортировать конфигурацию, подписанную ранее с помощью старого пароля, необходимо подписать файл конфигурации в формате *.xml* заново с помощью текущего пароля. Это позволит использовать старый файл конфигурации без необходимости экспортировать его на другой компьютер с работающей программой ESET Endpoint Security перед импортом.

> 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.

Список команд ecmd

Отдельные функции системы безопасности можно включать и временно отключать с помощью команды выполнения клиентской задачи ESET PROTECT. Эти команды не перезаписывают параметры политик, и все приостановленные политики вернутся в исходное состояние после выполнения команды или перезагрузки устройства. Чтобы воспользоваться этой функцией, настройте запуск командной строки в поле с этим же именем.

Просмотрите список команд для каждого компонента системы безопасности ниже:

Функция системы безопасности	Команда временной приостановки	Команда включения
Защита файловой системы в режиме реального времени	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Защита документов	ecmd /setfeature document pause	ecmd /setfeature document enable
Контроль устройств	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Режим презентации	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Технология Anti-Stealth	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Персональный файервол	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Защита от сетевых атак (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Защита от ботнетов	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Контроль доступа в Интернет	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
защита доступа в Интернет;	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Защита почтового клиента	ecmd /setfeature email pause	ecmd /setfeature email enable
Защита от спама	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Защита от фишинга	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Сканирование в состоянии простоя

Настройки сканирования в состоянии простоя можно изменить в меню **Расширенные параметры** в разделе **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Сканирование в состоянии простоя** > **Сканирование в состоянии простоя**. Эти 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.

Импорт и экспорт параметров

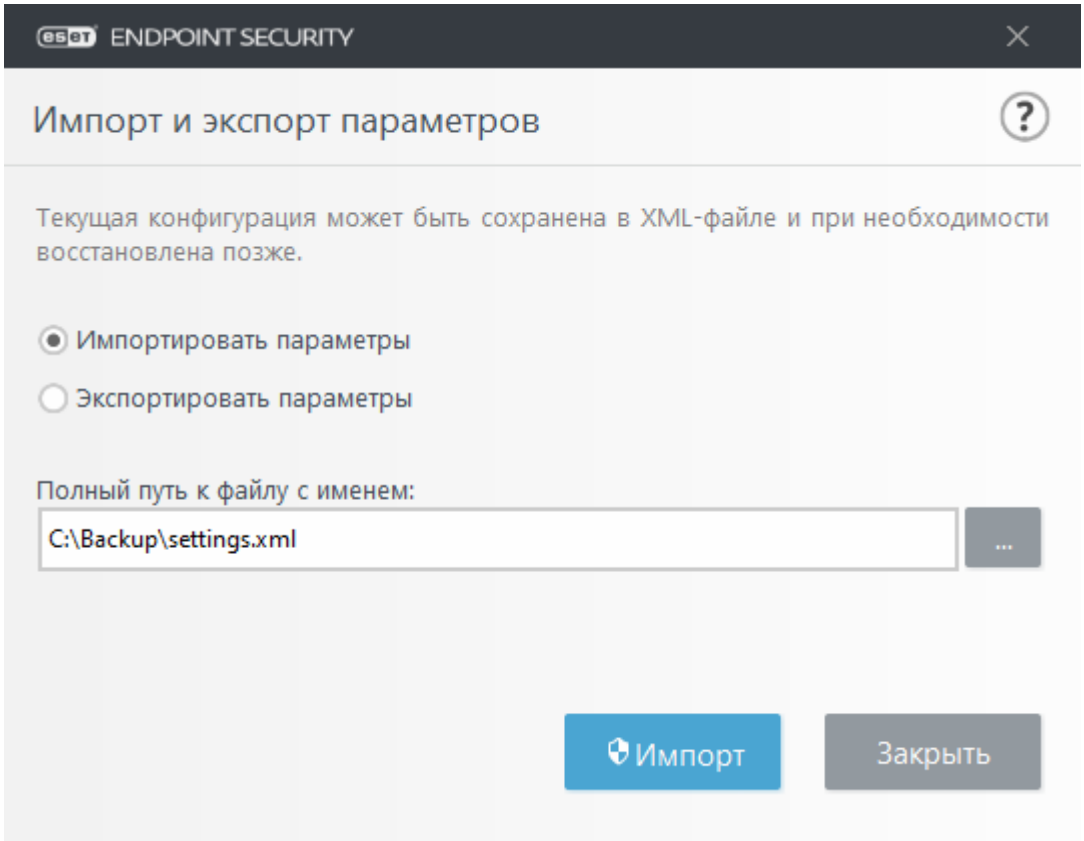
Можно импортировать и экспортировать пользовательский XML-файл конфигурации ESET Endpoint Security с помощью меню **Настройка**.

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.

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



Восстановление всех параметров по умолчанию

Нажмите **По умолчанию** в расширенных параметрах (F5), чтобы скинуть все настройки программы для всех модулей. Они вернутся к состоянию после новой установки.

См. также Параметры импорта и экспорта.

Восстановление всех параметров в этом разделе

Нажмите на стрелку с изгибом , чтобы скинуть все настройки в этом разделе до настроек по умолчанию, определенных ESET.

Обратите внимание, что после нажатия **Вернуть значения по умолчанию** все созданные изменения будут потеряны.

Восстановить содержимое таблиц: при активации этой функции все правила, задачи и профили, добавленные автоматически или вручную, будут удалены.

См. также Параметры импорта и экспорта.

При сохранении конфигурации произошла ошибка

Это сообщение об ошибке показывает, что настройки не были корректно сохранены из-за ошибки.

Обычно это означает, что пользователь, пытавшийся изменить параметры программы:

• имеет недостаточно прав доступа или не имеет необходимых разрешений операционной системы, необходимых для изменения файлов конфигурации и системного реестра.
> Для внесения необходимых изменений системный администратор должен авторизоваться.

• недавно включил режим «Обучение» в системе HIPS или файерволе и попытался внести изменения в расширенные параметры.
> Чтобы сохранить конфигурацию и избежать конфликта конфигурации, закройте расширенные параметры без сохранения и повторите попытку внести необходимые изменения.

Второй наиболее распространенной причиной может быть неправильная работа программы, ее повреждение и, соответственно, необходимость переустановки.

Удаленный мониторинг и управление

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

ERMM — плагин ESET для RMM

- Установка ESET Endpoint Security, используемая по умолчанию, содержит файл `ermm.exe` в каталоге приложения Endpoint:
  C:\Program Files\ESET\ESET Security\ermm.exe

- `ermm.exe` — это программа командной строки, которая позволяет управлять продуктами для конечных точек и обмениваться данными с любым плагином RMM.

- `ermm.exe` обменивается данными с плагином RMM, который в свою очередь обменивается данными с агентом RMM, подключенным к серверу RMM. По умолчанию средство ESET RMM отключено.

Дополнительные ресурсы

- Командная строка ERMM

- Список команд ERMM JSON

- Активация удаленного мониторинга и управленияESET Endpoint Security

Плагины ESET Direct Endpoint Management для сторонних решений RMM

Сервер RMM работает как служба на стороннем сервере. Дополнительные сведения см. в следующих онлайн-руководствах пользователя ESET Direct Endpoint Management:

- Плагин ESET Direct Endpoint Management для ConnectWise Automate

- Плагин ESET Direct Endpoint Management для DattoRMM

- ESET Direct Endpoint Management для Solarwinds N-Central

- ESET Direct Endpoint Management для NinjaRMM

Командная строка ERMM

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=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 information about products**
	сведения о приложении	Get information about product
	сведения о лицензии	Get information about license
	состояние защиты	Get protection status
	журналы	Get logs

Context	Command	Description
	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

Список команд ERMM 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

get protection-status

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

get application-info

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 antispyware 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
}
}
```

get license-info

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

result

```
{
"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
}
```

get logs

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, devctrllog } : 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

```
{
"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"
}
}
```

result

```
{
"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":""
}]
}
},
"error":null
}
```

get activation-status

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
}
```

get scan-info

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
}
```


get configuration

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":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"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
}
```

start scan

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
}
```

start activation

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value

key	Activation key
offline	Path to offline file

Example

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

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

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

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
}
```

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 еженедельного сканирования компьютера
- Подключение продукта к ESET Security Management Center
  - Использование режима переопределения
  - Применение рекомендуемой политики для ESET Endpoint Security
- Настройка зеркала
- Как мне обновить свою систему до Windows 10, если у меня установлен продукт ESET Endpoint Security?

- Активация удаленного мониторинга и управления
- Блокировка загрузки файлов определенного типа из Интернета
- Сведения о свертывании ESET Endpoint Security

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.

- Рекомендации по защите от вирусов-шифраторов (программ-вымогателей)
- Вопросы и ответы по ESET Endpoint Security и ESET Endpoint Antivirus
- Создание или изменение правила файервола с целью разрешить подключения RDP в ESMC
- Адреса и порты, которые необходимо открыть в стороннем файерволе 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.

Обновление ESET Endpoint Security

Обновлять ESET Endpoint Security можно вручную или автоматически. Чтобы запустить обновление, в главном окне программы выберите команду **Обновить**, а затем щелкните **Проверить наличие обновлений**.

При установке программы с параметрами по умолчанию создается задача автоматического обновления. Она запускается каждый час. Чтобы изменить этот интервал, выберите **Сервис** > **Планировщик** (ознакомьтесь с дополнительными сведениями о планировщике).

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 (с веб-страницы ESET, с помощью установщика типа MSI или EXE и т. д.).

Чтобы активировать ESET Endpoint Security непосредственно из программы, откройте главное окно ESET Endpoint Security и в основном меню щелкните **Справка и поддержка** > **Активировать продукт** или **Состояние защиты** > **Активировать продукт**.

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

• **Используйте приобретенный лицензионный ключ**: уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.

• **ESET Business Account**. Учетная запись, созданная на портале ESET Business Account с использованием учетных данных (адрес электронной почты и пароль). Этот метод позволяет централизовано 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 Business Account.

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

Если у вас есть имя пользователя и пароль для активации продуктов ESET предыдущих версий, но вы не знаете, как активировать ESET Endpoint Security, преобразуйте устаревшие учетные данные в лицензионный ключ.

Не удалось активировать программу?

Изменить лицензию на продукт можно в любое время. Для этого щелкните **Справка и поддержка** > **Изменить лицензию** 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).

> ESET Security Management Center 7.2 или ESET PROTECT 8 может активировать клиентские компьютеры в автоматическом режиме, используя предоставленные администратором лицензии. Инструкции см. в ESET PROTECT Онлайн-справке.

Ввод лицензионного ключа при активации

Автоматические обновления являются важным компонентом вашей безопасности. ESET Endpoint Security будет получать обновления после активации с использованием **Лицензионного ключа**.

Если не ввести лицензионный ключ после установки, продукт активирован не будет. Сменить лицензию можно в главном окне программы. Для этого щелкните элемент **Справка и поддержка**, затем **Активировать лицензию** и в окне «Активация программы» введите данные лицензии, полученные в комплекте с продуктом ESET.

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

• Лицензионный ключ — это уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца и активации лицензии.

Во избежание неточностей рекомендуется скопировать Лицензионный ключ из электронного письма с регистрационными данными и вставить его в нужное поле.

Вход в ESET Business Account

Учетная запись администратора безопасности создается на портале ESET Business Account с указанием **адреса электронной почты** и **пароля**. В этой учетной записи отображены все компьютеры с лицензией. С помощью учетной записи администратора безопасности можно управлять несколькими лицензиями. Если такой учетной записи у вас нет, щелкните элемент **Создать учетную запись**: вы перейдете на портале ESET Business Account, на котором можно зарегистрироваться, указав свои учетные данные.

Если вы забыли пароль, щелкните элемент **Я не помню пароль**. Вы будете перенаправлены на портал ESET Business Account. Введите адрес электронной почты и щелкните **Войти** для подтверждения. Вам будет отправлено сообщение с указаниями по сбросу пароля.

Использование устаревших учетных данных лицензии для активации более нового продукта ESET для конечных точек

Если у вас уже есть имя пользователя и пароль и вы желаете получить лицензионный ключ, посетите ESET Business Account портал. На портале учетные данные можно преобразовать в лицензионный ключ.

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.

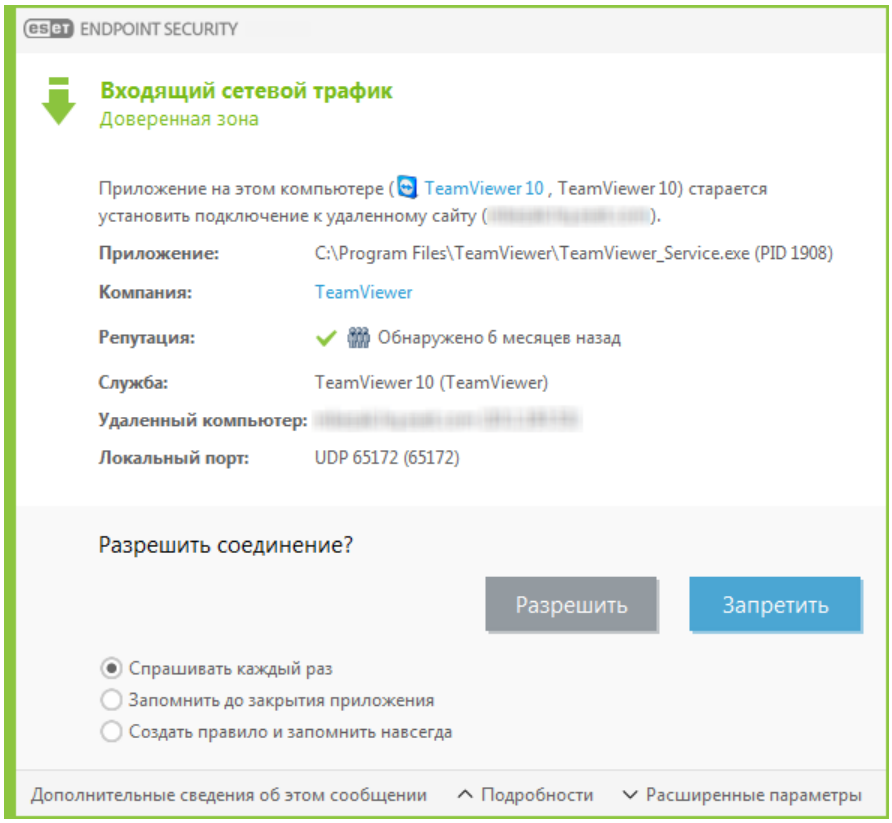
3. После завершения сканирования просмотрите журнал на предмет количества проверенных, зараженных и очищенных файлов.

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.

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 файервола для приложений еще до их обнаружения программой ESET Endpoint Security в окне настроек файервола. Для этого откройте главное окно программы > **Настройка** > **Сеть** > **Файервол** > щелкните значок шестеренки > **Настроить** > **Дополнительно** > **Правила**, а затем щелкните **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.

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 их 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.

Планирование еженедельного сканирования компьютера

Чтобы запланировать регулярную задачу, откройте главное окно программы и выберите **Сервис** > **Планировщик**. Ниже приведено краткое описание процедуры планирования задачи, предусматривающей сканирование локальных дисков каждую неделю. Подробные инструкции см. в статье нашей базы знаний.

Для того чтобы запланировать задачу сканирования, выполните следующие действия.

1. В главном окне планировщика нажмите **Добавить**.
2. В раскрывающемся меню выберите **Сканирование компьютера по требованию**.
3. Введите имя задачи и выберите частоту выполнения задачи **Еженедельно**.
4. Задайте день и время выполнения задачи.
5. Выберите установку **Выполнить задачу как можно скорее**, чтобы выполнить задачу позже, в случае если запланированное выполнение задачи не запустится по какой-либо причине (например, если компьютер выключен).
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.

Подключение ESET Endpoint Security к ESET PROTECT

Если после установки ESET Endpoint Security на компьютер вы хотите подключиться через ESET PROTECT, убедитесь, что на клиентской рабочей станции также установлено ПО ESET Management Agent. Это важная составляющая каждого клиентского решения, которое подключается к серверу ESMC Server.

- Установка или развертывание ESET Management Agent на клиентских рабочих станциях

Дополнительные сведения

- Документация по конечным точкам под удаленным управлением
- Использование режима переопределения
- Применение рекомендуемой политики для ESET Endpoint Security

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.

- Если режим переопределения включен, его нельзя отключить с помощью веб-консоли ESMC. Он будет отключен автоматически, когда закончится период времени переопределения. Кроме того, его можно отключить на клиентском компьютере.
- Пользователю, который использует режим переопределения, нужно также иметь права администратора Windows. В противном случае пользователь не может сохранить изменения настроек ESET Endpoint Security.
- Групповая аутентификация Active Directory поддерживается для ESET Endpoint Security версии 7.0.2100.4 и более поздних версий.

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

1. Перейдите в раздел **Политики** > **Создать политику**.

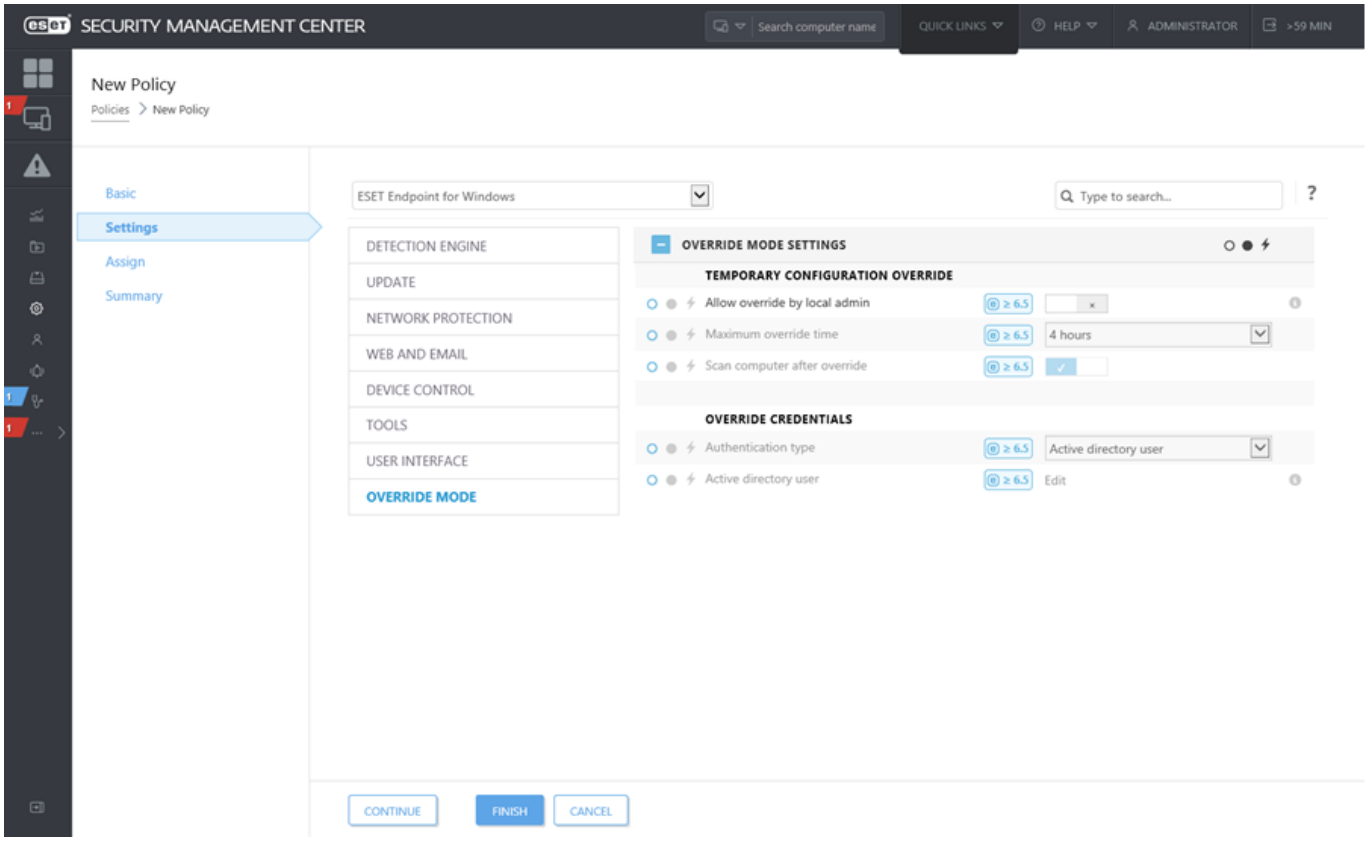
2. В разделе **Основная информация** введите **имя** и **описание** этой политики.

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.



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 ESMC, чтобы администратор мог создать на их основе новую политику.

Для этого выполните следующие действия:

1.Перейдите в раздел **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 ESMC 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.

Применение рекомендуемой политики для ESET Endpoint Security

После подключения ESET Endpoint Security к ESET Security Management Center лучше всего применить рекомендуемую политику или пользовательскую политику.

Для ESET Endpoint Security есть несколько встроенных политик:

Политика	Описание
Защита от вирусов — сбалансированная настройка	Конфигурация безопасности, рекомендуемая для большинства настроек.
Защита от вирусов — максимальная безопасность	Использование машинного обучения, глубокой поведенческой проверки и фильтрации SSL. Есть влияние на обнаружение потенциально небезопасных, нежелательных и подозрительных приложений.
Облачная система репутации и обратной связи	Включает облачную систему репутации и обратной связи ESET LiveGrid®, чтобы улучшить обнаружение новейших угроз и предоставлять сведения о вредоносных и неизвестных потенциальных угрозах для дальнейшего анализа.
Контроль устройств — максимальная безопасность	Все устройства блокируются. Когда с устройства инициируется подключение, требуется разрешение администратора.
Контроль устройств — только для чтения	Все устройства доступны только для чтения. Запись запрещена.
Файервол — блокировать весь трафик, кроме соединения с ESMC и EEI	Блокировка всего трафика, кроме подключения к ESET Security Management Center и серверу ESET Enterprise Inspector (только ESET Endpoint Security).
Ведение журнала — полноценное ведение журнала диагностики	Благодаря этому шаблону администратор получает доступ ко всем журналам тогда, когда это нужно. В журнал вносятся все элементы, начиная с элементов минимальной детализации, в том числе HIPS, параметры Threatsense и данные файервола. Журналы автоматически удаляются через 90 дней после создания.
Ведение журнала — внесение в журнал только важных событий	Политика обеспечивает внесение в журнал предупреждений, ошибок и критических событий. Журналы автоматически удаляются через 90 дней после создания.
Внешний вид — сбалансированная настройка	Используются параметры внешнего вида по умолчанию. Включено отображение состояний и оповещений.
Внешний вид — невидимый режим	Оповещения, уведомления, графический интерфейс, интеграция в контекстное меню не отображаются. Файл egui.exe не запускается. Программа предназначена для управления только через ESET PROTECT Cloud.
Внешний вид — ограниченное взаимодействие с пользователем	Отображение состояний и оповещений отключено, графический интерфейс отображается.

Чтобы применить политику с именем **Защита от вирусов — максимальная безопасность**, которая приводит в исполнение более 50 рекомендуемых параметров для решения ESET Endpoint Security, установленного на рабочих станциях, выполните следующие действия.

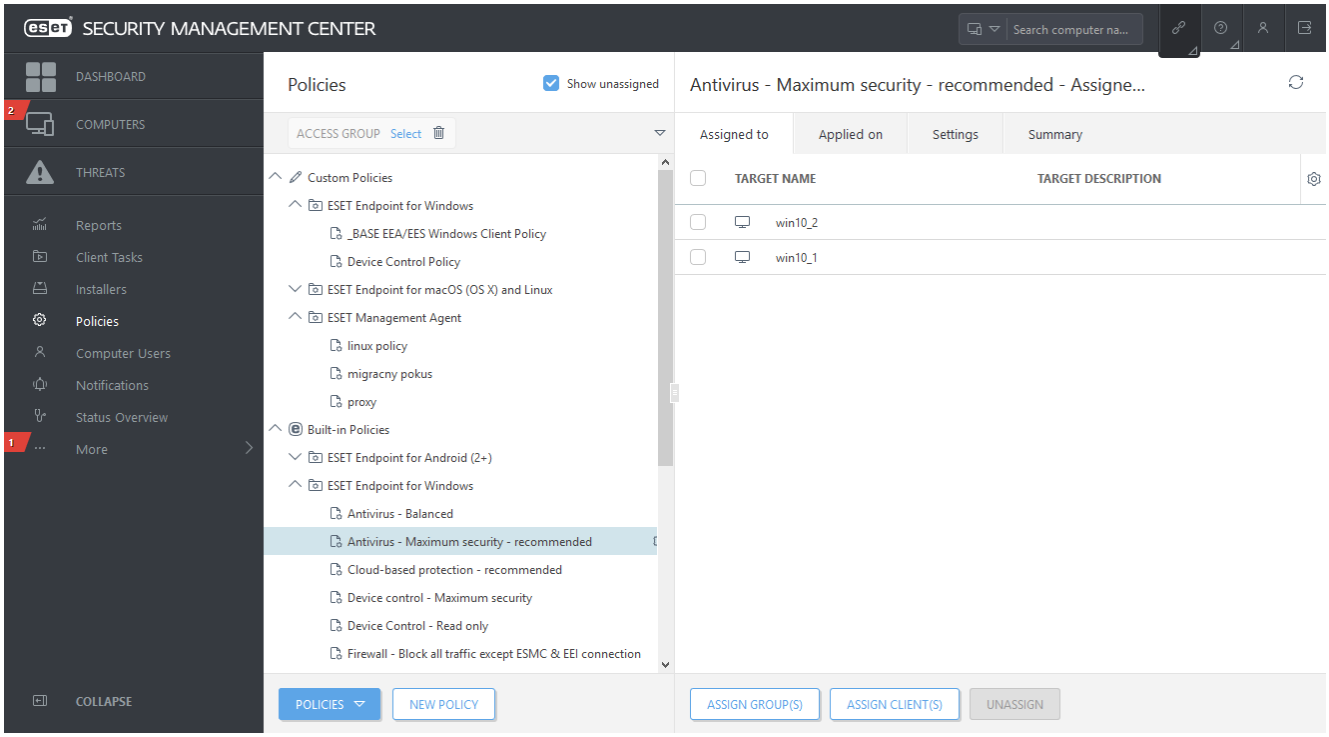
> Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:
> • Применение рекомендуемой или предварительно заданной политики для ESET Endpoint Security с помощью ESMC

1. Откройте веб-консоль ESMC.

2. Перейдите в раздел **Политики** и разверните **Встроенные политики** > **ESET Endpoint для Windows**.

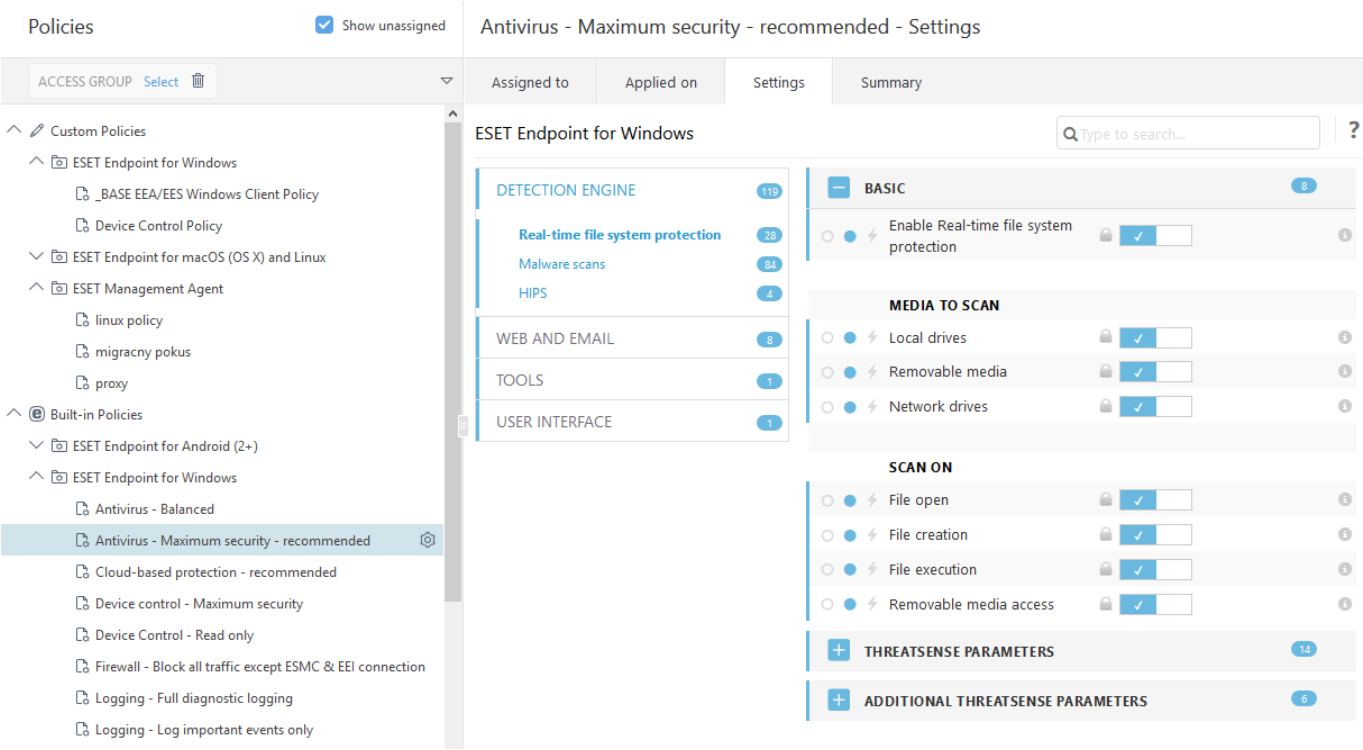
3. Щелкните элемент **Защита от вирусов — максимальная безопасность — рекомендуется**.

4. На вкладке **Назначено для** щелкните **Назначить клиентам** или **Назначить группам** и выберите компьютеры, для которых нужно применить эту политику.



Чтобы узнать, какие параметры применяются для этой политики, перейдите на вкладку **Параметры** и разверните дерево «Расширенные параметры».

- Синяя точка означает, что параметр изменен для этой политики
- Число в синей рамке соответствует количеству параметров, измененных этой политикой
- Дополнительные сведения о политиках ESMC см. здесь



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

1. Нажмите клавишу **F5**, чтобы получить доступ к расширенным параметрам, и выберите **Обновление** > **Профили** > **Зеркало обновлений**.

2. Разверните узел **Обновления** и убедитесь, что в разделе **Обновления модулей** включен параметр **Выбирать автоматически**.

3. Разверните узел **Зеркало обновлений** и включите параметры **Создать зеркало обновления** и **Включить HTTP-сервер**.

Дополнительные сведения см. в разделе Зеркало обновлений.

Настройка сервера зеркала для передачи обновлений через общую сетевую папку

1. Создайте общую папку на локальном или сетевом устройстве. Папка должна быть доступна для чтения всем пользователям решений ESET для обеспечения безопасности, а также для записи из локальной системной учетной записи.

2. Активируйте элемент **Создать зеркало обновления** в разделе **Расширенные параметры** > **Обновления** > **Профили** > **Зеркало обновлений**.

3. Выберите соответствующую **папку для хранения**, щелкнув **Очистить** и **Изменить**. Найдите и выберите созданную общую папку.

> Если через внутренний HTTP-сервер передавать обновления модулей не нужно, снимите флажок **Создать зеркало обновления**.

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

> 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 7.x:

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

Загрузить ESET Endpoint Security 7 (32-разрядная версия) Загрузить ESET Endpoint Antivirus 7 (32-разрядная версия)

Загрузить ESET Endpoint Security 7 (64-разрядная версия) Загрузить ESET Endpoint Antivirus 7 (64-разрядная версия)

Версия 5.x:

> Для продуктов ESET Endpoint версии 5 уже закончился срок службы. Это означает, что они больше не доступны публично для загрузки. Настоятельно рекомендуем выполнить обновление до последней версии продуктов ESET Endpoint.

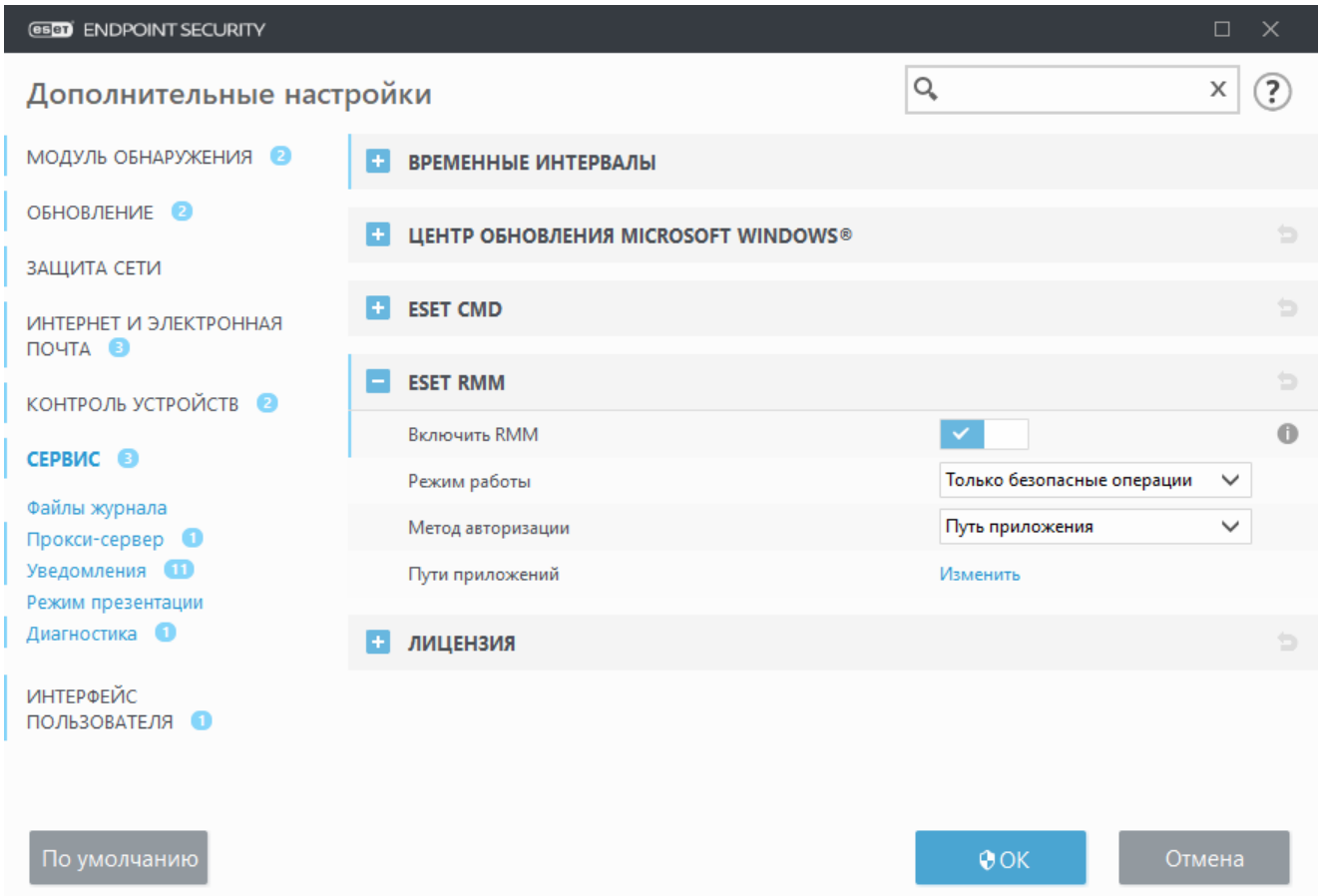
Версии на других языках:

Если вы ищете версию продукта ESET для конечных точек на другом языке, посетите нашу страницу загрузок.

> Дополнительные сведения о совместимости продуктов ESET для бизнеса с Windows 10.

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. Процесс RMM может управлять программой ESET Endpoint Security начиная с версии 6.6.2028.0.



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

Режим работы: выберите **Только безопасные операции**, чтобы разрешить интерфейс RMM только для безопасных операций и операций, которым разрешено только чтение. Выберите **Все операции**, чтобы разрешить интерфейс RMM для всех операций.

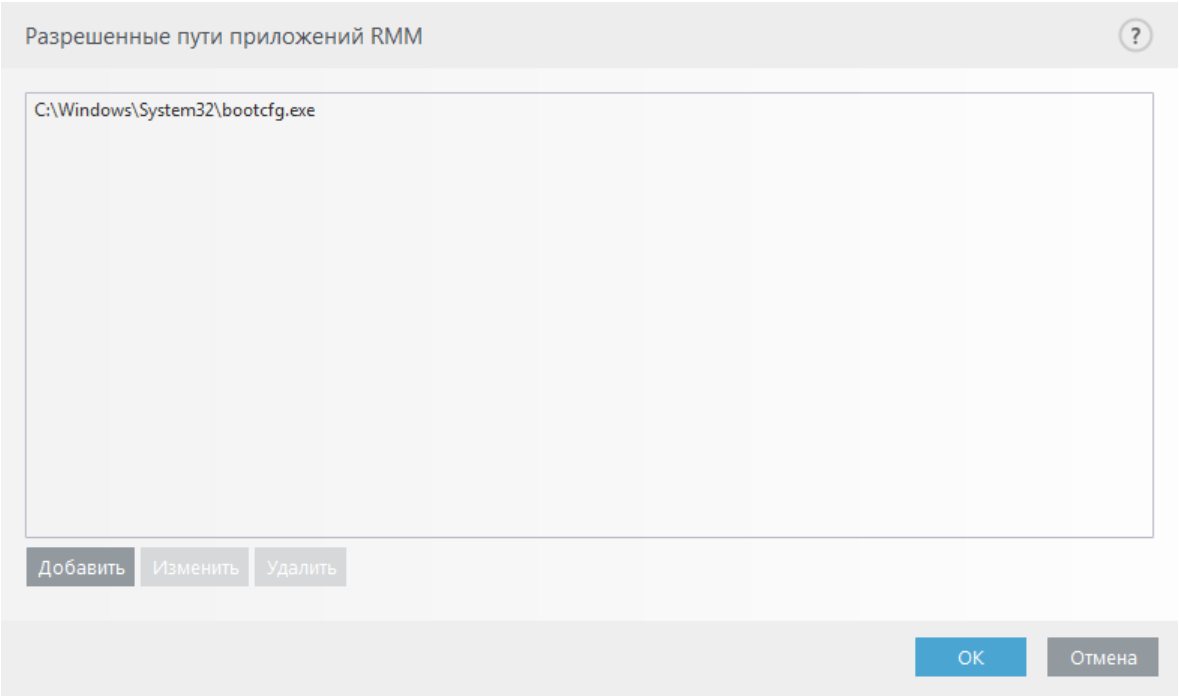
Условие	Режим только безопасных операций	Режим всех операций
Получить сведения о приложении	✔	✔
Получить конфигурацию	✔	✔
Получить сведения о лицензии	✔	✔
Получить журналы	✔	✔
Получить данные о состоянии защиты	✔	✔

Условие	Режим только безопасных операций	Режим всех операций
Получить данные о состоянии обновления	✔	✔
Настройка конфигурации		✔
Запуск активации		✔
Запуск сканирования	✔	✔
Запуск обновления	✔	✔

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

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

Пути приложений: определенное приложение, которому разрешается запускать процесс RMM. Если вы выбрали метод авторизации **Путь приложения**, 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 компаниейESETT программа командной строки, которая позволяет управлять продуктами для конечных точек и обмениваться данными с любым подключаемым модулем RMM.

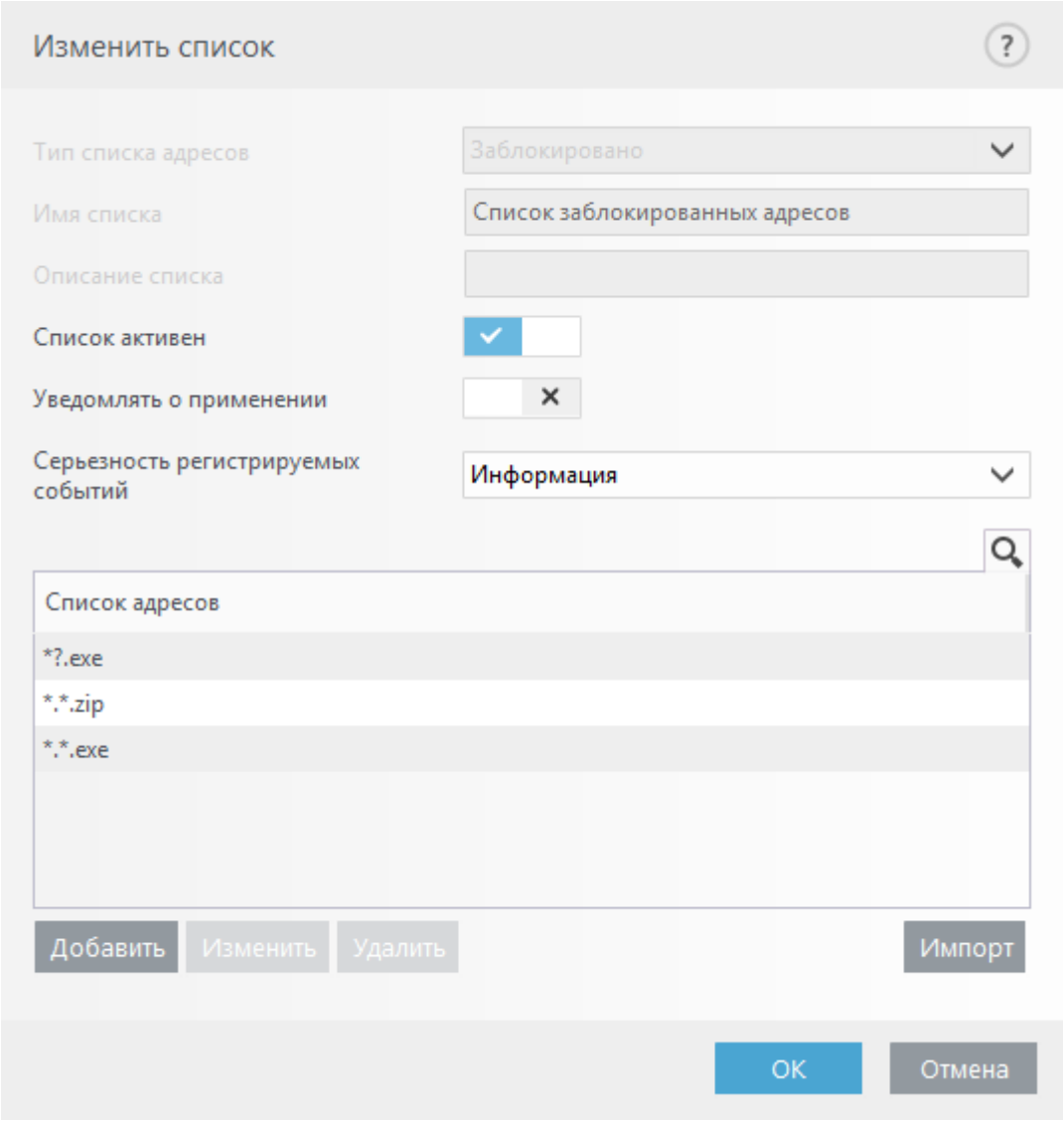
• Подключаемый модуль RMM — это стороннее приложение, работающее локально в системе Endpoint Windows. Он предназначен для обмена данными с определенным агентом RMM (например, только Kaseya) и с исполняемым файлом ermm.exe.

• 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.

Блокировка загрузки файлов определенного типа из Интернета

Если вы не хотите разрешать загрузку определенных типов файлов (например, EXE, PDF или ZIP) из Интернета, используйте Управление URL-адресами с комбинацией подстановочных символов. Нажмите клавишу F5, чтобы перейти в раздел «**Расширенные параметры**». Выберите «**Интернет и электронная почта** > **Защита доступа в Интернет**» и разверните ветку «**Управление URL-адресами**». Щелкните «**Изменить»** рядом со **списком адресов**.

В окне **«Список адресов»** выберите **«Список заблокированных адресов»** и нажмите кнопку **«Редактировать»** или **«Добавить»**, чтобы создать новый список. Откроется новое окно. Если вы создаете новый список, выберите **«Заблокировано»** в раскрывающемся меню **«Тип списка адресов»** и назовите список. Если вы хотите получать уведомления о доступе к типу файла из текущего списка, включите **оповещение при применени**и ползунка. В раскрывающемся меню выберите **«Серьезность регистрируемых событий»**. Удаленный администратор может собирать записи согласно с требованиями об уровне **предупреждений**.



Щелкните «**Добавить**», чтобы задать маску, определяющую типы файлов, которые вы хотите заблокировать при загрузке. Введите полный URL-адрес, если необходимо заблокировать загрузку определенного файла с определенного веб-сайта, например *http://example.com/file.exe*. Вы можете использовать подстановочные знаки для охвата группы файлов. Вопросительный знак (?) представляет собой единственный символ, тогда как звездочка (*) представляет собой строку любых символов произвольной длины. Например, маска **/*.zip* позволяет заблокировать загрузку любых ZIP-файлов.

Обратите внимание, что вы можете блокировать загрузку файлов определенного типа из Интернета с помощью этого метода только в том случае, если расширение файла входит в URL-адрес файла. Если на веб-странице используются URL-адреса для загрузки, например *www.example.com/download.php?fileid=42*, файл, к которому ведет эта ссылка, будет загружен, даже если его расширение заблокировано.

Сведения о свертывании ESET Endpoint Security

При удаленном управлении вы можете применить предварительно заданную политику «Видимость».

В противном случае выполните эти действия вручную:

1. Нажмите **F5**, чтобы получить доступ к расширенным параметрам, и разверните страницу **Интерфейс** > **Элементы интерфейса**.

2. Установите нужное значение для **Режима запуска**. Дополнительные сведения о режимах запуска.

3. Отключите функции **Показывать заставку при запуске** и **Использовать звуки**.

4. Настройте уведомления.

5. Настройте состояния приложения.

6. Настройте сообщения подтверждения.

7. Настройте окна предупреждений и сообщений.

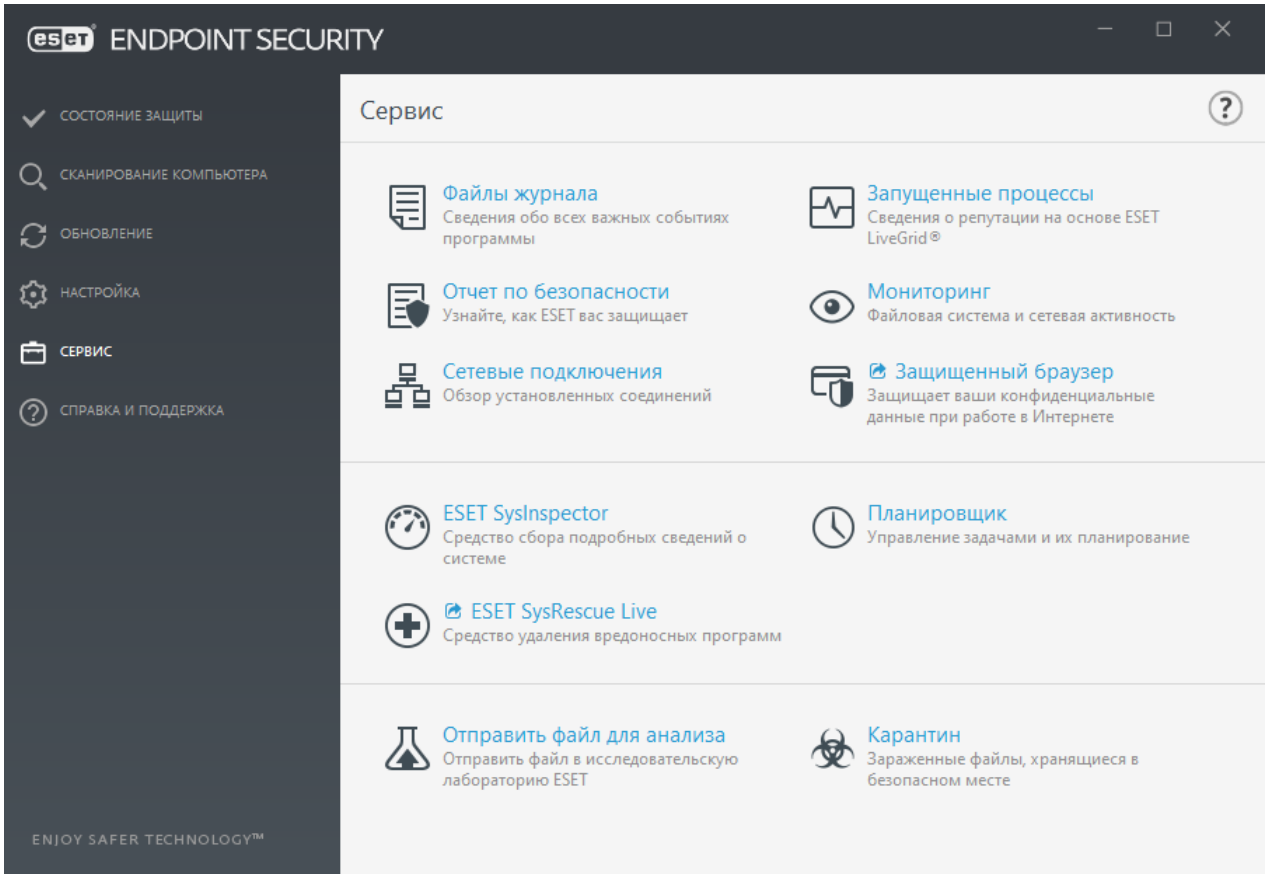
Устранение ошибки «Не удалось перенаправить защищенный браузер на запрошенную веб-страницу»

Чтобы устранить эту ошибку, воспользуйтесь приведенными далее инструкциями.

> **После выполнения каждого шага проверяйте, работает ли защищенный браузер.**
> Если окно браузера все равно не работает, выполните следующий шаг.

1. Откройте главное окно своего продукта ESET.

2. Щелкните **Инструменты** > **Защищенный браузер**. Когда откроется окно «Защищенный браузер», перейдите к следующему этапу.



3. Очистите кэш браузера. Как очистить кэш в Firefox или в Google Chrome?

4. Убедитесь, что используете новейшие версии операционной системы Windows и бизнес-продукта ESET для Windows: проверить наличие последней версии продукта ESET для бизнеса.

5. Отключите защищенный браузер и перезапустите компьютер. Повторно включите защищенный браузер и попробуйте запустить его окно.

6. Проверьте, не добавлен ли ваш браузер в список исключенных в разделе **Расширенные параметры** > **Интернет и электронная почта** > **Фильтрация протоколов** > **Исключенные приложения**.

7. Возможно, возник конфликт со сторонним защитным программным обеспечением или файерволом. Возможно, следует проверить такое программное обеспечение или удалить его в окне установки и удаления программ.

8. Если вы не обновляли продукт ESET на предыдущих этапах, удалите и повторно установите его. После перезагрузки компьютера выключите и снова включите функцию «Защищенный браузер».

Защищенный браузер — это дополнительный уровень безопасности, разработанный для защиты ваших финансовых данных при осуществлении финансовых операций в Интернете.

В большинстве случаев защищенный браузер запускается в используемом по умолчанию браузере, когда вы посещаете известный веб-сайт интернет-банкинга. Чтобы открыть защищенный браузер непосредственно, щелкните элемент **Инструменты** в ESET Endpoint

Security, а потом щелкните элемент **Защищенный браузер**.

Дополнительные сведения о функции «Защищенный браузер» см. в статьях базы знаний ESET, доступных на английском и некоторых других языках.

- Как использовать Защищенный браузер ESET?
- Включение и отключение защиты банковской оплаты ESET для определенного веб-сайта
- Приостановка и отключение функции «Защита банковской оплаты» в продуктах ESET для Windows для домашнего использования
- Защита банковской оплаты ESET — распространенные ошибки
- Глоссарий ESET | Защита банковской оплаты

Если вы все еще не можете решить проблему, отправьте сообщение электронной почты в службу технической поддержки ESET.

Лицензионное соглашение с конечным пользователем

ВАЖНО! Внимательно прочитайте изложенные далее условия использования программного продукта, прежде чем загружать, устанавливать, копировать или использовать его. **ЗАГРУЖАЯ, УСТАНАВЛИВАЯ, КОПИРУЯ ИЛИ ИСПОЛЬЗУЯ ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВЫ ВЫРАЖАЕТЕ СВОЕ СОГЛАСИЕ С ИЗЛОЖЕННЫМИ УСЛОВИЯМИ И С ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ.**

Лицезионное соглашение с конечным пользователем

Согласно условиям данного Лицензионного соглашения с конечным пользователем (далее — «Соглашение»), заключенного компанией ESET, spol. s r. o., зарегистрированной по адресу Einsteinova 24, 851 01 Bratislava, Slovak Republic, внесенной в коммерческий регистр окружного суда Bratislava I, раздел Sro, запись № 3586/B, BIN 31333532 (далее — «ESET» или «Поставщик»), и вами, физическим или юридическим лицом (далее — «Вы» или «Конечный пользователь»), вы получаете право использовать Программное обеспечение, указанное в статье 1 настоящего Соглашения. Программное обеспечение, указанное в статье 1 настоящего Соглашения, может храниться на носителях данных, отправляться по электронной почте, загружаться через Интернет, загружаться с серверов Поставщика или получаться из других источников, которые удовлетворяют перечисленным ниже условиям.

ЭТО СОГЛАШЕНИЕ КАСАЕТСЯ ПРАВ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ И НЕ ЯВЛЯЕТСЯ ДОГОВОРОМ ПРОДАЖИ. Поставщик остается владельцем экземпляра Программного обеспечения и материального носителя, на котором Программное обеспечение было поставлено в торговой упаковке, а также всех копий Программного обеспечения, на которые Конечный пользователь имеет право в соответствии с настоящим Соглашением.

Выбор варианта «Принимаю» в процессе установки, загрузки, копирования или использования

этого Программного обеспечения выражает Ваше согласие с условиями настоящего Соглашения. Если Вы не согласны с каким-либо из условий этого Соглашения, немедленно выберите вариант «Не принимаю», отмените установку или загрузку, уничтожьте или верните Программное обеспечение, установочные носители, сопроводительную документацию, а также квитанцию об оплате в компанию ESET или в организацию, в которой было приобретено Программное обеспечение.

ИСПОЛЬЗОВАНИЕ ВАМИ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЗНАЧАЕТ, ЧТО ВЫ ПРОЧЛИ ДАННОЕ СОГЛАШЕНИЕ, ПОНЯЛИ ЕГО ПОЛОЖЕНИЯ И СОГЛАСНЫ СЧИТАТЬ ИХ ОБЯЗЫВАЮЩИМИ.

1. **Программное обеспечение.** Термин "Программное обеспечение" в настоящем Соглашении означает: (i) компьютерную программу, которая сопровождается настоящим Соглашением, и все ее компоненты; (ii) все содержимое на дисках, компакт-дисках, DVD-дисках, в электронных сообщениях и каких-либо вложениях или на других носителях, которые были поставлены вместе с настоящим Соглашением, в том числе форму объектного кода Программного обеспечения, поставляемую на носителе данных, по электронной почте или загружаемую через Интернет; (iii) любые пояснительные материалы или любую другую возможную документацию, связанную с Программным обеспечением, главным образом какое-либо описание Программного обеспечения, его спецификации, какое-либо описание свойств или работы Программного обеспечения, какое-либо описание рабочей среды, в которой используется Программное обеспечение, инструкции по использованию или установке Программного обеспечения или какое-либо описание использования Программного обеспечения (далее — Документация); (iv) копии Программного обеспечения, пакеты исправления возможных ошибок Программного обеспечения, дополнения к Программному обеспечению, расширения Программного обеспечения, измененные версии Программного обеспечения и обновления компонентов Программного обеспечения (при наличии), на которые Поставщик предоставил Вам лицензию в соответствии со статьей 3 настоящего Соглашения. Программное обеспечение предоставляется исключительно в форме исполняемого объектного кода.

2. **Установка, компьютер и лицензионный ключ**. Программное обеспечение, поставляемое на носителе данных, по электронной почте, загруженное через Интернет или с серверов Поставщика или полученное из других источников, подлежит установке. Установка Программного обеспечения должна происходить на должным образом настроенном компьютере, который отвечает минимальным требованиям, изложенным в Документации. Способ установки описан в Документации. Компьютер, на котором выполняется установка, не должен содержать программное или аппаратное обеспечение, которое может негативно повлиять на работу Программного обеспечения. Компьютер означает оборудование, в том числе, среди прочего, персональные компьютеры, ноутбуки, рабочие станции, карманные компьютеры, смартфоны, карманные или другие электронные устройства, для которых разрабатывается Программное обеспечение, на котором его будут устанавливать и/или использовать. Лицензионный ключ означает уникальную последовательность символов, букв, цифр или специальных знаков, предоставляемых конечному пользователю, чтобы разрешить законно использовать Программное обеспечение или его определенную версию либо продлить срок действия Лицензии в соответствии с настоящим Соглашением.

3. **Лицензия**. Если Вы приняли все условия, предусмотренные в настоящем Соглашении, и соблюдаете их, Поставщик предоставляет Вам следующие права (далее — «Лицензия»).

a) **Установка и использование.** Вы получаете неисключительное не подлежащее передаче право установить Программное обеспечение на жесткий диск компьютера или иной носитель для хранения данных, установки и хранения Программного обеспечения в памяти компьютера,

а также внедрить, хранить и отображать Программное обеспечение.

b) **Оговорка по количеству лицензий.** Право на использование Программного обеспечения ограничено определенным количеством Конечных пользователей. Под одним Конечным пользователем подразумевается (i) установка Программного обеспечения на один компьютер или (ii) в случае ограничения лицензии количеством почтовых ящиков пользователь компьютера, который принимает электронную почту через пользовательский почтовый агент (далее — «Пользовательский почтовый агент»). Если Пользовательский почтовый агент принимает электронную почту, а затем автоматически распределяет ее среди нескольких пользователей, количество Конечных пользователей должно определяться в соответствии с фактическим количеством пользователей, получающих электронную почту. Если почтовый сервер выполняет функции почтового шлюза, количество Конечных пользователей будет равняться количеству пользователей почтового сервера, которых обслуживает этот шлюз. Если один пользователь владеет несколькими адресами электронной почты (например, при использовании псевдонимов) и принимает почту по ним, а почта не распределяется автоматически клиентом другим пользователям, необходима Лицензия только для одного компьютера. Одну Лицензию нельзя использовать одновременно на нескольких компьютерах. Конечный пользователь имеет право вводить Лицензионный ключ в Программное обеспечение только в той степени, в которой он имеет право использовать Программное обеспечение в соответствии с ограничением по количеству Лицензий, выданных Поставщиком. Лицензионный ключ считается конфиденциальной информацией. Вы не должны передавать Лицензию третьим сторонам или разрешать третьим сторонам использовать Лицензионный ключ, если это не разрешено настоящим Соглашением или Поставщиком. Если Ваш Лицензионный ключ взломан, немедленно сообщите об этом Поставщику.

c) **Выпуск для бизнеса.** Для использования Программного обеспечения на почтовых серверах, серверах ретрансляции электронной почты, почтовых шлюзах и шлюзах Интернета необходима версия Программного обеспечения для бизнеса.

d) **Срок Лицензии.** Ваше право на использование Программного обеспечения ограничено определенным сроком.

e) **Программное обеспечение, получаемое через изготовителей комплектного оборудования.** Программное обеспечение, получаемое через изготовителей комплектного оборудования, можно использовать только на том компьютере, на котором оно было получено. Такое программное обеспечение нельзя перенести на другой компьютер.

f) **Не предназначенные для продажи и пробные версии Программного обеспечения.** Программное обеспечение, классифицированное как не предназначенная для продажи или пробная версия, не может быть связано с каким-либо платежом и должно использоваться исключительно для демонстрации или тестирования функций Программного обеспечения.

g) **Прекращение действия Лицензии.** Действие Лицензии прекращается автоматически по окончании периода, на который она была выдана. Если Вы нарушаете любое положение настоящего Соглашения, Поставщик получает право выйти из него, что никак не повлияет на его возможности воспользоваться любыми правами и средствами судебной защиты, доступными ему в таких обстоятельствах. В случае отмены Лицензии Вы обязаны немедленно за собственный счет удалить, разрушить или вернуть Программное обеспечение и все его резервные копии в компанию ESET или в организацию, в которой оно было приобретено. В случае прекращения действия Лицензии Поставщик также имеет право запретить Конечному пользователю использовать функции Программного обеспечения, которые требуют подключения к серверам Поставщика или серверам третьих лиц.

4. **Функции, для которых необходим сбор данных и подключение к Интернету.** Для корректной работы Программного обеспечения необходимо подключение к Интернету, поскольку Программное обеспечение должно регулярно подключаться к серверам Поставщика или третьих лиц, а также собирать соответствующие данные в соответствии с документом Политика конфиденциальности. Подключение к Интернету необходимо для использования перечисленных далее функций Программного обеспечения.

a) **Обновление Программного обеспечения.** Поставщик имеет право время от времени выпускать обновления Программного обеспечения («Обновления»), но не обязан их предоставлять. Эта функция включена при использовании стандартных параметров Программного обеспечения. Это значит, что Обновления устанавливаются автоматически, если Конечный пользователь не отключит их автоматическую установку. Для предоставления обновлений необходима проверка подлинности лицензии, включая информацию о компьютере и/или платформе, на которой установлено Программное обеспечение, в соответствии с документом Политика конфиденциальности.

b) **Отправка зараженных файлов и информации Поставщику.** Программное обеспечение оснащено функциями, которые собирают образцы компьютерных вирусов и других вредоносных программ, а также подозрительные, проблемные, потенциально нежелательные или потенциально опасные объекты, такие как файлы, URL-адреса, IP-пакеты и кадры Ethernet (именуемые в дальнейшем «Заражения»), и отправляют их Поставщику, в том числе, среди прочего, информацию о процессе установки, о компьютере и/или платформе, на которых установлено Программное обеспечение, и/или информацию об операциях и функциональности программного обеспечения, и/или информацию об устройствах локальной сети, например сведения о типе, поставщике, модели и/или названии устройства (далее — «Информация»). Информация и Заражения могут содержать данные (в том числе случайно или непредумышленно полученные персональные данные) о Конечном пользователе или других пользователях компьютера, на котором установлено Программное обеспечение, и о файлах, пораженных Заражениями с соответствующими метаданными.

Информацию и Заражения могут собирать следующие функции Программного обеспечения:

i. Функция LiveGrid Reputation System отвечает за сбор и отправку Поставщику в одном направлении хэшей, связанных с Заражениями. Эта функция включена при использовании стандартных параметров Программного обеспечения.

ii. Система обратной связи LiveGrid отвечает за сбор и отправку Поставщику Заражений со связанными метаданными и Информации. Конечный пользователь может активировать эту функцию в процессе установки Программного обеспечения.

Поставщик обязуется использовать полученные Заражения и Информацию только для анализа и исследования Заражений, улучшения Программного обеспечения и усовершенствования проверки подлинности Лицензии, а также принять необходимые меры предосторожности по сохранению конфиденциальности Информации и Заражений. Активируя эту функцию Программного обеспечения, Вы соглашаетесь на отправку Заражений и Информации Поставщику, а также даете ему необходимое разрешение, регулируемое соответствующими правовыми нормами, на обработку полученной Информации. Данную функцию можно отключить в любой момент.

Для целей настоящего Соглашения необходимо собирать, обрабатывать и хранить данные, позволяющие Поставщику идентифицировать Вас в соответствии с документом Политика конфиденциальности. Настоящим Вы подтверждаете, что Поставщик с помощью своих средств

может проверять, используете ли Вы Программное обеспечение в соответствии с положениями настоящего Соглашения. Вы соглашаетесь на передачу информации в процессе обмена данными между Программным обеспечением и компьютерными системами Поставщика или его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, с целью обеспечения работы и проверки возможности использования Программного обеспечения и защиты прав Поставщика.

После заключения этого Соглашения Поставщик или любой из его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, получат право передавать, обрабатывать и хранить важные данные, позволяющие идентифицировать Вашу личность, в целях оплаты и исполнения настоящего Соглашения, а также для отправки уведомлений на Ваш компьютер. Настоящим Вы соглашаетесь получать уведомления и сообщения в отношении продукта, в том числе информацию рекламного характера.

Сведения о конфиденциальности, защите персональных данных и Ваших правах как субъекта персональных данных приведены в Политике конфиденциальности, которая доступна на веб-сайте Поставщика, а также непосредственно в процессе установки. Вы также можете открыть ее из справки Программного обеспечения.

5. **Использование прав Конечного пользователя**. Права Конечного пользователя необходимо использовать лично, либо их могут использовать Ваши сотрудники. Вы имеете право на использование Программного обеспечения только для защиты своих действий и компьютеров или компьютерных систем, на которые приобретена Лицензия.

6. **Ограничения прав.** Не разрешается копировать, распространять Программное обеспечение, извлекать его компоненты и создавать производные работы на его основе. При использовании Программного обеспечения Вы обязаны соблюдать перечисленные далее ограничения.

a) Вы можете создать одну резервную копию Программного обеспечения на носителе постоянного хранения данных при условии, что эта резервная копия не установлена и не используется ни на каком компьютере. Создание любых иных копий Программного обеспечения является нарушением этого Соглашения.

b) Вы не должны использовать, изменять, переводить или воспроизводить Программное обеспечение и передавать права на использование Программного обеспечения или копии Программного обеспечения любым способом, отличным от описанного в настоящем Соглашении.

c) Вы не должны продавать, передавать на условиях сублицензии, сдавать в аренду или передавать во временное пользование Программное обеспечение, а также использовать Программное обеспечение для предоставления коммерческих услуг.

d) Запрещается вскрывать технологию, декомпилировать или разбирать код Программного обеспечения и иными способами пытаться получить исходный код Программного обеспечения за исключением того, в чем данное ограничение противоречит действующему законодательству.

e) Вы соглашаетесь использовать Программное обеспечение только способом, соответствующим всем действующим законодательным нормам страны, в которой используется Программное обеспечение, в том числе применимым ограничениям относительно авторского права, других прав на интеллектуальную собственность и так далее.

f) Вы соглашаетесь использовать Программное обеспечение и его функции только способом, который не ограничивает возможности доступа к этим услугам других Конечных пользователей. Поставщик оставляет за собой право ограничить объем услуг, предоставляемых отдельным Конечным пользователям, чтобы обеспечить использование услуг максимально возможным числом Конечных пользователей. Ограничение объема услуг должно также означать полное прекращение возможности использовать любую из функций Программного обеспечения, а также удаление Данных и информации на серверах Поставщика или сторонних серверах, относящихся к определенной функции Программного обеспечения.

g) Вы обязуетесь не предпринимать действий, связанных с использованием Лицензионного ключа, которые противоречат условиям настоящего Соглашения или приводят к предоставлению Лицензионного ключа лицу, не имеющему права использовать Программное обеспечение, например передачу использованного или неиспользованного Лицензионного ключа в любой форме, а также несанкционированное воспроизведение или распространение дублированных или сгенерированных лицензионных ключей или использование Программного обеспечения с помощью Лицензионного ключа, полученного не от Поставщика.

7. **Авторское право**. Программное обеспечение и все права на него, в том числе, среди прочего, право собственности и права на объекты интеллектуальной собственности, принадлежат компании ESET и/или ее лицензиарам. Эти права защищены международными соглашениями и всеми прочими применимыми законодательными нормами страны, в которой используется Программное обеспечение. Внутренняя структура, устройство и код Программного обеспечения являются ценной коммерческой тайной и конфиденциальной информацией, принадлежащими компании ESET и/или ее лицензиарам. Запрещается копировать Программное обеспечение кроме случаев, описанных в статье 6(a). Любые копии, которые разрешено создать в соответствии с Соглашением, должны содержать оригинальные отметки о защите авторских прав и другие уведомления о правах интеллектуальной собственности, которые присутствуют в самом Программном обеспечении. Если Вы вскрываете технологию, декомпилируете, разбираете исходный код Программного обеспечения или иным способом пытаетесь получить исходный код Программного обеспечения в нарушение положений этого Соглашения, любая полученная таким образом информация автоматически и безоговорочно должна считаться подлежащей передаче Поставщику и принадлежащей ему полностью с момента создания вне зависимости от прав Поставщика в отношении нарушения этого Соглашения.

8. **Сохранение прав**. Настоящим Поставщик сохраняет за собой все права на Программное обеспечение, за исключением прав, явно предоставленных Вам как Конечному пользователю Программного обеспечения в соответствии с условиями настоящего Соглашения.

9. **Несколько языковых версий, программное обеспечение на носителях двух типов, несколько копий**. Если Программное обеспечение поддерживает несколько платформ или языков или если Вы получили несколько экземпляров программного обеспечения, разрешается использовать Программное обеспечение только на том количестве компьютеров и в тех версиях, на которые была приобретена Лицензия. Запрещается продавать, передавать на условиях сублицензии, сдавать в аренду, передавать во временное или постоянное пользование версии или копии Программного обеспечения, которые не используются Вами.

10. **Момент вступления в силу и прекращение действия Соглашения**. Настоящее Соглашение вступает в законную силу с дня, когда Вы согласились с его условиями. Завершить действие Соглашения можно в любой момент, необратимо удалив, разрушив или вернув за свой счет Программное обеспечение, все резервные копии и любые относящиеся к нему материалы, предоставленные Поставщиком или одним из его коммерческих партнеров.

Независимо от способа прекращения действия этого Соглашения положения статей 7, 8, 11, 13, 19 и 21 остаются действительными без ограничения по времени.

11. **ГАРАНТИИ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ**. ВЫСТУПАЯ В КАЧЕСТВЕ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ, ВЫ ПОДТВЕРЖДАЕТЕ СВОЮ ОСВЕДОМЛЕННОСТЬ В ТОМ, ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ НА УСЛОВИЯХ «КАК ЕСТЬ» БЕЗ КАКИХ-ЛИБО ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ГАРАНТИЙ ЛЮБОГО ТИПА, НАСКОЛЬКО ЭТО ПОЗВОЛЯЮТ СООТВЕТСТВУЮЩИЕ ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ. НИ ПОСТАВЩИК, НИ ЕГО ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ, НИ ПРАВООБЛАДАТЕЛИ НЕ ДЕЛАЮТ НИКАКИХ ЗАЯВЛЕНИЙ И НЕ ПРЕДОСТАВЛЯЮТ НИКАКИХ ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ОБЯЗАТЕЛЬСТВ ИЛИ ГАРАНТИЙ, В ЧАСТНОСТИ ГАРАНТИЙ ПРОДАЖ ИЛИ ГАРАНТИЙ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОГО ИСПОЛЬЗОВАНИЯ, А ТАКЖЕ ГАРАНТИЙ ТОГО, ЧТО ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ НАРУШАЕТ НИКАКИХ ПАТЕНТОВ, АВТОРСКИХ ПРАВ, ПРАВ НА ТОВАРНЫЕ ЗНАКИ И ДРУГИХ ПРАВ ТРЕТЬИХ ЛИЦ. ПОСТАВЩИК И ЛЮБЫЕ ДРУГИЕ ЛИЦА НЕ ГАРАНТИРУЮТ, ЧТО ФУНКЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БУДУТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ ИЛИ ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БУДЕТ РАБОТАТЬ БЕЗ СБОЕВ И ОШИБОК. РИСК ПРИ ВЫБОРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, А ТАКЖЕ ПРИ УСТАНОВКЕ, ИСПОЛЬЗОВАНИИ И ПОЛУЧЕНИИ РЕЗУЛЬТАТОВ, КОТОРЫХ ВЫ БУДЕТЕ ДОСТИГАТЬ С ПОМОЩЬЮ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ЛЕЖИТ НА ВАС.

12. **Отказ от других обязательств**. Настоящее Соглашение не предусматривает никаких обязательств для Поставщика и его лицензиаров за исключением тех, которые изложены в настоящем Соглашении.

13. **ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ**. В ТОЙ СТЕПЕНИ, В КОТОРОЙ ЭТО РАЗРЕШЕНО ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ПОСТАВЩИК, ЕГО СОТРУДНИКИ ИЛИ ЛИЦЕНЗИАРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКУЮ-ЛИБО УПУЩЕННУЮ ПРИБЫЛЬ, ВЫРУЧКУ, ПРОДАЖИ, ДАННЫЕ ИЛИ РАСХОДЫ НА ЗАКУПКУ ВЗАИМОЗАМЕНЯЕМЫХ ТОВАРОВ ИЛИ УСЛУГ, ПОВРЕЖДЕНИЕ ИМУЩЕСТВА, ТЕЛЕСНЫЕ ПОВРЕЖДЕНИЯ, ПРИОСТАНОВКУ РАБОТЫ, ПОТЕРЮ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ИЛИ ЗА КАКИЕ-ЛИБО ФАКТИЧЕСКИЕ, ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, ЭКОНОМИЧЕСКИЕ, КОМПЕНСИРУЕМЫЕ, ШТРАФНЫЕ, КОСВЕННЫЕ ИЛИ ПРЕДСКАЗУЕМЫЕ КОСВЕННЫЕ УБЫТКИ, НАНЕСЕННЫЕ В РЕЗУЛЬТАТЕ ВЫПОЛНЕНИЯ СОГЛАШЕНИЯ, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ ИЛИ НЕБРЕЖНОСТИ, НЕЗАВИСИМО ОТ ПРИЧИНЫ И ВИДА ОТВЕТСТВЕННОСТИ, ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ИЛИ ОТСУТСТВИЯ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПОСТАВЩИК, ЕГО ЛИЦЕНЗИАРЫ ИЛИ АФФИЛИРОВАННЫЕ ЛИЦА ОСВЕДОМЛЕНЫ О ВОЗМОЖНОСТИ ВОЗНИКНОВЕНИЯ ТАКОГО УЩЕРБА. ПОСКОЛЬКУ ЗАКОНОДАТЕЛЬСТВО НЕКОТОРЫХ СТРАН И ОТДЕЛЬНЫЕ ЗАКОНЫ НЕ РАЗРЕШАЮТ ИСКЛЮЧАТЬ ТАКУЮ ОТВЕТСТВЕННОСТЬ, НО ПОЗВОЛЯЮТ ОГРАНИЧИВАТЬ ЕЕ, В ТАКИХ СЛУЧАЯХ ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА, ЕГО СОТРУДНИКОВ, ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ ОГРАНИЧИВАЕТСЯ СУММОЙ, ВЫПЛАЧЕННОЙ ВАМИ ЗА ЛИЦЕНЗИЮ.

14. Ни одно из положений настоящего Соглашения не затрагивает законные права любой стороны, выступающей в качестве потребителя, даже если они противоречат таким правам.

15. **Техническая поддержка**. ESET или привлеченные компанией ESET третьи лица предоставляют техническую поддержку по собственному усмотрению без каких-либо гарантий или заявлений. Конечный пользователь обязан создать резервную копию всех существующих данных, программного обеспечения или программных средств, прежде чем обратиться за технической поддержкой. ESET и (или) третьи лица, привлеченные ESET, не могут принять на себя ответственность за повреждение или потерю данных, собственности, программного обеспечения или оборудования, а также за упущенную прибыль, которые связаны с

предоставлением технической поддержки. ESET и (или) привлеченные ESET третьи лица оставляют за собой право принять решение о том, что устранить конкретную проблему невозможно в рамках технической поддержки. ESET оставляет за собой право отказать в предоставлении технической поддержки, приостановить или прекратить ее оказание по своему собственному усмотрению. Сведения о лицензии, Информация и другие данные в соответствии с Политикой конфиденциальности могут потребоваться для предоставления технической поддержки.

16. **Передача лицензии**. Программное обеспечение может быть перенесено с одного компьютера на другой, если это не противоречит условиям настоящего Соглашения. Если это не противоречит условиям Соглашения, Конечный пользователь может только перманентно передать Лицензию и все права по настоящему Соглашению другому Конечному пользователю с согласия Поставщика, если соблюдаются следующие условия: (i) у первого Конечного пользователя не остается никаких экземпляров Программного обеспечения; (ii) передача прав должна быть непосредственной, т. е. от исходного Конечного пользователя к новому; (iii) новый Конечный пользователь должен принять все права и обязательства исходного Конечного пользователя по настоящему Соглашению; (iv) исходный Конечный пользователь должен предоставить новому Конечному пользователю документацию, позволяющую проверить подлинность Программного обеспечения в соответствии со статьей 17.

17. **Проверка подлинности Программного обеспечения**. Конечный пользователь может продемонстрировать наличие у него прав на использование Программного обеспечения одним из следующих способов: (i) с помощью лицензионного сертификата, выданного Поставщиком или третьим лицом, которое назначено Поставщиком; (ii) письменным лицензионным соглашением, если таковое было заключено; (iii) путем предоставления отправленного Поставщиком сообщения электронной почты, в котором содержатся сведения о лицензии (имя пользователя и пароль). Сведения о лицензии и идентификационные данные Конечного пользователя в соответствии с Политикой конфиденциальности могут потребоваться для проверки подлинности программного обеспечения.

18. **Предоставление лицензии органам власти и правительству США**. Программное обеспечение будет предоставлено органам власти, в том числе правительству Соединенных Штатов Америки, в соответствии с правами и ограничениями, описанными в настоящем Соглашении.

19. **Соответствие нормам регулирования внешней торговли**.

a) Вы не будете прямо или косвенно экспортировать, реэкспортировать, передавать или иным образом предоставлять Программное обеспечение кому-либо, а также не будете использовать его каким-либо образом либо иметь отношение к каким-либо действиям, в результате чего компания ESET или ее холдинговые компании, ее филиалы, филиалы ее холдинговых компаний, прочие субъекты, находящиеся под управлением ее холдинговых компаний (далее — «Аффилированные лица»), может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением. К законодательству по регулированию внешней торговли относится:

i. Любое законодательство, которое предназначено для регулирования, ограничения или введения лицензионных требований в сфере экспорта, реэкспорта или передачи товаров, программного обеспечения, технологий, услуг и которое принимается любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно

настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица (далее — «Законодательство по регулированию внешней торговли»).

ii. Любые экономические, финансовые, торговые и прочие санкции, ограничения, эмбарго, запреты на импорт или экспорт, запреты на перевод денежных средств или активов либо на предоставление услуг, а также эквивалентные меры, которые вводятся в действие любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица (далее — «Санкционное законодательство»).

b) Компания ESET имеет право приостановить выполнение своих обязательств согласно настоящим Условиям либо незамедлительно прекратить действие настоящих Условий в следующих случаях:

i. В случае, если компания ESET устанавливает, что по ее обоснованному мнению Пользователь нарушил или может нарушить положения Статьи 19-a настоящего Соглашения.

ii. В случае, если Конечный пользователь и/или Программное обеспечение попадут под действие Законодательства по регулированию внешней торговли, и, как результат, компания ESET установит, что по ее обоснованному мнению продолжение выполнения своих обязательств согласно настоящему Соглашению может привести к тому, что компания ESET или ее Аффилированные лица может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением.

c) Ни одна часть настоящего Соглашения не предназначена, не может интерпретироваться или истолковываться так, чтобы побуждать либо обязывать любую его сторону действовать или воздерживаться от действий (или согласиться действовать или воздерживаться от действий) каким-либо образом, который противоречит любому применимому Законодательству по регулированию внешней торговли, преследуется или запрещается им.

20. **Уведомления**. Все уведомления, возвращаемое Программное обеспечение и документация должны быть доставлены по адресу: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Применимое законодательство**. Данное Соглашение регулируется и толкуется в соответствии с законодательством Словацкой Республики. Конечный пользователь и Поставщик согласны, что принципы коллизионного права и Конвенция Организации Объединенных Наций о договорах международной купли-продажи товаров не применяются. Вы явным образом соглашаетесь с тем, что эксклюзивная юрисдикция по решению любых споров и вопросов с Поставщиком или относительно способа использования Программного обеспечения принадлежит окружному суду I в Братиславе.

22. **Общие положения**. Если любое положение настоящего Соглашения оказывается недействительным или невыполнимым, это не отражается на действительности остальных положений Соглашения, которые по-прежнему будут действительными и выполнимыми в соответствии с указанными здесь условиями. При наличии расхождений между разными языковыми версиями настоящего Соглашения преимуществом обладает версия на английском языке. Любые поправки к настоящему Соглашению могут иметь место только в письменной форме и должны быть подписаны действующим на основе закона компетентным и уполномоченным представителем Поставщика.

Это полное Соглашение между Поставщиком и Вами относительно использования Программного обеспечения, которое заменяет все предыдущие заверения, обсуждения, гарантии или уведомления или рекламные материалы в отношении Программного обеспечения.

EULA ID: BUS-STANDARD-20-01

Политика конфиденциальности

Компания ESET, spol. s r. o., зарегистрированная по адресу Einsteinova 24, 851 01 Bratislava, Словацкая Республика, внесенная в реестр юридических лиц окружного суда I в Братиславе, раздел Sro, запись № 3586/B, регистрационный номер предприятия 31333532, в качестве оператора данных (далее — «ESET» или «Мы») стремится обеспечить прозрачность своих действий, связанных с обработкой личных данных и обеспечением конфиденциальности клиентов. Поэтому Мы публикуем Политику конфиденциальности, исключительно чтобы уведомить клиента (далее — «Конечный пользователь» или «Вы») о нижеследующем:

- Обработка персональных данных,
- Конфиденциальность данных,
- права субъекта данных.

Обработка персональных данных

Услуги, предоставляемые ESET и реализованные в нашем продукте, предоставляются в соответствии с Лицензионным соглашением с конечным пользователем (далее — «Лицензионное соглашение»), но некоторые из них могут потребовать особого внимания. Мы хотим рассказать Вам подробнее о сборе данных, связанных с предоставлением наших служб. Мы предоставляем различные услуги, описанные в Лицензионном соглашении и документации, например услугу обновления, систему ESET LiveGrid®, защиту от ненадлежащего использования данных, поддержку и т. д. Чтобы все это работало, нам необходимо собирать следующую информацию.

- обновления и другую статистику, содержащую данные о процессе установки и Вашем компьютере, в том числе тип платформы, операции и функции Наших программ, например версию ОС, характеристики оборудования, идентификаторы инсталляций и лицензий, IP- и MAC-адреса, конфигурации программ;
- Однонаправленные хеш-функции, связанные с заражениями и входящие в систему репутации ESET LiveGrid®, которая повышает эффективность решений для защиты от вредоносных программ и благодаря которой сканируемые файлы сопоставляются с элементами белого и черного списков в облаке.
- Подозрительные образцы метаданных из внешних источников в рамках системы обратной связи ESET LiveGrid®, благодаря которой ESET может мгновенно реагировать на нужды пользователей и своевременно адаптироваться под новейшие угрозы. Мы рассчитываем на то, что вы будете присылать нам:
  - зараженные элементы, такие как потенциальные образцы вирусов и прочих вредоносных программ; подозрительные, проблемные, потенциально нежелательные и небезопасные объекты, такие как исполняемые файлы, сообщения электронной почты, про которые

сообщили вы как про спам или которые выявил наш продукт;

- информацию об устройствах в локальной сети, например тип, производитель, модель и/или название;
- сведения о пользовании Интернетом, например IP-адрес, географическое расположение, пакеты IP, URL-адреса и кадры Ethernet;
- файлы аварийных дампов и их содержимое.

Мы не стремимся собирать какие-либо данные, кроме обозначенных выше, но иногда этого невозможно избежать. Случайно собранные данные могут входить в состав вредоносных программ (будучи собранными без вашего ведома и одобрения) либо входить в имена файлов и URL-адреса, и Мы не намерены делать их частью наших систем или обрабатывать их для целей, указанных в настоящей Политике конфиденциальности.

- Сведения о лицензиях, например идентификаторы лицензий, и личные данные, например имя, фамилия, адрес, электронная почта, необходимые для выставления счетов, проверки подлинности лицензий и предоставления наших услуг.
- Для обслуживания и предоставления поддержки может потребоваться контактная информация и данные, указанные в Ваших запросах на поддержку. Исходя из выбранного способа общения, Мы можем фиксировать Ваш электронный адрес, номер телефона, информацию о лицензии, сведения о программах и описание Вашего инцидента. Возможно, служба поддержки попросит Вас предоставить дополнительную информацию, чтобы упростить решение проблемы.

Конфиденциальность данных

ESET — это международная компания. Наша сеть распространения, обслуживания и поддержки состоит из аффилированных лиц и партнеров. Мы можем обмениваться информацией, которую обрабатывает ESET, с аффилированными лицами для выполнения соглашений EULA, например для предоставления поддержки или выставления счетов. В зависимости от Вашего расположения и выбранной услуги Нам, возможно, потребуется передать Ваши данные в страну, в которой не действуют нормативы Европейской Комиссии. Даже в этом случае сведения передаются лишь при необходимости и в соответствии с законодательством в сфере защиты данных. Во всех случаях без исключения должны применяться стандартные контрактные условия, обязательные корпоративные правила или другие соответствующие средства защиты.

Мы стремимся хранить данные не дольше, чем это необходимо для предоставления услуг в соответствии с Лицензионным соглашением. Длительность нашего периода хранения может превышать срок действия вашей лицензии — это дает Вам возможность простого и удобного продления. Сведенная к минимуму и анонимизированная статистика, а также прочие данные системы ESET LiveGrid® могут в дальнейшем обрабатываться в статистических целях.

ESET проводит соответствующие технические и организационные мероприятия, чтобы гарантировать уровень безопасности согласно возможным рискам. Мы делаем все возможное для непрерывного обеспечения конфиденциальности, целостности, доступности и устойчивости систем и служб обработки. Однако, если произойдет утечка данных, которая будет угрожать Вашим правам и свободам, Мы готовы уведомить органы по надзору, а также субъекты данных. Как субъект данных Вы имеете право подать жалобу в наблюдательный орган.

Права субъекта данных

ESET действует согласно словацким законам и законам о защите данных ЕС. Согласно условиям, которые определены действующим законодательством по защите данных, Вы как субъект данных имеете следующие права:

- запросить доступ к своим персональным данным, которыми располагает ESET;
- запросить исправление неточных данных (у Вас также есть право на дополнение неполных данных);
- запросить уничтожение своих персональных данных;
- запросить ограничение обработки своих персональных данных;
- право на запрет обработки данных;
- право на подачу жалобы, а также
- запросить переносимость данных.

Мы считаем, что все обрабатываемые нами сведения являются ценными и необходимыми для реализации наших законных интересов, которые заключаются в предоставлении услуг и продуктов нашим клиентам.

Если Вы хотите воспользоваться своими правами субъекта данных или у Вас возникнет вопрос или проблема, отправьте нам письмо по адресу:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk