

# ESET Endpoint Antivirus

## Руководство пользователя

[Щелкните здесь чтобы отобразить этого документа \(онлайн-справка\)](#)

Авторское право ©2024 ESET, spol. s r.o.

ESET Endpoint Antivirus 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. 12.04.2024

|   |           |
|---|-----------|
| <b>1 ESET Endpoint Antivirus</b>  | <b>1</b>  |
| <b>1.1 Новые возможности</b>  | <b>2</b>  |
| <b>1.2 Требования к системе</b>   | <b>3</b>  |
| 1.2 Поддерживаемые языки  | 4         |
| <b>1.3 Журналы изменений</b>  | <b>5</b>  |
| <b>1.4 Профилактика</b>   | <b>6</b>  |
| <b>1.5 Страницы справочной системы</b>  | <b>7</b>  |
| <b>2 Документация по конечным точкам под удаленным управлением</b>                                  | <b>8</b>  |
| <b>2.1 Знакомство с ESET PROTECT</b>  | <b>10</b> |
| <b>2.2 Знакомство с ESET PROTECT Cloud</b>  | <b>11</b> |
| <b>2.3 Защищенные паролем параметры</b>   | <b>12</b> |
| <b>2.4 Что такое политики</b>   | <b>13</b> |
| 2.4 Объединение политик   | 13        |
| <b>2.5 Принцип действия флажков</b>   | <b>14</b> |
| <b>3 Установка</b>  | <b>15</b> |
| <b>3.1 Установка с помощью средства ESET AV Remover</b>   | <b>16</b> |
| 3.1 ESET AV Remover   | 17        |
| 3.1 Ошибка во время удаления с помощью средства ESET AV Remover                                     | 19        |
| <b>3.2 Установка (.exe)</b>   | <b>20</b> |
| 3.2 Изменение папки установки (.exe)  | 21        |
| <b>3.3 Установка (.msi)</b>   | <b>21</b> |
| 3.3 Расширенная установка (.msi)  | 23        |
| <b>3.4 Минимальная установка модулей</b>  | <b>24</b> |
| <b>3.5 Установка с помощью командной строки</b>   | <b>25</b> |
| <b>3.6 Развертывание с помощью GPO или SCCM</b>   | <b>30</b> |
| <b>3.7 Обновление до новой версии</b>   | <b>32</b> |
| 3.7 Автоматическое обновление устаревшей версии продукта  | 33        |
| <b>3.8 Обновления для обеспечения безопасности и стабильности</b>                                   | <b>33</b> |
| <b>3.9 Активация программы</b>  | <b>34</b> |
| 3.9 Ввод лицензионного ключа при активации  | 35        |
| 3.9 Учетная запись ESET HUB   | 35        |
| 3.9 Использование устаревших учетных данных лицензии для активации продукта ESET для конечных точек | 36        |
| 3.9 Сбой активации  | 36        |
| 3.9 Регистрация   | 36        |
| 3.9 Ход выполнения активации  | 36        |
| 3.9 Активация выполнена   | 36        |
| <b>3.10 Распространенные проблемы, возникающие при установке</b>                                    | <b>37</b> |
| <b>4 Руководство для начинающих</b>   | <b>37</b> |
| <b>4.1 Значок на панели задач</b>   | <b>37</b> |
| <b>4.2 Сочетания клавиш</b>   | <b>38</b> |
| <b>4.3 Профили</b>  | <b>38</b> |
| <b>4.4 Контекстное меню</b>   | <b>40</b> |
| <b>4.5 Настройка обновлений</b>   | <b>40</b> |
| <b>4.6 Настройка защиты сети</b>  | <b>42</b> |
| <b>4.7 Заблокированные хэши</b>   | <b>43</b> |
| <b>5 Работа с ESET Endpoint Antivirus</b>   | <b>44</b> |
| <b>5.1 Состояние защиты</b>   | <b>45</b> |
| <b>5.2 Сканирование компьютера</b>  | <b>48</b> |
| 5.2 Средство запуска выборочного сканирования   | 51        |
| 5.2 Ход сканирования  | 53        |

|  |           |
|--|-----------|
| 5.2 Журнал проверки сканирования компьютера .....                          | 55        |
| <b>5.3 Обновление .....</b>  | <b>57</b> |
| 5.3 Создание задач обновления .....  | 60        |
| <b>5.4 Настройка .....</b>   | <b>60</b> |
| 5.4 Компьютер .....  | 61        |
| 5.4 Обнаружение угрозы .....   | 63        |
| 5.4 Сеть .....   | 65        |
| 5.4 Устранение неполадок с доступом к сети .....                           | 66        |
| 5.4 Временный черный список IP-адресов .....                               | 67        |
| 5.4 Журналы защиты сети .....  | 68        |
| 5.4 Решение проблем с функцией защиты сети ESET .....                      | 68        |
| 5.4 Ведение журнала и создание правил и исключений на основе журнала ..... | 69        |
| 5.4 Создание правил на основе журнала .....                                | 69        |
| 5.4 Расширенное ведение журналов для защиты сети .....                     | 69        |
| 5.4 Решение проблем со сканером сетевого трафика .....                     | 70        |
| 5.4 Сетевая угроза заблокирована .....                                     | 71        |
| 5.4 Интернет и электронная почта .....                                     | 72        |
| 5.4 Защита от фишинга .....  | 73        |
| 5.4 Импорт и экспорт параметров .....                                      | 74        |
| <b>5.5 Служебные программы .....</b>                                       | <b>75</b> |
| 5.5 Файлы журналов .....   | 76        |
| 5.5 Фильтрация журнала .....   | 79        |
| 5.5 Журналы аудита .....   | 80        |
| 5.5 Запущенные процессы .....  | 81        |
| 5.5 Отчет по безопасности .....  | 83        |
| 5.5 ESET SysInspector .....  | 84        |
| 5.5 Планировщик .....  | 85        |
| 5.5 Параметры сканирования по расписанию .....                             | 87        |
| 5.5 Обзор запланированных задач .....                                      | 88        |
| 5.5 Сведения о задаче .....  | 88        |
| 5.5 Время задачи .....   | 89        |
| 5.5 Время выполнения задачи: однократно .....                              | 89        |
| 5.5 Время выполнения задачи: ежедневно .....                               | 89        |
| 5.5 Время выполнения задачи: еженедельно .....                             | 89        |
| 5.5 Время выполнения задачи: при определенных условиях .....               | 90        |
| 5.5 Пропущенная задача .....   | 90        |
| 5.5 Сведения о задаче: обновление .....                                    | 90        |
| 5.5 Сведения о задаче: запуск приложения .....                             | 91        |
| 5.5 Отправка образцов на анализ .....                                      | 91        |
| 5.5 Выбор образца для анализа — подозрительный файл .....                  | 92        |
| 5.5 Выбор образца для анализа — подозрительный сайт .....                  | 92        |
| 5.5 Выбор образца для анализа — ложно обнаруженный файл .....              | 93        |
| 5.5 Выбор образца для анализа — ложно обнаруженный сайт .....              | 93        |
| 5.5 Выбор образца для анализа — другое .....                               | 94        |
| 5.5 Карантин .....   | 94        |
| <b>5.6 Справка и поддержка .....</b>                                       | <b>96</b> |
| 5.6 О программе ESET Endpoint Antivirus .....                              | 96        |
| 5.6 Отправка данных о конфигурации системы .....                           | 97        |
| 5.6 Служба технической поддержки .....                                     | 98        |
| <b>6 Дополнительные настройки .....</b>                                    | <b>98</b> |
| <b>6.1 Модуль обнаружения .....</b>  | <b>99</b> |

|  |     |
|--|-----|
| 6.1 Исключения   | 100 |
| 6.1 Исключения для быстрогодействия  | 100 |
| 6.1 Добавление или изменение исключений для быстрогодействия                                   | 102 |
| 6.1 Формат исключения пути   | 103 |
| 6.1 Исключения из обнаружения  | 104 |
| 6.1 Добавление или изменение исключений из обнаружения   | 107 |
| 6.1 Создание исключения из обнаружения мастера   | 108 |
| 6.1 Модуль обнаружения расширенных параметров  | 109 |
| 6.1 Сканер сетевого трафика  | 109 |
| 6.1 Защита на основе облака  | 109 |
| 6.1 Фильтр «Исключение» для защиты на основе облака  | 113 |
| 6.1 Процессы сканирования вредоносных программ   | 113 |
| 6.1 Профили сканирования   | 114 |
| 6.1 Объекты сканирования   | 115 |
| 6.1 Сканирование в состоянии простоя   | 115 |
| 6.1 Сканирование в состоянии простоя   | 116 |
| 6.1 сканирование при запуске   | 116 |
| 6.1 Автоматическая проверка файлов при запуске системы   | 117 |
| 6.1 Съёмные носители   | 117 |
| 6.1 Защита документов  | 118 |
| 6.1 Система HIPS (система предотвращения вторжений на узел)                                    | 119 |
| 6.1 Исключения системы HIPS  | 122 |
| 6.1 Расширенные параметры HIPS   | 122 |
| 6.1 Драйверы, загрузка которых разрешена всегда  | 123 |
| 6.1 Интерактивное окно HIPS  | 123 |
| 6.1 Потенциальное поведение Программ-вымогателей обнаружено                                    | 125 |
| 6.1 Управление правилами HIPS  | 125 |
| 6.1 Параметры правил HIPS  | 126 |
| 6.1 Добавление пути к приложению или реестру для системы HIPS                                  | 129 |
| <b>6.2 Обновление</b>  | 129 |
| 6.2 Откат обновления   | 133 |
| 6.2 Обновление программы   | 134 |
| 6.2 Параметры подключения  | 135 |
| 6.2 Зеркало обновлений   | 137 |
| 6.2 HTTP-сервер и SSL для зеркала  | 139 |
| 6.2 Обновление с зеркала   | 139 |
| 6.2 Устранение проблем при обновлении с зеркала  | 141 |
| <b>6.3 Защита</b>  | 142 |
| 6.3 Защита в режиме реального времени  | 147 |
| 6.3 Исключения для процессов   | 149 |
| 6.3 Добавление или изменение исключений процессов  | 150 |
| 6.3 Момент изменения конфигурации защиты в режиме реального времени                            | 150 |
| 6.3 Проверка модуля защиты в режиме реального времени  | 151 |
| 6.3 Решение проблем, возникающих при работе защиты файловой системы в режиме реального времени | 151 |
| 6.3 Защита доступа к сети  | 152 |
| 6.3 Профили сетевых подключений  | 153 |
| 6.3 Добавление и изменение профилей сетевых подключений  | 154 |
| 6.3 Активаторы   | 155 |
| 6.3 Наборы IP-адресов  | 156 |
| 6.3 Редактирование наборов IP-адресов  | 157 |
| 6.3 Защита от сетевых атак (IDS)   | 158 |

|   |            |
|---|------------|
| 6.3 Правила IDS .....                                       | 158        |
| 6.3 Защита от атак методом подбора .....                    | 161        |
| 6.3 Правила .....   | 161        |
| 6.3 Исключения .....  | 164        |
| 6.3 Расширенные параметры .....                             | 164        |
| 6.3 SSL/TLS .....   | 166        |
| 6.3 Правила сканирования приложений .....                   | 168        |
| 6.3 Правила сертификата .....                               | 169        |
| 6.3 Зашифрованный сетевой трафик .....                      | 170        |
| 6.3 Защита почтового клиента .....                          | 170        |
| 6.3 Защита транспортного уровня .....                       | 170        |
| 6.3 Исключенные приложения .....                            | 172        |
| 6.3 Исключенные IP-адреса .....                             | 173        |
| 6.3 Защита почтового ящика .....                            | 174        |
| 6.3 Интеграции .....  | 175        |
| 6.3 Панель инструментов Microsoft Outlook .....             | 175        |
| 6.3 Окно подтверждения .....                                | 176        |
| 6.3 Повторно сканировать сообщения .....                    | 176        |
| 6.3 Реагирование .....                                      | 176        |
| 6.3 ThreatSense .....                                       | 177        |
| 6.3 Защита доступа в Интернет .....                         | 180        |
| 6.3 Исключенные приложения .....                            | 182        |
| 6.3 Исключенные IP-адреса .....                             | 182        |
| 6.3 Управление списком URL-адресов .....                    | 183        |
| 6.3 Список адресов .....                                    | 185        |
| 6.3 Создание списка адресов .....                           | 186        |
| 6.3 Как добавить маску URL-адреса .....                     | 187        |
| 6.3 Сканирование трафика HTTP(S) .....                      | 187        |
| 6.3 ThreatSense .....                                       | 188        |
| 6.3 Контроль устройств .....                                | 191        |
| 6.3 Редактор правил для контроля устройств .....            | 192        |
| 6.3 Обнаруженные устройства .....                           | 193        |
| 6.3 Добавление правил контроля устройств .....              | 193        |
| 6.3 Группы устройств .....                                  | 196        |
| 6.3 ThreatSense .....                                       | 198        |
| 6.3 Уровни очистки .....                                    | 201        |
| 6.3 Исключенные из сканирования расширения файлов .....     | 201        |
| 6.3 Дополнительные параметры ThreatSense .....              | 202        |
| <b>6.4 Служебные программы .....</b>                        | <b>203</b> |
| 6.4 Временные интервалы .....                               | 203        |
| 6.4 Центр обновления Microsoft Windows® .....               | 204        |
| 6.4 Диалоговое окно — обновление операционной системы ..... | 205        |
| 6.4 Информация об обновлениях .....                         | 205        |
| 6.4 ESET CMD .....  | 205        |
| 6.4 Удаленный мониторинг и управление .....                 | 208        |
| 6.4 Командная строка ERMM .....                             | 209        |
| 6.4 Список команд ERMM JSON .....                           | 210        |
| 6.4 получить состояние защиты .....                         | 211        |
| 6.4 получить сведения о приложении .....                    | 212        |
| 6.4 получить сведения о лицензии .....                      | 214        |
| 6.4 получить журналы .....                                  | 214        |

|   |            |
|---|------------|
| 6.4 получить состояние активации .....  | 215        |
| 6.4 получить сведения о сканировании .....  | 216        |
| 6.4 получить конфигурацию .....   | 217        |
| 6.4 получить состояние обновления .....   | 218        |
| 6.4 запуск сканирования .....   | 219        |
| 6.4 запуск активации .....  | 219        |
| 6.4 запуск деактивации .....  | 220        |
| 6.4 запуск обновления .....   | 221        |
| 6.4 настройка конфигурации .....  | 221        |
| 6.4 Проверка лицензии с интервалом .....  | 222        |
| 6.4 Файлы журнала .....   | 222        |
| 6.4 Режим презентации .....   | 224        |
| 6.4 Диагностика .....   | 224        |
| 6.4 Служба технической поддержки .....  | 226        |
| <b>6.5 Подключение .....</b>  | <b>226</b> |
| <b>6.6 Интерфейс пользователя .....</b>   | <b>227</b> |
| 6.6 Элементы интерфейса .....   | 228        |
| 6.6 Настройка доступа .....   | 229        |
| 6.6 Пароль для доступа к расширенным параметрам .....   | 230        |
| 6.6 Пароль .....  | 231        |
| 6.6 Безопасный режим .....  | 231        |
| <b>6.7 Уведомления .....</b>  | <b>231</b> |
| 6.7 Состояния приложения .....  | 232        |
| 6.7 Уведомления на рабочем столе .....  | 233        |
| 6.7 Настройка уведомлений .....   | 235        |
| 6.7 Диалоговое окно «Уведомления на рабочем столе» .....  | 235        |
| 6.7 Интерактивные предупреждения .....  | 236        |
| 6.7 Список интерактивных предупреждений .....   | 238        |
| 6.7 Подтверждения .....   | 239        |
| 6.7 Ошибка «Конфликт дополнительных настроек» .....   | 240        |
| 6.7 Требуется перезагрузка .....  | 240        |
| 6.7 Рекомендуется перезагрузка .....  | 241        |
| 6.7 Переадресация .....   | 241        |
| 6.7 Восстановление всех параметров по умолчанию .....   | 244        |
| 6.7 Восстановление всех параметров в этом разделе .....   | 244        |
| 6.7 При сохранении конфигурации произошла ошибка .....  | 244        |
| <b>6.8 Сканер командной строки .....</b>  | <b>245</b> |
| <b>7 Часто задаваемые вопросы .....</b>   | <b>247</b> |
| <b>7.1 Вопросы и ответы по автоматическому обновлению .....</b>   | <b>248</b> |
| <b>7.2 Выполнение обновления ESET Endpoint Antivirus .....</b>  | <b>252</b> |
| <b>7.3 Удаление вируса с компьютера .....</b>   | <b>252</b> |
| <b>7.4 Создание задачи в планировщике .....</b>   | <b>253</b> |
| 7.4 Планирование еженедельного сканирования компьютера .....  | 254        |
| <b>7.5 Подключение ESET Endpoint Antivirus к ESET PROTECT .....</b>   | <b>254</b> |
| 7.5 Использование режима переопределения .....  | 254        |
| 7.5 Применение рекомендуемой политики для ESET Endpoint Antivirus .....   | 256        |
| <b>7.6 Настройка зеркала .....</b>  | <b>259</b> |
| <b>7.7 Как мне обновить свою систему до Windows 10, если у меня установлен продукт ESET Endpoint Antivirus? .....</b> | <b>260</b> |
| <b>7.8 Активация удаленного мониторинга и управления .....</b>  | <b>260</b> |
| <b>7.9 Блокировка загрузки файлов определенного типа из Интернета .....</b>   | <b>262</b> |

|   |     |
|---|-----|
| 7.10 Сведения о свертывании ESET Endpoint Antivirus ..... | 264 |
| 8 Лицензионное соглашение с конечным пользователем .....  | 264 |
| 9 Политика конфиденциальности .....                       | 274 |



# ESET Endpoint Antivirus

ESET Endpoint Antivirus представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Новейшая версия антивирусного ядра ESET LiveGrid® 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 Antivirus — это комплексное решение для обеспечения безопасности, созданное благодаря нашим долгосрочным усилиям и сочетающее максимальную защиту с минимальным влиянием на работу системы. 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 Antivirus предназначено в первую очередь для рабочих станций в среде небольших предприятий.

В разделе [Установка](#) представлены справочные статьи с разделами и подразделами, в которых можно найти необходимые сведения, в том числе о [загрузке](#), [установке](#) и [активации](#).

[Использование ESET Endpoint Antivirus 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

|                             |  |
|-----------------------------|--|
| <b>Улучшенный интерфейс</b> | 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 Antivirus и содержит динамически обновляемые статьи по поддержке. |
| <b>Темный режим</b>         | Расширение, с помощью которого можно быстро включить темную тему для экрана. Предпочитаемую цветовую схему можно выбрать в разделе <a href="#">Элементы интерфейса</a> .   |

|  |  |
|--|--|
| <b>Защита от вирусов и шпионских программ</b>                      | Упреждающее обнаружение и очистка большого количества известных и неизвестных вирусов, <a href="#">червей</a> , <a href="#">троянских программ</a> и <a href="#">руткитов</a> . Метод расширенной эвристики идентифицирует даже ранее 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 <a href="#">защиты от фишинга</a> 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). |
| <b>Регулярные обновления</b>                                       | Регулярное обновление модуля обнаружения (ранее известного, как база данных сигнатур вирусов) и программных модулей — лучший способ обеспечить максимальный уровень безопасности компьютера.   |
| <b>ESET LiveGrid® (репутация на основе облака)</b>                 | Вы можете проверить репутацию запущенных процессов и файлов непосредственно с помощью ESET Endpoint Antivirus.   |
| <b>Удаленное управление</b>  | 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 (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.  |
| <b>Защита от сетевых атак</b>                                      | Анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который расценивается как опасный, блокируется.  |
| <b>Контроль доступа в Интернет (только ESET Endpoint Security)</b> | Контроль 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

### Новые возможности в ESET Endpoint Antivirus версии 10.1

#### Intel® Threat Detection Technology

Аппаратная технология, которая выявляет программы-вымогатели, когда они пытаются избежать обнаружения в памяти. Интеграция этой технологии повышает защиту от программ-вымогателей и поддерживает общую производительность системы на высоком уровне. См. информацию о [поддерживаемых процессорах](#).

#### Темный режим и измененный дизайн интерфейса

Графический интерфейс в этой версии был изменен и модернизирован. Благодаря добавлению темного режима вы можете выбрать светлую или темную цветовую схему для графического интерфейса ESET Endpoint Antivirus в разделе [Элементы интерфейса](#).

## Переработанный раздел «Расширенные параметры»

Раздел [Расширенные параметры](#) был переработан, в результате чего настройки сгруппированы так, чтобы улучшить работу пользователя.

## Различные исправления ошибок и улучшения производительности

# Требования к системе

Для правильной работы ESET Endpoint Antivirus 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  
процессор ARM64, 1 ГГц и выше


## Операционные системы

Microsoft® Windows® 11

Microsoft® Windows® 10

 Подробный список поддерживаемых версий Microsoft® Windows® 10 и Microsoft® Windows® 11 см. в [политике поддержки операционной системы Windows](#).

 Регулярно обновляйте операционную систему.

 Для установки или обновления продуктов ESET, выпущенных после июля 2023 года, во всех операционных системах Windows должна быть установлена поддержка подписывания кода Azure. [Дополнительные сведения](#).

## Требования для функций ESET Endpoint Antivirus

В таблице ниже указаны требования к системе для определенных функций ESET Endpoint Antivirus.

| Функция                             | Требования  |
|-------------------------------------|---|
| Intel® Threat Detection Technology  | См. информацию о <a href="#">поддерживаемых процессорах</a> . |
| Специализированное средство очистки | Процессор не на архитектуре ARM64.                            |
| Блокировщик эксплойтов              | Процессор не на архитектуре ARM64.                            |
| Глубокая поведенческая проверка     | Процессор не на архитектуре ARM64.                            |

**i** Установщик ESET Endpoint Antivirus, созданный в ESET PROTECT, поддерживает многосеансовый режим в ОС Windows 10 Корпоративная для виртуальных рабочих столов и в ОС Windows 10.

## 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, рекомендуем сначала провести тестирование возможностей использования на основании требований к производительности.

- i**
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 необходимо, чтобы загрузить установщик, установить продукт, хранить копию пакета для установки в данных программы и сохранять резервные копии обновлений программы, которые нужны для функции отката. Продукт может использовать больше дискового пространства при разных настройках (например, когда хранится больше резервных копий обновлений программы, дампов памяти или больших записей журнала) либо на зараженном компьютере (вследствие использования функции карантина). Рекомендуем поддерживать достаточное количество свободного дискового пространства, чтобы обеспечить возможность обновления операционной системы и продукта ESET.
  3. Хотя это и не рекомендуется, продукт можно обновить вручную со съемного носителя.

## Поддерживаемые языки

Продукт ESET Endpoint Antivirus 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 |

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

\* Продукт ESET Endpoint Antivirus 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 правом верхнем углу).

## Журналы изменений

# Профилактика

При использовании компьютера, особенно во время работы в Интернете, необходимо помнить, что ни одна система защиты от вирусов не способна полностью устранить опасность [обнаружений](#) и [удаленных атак](#). Для максимального уровня безопасности и комфорта пользователь должен правильно использовать решение для защиты от вирусов и следовать нескольким полезным правилам.

## Регулярно обновляйте систему защиты от вирусов

Согласно статистическим данным, полученным от системы ESET LiveGrid®, ежедневно появляются тысячи новых уникальных заражений. Они созданы для обхода существующих мер безопасности и приносят доход их авторам за счет других пользователей. Специалисты лаборатории ESET Virus Lab ежедневно анализируют такие угрозы, подготавливают и выпускают обновления для непрерывного повышения уровня защиты пользователей. Для максимальной эффективности функцию обновления необходимо правильно настроить 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 уязвимости в системе для повышения 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 Microsoft Edge, — это два примера, для которых регулярно выпускаются обновления безопасности.

## Резервное копирование важных данных

Авторов вредоносных программ обычно не беспокоят проблемы пользователей, и действия их продуктов зачастую приводят к полной неработоспособности операционной системы и потере важных данных. Необходимо регулярно создавать резервные копии своих 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

Известные и неизвестные вирусы, черви, троянские программы и руткиты обнаруживаются модулем защиты файловой системы в реальном 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

Самое полезное и эффективное правило — всегда будьте осторожны. На данный момент для работы многих заражений (их выполнения и распространения) необходимо вмешательство пользователя. Если соблюдать внимательность при открытии новых файлов, можно значительно сэкономить время и силы, которые в противном случае были бы потрачены на очистку заражений. 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 руководство пользователя ESET Endpoint Antivirus. Представленная здесь информация ознакомит вас с программным продуктом и сделает использование компьютера более безопасным.

### Начало работы

Прежде чем приступить к использованию ESET Endpoint Antivirus, обратите внимание, что данным продуктом можно [управлять удаленно с помощью ESET PROTECT](#). 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 Antivirus. Также к вашим услугам руководство по настройке и изменению основных параметров ESET Endpoint Antivirus.

## Использование страниц справочной системы ESET Endpoint Antivirus

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 Antivirus. 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   |
|-----------------------------|--|
| <b>Жирный шрифт</b>         | 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.   |
| <a href="#">Гиперссылка</a> | 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 Antivirus 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

ESET Endpoint Antivirus Решением можно управлять удаленно с помощью ESET PROTECT или ESET PROTECT Cloud.

- [Знакомство с ESET PROTECT](#)
- [Знакомство с ESET PROTECT Cloud](#)
- Решение [ESET HUB](#) — это центральная точка доступа к унифицированной платформе безопасности ESET PROTECT. Оно обеспечивает централизованное управление идентификацией, подписками и пользователями для всех модулей платформы ESET. Инструкции по активации продукта см. в разделе [Управление лицензиями ESET PROTECT](#). Решение ESET HUB полностью заменит ESET Business Account и ESET MSP Administrator.
- [ESET Business Account](#) — это портал управления лицензиями для бизнес-продуктов ESET. Ознакомьтесь с разделом [Управление лицензиями ESET PROTECT](#) для получения инструкций по активации своего продукта или воспользуйтесь [интернет-справкой ESET Business Account](#), 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](#).

## Дополнительные продукты безопасности

- [ESET Inspect](#) — 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.
- [ESET Endpoint Encryption](#) — это комплексное приложение безопасности, предназначенное для защиты данных при хранении и передаче. С помощью ESET Endpoint Encryption можно шифровать файлы, папки и сообщения электронной почты, а также создавать зашифрованные виртуальные диски, сжимать архивы и использовать настольный уничтожитель документов для безопасного удаления файлов.

## Сторонние средства удаленного управления

- [Удаленный мониторинг и управление \(RMM\)](#)

## Рекомендации

- [Подключите все конечные точки с решением ESET Endpoint Antivirus 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 Antivirus

## Практические руководства

- [Использование режима переопределения](#)
- [Развертывание ESET Endpoint Antivirus 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 угрозы, 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.

- [ESET PROTECT сервер](#) — Он управляет связью с агентами, собирает и сохраняет данные приложений в базе данных. Сервер ESET PROTECT устанавливается на сервера под управлением Windows или Linux, а также в качестве виртуального устройства.
- [Веб-консоль ESET PROTECT](#). Веб-консоль 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](#) — 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.
- [ESET Rogue Detection Sensor](#) — обнаруживает неуправляемые компьютеры, присутствующие в сети, и отправляет сведения о них на сервер ESET PROTECT. Это дает возможность управлять новыми клиентскими компьютерами в ESET PROTECT без необходимости искать и добавлять их вручную. Rogue Detection Sensor запоминает компьютеры, которые были обнаружены, и не будет отправлять одну и ту же информацию дважды.
- [ESET Bridge](#) — 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.
- [Mobile Device Connector](#) — 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](#) — доступно для пользователей, которым требуется запустить ESET PROTECT в виртуализированной среде.
- [ESET PROTECT Virtual Agent Host](#) — это компонент решения ESET PROTECT, который виртуализует сущности агентов для управления виртуальными машинами, на которых нет агентов. 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](#). Выполняет развертывание комплексных пакетов, созданных в веб-консоли <%PRODUCT%>. Это удобный способ распространения агентов ESET Management с продуктом ESET на компьютерах по сети.

**i** Дополнительные сведения см. в [справке о решении ESET PROTECT в Интернете](#).

## 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 . 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.

ESET PROTECT Cloud состоит из следующих компонентов.

- [ESET PROTECT Cloud Экземпляр](#) — Он управляет связью с агентами, собирает и сохраняет данные приложений в базе данных.
- [Веб-консоль ESET PROTECT Cloud](#). Веб-консоль 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. Использовать ESET PROTECT Cloud можно в любом месте и с помощью любого устройства с подключением к Интернету.
- [ESET Management Агент](#) — облегчает обмен данными между ESET PROTECT Cloud и клиентскими компьютерами. Агент должен быть установлен на клиентском компьютере, чтобы установить связь между этим компьютером и ESET PROTECT Cloud. 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 Cloud можно [развернуть агент ESET Management](#) на неуправляемых компьютерах. Можно также [вручную установить агент ESET Management](#) на клиентских компьютерах, если это необходимо.
- [ESET Bridge](#) — Это служба, которую можно использовать вместе с ESET PROTECT Cloud, чтобы:
  - Рассылать обновления на клиентские компьютеры и установочные пакеты — агенту ESET Management.

- Пересылать данные с агентов ESET Management на ESET PROTECT Cloud.
- [Управление мобильными устройствами](#) — это компонент, позволяющий использовать средства управления мобильными устройствами в ESET PROTECT Cloud для управления мобильными устройствами (Android и iOS) и администрирования ESET Endpoint Security для Android.
- [Управление уязвимостями и исправлениями](#) — это функция, доступная в ESET PROTECT Cloud. Она регулярно сканирует рабочую станцию для обнаружения любого установленного программного обеспечения, которое может быть уязвимым для угроз безопасности. [Управление исправлениями](#) помогает устранить эти угрозы с помощью автоматического обновления программного обеспечения, обеспечивая более высокий уровень безопасности устройств.

**i** Дополнительные сведения см. в [справке о решении ESET PROTECT Cloud в Интернете](#).

## Защищенные паролем параметры

Чтобы обеспечить максимальную безопасность вашей системы, ESET Endpoint Antivirus 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 Antivirus на подключенных клиентских компьютерах. Чтобы создать новую политику, необходимо выполнить следующие действия.

1. В веб-консоли ESET PROTECT 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 Antivirus 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 окне уведомления создайте новый пароль, подтвердите его и щелкните **ОК**. Щелкните **Продолжить**.
8. Назначьте политику клиентам. Щелкните **Назначить** и выберите компьютеры или группы компьютеров для защиты паролем. Щелкните **ОК**, 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. Политика может применяться непосредственно к отдельным компьютерам и 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 порядке статических групп. В случае динамических групп политики сначала применяются к дочерним динамическим группам. Это позволяет применять политики с более высоким влиянием к верхним группам в дереве, а более конкретные политики — к подгруппам. Используя [флажки](#), ESET Endpoint Antivirus пользователь, имеющий доступ к группам, расположенным выше в иерархии, может переопределить политики нижних групп. Алгоритм описан в [Онлайн-справке ESET PROTECT](#).

**i** Более общие политики (например, для сервера обновлений) рекомендуется назначать более высоким группам в дереве групп. 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 Antivirus 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.

|  |   |
|--|---|
|  <b>Не применять</b>              | Любой параметр с этим флажком политикой игнорируется. Поскольку этот параметр не задан политикой, его можно изменить с помощью других политик, применяемых позже.   |
|  <b>Применить</b>                 | Параметры с флажком « <b>Применить</b> » 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.    |
|  <b>Принудительно применить</b> | Настройки с флажком <b>Принудительно применить</b> имеют высший приоритет и не могут быть перезаписаны какой-либо политикой, примененной позже (даже если у нее также есть флажок <b>Принудительно применить</b> ). 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, включая Политики, 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**.

## Установка

Существует несколько методов установки ESET Endpoint Antivirus на клиентской рабочей станции, если только вы не [развертываете ESET Endpoint Antivirus удаленно на клиентские рабочие станции с помощью ESET PROTECT или ESET PROTECT Cloud](#).



Вы можете выполнить обновление с ESET Endpoint Antivirus до ESET Endpoint Security, запустив установщик ESET Endpoint Security при уже установленном решении ESET Endpoint Antivirus. Однако необходимо устанавливать такую же или более позднюю версию.

| Методы   | Назначение  | Ссылка для загрузки  |
|--|---|--|
| <a href="#">Установка с помощью средства ESET AV Remover</a> | Средство ESET AV Remover поможет удалить практически любую установленную в системе антивирусную программу, чтобы вы могли продолжить установку. | <a href="#">Загрузить 64-разрядную версию</a><br><a href="#">Загрузить 32-разрядную версию</a> |

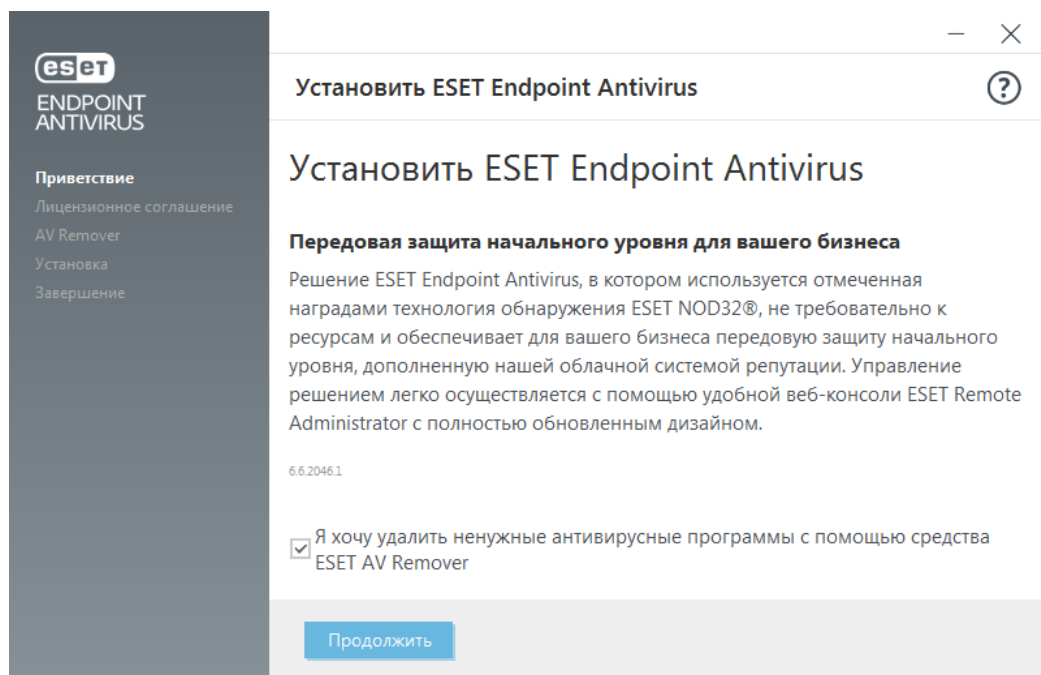
| Методы   | Назначение  | Ссылка для загрузки  |
|--|---|--|
| <a href="#">*** Установка (.exe)</a>                 | Процесс установки без ESET AV Remover.  | <a href="#">Загрузить 64-разрядную версию</a><br><a href="#">Загрузить 32-разрядную версию</a> |
| <a href="#">Установка (.msi)</a>                     | 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 PROTECT. | <a href="#">Загрузить 64-разрядную версию</a><br><a href="#">Загрузить 32-разрядную версию</a> |
| <a href="#">Установка с помощью командной строки</a> | ESET Endpoint Antivirus можно установить локально с помощью командной строки или удаленно с помощью клиентской задачи ESET PROTECT.   | N/A  |
| <a href="#">Развертывание с помощью GPO или SCCM</a> | Используйте средства управления, например GPO или SCCM, чтобы развернуть ESET Management Agent и ESET Endpoint Antivirus на клиентских рабочих станциях.  | N/A  |
| <a href="#">Развертывание с помощью средств RMM</a>  | С помощью плагинов ESET DEM для средства удаленного мониторинга и управления (RMM) можно развернуть ESET Endpoint Antivirus на клиентских рабочих станциях.   | N/A  |

Продукт ESET Endpoint Antivirus [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 Antivirus без использования ESET AV Remover, нажмите кнопку **Продолжить**, не устанавливая этот флажок.

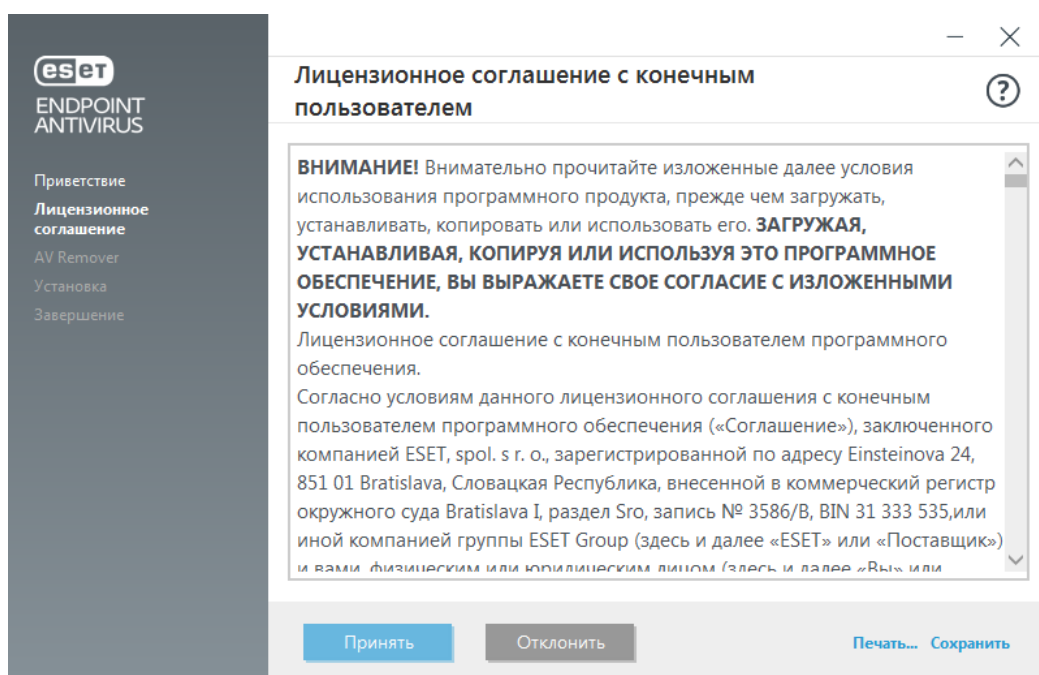




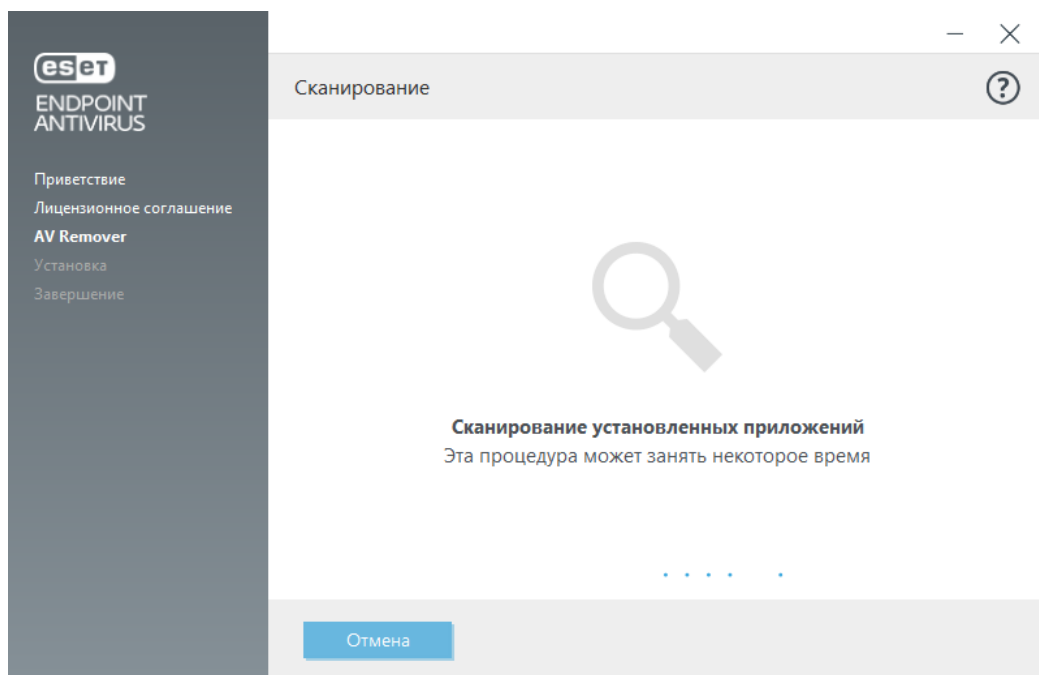
## ESET AV Remover

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.

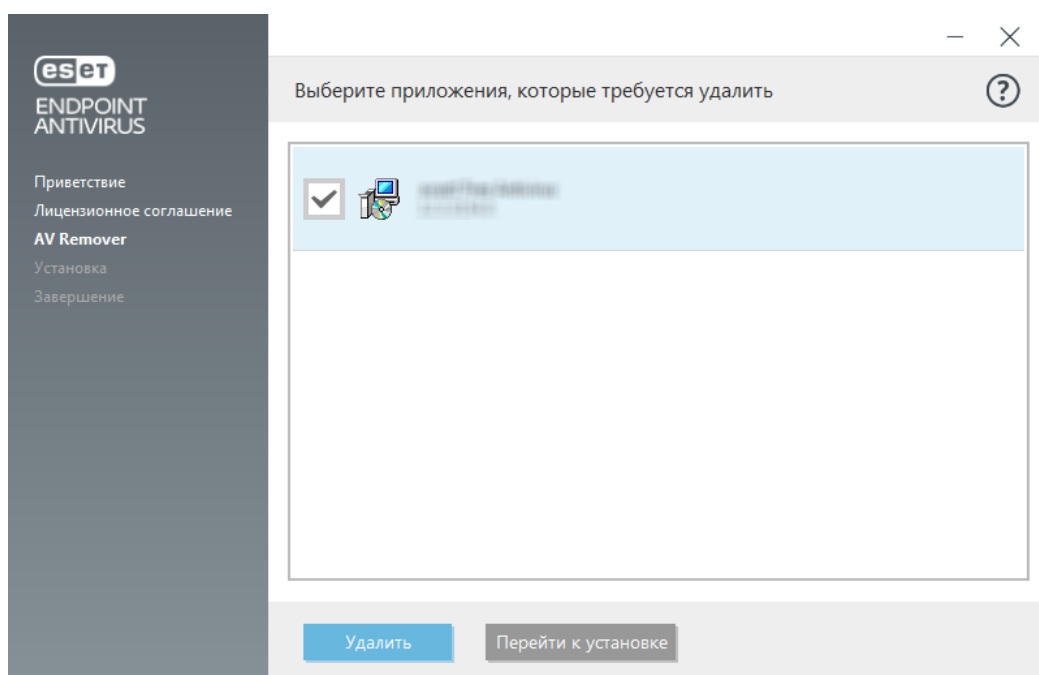
1. Чтобы просмотреть список антивирусных программ, которые можно удалить с помощью ESET AV Remover, [ознакомьтесь с соответствующей статьей базы знаний ESET](#).
2. Прочтите лицензионное соглашение с конечным пользователем и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с его условиями. Нажав кнопку **Отклонить**, вы перейдете к установке ESET Endpoint Antivirus. При этом уже установленное на компьютере приложение для обеспечения безопасности удалено не будет.



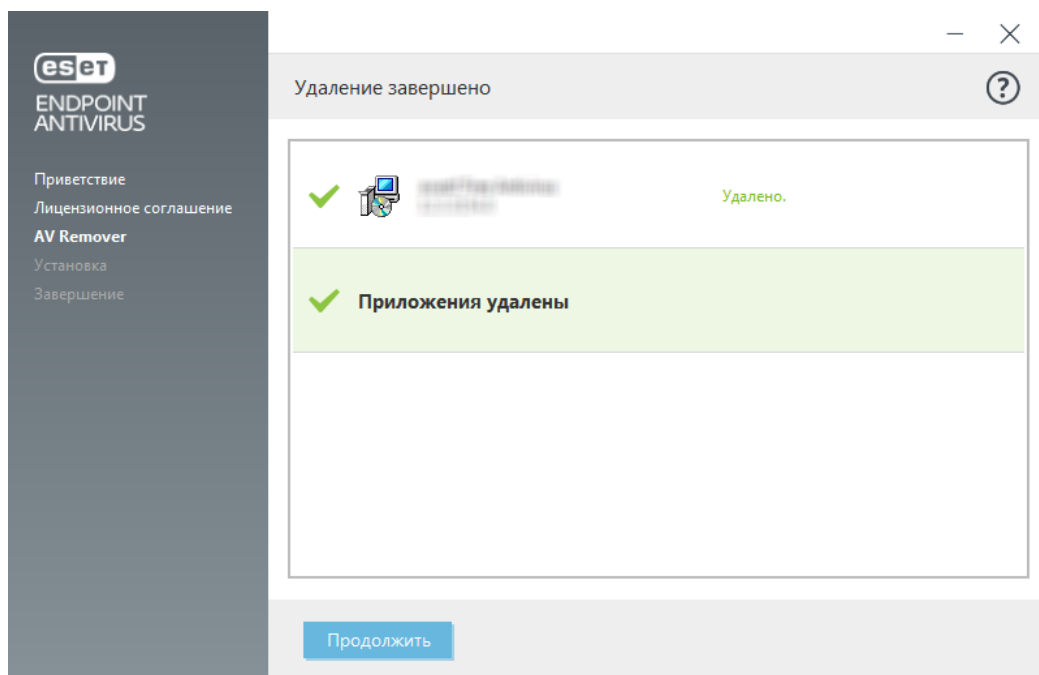
2. Средство ESET AV Remover начнет поиск установленного в системе антивирусного ПО.



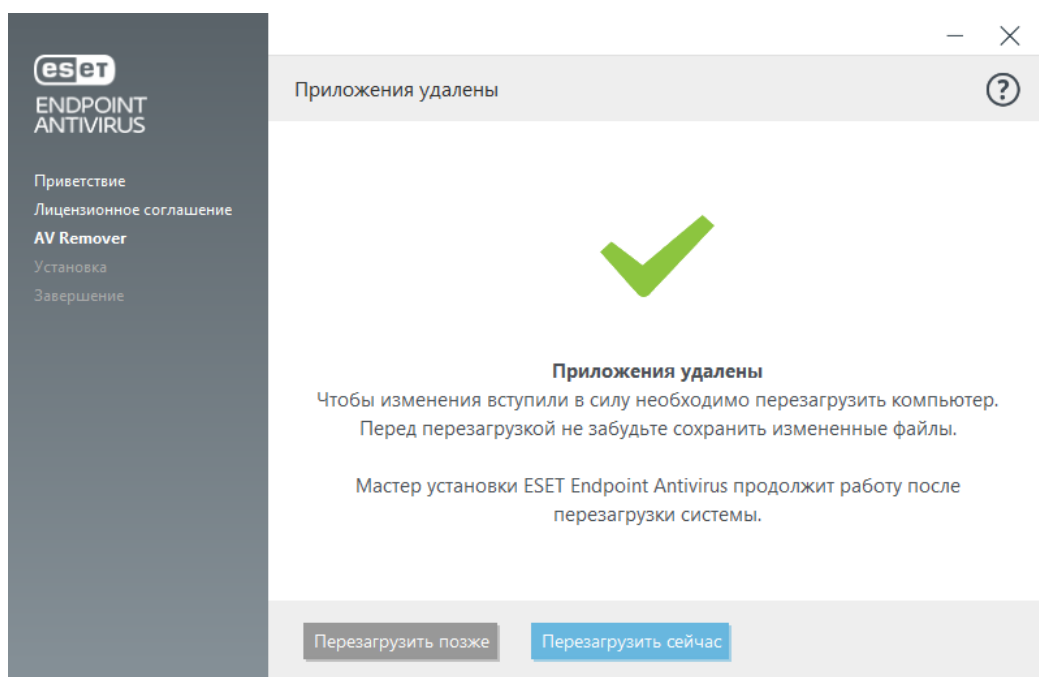
2. Выберите все обнаруженные приложения и нажмите кнопку **Удалить**. Процедура удаления может занять некоторое время.



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



6. Чтобы изменения вступили в силу и продолжить установку ESET Endpoint Antivirus, 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.

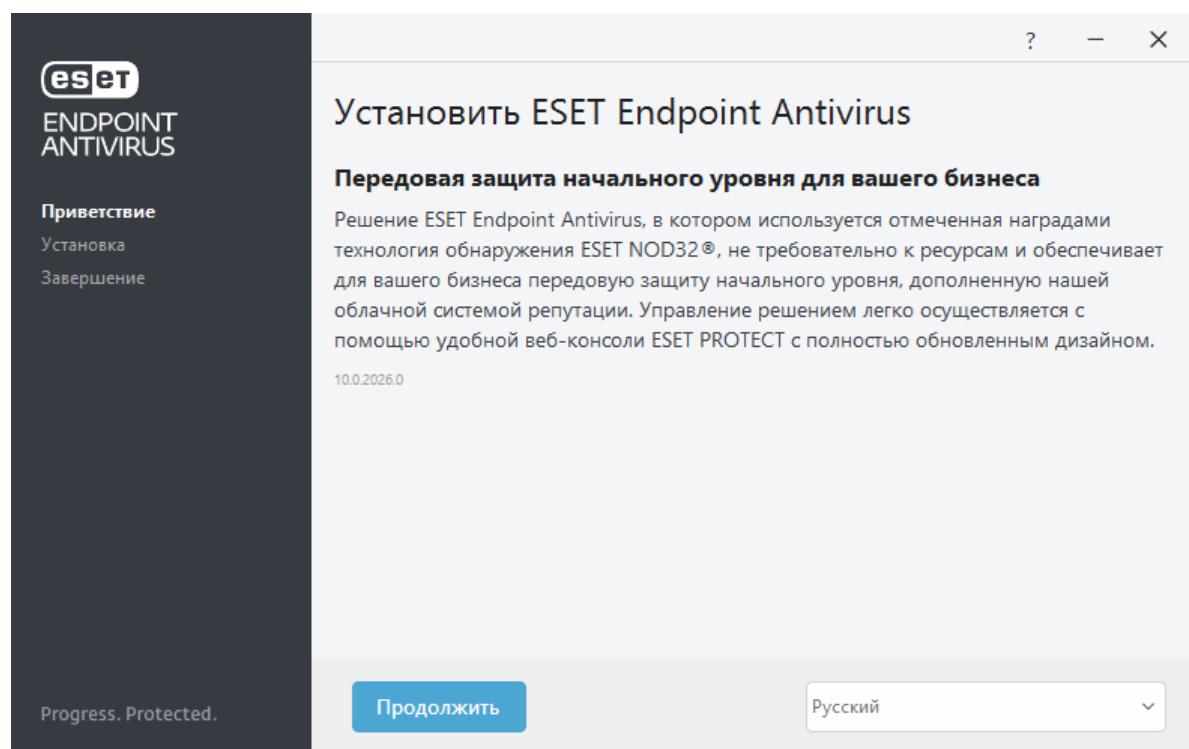
В случае необходимости обратитесь в [службу технической поддержки ESET](#), создайте запрос на обслуживание и приготовьте файл **AppRemover.log** (он потребуется специалистам ESET). Файл **AppRemover.log** расположен в папке **eset**. Эта папка хранится в расположении **%TEMP%**. Для доступа к нему используйте 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.



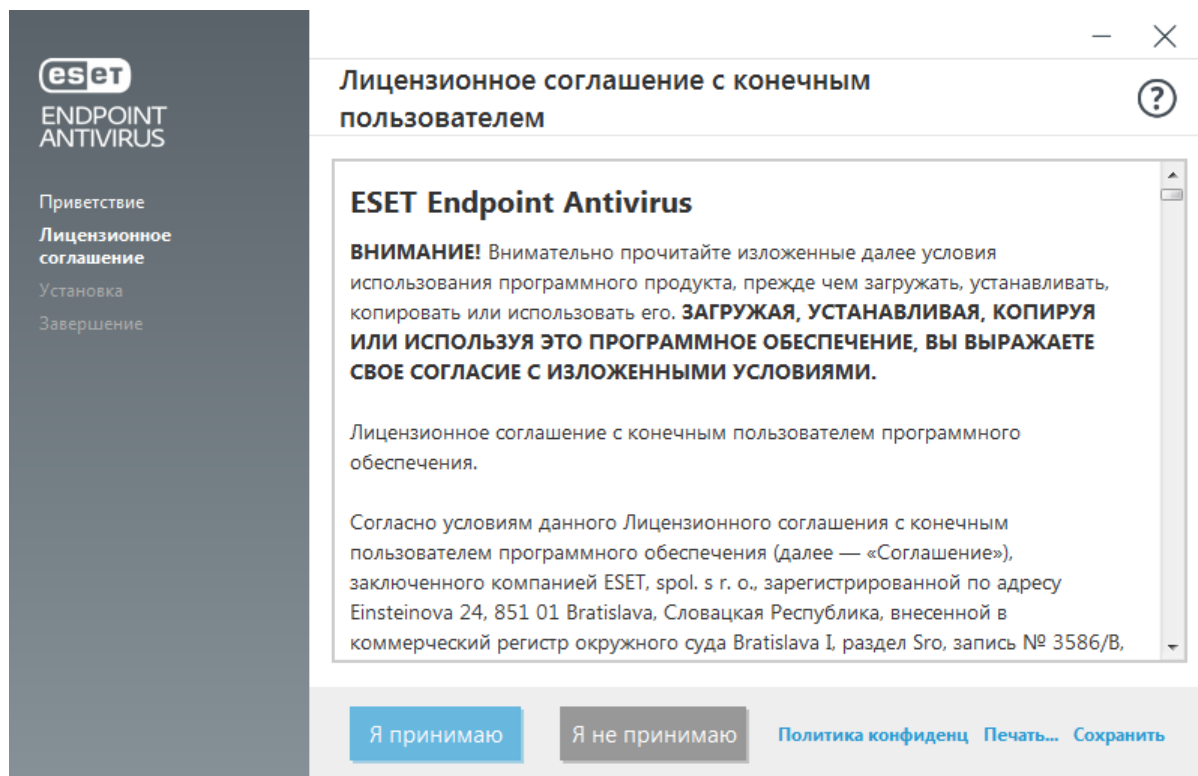
Убедитесь, что на компьютере не установлены другие программы защиты от вирусов. Если на одном компьютере установлено два и более решения для защиты от вирусов, между ними может возникнуть конфликт. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера. Список инструментов для удаления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



1. Выберите настройки для следующих функций, прочитайте [Лицензионное соглашение с конечным пользователем](#) и [Политику конфиденциальности](#) и щелкните **Продолжить** или **Разрешить все и продолжить**, чтобы включить все функции:

- [Система обратной связи ESET LiveGrid®](#)
- [Обнаружение потенциально нежелательных приложений](#)

Нажимая **Продолжить** или **Разрешить все и продолжить**, вы принимаете Лицензионное соглашение с конечным пользователем и соглашаетесь с Политикой конфиденциальности. Вы можете установить ESET Endpoint Antivirus в определенную папку, нажав [Изменить папку установки](#).



2. После завершения установки вам будет предложено [активировать ESET Endpoint Antivirus](#).

## Изменение папки установки (.exe)

Во время установки можно **изменить папку установки**. Выберите расположение для установки ESET Endpoint Antivirus. 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:

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

*C:\ProgramData\ESET\ESET Security\*

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

Щелкните **Назад** и продолжите процесс установки.

## Установка (.msi)

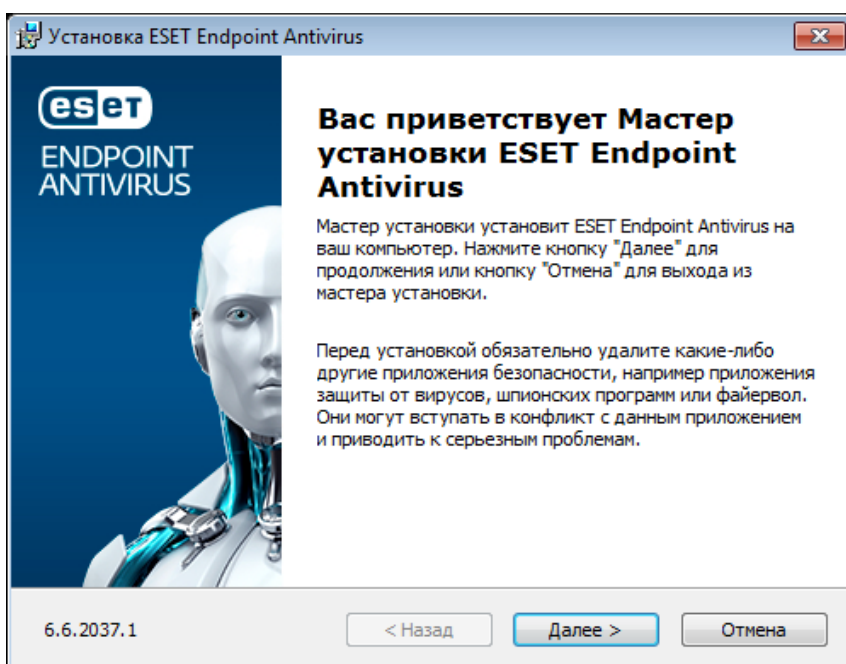
После запуска MSI-файла мастер установки поможет установить программу.

✓ 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 PROTECT.

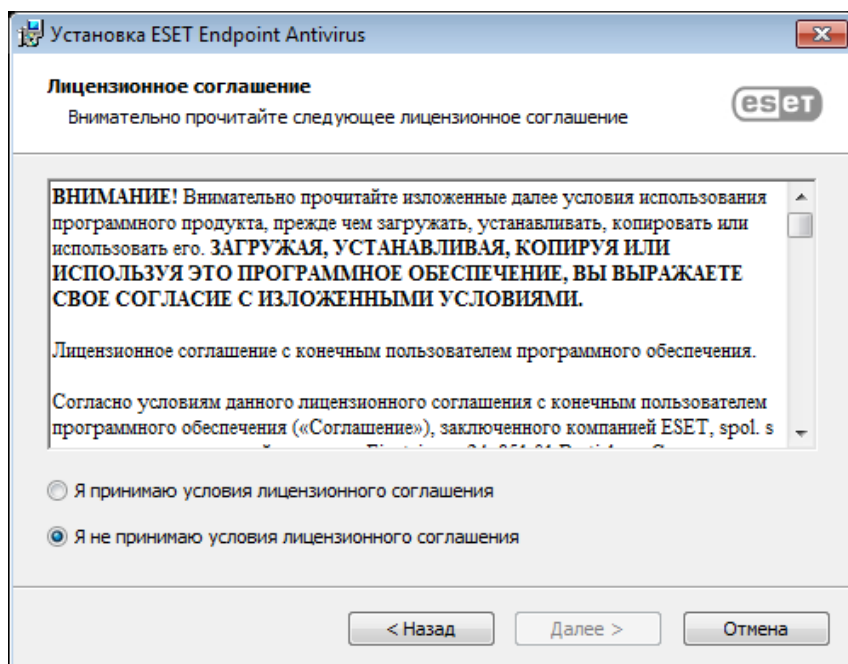
! Убедитесь, что на компьютере не установлены другие программы защиты от вирусов. Если на одном компьютере установлено два и более решения для защиты от вирусов, между ними может возникнуть конфликт. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера. Список инструментов для удаления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

i Установщик ESET Endpoint Antivirus, созданный в ESET PROTECT, поддерживает многосеансовый режим в ОС Windows 10 Корпоративная для виртуальных рабочих столов и в ОС Windows 10.

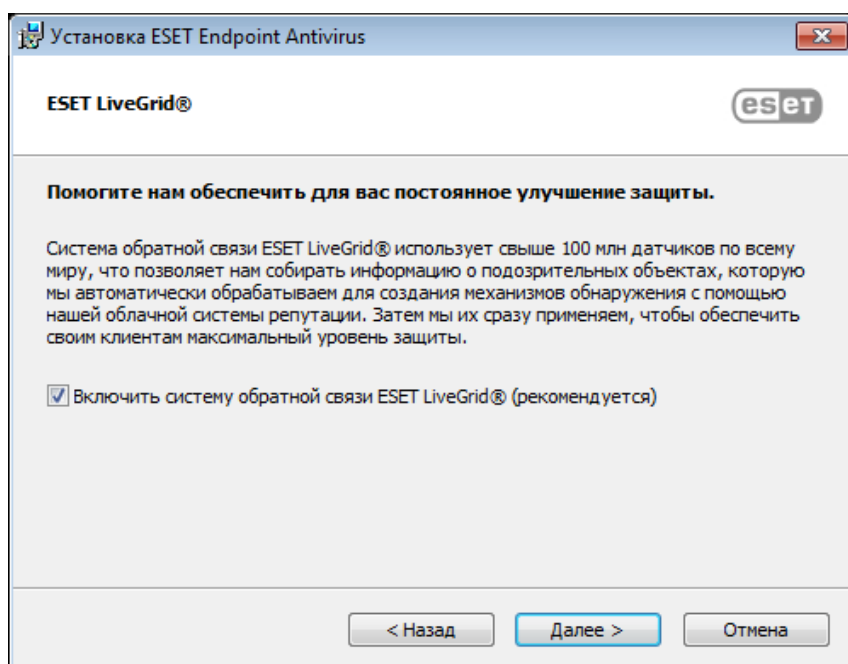
1. Выберите нужный язык и нажмите кнопку **Далее**.



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 лучше защищать своих клиентов. С помощью этой системы вы можете отправлять новые угрозы в вирусную лабораторию ESET, где они анализируются, обрабатываются и добавляются в модуль обнаружения. Щелкните элемент **Дополнительные параметры**, чтобы [настроить дополнительные параметры установки](#).



4. Последний шаг: подтверждение установки. Для этого нужно нажать **Установить**. После завершения установки вам будет предложено [активировать ESET Endpoint Antivirus](#).

## Расширенная установка (.msi)

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

1. Во время установки можно **изменить папку установки**. Выберите расположение для установки ESET Endpoint Antivirus. По умолчанию программа устанавливается в указанные ниже папки.

*C:\Program Files\ESET\ESET Security\*

Можно указать расположение для модулей и данных программы. По умолчанию они устанавливаются в указанные ниже папки:

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

*C:\ProgramData\ESET\ESET Security\*

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

2. Выберите компоненты продукта, которые следует установить. Вы можете выбрать свои предпочтения для [сканирования компьютера](#) и всех доступных [видов защиты](#). 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.
3. Чтобы запустить процесс установки, нажмите кнопку **Установить**.

## Минимальная установка модулей

Чтобы уменьшить сетевой трафик, связанный с размером установщика, и сохранить ресурсы, ESET поставляется с установщиком с минимальным количеством модулей. Установщик содержит только важные модули, а все остальные модули будут загружаться во время первоначального обновления модуля после активации программы. Главным преимуществом является значительно меньший размер установщика. После активации продукта ESET Endpoint Antivirus загружает только последние модули приложения.

Минимальный установщик модулей по-прежнему содержит следующие модули:

- Загрузчики
- Обмен данными с Direct Cloud
- Поддержка перевода
- Конфигурация
- SSL

После активации программы отобразится состояние **Инициализация защиты**, в котором будет сообщаться об инициализации функций.



При возникновении проблемы с загрузкой модулей (например, из-за настроек прокси-сервера, отсутствия сети и т. д.) отображается предупреждающее состояние приложения **Требуется вмешательство**. В главном окне программы щелкните **Обновление > Проверить наличие обновлений**, чтобы снова запустить процесс.



После нескольких неудачных попыток отобразится состояние приложения **Настройка защиты не выполнена**, выделенное красным цветом. Щелкните «Повторить попытку», чтобы снова запустить настройку защиты. Если процесс инициализации завершается неудачей и вам все еще не удастся загрузить модули, [загрузите полные установщики MSI здесь](#).

Если у клиентских компьютеров нет подключения к Интернету или они работают в автономном режиме и при этом им нужны обновления, используйте следующие способы загрузки файлов обновлений с серверов обновлений ESET:

- [Обновление с зеркала](#)
- [Использование средства «Зеркало»](#)

## Установка с помощью командной строки

ESET Endpoint Antivirus можно установить локально с помощью командной строки или удаленно с помощью клиентской задачи в ESET PROTECT.

### 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 msisexec.

## 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 Antivirus включает такой набор функций:

| 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 |

| Описание  | Имя функции             | Родительский элемент функции | Наличие        |
|---|-------------------------|------------------------------|----------------|
| 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 почтового клиента 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 |
| <a href="#">Плагин ESET Inspect</a>   | 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 UPDITEMIRROR.

## Список свойств конфигурации

| Свойство                         | Значение                      | Функция   |
|----------------------------------|-------------------------------|---|
| CFG_POTENTIALLYUNWANTED_ENABLED= | 0 — отключено<br>1 — включено | <a href="#">Обнаружение потенциально нежелательных приложений</a> |
| CFG_LIVEGRID_ENABLED=            | <a href="#">См. ниже</a>      | См. <a href="#">свойство LiveGrid</a> ниже                        |

| Свойство                 | Значение                      | Функция  |
|--------------------------|-------------------------------|--|
| FIRSTSCAN_ENABLE=        | 0 — отключено<br>1 — включено | Запланируйте и выполните <a href="#">сканирование компьютера</a> после установки                                   |
| CFG_PROXY_ENABLED=       | 0 — отключено<br>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 аутентификации  |
| CFG_PROXY_PASSWORD=      | <password>                    | Пароль для аутентификации  |
| ACTIVATION_DATA=         | <a href="#">См. ниже</a>      | Активация программы, лицензионный ключ или автономный файл лицензии  |
| ACTIVATION_DLG_SUPPRESS= | 0 — отключено<br>1 — включено | При значении «1» диалоговое окно активации программы не отображается при первом запуске                            |
| ADMINCFG=                | <path>                        | Путь к <a href="#">экспортированному файлу конфигурации в формате XML</a> (значение по умолчанию: <i>cfg.xml</i> ) |

## Свойство [LiveGrid®](#)

При установке ESET Endpoint Antivirus `CCFG_LIVEGRID_ENABLED`, продукт после установки будет работать следующим образом:

| Функция  | CFG_LIVEGRID_ENABLED=0 | CFG_LIVEGRID_ENABLED=1 |
|--|------------------------|------------------------|
| <b>Система репутации ESET LiveGrid®</b>              | Вкл.                   | Вкл.                   |
| <b>Система отзывов ESET LiveGrid®</b>                | Выкл.                  | Вкл.                   |
| <b>Отправить анонимную статистическую информацию</b> | Выкл.                  | Вкл.                   |

## Свойство ACTIVATION\_DATA

| Формат   | Методы   |
|--|--|
| ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE                         | <a href="#">Активация с помощью лицензионного ключа ESET</a> (необходим доступ в Интернет) |
| ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf | <a href="#">Активация с помощью автономного файла лицензии</a>                             |

## Свойства языка

Язык ESET Endpoint Antivirus (нужно указать оба свойства).

| Свойство           | Значение  |
|--------------------|---|
| PRODUCT_LANG=      | LCID Decimal (идентификатор языка в формате десятичного числа): например, языку «Английский (США)» соответствует значение 1033. См. <a href="#">СПИСОК КОДОВ ЯЗЫКОВ</a> . |
| PRODUCT_LANG_CODE= | LCID String (имя языка и культуры) строчными буквами: например, «en-us» означает «Английский (США)». См. <a href="#">СПИСОК КОДОВ ЯЗЫКОВ</a> .                            |

## Свойства перезапуска

Укажите следующие параметры для перезапуска компьютера после установки:

| Свойство            | Значение                      | Функция   |
|---------------------|-------------------------------|---|
| REBOOT_WHEN_NEEDED= | 0 — отключено<br>1 — включено | Если этот параметр включен, после установки компьютер будет перезапущен.                                  |
| REBOOT_CANCELABLE=  | 0 — отключено<br>1 — включено | Если этот параметр включен, пользователь может отменить перезапуск компьютера.                            |
| REBOOT_POSTPONE=    | значение в секундах           | Максимальное количество времени в секундах, на которое пользователь может отложить перезапуск компьютера. |

**i** Параметры REBOOT\_CANCELABLE и REBOOT\_POSTPONE доступны только в том случае, если включен параметр REBOOT\_WHEN\_NEEDED.

## Примеры установки с помощью командной строки

**!** Прежде чем начинать установку, обязательно прочитайте [лицензионное соглашение с конечным пользователем](#) 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 Antivirus была произведена его автоматическая настройка, в команде установки можно указать основные параметры конфигурации.

Установите ESET Endpoint Antivirus 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 Antivirus 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 Antivirus на клиентской рабочей станции](#), 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 Antivirus с помощью ESET PROTECT. В вашей сети должно быть установлено решение ESET PROTECT.

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 ESET PROTECT.
5. [Разверните и активируйте ESET Endpoint Antivirus 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 \(GPO\)](#)

### Неуправляемый

Если компьютеры неуправляемые, ESET Endpoint Antivirus можно развернуть напрямую на клиентских рабочих станциях. Это не рекомендуется, потому что тогда вы не сможете контролировать и применять политики продуктов ESET для конечных точек на рабочих станциях.

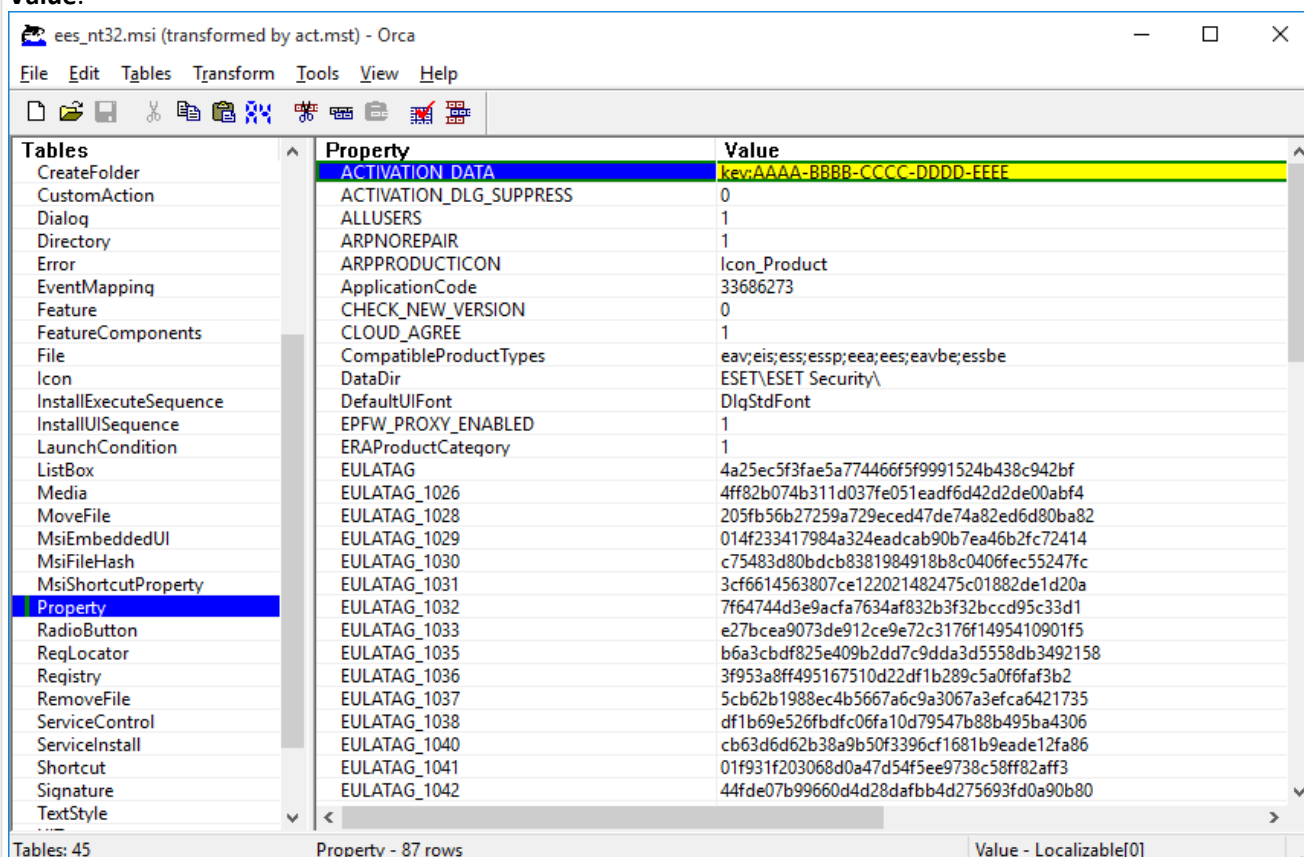
По умолчанию продукт ESET Endpoint Antivirus не активирован после установки и работать не будет.

### Вариант 1 (установка программного обеспечения)

1. [Загрузите установочный файл с расширением .msi](#) для ESET Endpoint Antivirus.
2. Создайте пакет преобразования с расширением .mst на основе файла .msi (например, используйте редактор .msi Orca), чтобы добавить свойство активации программы (см. ACTIVATION\_DATA в разделе [Установка с помощью командной строки](#)).

## [Показать этапы создания файла с расширением .mst в Orca](#)

1. Открыть Orca
2. Загрузите установочный файл с расширением .msi, щелкнув **File > Open**.
3. Щелкните элемент **Transform > New Transform**.
4. Щелкните элемент **Property** в разделе **Tables**, а затем в меню **Tables > Add row**.
5. В окнах **Add Row** введите ACTIVATION\_DATA в поле **Property** и информацию о лицензии в поле **Value**.



6. Щелкните **Преобразование > Создать преобразование**, чтобы сохранить файл с расширением .mst.

1. Необязательно: чтобы [импортировать](#) пользовательский файл конфигурации ESET Endpoint Antivirus с расширением .xml (например, чтобы активировать RMM или настроить параметры прокси-сервера), поместите файл cfg.xml в то расположение, где находится установочный файл с расширением .msi.
2. Удаленно разверните установщик .msi с файлом .mst посредством метода GPO (установка программного обеспечения) или SCCM.

## Вариант 2 (с использованием запланированной задачи)

1. [Загрузите установочный файл с расширением .msi](#) для ESET Endpoint Antivirus.
2. Подготовьте сценарий [установки с помощью командной строки](#), включив в него свойство активации программы (см. ACTIVATION\_DATA).
3. Откройте доступ к установочному файлу с расширением .msi и файлу сценария с расширением .cmd всем рабочим станциям в сети.
4. Необязательно: чтобы [импортировать](#) пользовательский файл конфигурации ESET Endpoint Antivirus с расширением .xml (например, чтобы активировать RMM или настроить параметры прокси-сервера), поместите файл cfg.xml в то расположение, где находится установочный файл с расширением .msi.



5. Примените подготовленный сценарий установки с помощью командной строки, используя GPO или SCCM.

- При использовании GPO выберите «Предпочтения групповой политики» > «Задачи планирования групповой политики» > «Немедленная задача».

**i** На случай, если вы не хотите использовать ESET PROTECT для удаленного управления продуктами ESET для конечных точек, ESET Endpoint Antivirus содержит плагин ESET для удаленного мониторинга и управления (RMM), позволяющий контролировать системы программного обеспечения с помощью локально установленного агента, к которому может получать доступ поставщик службы управления. [Дополнительные сведения](#)

## Обновление до новой версии

Новые версии ESET Endpoint Antivirus выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы.

Обновление до новой версии можно выполнить одним из нескольких способов.

1. Автоматически с помощью ESET PROTECT, или ESET PROTECT Cloud.
2. Автоматически [с помощью GPO или SCCM](#).
3. Автоматически с помощью обновления программы.  
Поскольку обновления программы распространяются среди всех пользователей и могут повлиять на некоторые конфигурации компьютеров, они выпускаются только после длительного тестирования с целью обеспечения бесперебойной работы на всех возможных конфигурациях. Чтобы перейти на новую версию сразу после ее выпуска, воспользуйтесь одним из перечисленных ниже способов.  
Убедитесь, что включен параметр **Режим обновления** в разделе [Расширенные параметры](#) > **Обновление** > **Профили** > **Обновления 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 или ESET PROTECT Cloud. 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

Для обновления ESET Endpoint Antivirus вручную на отдельных клиентских рабочих станциях выполните следующие действия.

1. Убедитесь, что [поддерживается установленная в настоящий момент версия](#).
2. Убедитесь, что ваша операционная система [поддерживается](#).



2. Загрузите и [установите последнюю версию](#) поверх предыдущей.



Успешная установка последней версии поверх предыдущей не гарантирована для версий с уровнем поддержки «Окончание срока службы». Для получения сведений об уровне поддержки ESET Endpoint Antivirus см. [политику касательно окончания срока службы](#). Чтобы обновить неподдерживаемые версии, сначала следует удалить ESET Endpoint Antivirus. Для получения дополнительных сведений об обновлении ESET Endpoint Antivirus на клиентской рабочей станции ознакомьтесь со следующей [статьей 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 Antivirus — это важный аспект поддержания полной защиты от вредоносного кода. Каждая новая версия ESET Endpoint Antivirus включает множество улучшений и исправлений ошибок. Настоятельно рекомендуется периодически обновлять ESET Endpoint Antivirus, чтобы предотвратить появление уязвимостей и угроз безопасности. ESET Endpoint Antivirus проходит определенные этапы жизненного цикла продукта, как любой другой продукт ESET.

Подробнее об:

[Политика касательно окончания срока службы \(для бизнес-продуктов\)](#)



[Обновление программы](#)

[Исправления для обеспечения безопасности и стабильности](#)

Дополнительные сведения об изменениях в ESET Endpoint Antivirus 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.

## Активация программы

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.).

ESET Endpoint Antivirus можно активировать в [главном окне программы](#) в разделе **Справка и поддержка > Активировать продукт** или **Состояние защиты > Активировать продукт**.

Для активации ESET Endpoint Antivirus 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 HUB:** [учетная запись ESET HUB](#), которую вы должны создать. Решение ESET HUB — это центральная точка доступа к унифицированной платформе безопасности ESET PROTECT. Оно обеспечивает централизованное управление идентификацией, подписками и пользователями для всех модулей платформы ESET. Вы можете использовать этот вариант для активации ESET Endpoint Antivirus также с помощью старых средств управления лицензиями: [ESET Business Account](#) или [ESET MSP Administrator](#).
- **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 PROTECT. Этот параметр можно использовать и в тех случаях, когда нужно активировать клиент позже.

Если у вас есть имя пользователя и пароль, использованные для активации продуктов ESET предыдущих версий, [преобразуйте эти устаревшие учетные данные в лицензионный ключ](#).

Изменить лицензию на продукт можно в любой момент в [главном окне программы](#) в разделе **Справка и поддержка > Изменить лицензию**. Отобразится открытый идентификатор лицензии, предназначенный для ее идентификации в службе поддержки ESET.

**i** ESET PROTECT может активировать клиентские компьютеры в автоматическом режиме, используя предоставленные администратором лицензии. Инструкции см. в [интернет-справке ESET PROTECT](#).

**!** [Не удалось активировать программу?](#)

## Ввод лицензионного ключа при активации

Автоматические обновления являются важным компонентом вашей безопасности. ESET Endpoint Antivirus 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.

## Учетная запись ESET HUB

Решение ESET HUB — это центральная точка доступа к унифицированной платформе безопасности ESET PROTECT. Оно обеспечивает централизованное управление идентификацией, подписками и пользователями для всех модулей платформы ESET. ESET HUB обеспечивает следующие возможности:

- Получение обзора по подпискам касательно безопасности
- Проверка использования и статусов служб, на которые оформлена подписка
- Выделение и контроль детализированного доступа к отдельным платформам ESET
- Единый вход для всех связанных и доступных платформ ESET

Вы можете использовать этот вариант для активации ESET Endpoint Antivirus также с помощью старых средств управления лицензиями: [ESET Business Account](#) или [ESET MSP Administrator](#).

Вы можете [создать учетную запись ESET HUB](#) и авторизоваться, используя **адрес электронной почты** и **пароль**.

Если вы забыли пароль, щелкните элемент **Я не помню пароль**. Вы будете перенаправлены на ESET HUB. Введите адрес электронной почты и щелкните **Войти** для подтверждения. Затем вам будет отправлено сообщение с инструкциями по сбросу пароля.

# Использование устаревших учетных данных лицензии для активации 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.

## Сбой активации

Если активация ESET Endpoint Antivirus завершилась неудачей, наиболее распространенными сценариями являются:

- Лицензионный ключ уже используется.
- Вы ввели недопустимый лицензионный ключ.
- В форме активации отсутствует или указана недопустимая информация.
- Ошибка обмена данными с сервером активации.
- 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 удастся 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](#)

## Регистрация

Зарегистрируйте лицензию, заполнив поля регистрационной формы и нажав **Продолжить**. Обязательны к заполнению поля, возле которых в скобках дано соответствующее указание. Данная информация будет использоваться только в целях, связанных с вашей лицензией ESET.

## Ход выполнения активации

Выполняется активация ESET Endpoint Antivirus. Это может занять некоторое время.

## Активация выполнена

Продукт ESET Endpoint Antivirus успешно активирован. Теперь ESET Endpoint Antivirus будет регулярно загружать обновления, следить за безопасностью компьютера и устранять все известные угрозы. Чтобы завершить активацию продукта, нажмите кнопку **Готово**.

# Распространенные проблемы, возникающие при установке

Если во время установки возникают проблемы, мастер установки предоставляет решение для устранения неполадок, которое поможет с ними справиться, если это возможно.


Щелкните **Запустить устранение неполадок**. Когда решение для устранения неполадок завершит работу, выполните рекомендуемые действия.

Если проблема не будет устранена, см. список [распространенных ошибок установки и решений для них](#).

## Руководство для начинающих

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

## 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 (в области уведомлений Windows), 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. С помощью раскрывающегося меню **Интервал времени** можно указать, на какое время отключается защита.

**Расширенные параметры:** вызов [расширенных параметров](#) ESET Endpoint Antivirus. Чтобы открыть расширенные параметры в [главном окне программы](#), нажмите клавишу F5 на клавиатуре или выберите **Настройка > Расширенные параметры**.

[Файлы журнала:](#) файлы журнала содержат информацию о важных программных событиях и предоставляют общие сведения об обнаружениях.

**Открыть ESET Endpoint Antivirus:** если щелкнуть этот значок на панели задач (в области уведомлений Windows), откроется [главное окно программы](#) ESET Endpoint Antivirus.

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

**Режим цвета:** открывает [настройки интерфейса](#), с помощью которых можно изменить цвет графического интерфейса.

**Проверить наличие обновлений:** запуск обновления программы или модуля, чтобы обеспечить защиту. ESET Endpoint Antivirus автоматически проверяет наличие обновлений несколько раз в день.

**О программе:** отображение информации о системе, сведений об установленной версии ESET Endpoint Antivirus и установленных модулях программы, а также данных об операционной системе и системных ресурсах.

## Сочетания клавиш

Для более удобной навигации в ESET Endpoint Antivirus можно использовать следующие сочетания клавиш:

| Сочетания клавиш               | Действие  |
|--------------------------------|---|
| F1                             | вызов справки   |
| F5                             | вызов окна <a href="#">Расширенных параметров</a>   |
| Стрелка вверх или стрелка вниз | навигация в пунктах раскрывающегося меню  |
| TAB                            | переход к следующему элементу графического интерфейса пользователя в окне                             |
| Shift+TAB                      | переход к предыдущему элементу графического интерфейса пользователя в окне                            |
| ESC                            | заккрытие 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                          |
| ALT + стрелка влево            | переход назад   |
| ALT + стрелка вправо           | переход вперед  |
| ALT+Home                       | переход на домашнюю страницу  |

Для навигации также можно использовать кнопки мыши назад или вперед.

## Профили

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

## Сканирование компьютера

В ESET Endpoint Antivirus 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).

Чтобы создать профиль, откройте раздел [Расширенные параметры](#) > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Сканирование по требованию** > **Список профилей** > **Изменить**. 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 [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 **i Всегда исправлять обнаружение**. Введите имя нового профиля в окне **Диспетчер профилей** и нажмите кнопку **Добавить**. Выберите новый профиль в раскрывающемся меню **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **ОК**, чтобы сохранить новый профиль.

## Обновление

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

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

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



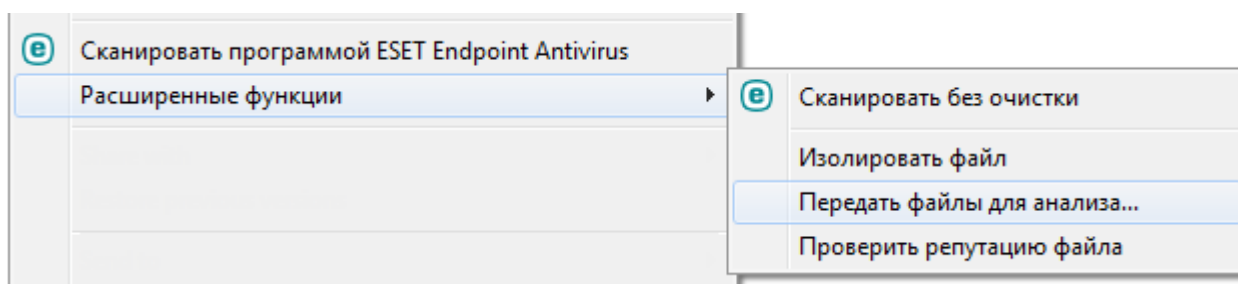
**Список профилей:** создание или редактирование профилей обновления.

## 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 Antivirus можно интегрировать в контекстное меню. Настройка этих функций выполняется в разделе [Расширенные параметры](#) > **Интерфейс** > **Элементы интерфейса**.

**Интегрировать с контекстным меню:** возможность интеграции элементов управления ESET Endpoint Antivirus в контекстное меню.



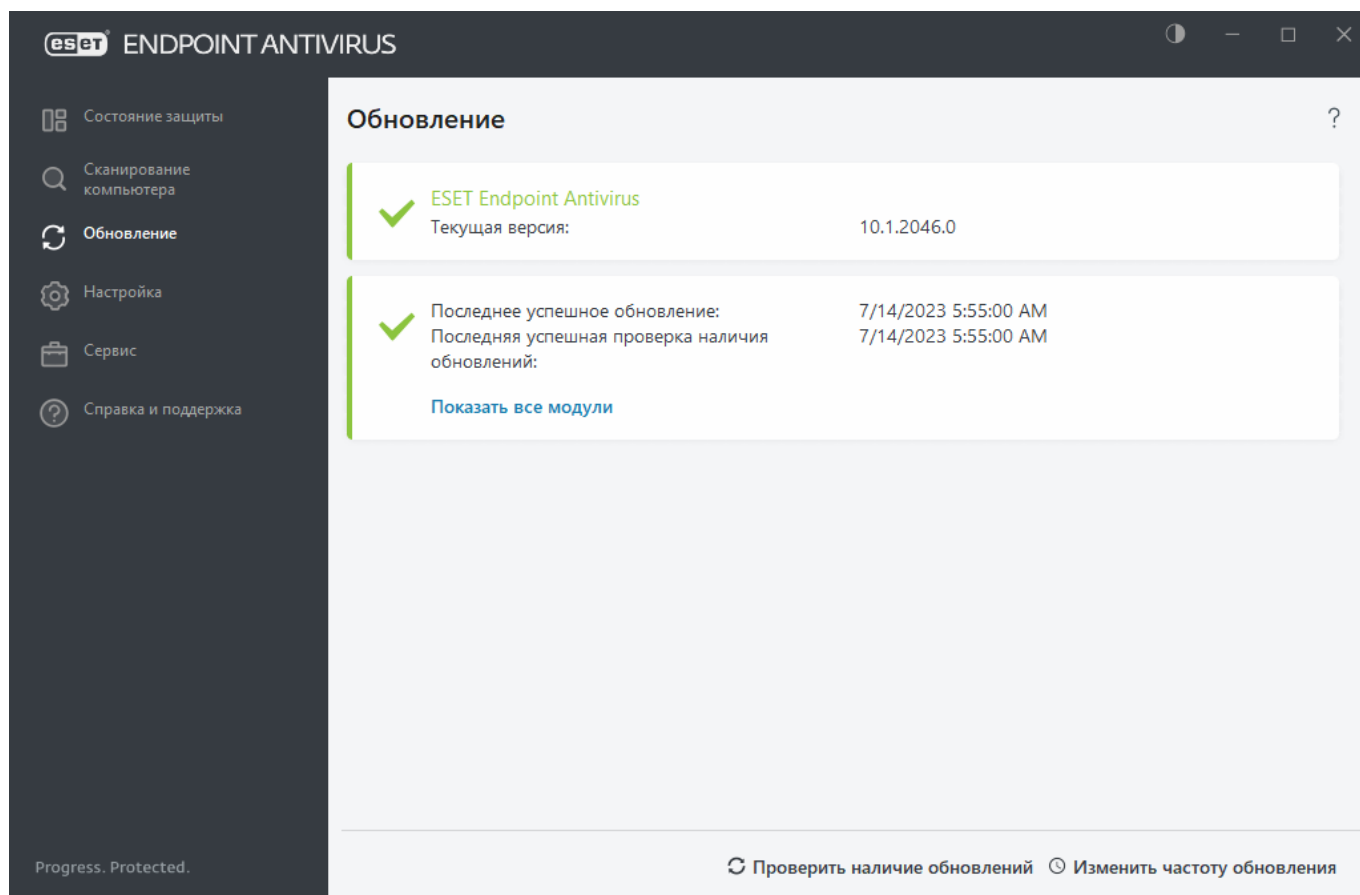
## Настройка обновлений

Регулярное обновление ESET Endpoint Antivirus — лучший способ обеспечить максимальную безопасность компьютера. Модуль обновления поддерживает актуальность программных модулей и компонентов системы.

Выбрав пункт **Обновление** в [главном окне программы](#), можно просмотреть информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления.

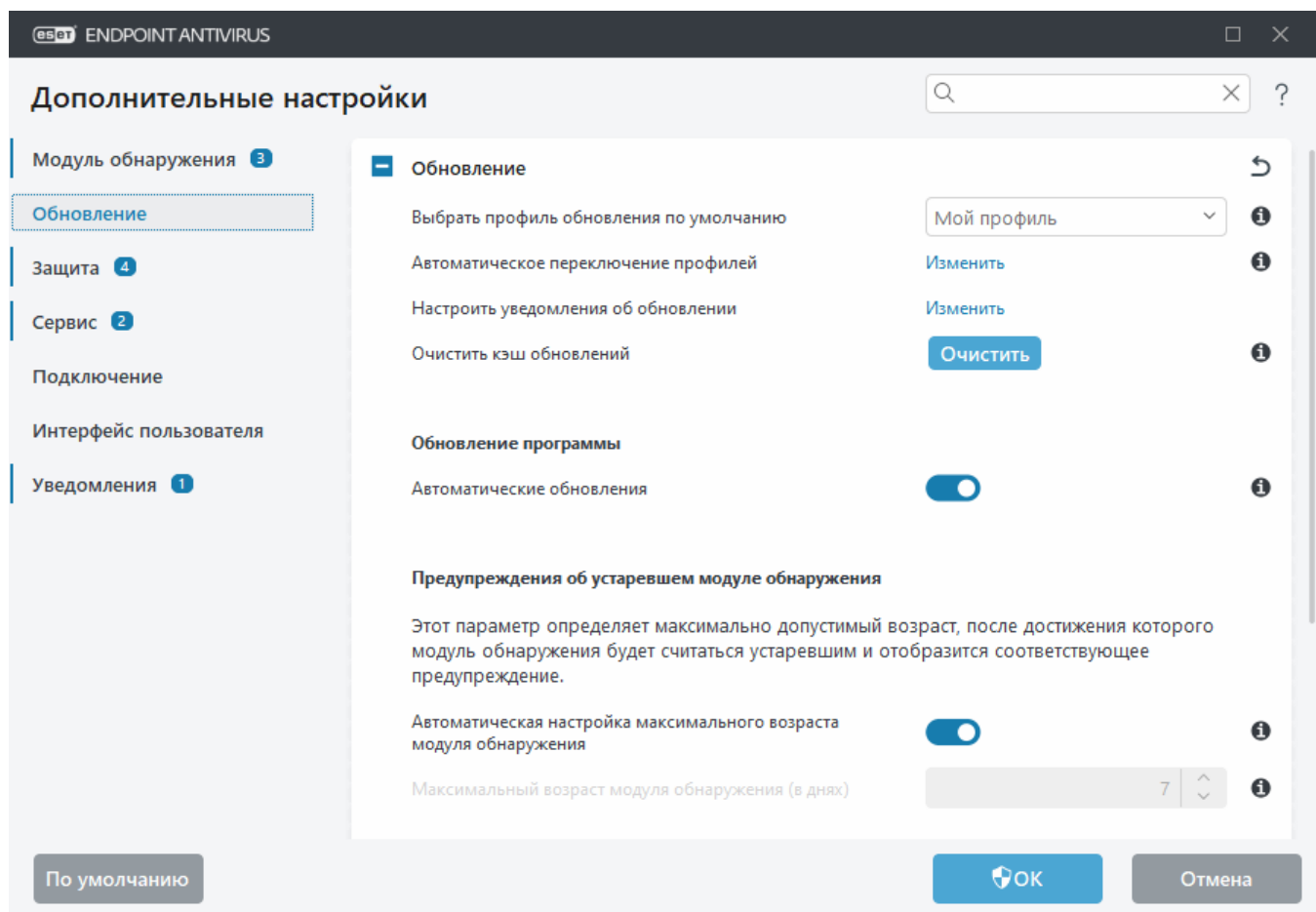
Кроме автоматического обновления, можно выполнить обновление вручную, нажав кнопку **Проверить наличие обновлений**.





Раздел [Расширенные параметры](#) > **Обновление** содержит дополнительные опции обновления, такие как режим обновления, доступ к прокси-серверу и подключения к локальной сети.

Если при обновлении возникнут проблемы, щелкните **Очистить**, чтобы удалить кэш обновления. Если обновить модули программы все равно не удастся, см. раздел [Устранение неполадок при получении сообщения «Обновление модулей не выполнено»](#).

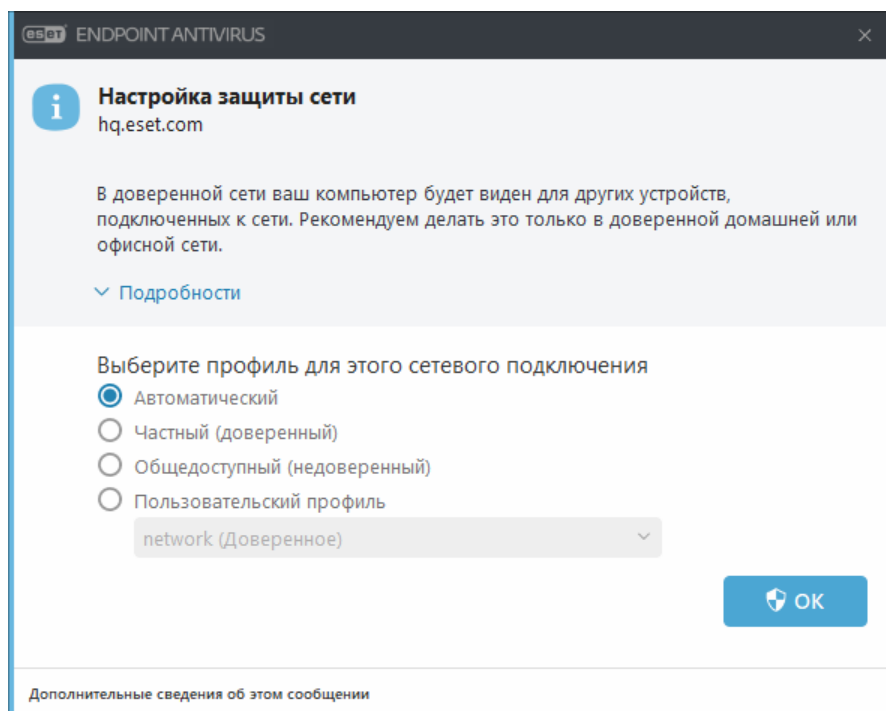


Опция **Выбирать автоматически** в разделе [Расширенные параметры](#) > **Обновление** > **Профили** > **Обновления** > **Обновление модулей** по умолчанию включена. Если для получения обновлений вы используете сервер обновлений ESET, рекомендуем не менять его значение.

Для оптимальной работы программа должна автоматически обновляться. Автоматическое обновление происходит 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 разделе [Активация ESET Endpoint Antivirus](#).

## Настройка защиты сети

По умолчанию ESET Endpoint Antivirus использует параметры Windows при обнаружении новой сети. Чтобы при обнаружении новой сети отображалось диалоговое окно, установите для параметра [Назначение профиля защиты сети](#) значение **Запросить**. Конфигурация защиты сети отображается при каждом подключении вашего компьютера к новой сети.



Вы можете выбрать один из следующих [профилей сетевых подключений](#).

**Автоматически:** ESET Endpoint Antivirus автоматически выберет профиль на основе [активаторов](#), настроенных для каждого профиля.

**Конфиденциально** — для доверенной сети (домашней или офисной сети). Ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также системные ресурсы доступны другим пользователям сети (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Этот параметр рекомендуется использовать при доступе к безопасной локальной сети. Этот профиль автоматически назначается сетевому подключению, если оно настроено как доменная или частная сеть в Windows.

**Общедоступная** — для недоверенных (общедоступных) сетей. Файлы и папки в вашей системе не являются общими для других пользователей в сети, и другие пользователи сети их не видят, а общий доступ к системным ресурсам отключен. Этот параметр рекомендуется использовать при доступе к беспроводным сетям. Этот профиль автоматически назначается любому сетевому подключению, которое не настроено как доменная или частная сеть в Windows.

**Пользовательский профиль:** вы можете выбрать [созданный вами профиль](#) в раскрывающемся меню. Эта опция доступна только в том случае, если вы создали хотя бы один пользовательский профиль.



Неправильная конфигурация сети может представлять угрозу безопасности вашего компьютера.

## Заблокированные хэши

Использование ESET Inspect в среде позволяет администраторам блокировать доступ к указанным исполняемым файлам на основе их хэша. Если администратор заблокировал доступ

к исполняемому файлу, а вы пытаетесь получить к нему доступ, ESET Endpoint Antivirus отобразит следующее уведомление:

**Доступ к файлу заблокирован:** приложение (отображается имя приложения) попыталось получить доступ к файлу, который не разрешен администратором.

Если вы администратор и хотите разрешить доступ к приложению, указанному в уведомлении, см. раздел [Заблокированные хэши](#) в интернет-справке ESET Inspect. Если вы пользователь и хотите изменить поведение этого приложения, обратитесь к администратору.

## Работа с ESET Endpoint Antivirus

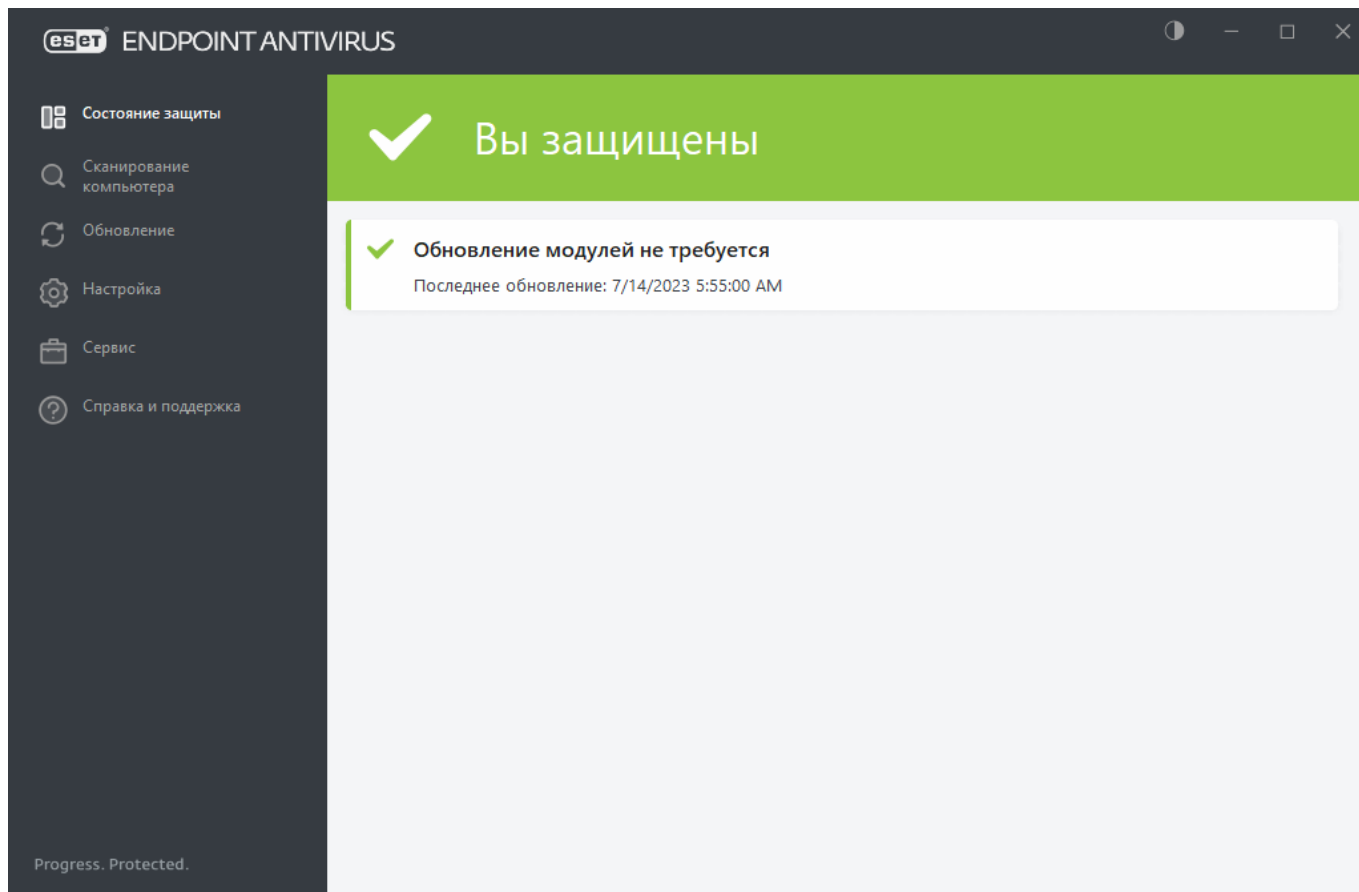
Главное окно программы ESET Endpoint Antivirus разделено на две части. Основное окно справа содержит информацию, относящуюся к параметру, выбранному в главном меню слева.

### Иллюстрированные инструкции

**i** Иллюстрированные инструкции на английском и еще нескольких языках можно найти в разделе [Открытие главного окна программы в продуктах ESET для Windows](#).

Цветовую схему графического интерфейса ESET Endpoint Antivirus можно выбрать в правом верхнем углу главного окна программы. Щелкните значок **Цветовая схема** (значок изменяется в зависимости от выбранной в данный момент цветовой схемы) рядом со значком **Свернуть** и выберите цветовую схему в раскрывающемся меню:

- **Соответствовать цвету системы:** цветовая схема ESET Endpoint Antivirus задается согласно настройкам операционной системы.
- **Темная:** выбор темной цветовой схемы для ESET Endpoint Antivirus (темный режим).
- **Светлая:** выбор стандартной (светлой) цветовой схемы для ESET Endpoint Antivirus.



Опции главного меню:

[Состояние защиты](#): этот пункт предоставляет информацию о состоянии защиты ESET Endpoint Antivirus.

[Сканирование компьютера](#): настройка и запуск сканирования компьютера или создание выборочного сканирования.

[Обновление](#): отображение информации об обновлении модуля и модуля обнаружения.

[Инструменты](#) – Функциям, которые помогают упростить процесс администрирования программы и содержат дополнительные возможности для опытных пользователей.

[Настройка](#): опции конфигурации для функций защиты ESET Endpoint Antivirus и доступ к [расширенным параметрам](#).

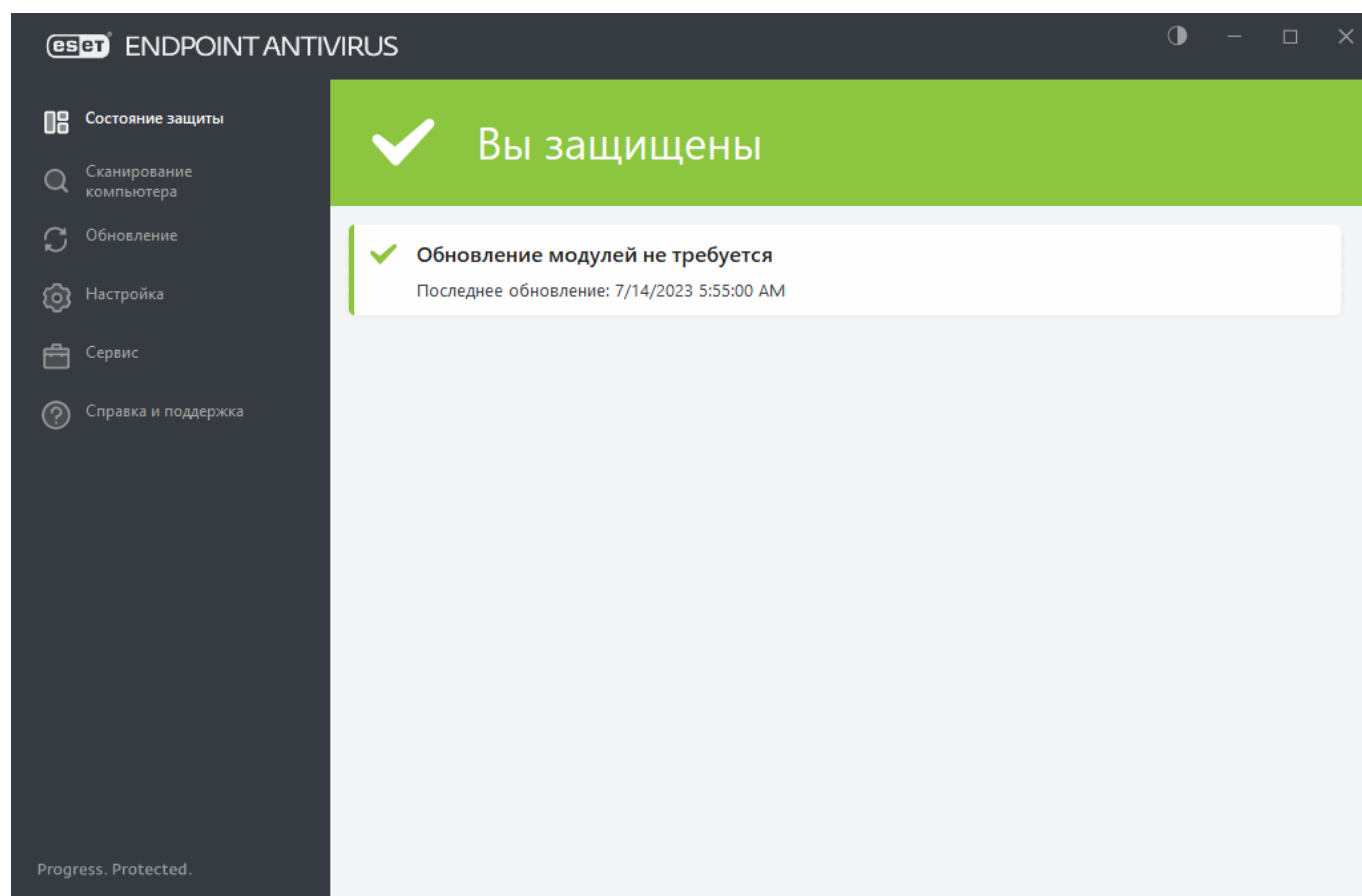
[Справка и поддержка](#): информация о вашей лицензии, установленном продукте ESET, а также ссылки на [интернет-справку](#), [базу знаний ESET](#) и [службу технической поддержки](#).

## Состояние защиты

В окне **Состояние защиты** отображается информация о текущей защите компьютера и последнем обновлении. Зеленый значок **Максимальная защита** означает, что обеспечивается максимальная степень защиты.

В окне **Состояние защиты** отображаются [уведомления](#) с подробной информацией и рекомендуемыми решениями для повышения безопасности ESET Endpoint Antivirus, включения

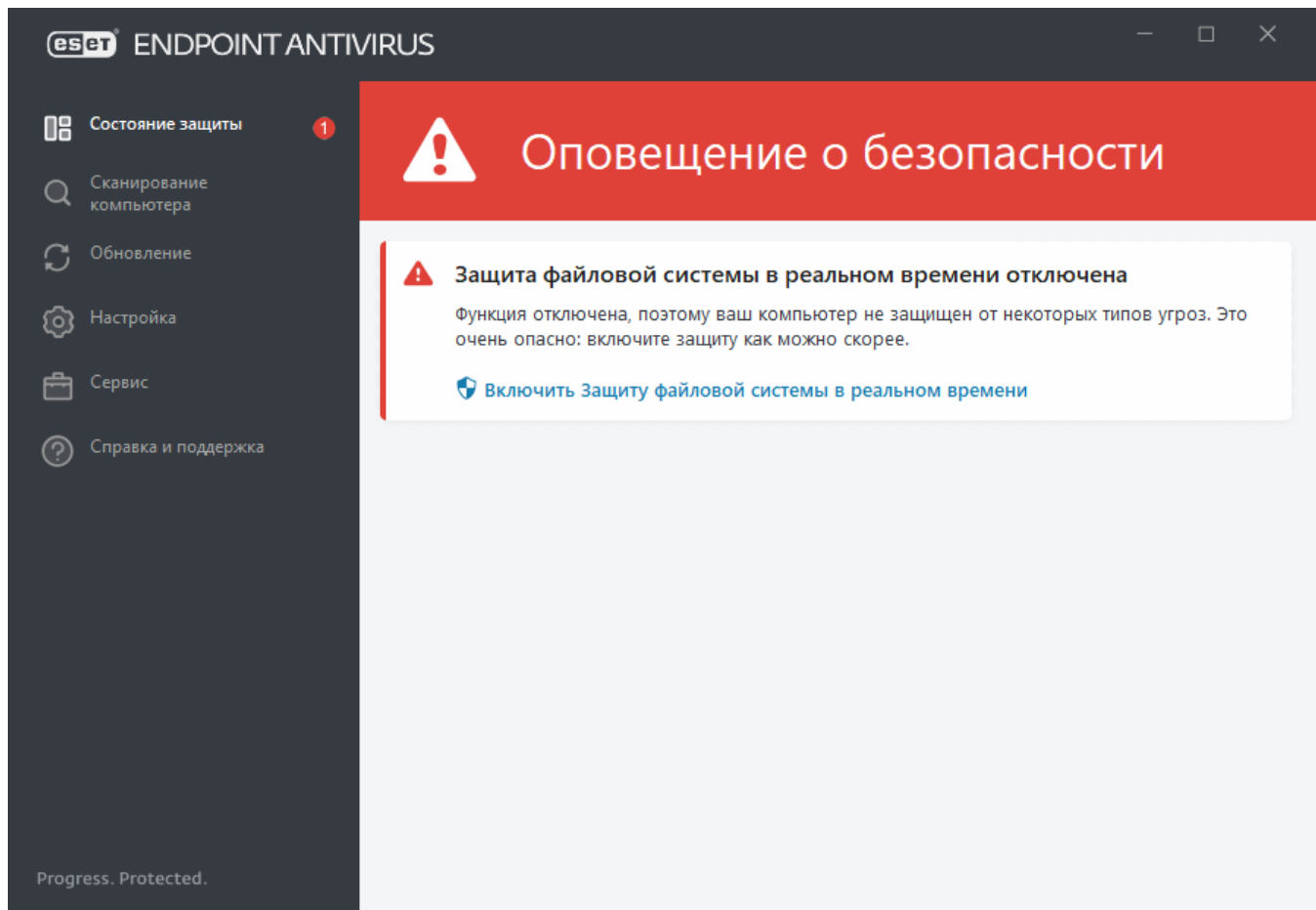
дополнительных функций и обеспечения максимальной защиты.




Зеленый значок и зеленый статус **Вы под защитой** свидетельствуют о максимальном уровне защиты.

## Устранение неполадок программы

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 Antivirus не будут функционировать должным образом.
- **Защита от фишинга не работает:** эта функция не работает, так как не активны другие нужные модули программы.
- **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 настроенные [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. Компьютер не защищен от некоторых типов

угроз, и следует немедленно повторно включить защиту, нажав **Включить систему HIPS**.

- **Регулярные обновления не запланированы:** ESET Endpoint Antivirus не будет проверять наличие важных обновлений и получать их, если не запланировать задачу обновления.
- **Доступ к сети заблокирован** – отображается, если клиентское задание **Изолировать компьютер от сети** этой рабочей станции сработает от ESET PROTECT. 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 вашей лицензии скоро закончится/Срок действия вашей лицензии истекает сегодня:** признаком наличия этой проблемы является появление восклицательного знака в значке состояния защиты. После окончания срока действия лицензии программа больше не сможет выполнять обновления, а значок состояния защиты станет красным.
- **Защита почтового клиента от спама приостановлена:** щелкните **Включить защиту почтового клиента от спама**, чтобы снова 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 Antivirus, 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.



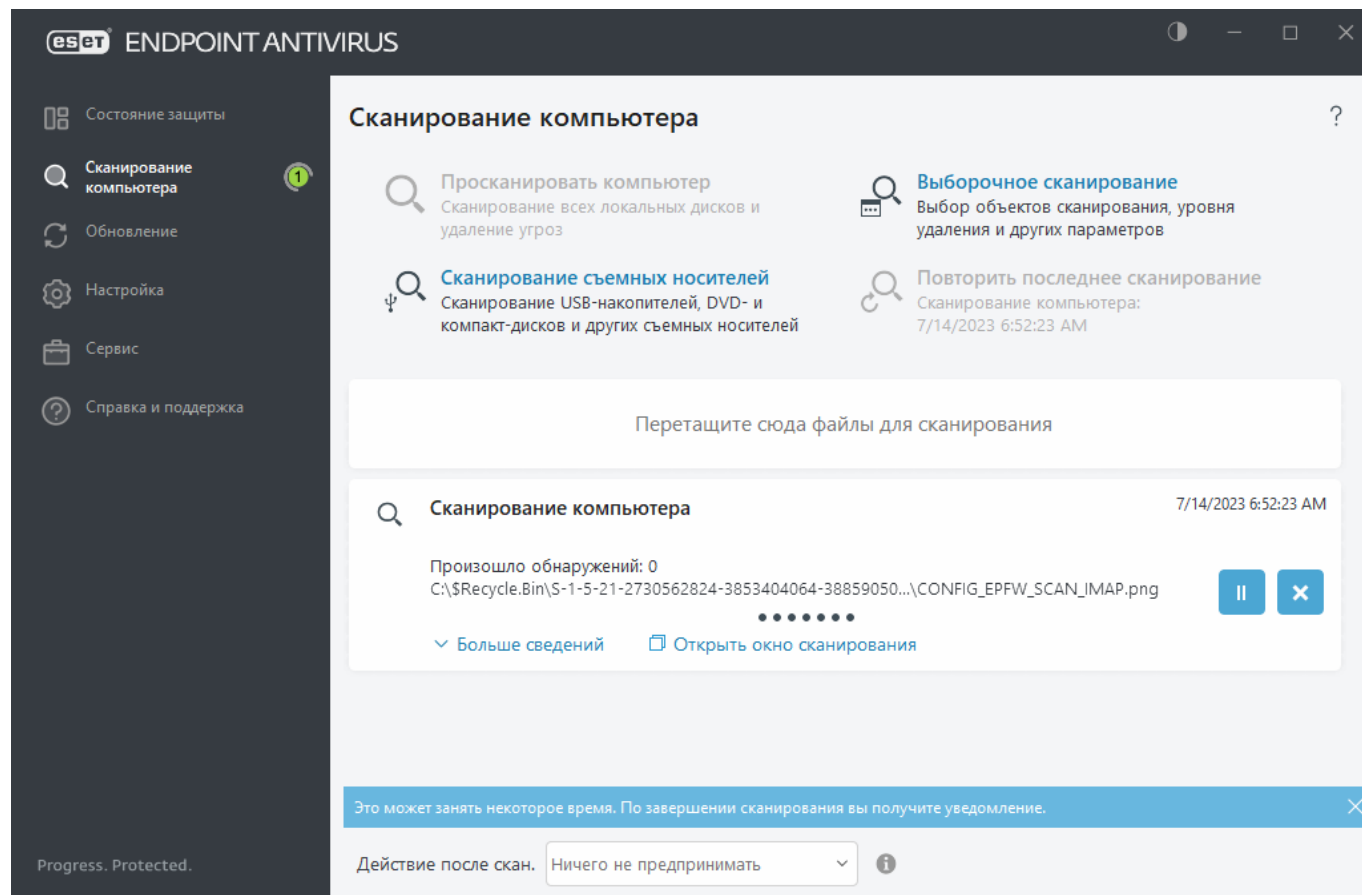
Если состояние относится к функции, заблокированной политикой ESET PROTECT, ссылка будет неактивна.

## Сканирование компьютера

Модуль сканирования по требованию является важной частью ESET Endpoint Antivirus. 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 predetermined profile of scanning and specify objects that need to be scanned.

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

## Просканировать компьютер

Функция **Просканировать компьютер** позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Преимущество функции **Просканировать компьютер** заключается в том, что оно удобно в выполнении и не требует тщательной настройки сканирования. При таком сканировании проверяются все файлы на локальных жестких дисках, а также автоматически очищаются или удаляются обнаруженные заражения. При этом автоматически используется уровень очистки по умолчанию. Дополнительную информацию о типах очистки см. в разделе [Очистка](#).

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.

В разделе **расширенных параметров сканирования** доступны следующие варианты сканирования.



## Выборочное сканирование

**Выборочное сканирование** позволяет указать параметры сканирования, в частности объекты и методы сканирования. Преимущество **выборочного сканирования** заключается в том, что вы можете детально конфигурировать параметры. Конфигурации можно сохранять в пользовательских профилях сканирования, которые удобно применять, если регулярно выполняется сканирование с одними и теми же параметрами.



## Сканирование съемных носителей

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

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



## Повторить последнее сканирование

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

В раскрывающемся меню **Действие после сканирования** можно настроить действие, которое будет выполняться автоматически после завершения сканирования:

- **Ничего не предпринимать:** после сканирования действия предприниматься не будут.
- **Выключить:** после сканирования компьютер отключается.
- **Перезапуск при необходимости:** компьютер перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Перезагрузить:** после сканирования открытые программы закрываются, а компьютер перезагружается.
- **Принудительный перезапуск при необходимости:** компьютер принудительно перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Принудительная перезагрузка:** все открытые программы принудительно закрываются, не дожидаясь вмешательства пользователя, и компьютер перезапускается после завершения сканирования.
- **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.

**i** Доступность действий **Сон** и **Гибернация** зависит от параметров питания и спящего режима операционной системы и возможностей вашего ноутбука или компьютера. Не забывайте, что компьютер в спящем режиме все же работает. Компьютер выполняет основные функции и потребляет электричество, когда работает от аккумулятора. Чтобы сохранить время работы батареи (например, если вы находитесь в пути), рекомендуется перевести компьютер в режим гибернации.

Выбранное действие будет запущено после того, как все запущенные процессы сканирования будут завершены. При выборе **Завершение работы** или **Перезагрузка** в диалоговом окне подтверждения будет отображаться 30-секундный обратный отсчет (щелкните **Отмена**, чтобы деактивировать запрошенное действие).

**i** Сканирование компьютера рекомендуется запускать не реже одного раза в месяц. Его можно сконфигурировать в качестве запланированной задачи в разделе **Сервис > Планировщик**. [Планирование еженедельного сканирования компьютера](#)

## Средство запуска выборочного сканирования

Выборочное сканирование позволяет сканировать оперативную память, сеть или определенные части диска (а не диск целиком). Для этого щелкните **Расширенное сканирование > Выборочное сканирование** и выберите конкретные объекты сканирования в древовидной структуре папок.

В раскрывающемся меню **Профиль** можно выбрать профиль, который будет использоваться для сканирования указанных объектов. По умолчанию используется профиль **Интеллектуальное сканирование**. Существует еще три предварительно заданных профиля сканирования: **Глубокое сканирование**, **Сканирование через контекстное меню** 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** > [ThreatSense](#).

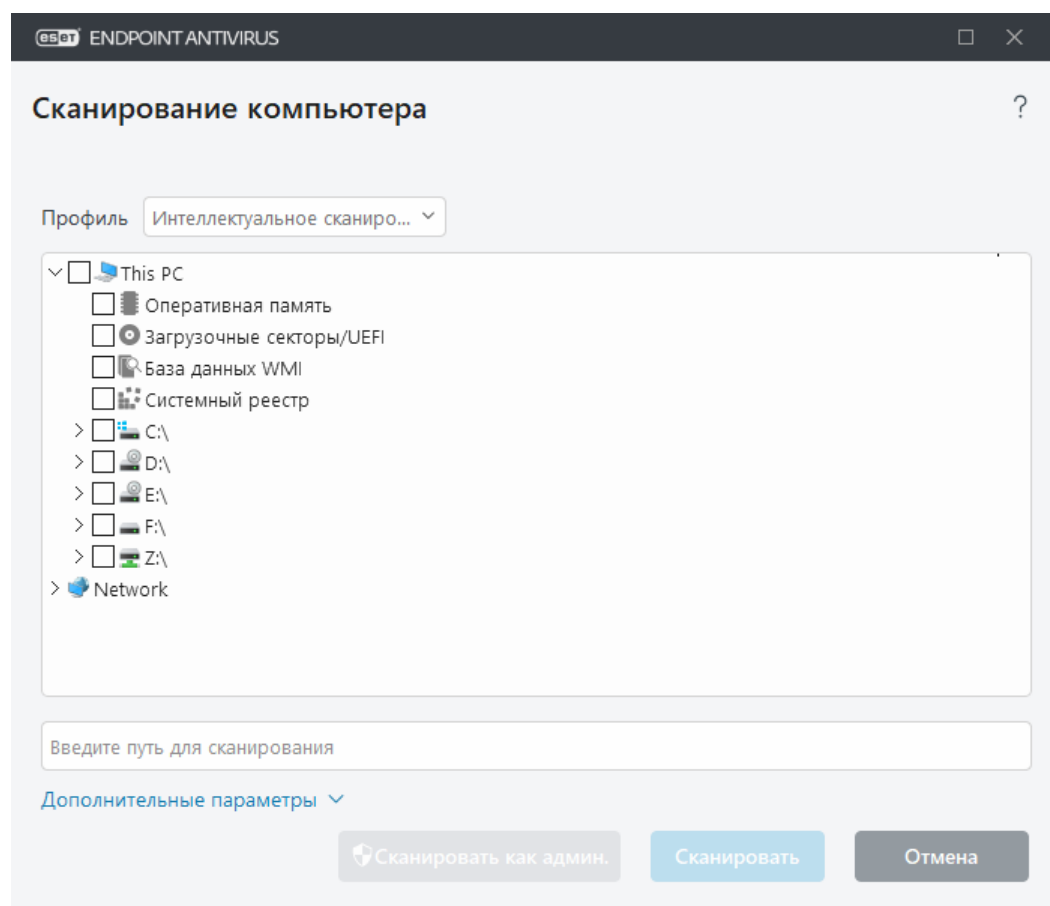
Структура папок (дерево) также содержит определенные объекты сканирования.

- **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 [гlossарии](#).
- **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 объекту сканирования (файлу или папке), введите его путь в текстовом поле под древовидной структурой. Путь вводится с учетом регистра. Чтобы включить объект в сканирование, установите его флажок в древовидной структуре.

### Планирование еженедельного сканирования компьютера

**i** Чтобы запланировать регулярную задачу, см. раздел [Планирование еженедельного сканирования компьютера](#).



Параметры очистки для сканирования можно настроить в разделе [Расширенные параметры](#) > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Сканирование по требованию** > **ThreatSense** > **Очистка**. Чтобы выполнить сканирование без очистки, щелкните **Дополнительные параметры** и выберите **Сканировать без очистки**. История сканирования сохраняется в журнале сканирования.

Если выбран параметр **Пропустить исключения**, файлы с ранее исключенными расширениями будут просканированы без исключений.

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 у текущего пользователя нет прав на доступ к файлам, которые следует просканировать. Данная кнопка недоступна, если текущий пользователь не может вызывать операции контроля учетных записей в качестве администратора.

**i** 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.

**i** Нормальной ситуацией является невозможность сканирования некоторых файлов, например защищенных паролем файлов или файлов, используемых исключительно операционной системой (обычно *pagefile.sys* и некоторых файлов журналов). Более подробную информацию можно найти в [статье нашей базы знаний](#).

**i** **Планирование еженедельного сканирования компьютера**  
Чтобы запланировать регулярную задачу, см. раздел [Планирование еженедельного сканирования компьютера](#).

**Ход сканирования:** индикатор выполнения показывает состояние текущего сканирования.

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

**Произошли обнаружения:** отображается общее количество просканированных файлов и угроз, обнаруженных и удаленных во время сканирования.

Щелкните элемент «Дополнительные сведения», чтобы отобразить следующую информацию:

- **Пользователь:** имя учетной записи пользователя, который запустил сканирование.
- **Просканировано объектов:** количество уже просканированных объектов.
- **Продолжительность:** прошедшее время.

Значок паузы: приостановка сканирования.

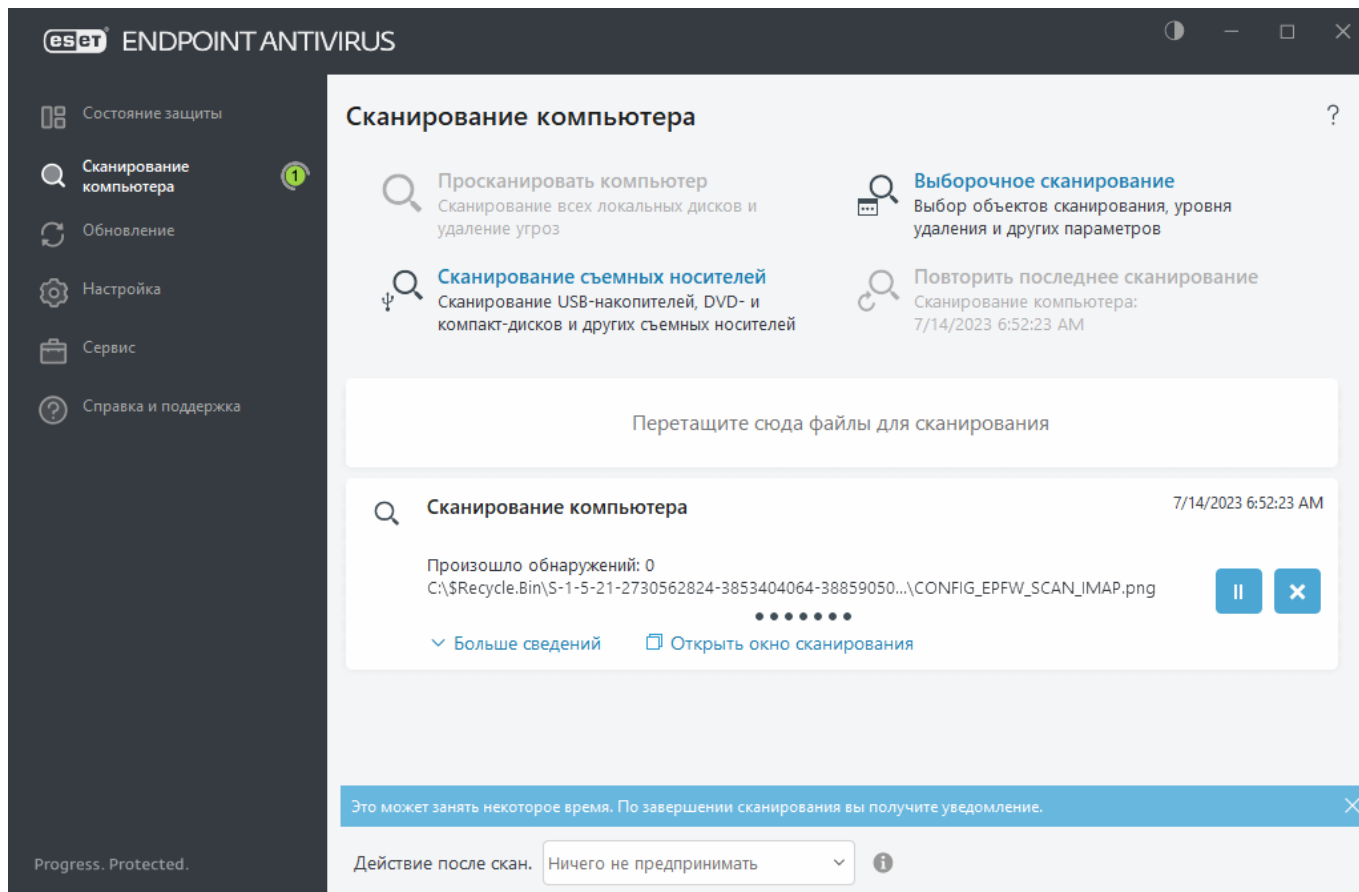
Значок возобновления: эта опция отображается, когда сканирование приостановлено. Щелкните этот значок, чтобы продолжить сканирование.

Значок остановки: завершение сканирования.

Щелкните элемент **Открыть окно сканирования**, чтобы открыть [журнал сканирования компьютера](#) с более подробной информацией о сканировании.

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

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



В раскрывающемся меню **Действие после сканирования** можно настроить действие, которое будет выполняться автоматически после завершения сканирования:

- **Ничего не предпринимать:** после сканирования действия предприниматься не будут.
- **Выключить:** после сканирования компьютер отключается.
- **Перезапуск при необходимости:** компьютер перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Перезагрузить:** после сканирования открытые программы закрываются, а компьютер перезагружается.
- **Принудительный перезапуск при необходимости:** компьютер принудительно перезапускается, только если нужно завершить очистку обнаруженных угроз.
- **Принудительная перезагрузка:** все открытые программы принудительно закрываются, не дожидаясь вмешательства пользователя, и компьютер перезапускается после завершения сканирования.
- **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.

**i** Доступность действий **Сон** и **Гибернация** зависит от параметров питания и спящего режима операционной системы и возможностей вашего ноутбука или компьютера. Не забывайте, что компьютер в спящем режиме все же работает. Компьютер выполняет основные функции и потребляет электричество, когда работает от аккумулятора. Чтобы сохранить время работы батареи (например, если вы находитесь в пути), рекомендуется перевести компьютер в режим гибернации.

Выбранное действие будет запущено после того, как все запущенные процессы сканирования

будут завершены. При выборе **Завершение работы** или **Перезагрузка** в диалоговом окне подтверждения будет отображаться 30-секундный обратный отсчет (щелкните **Отмена**, чтобы деактивировать запрошенное действие).

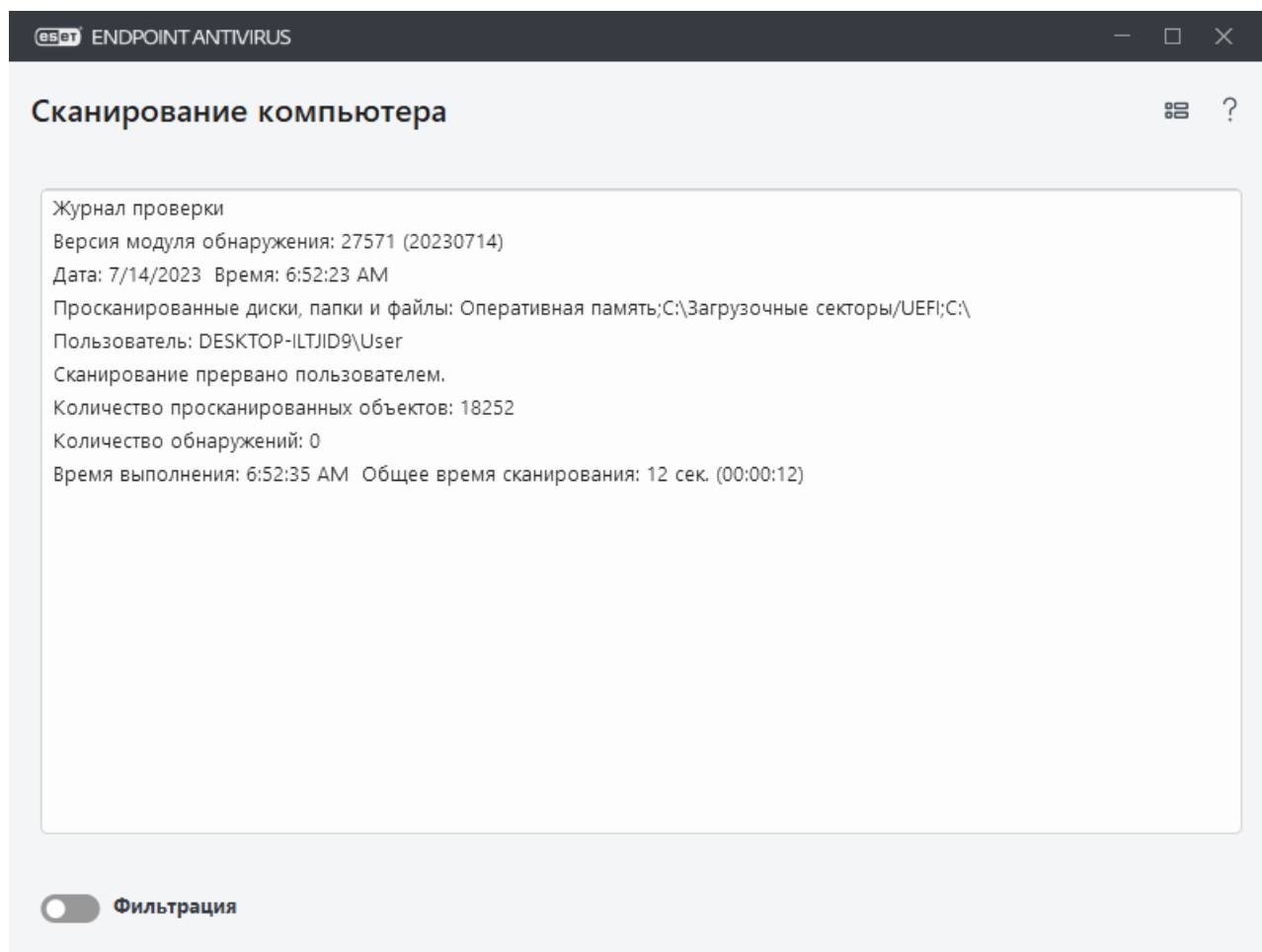
## Журнал проверки сканирования компьютера

В разделе [Файлы журнала](#) можно просмотреть подробную информацию, связанную с конкретным сканированием. Журнал сканирования содержит следующую информацию:


- Версия модуля обнаружения
- дата и время начала;
- список просканированных дисков, папок и файлов;
- Имя сканирования по расписанию (только [сканирование по расписанию](#))
- пользователь, запустивший сканирование;
- Состояние сканирования
- число просканированных объектов;
- количество обнаружений;
- время завершения;
- общее время сканирования.

**i** Новый запуск [задания сканирования компьютера по расписанию](#) пропускается, если все еще выполняется то же задание по расписанию, которое выполнялось ранее. В случае пропуска задания сканирования по расписанию будет создан журнал проверки компьютера с просканированными объектами в количестве 0 и статусом **Сканирование не началось, поскольку все еще выполнялось предыдущее сканирование**.

Чтобы найти предыдущие журналы сканирования, в [главном окне программы](#) выберите **Сервис > Файлы журнала**. В раскрывающемся меню выберите **Сканирование компьютера** и дважды щелкните нужную запись.



**i** Дополнительные сведения о записях «Не удастся открыть», «Ошибка открытия» и/или «Архив поврежден» см. в [статье базы знаний ESET](#).

Щелкните значок переключателя  **Фильтрация**, чтобы открыть окно [Фильтрация журнала](#), где можно уточнить поиск, задав пользовательские критерии. Чтобы просмотреть контекстное меню, щелкните правой кнопкой мыши запись в журнале:

| Действие                      | Использование   |
|-------------------------------|---|
| Фильтрация одинаковых записей | Активирует фильтрацию журнала. В журнале будут отображаться только записи того же типа, что у выбранной записи.   |
| Фильтр                        | При выборе этого параметра отображается окно «Фильтрация журнала», в котором можно задать критерии фильтрации для определенных записей журнала. Сочетание клавиш: <b>Ctrl+Shift+F</b> . |
| Включить фильтр               | Активирует параметры фильтра. Если вы активируете фильтр в первый раз, нужно установить параметры, и откроется окно «Фильтрация журнала».   |
| Отключить фильтр              | Выключает фильтр (то же самое, что щелкнуть переключатель внизу).   |
| Копировать                    | Копирует выделенные записи в буфер обмена. Сочетание клавиш: <b>Ctrl+C</b> .  |
| Копировать все                | Копирует все записи в окне.   |
| Экспорт                       | Экспортирует выделенные записи в XML-файл.  |
| Экспортировать все            | Экспортирует все записи в окне в XML-файл.  |



| Действие             | Использование   |
|----------------------|---|
| Описание обнаружения | Открывает энциклопедию угроз ESET, которая содержит подробную информацию об опасностях и симптомах выделенного заражения. |

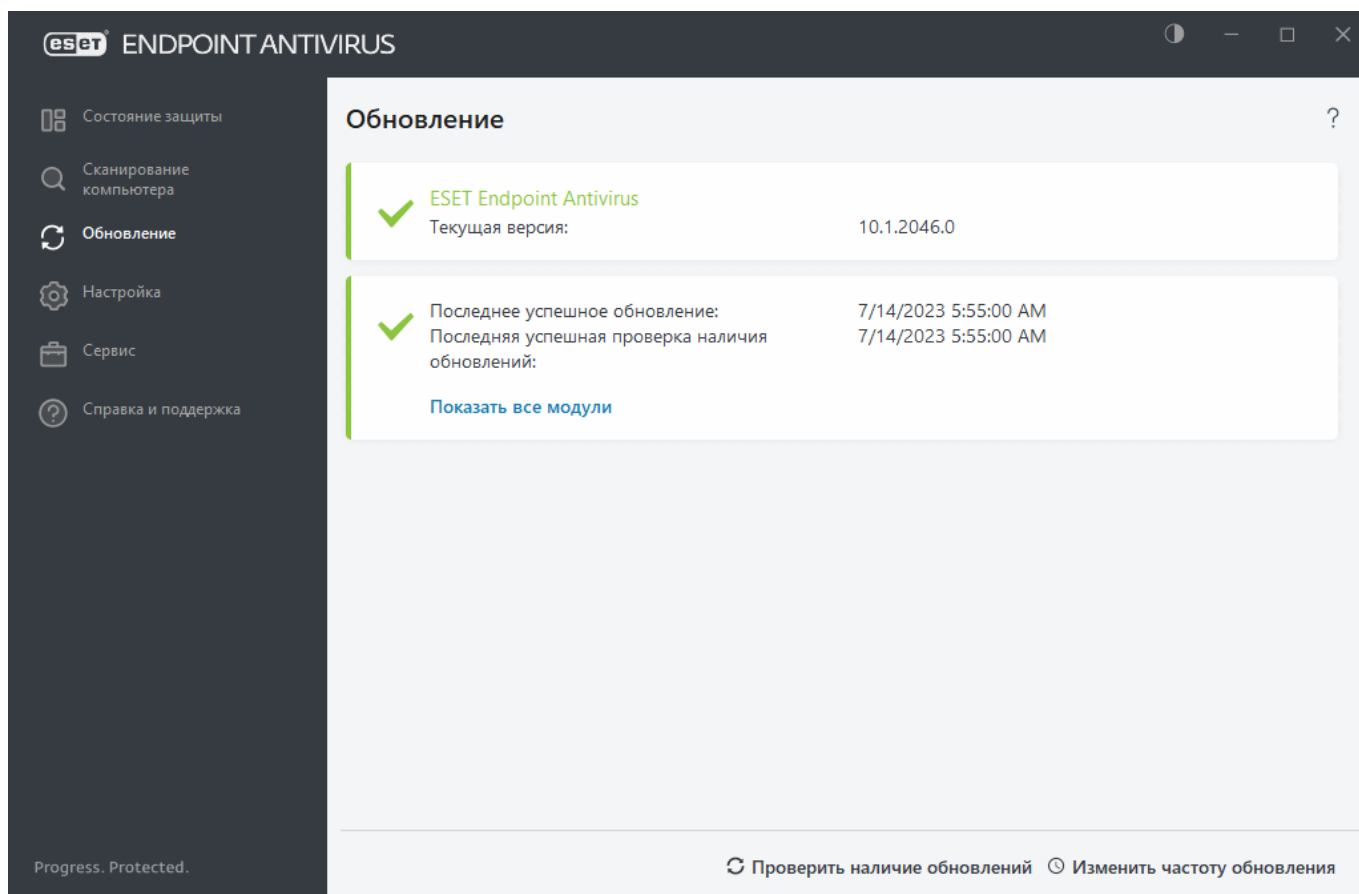
## Обновление

Регулярное обновление ESET Endpoint Antivirus — лучший способ обеспечить максимальный уровень безопасности компьютера. Модуль обновления поддерживает актуальность программных модулей и компонентов системы.

Выбрав пункт **Обновление** в [главном окне программы](#), можно просмотреть информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления.

Кроме автоматического обновления, можно выполнить обновление вручную, нажав кнопку **Проверить наличие обновлений**. Регулярное обновление программных модулей и компонентов является важным аспектом обеспечения полной защиты от вредоносного кода. Уделите особое внимание конфигурированию и работе программных модулей. Для получения обновлений необходимо активировать продукт с помощью вашего лицензионного ключа. Если это не было сделано во время установки, вам потребуется [активировать ESET Endpoint Antivirus](#), чтобы получить доступ к серверам обновления ESET. Компания ESET отправила вам лицензионный ключ по электронной почте после приобретения ESET Endpoint Antivirus.

Если активировать ESET Endpoint Antivirus 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.



**Текущая версия:** номер сборки ESET Endpoint Antivirus.

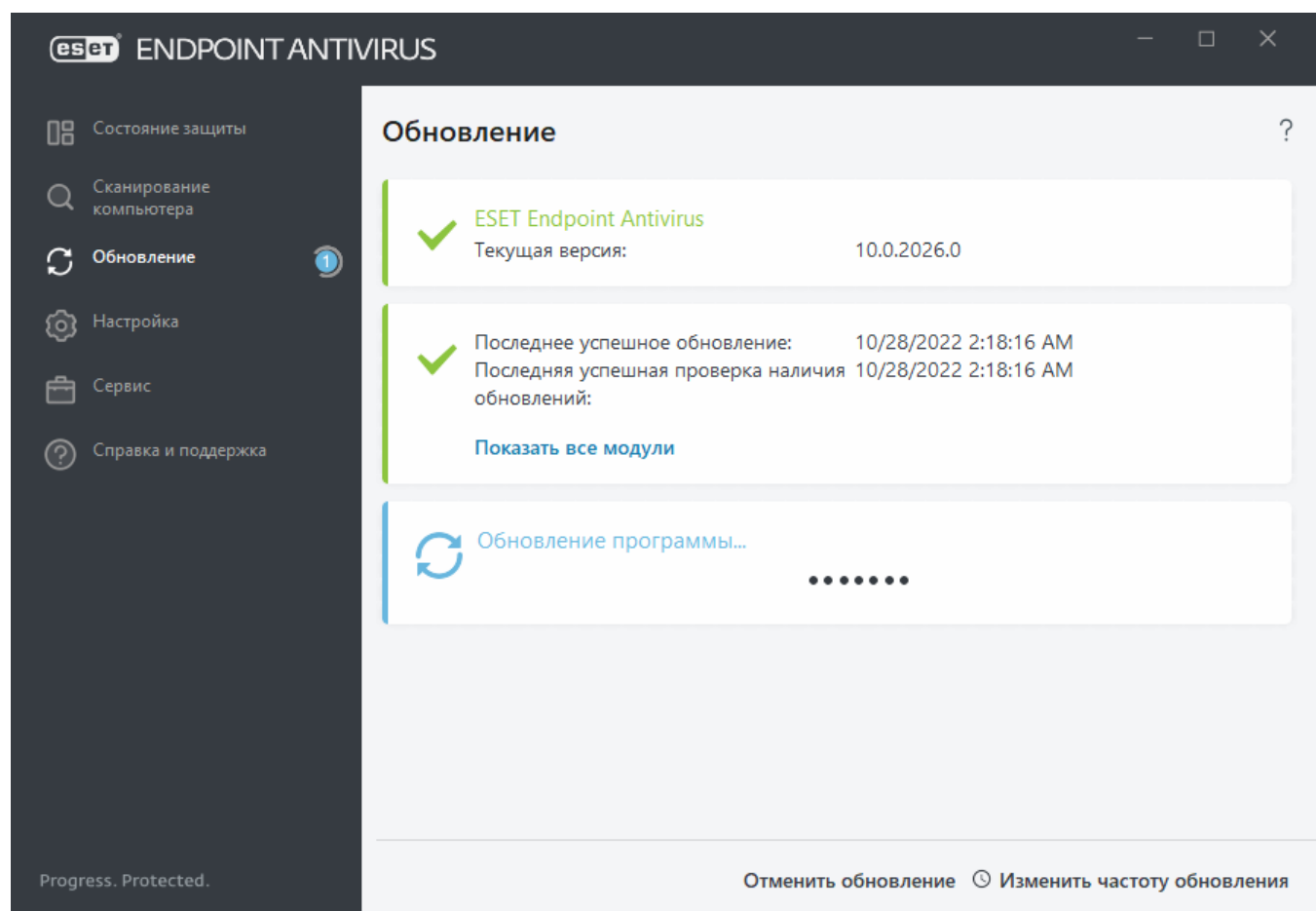
**Последнее успешное обновление:** дата и время последнего обновления. Следует убедиться, что в этом поле указана недавняя дата, поскольку это значит, что версия модуля обнаружения актуальна.

**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**.



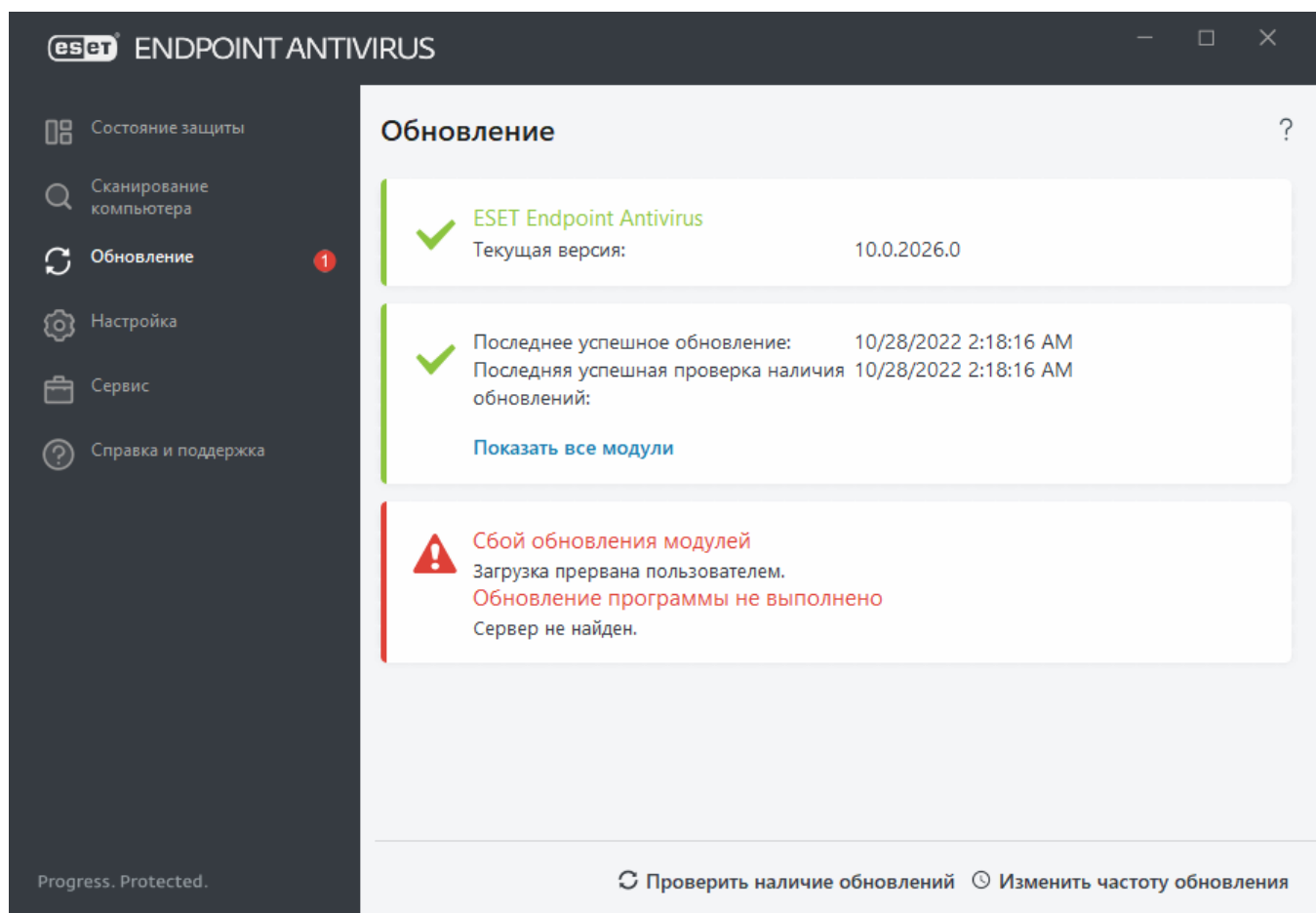
Обычно в окне **Обновление** отображается зеленый флажок, указывающий на то, что установлена актуальная версия программы. Если вы не видите этот флажок, программа устарела. При этом повышается риск заражения. Обновите модули программы как можно скорее.

## Ошибка обновления

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

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

1. **Недействительная лицензия:** ваша лицензия не активна. Рекомендуется проверить данные аутентификации. 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. Убедитесь, что у вас есть активное подключение к Интернету от вашего поставщика услуг Интернета.



**i** Более подробные сведения можно найти в этой [статье базы знаний ESET](#).

# 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 конфигурирования запланированной задачи щелкните **Сервис > Планировщик**. По умолчанию в ESET Endpoint Antivirus активированы указанные ниже задачи обновления:

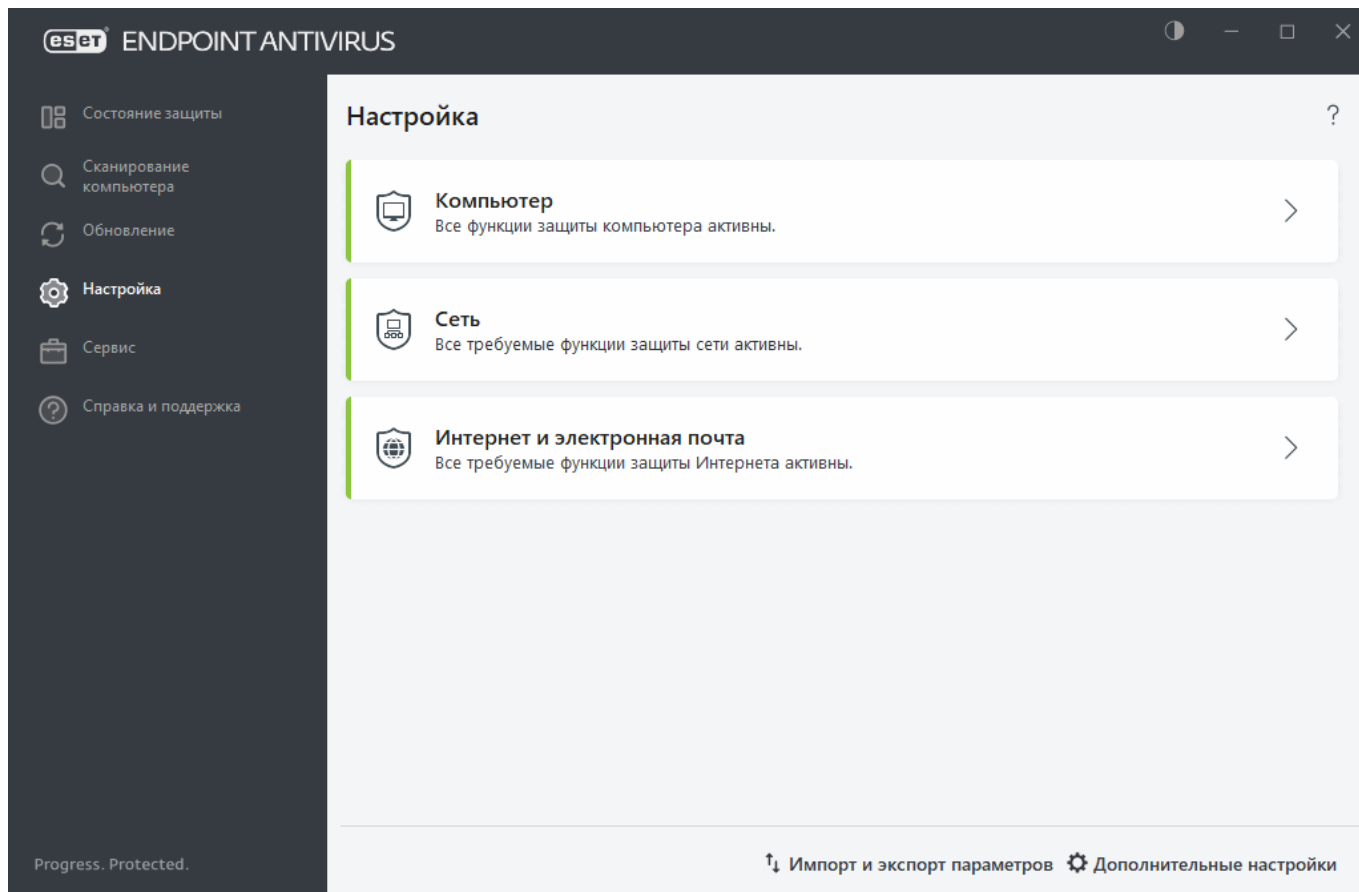
- **Регулярное автоматическое обновление**
- **Автоматическое обновление после входа пользователя в систему**

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](#).

## Настройка

Группы доступных функций защиты можно найти в [главном окне программы](#) в разделе **Настройка**.

**i** При создании политики из веб-консоли ESET PROTECT 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](#)

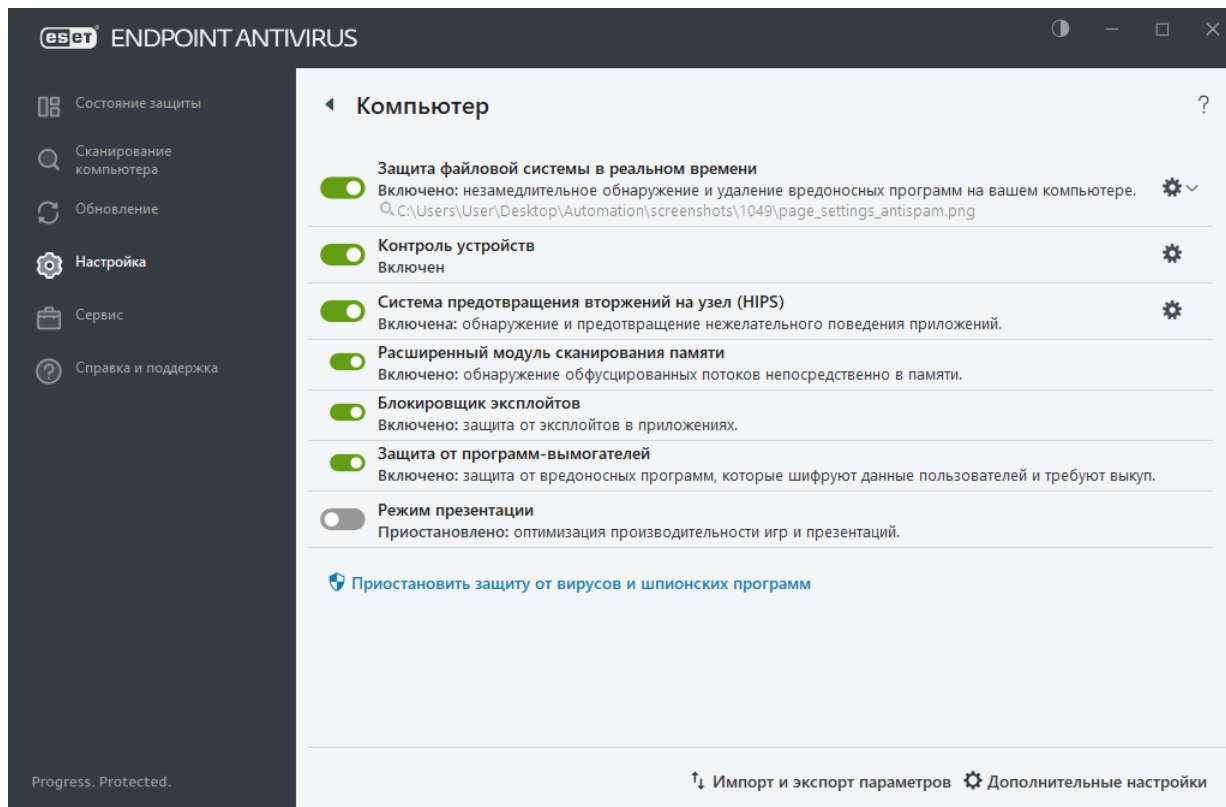
При применении политики ESET PROTECT будет отображаться значок блокировки  рядом с определенным компонентом. Политика, примененная решением ESET PROTECT, может быть переопределена локально после проверки подлинности пользователя, вошедшего в систему (например, администратора). Дополнительные сведения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

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


В нижней части окна настройки есть дополнительные параметры. Чтобы выполнить более подробную настройку параметров для каждого модуля, щелкните [Расширенные 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](#).

## Компьютер

Щелкните элемент **Компьютер** в [главном окне программы](#) в разделе **Настройка**, чтобы просмотреть общие сведения обо всех модулях защиты.




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. Щелкните значок шестеренки  рядом с элементом Защита файловой системы в режиме реального времени, затем выберите Изменить исключения, после чего 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.
- [Контроль устройств](#). Обеспечивает автоматическое [управление](#) устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). Данный модуль позволяет блокировать или изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним.
- [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 [гlossарии](#).
- **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 [гlossарии](#).
- **Защита от программ-вымогателей**: 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.](#)

- [Режим презентации](#) — это функция для тех пользователей, которые стремятся избежать перерывов в работе программного обеспечения и появления отвлекающих уведомлений, а также желают свести к минимуму нагрузку на процессор. 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**.

Чтобы приостановить или отключить отдельные модули защиты, щелкните значок переключателя .

 Отключение модулей может привести к снижению уровня защиты вашего компьютера.

## Обнаружение угрозы

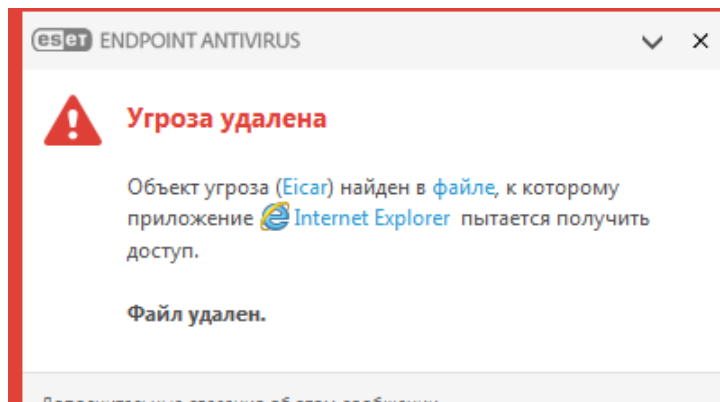
Заражения могут попасть на компьютер из различных источников, таких как [веб-сайты](#), общие папки, электронная почта или [съёмные носители](#) (накопители USB, внешние диски, компакт- или DVD-диски и т. д.).

## Стандартное поведение

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

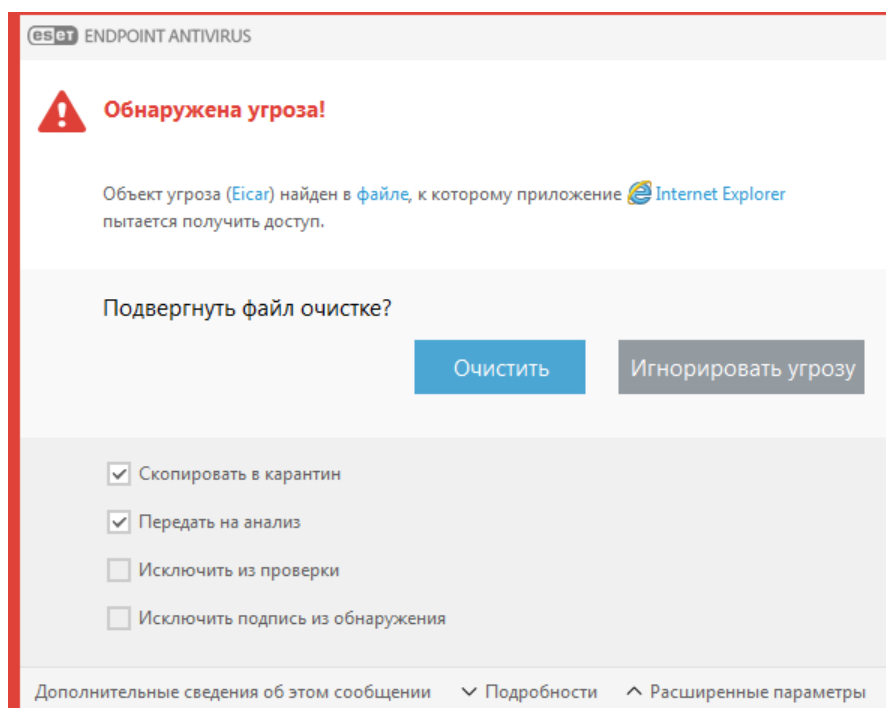
- [Защита файловой системы в режиме реального времени](#)
- [Защита доступа в Интернет](#)
- [Защита почтового клиента](#)
- [сканирование компьютера по требованию;](#)

Каждый модуль использует стандартный уровень очистки и пытается очистить файл, поместить его в [карантин](#) или прервать подключение. В правом нижнем углу экрана отображается окно уведомлений. 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, его следует удалить.

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 Antivirus, щелкнув элемент **Сервис > Карантин**.

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

- Для этого щелкните 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 Antivirus 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.

## Сеть

Откройте [главное окно программы](#) > **Настройка > Сеть**, чтобы настроить основные параметры защиты сети или устранить неполадки сетевого подключения.

Чтобы приостановить или отключить отдельные модули защиты, щелкните значок переключателя .

 Отключение модулей может привести к снижению уровня защиты вашего компьютера.

Щелкните значок шестеренки  рядом с модулем защиты, чтобы получить доступ к его расширенным настройкам.

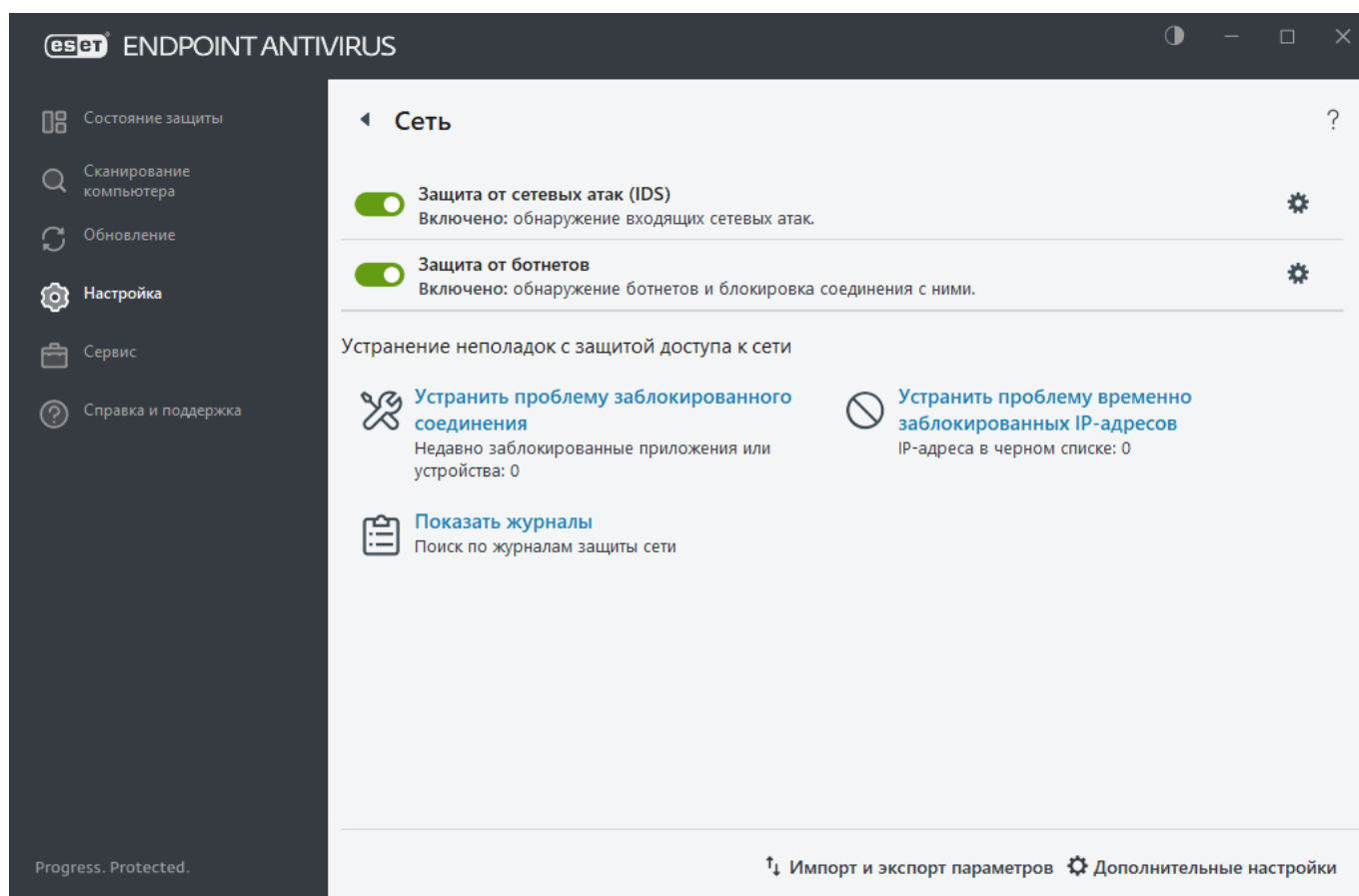
**Защита от сетевых атак (IDS):** анализ содержимого сетевого трафика и защита от сетевых атак. Любой трафик, который расценивается как опасный, блокируется. ESET Endpoint Antivirus сообщает о подключении к незащищенной беспроводной сети или сети со слабой защитой.

**Защита от ботнетов:** быстро и точно определяет вредоносные программы в системе.

**Устранить проблему заблокированного соединения:** помогает устранять проблемы с подключением, вызванные файерволом ESET. Для получения более подробной информации воспользуйтесь [мастером устранения неполадок](#).

**Устранить проблему временно заблокированных IP-адресов** — Просмотр [списка IP-адресов, которые обнаружены как источники атак и добавлены в черный список](#), чтобы блокировать соединение в течение определенного периода времени.

**Показать журналы:** открывает [файл журнала](#) защиты сети.



## Устранение неполадок с доступом к сети

Мастер устранения неполадок помогает устранить проблемы с подключениями, вызванные файерволом. Параметр **Устранение неполадок с доступом к сети** можно найти в [главном окне программы](#) в разделе **Настройка > Сеть > Устранить проблему заблокированного**

## соединения.

Выберите, что необходимо отобразить — соединение, заблокированное для **локальных приложений**, или заблокированный обмен данных с **удаленных устройств**.

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 проблемы с приложением продолжаются или ваше устройство не работает надлежащим образом, щелкните **Создание еще одного правила**, и все подключения, ранее заблокированные для этого устройства, будут разрешены. Если это не поможет, перезагрузите компьютер.



Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:

- [Добавление исключения с помощью мастера устранения неполадок](#)



Если правило не может быть создано, отобразится сообщение об ошибке. Щелкните **Повторить попытку** и повторите этот процесс, чтобы разблокировать обмен данными, или создайте еще одно правило из списка заблокированных подключений.

## 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 Antivirus выберите **Настройка > Сеть > 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.

# Журналы защиты сети

Функция защиты сети программы ESET Endpoint Antivirus сохраняет сведения обо всех важных событиях в файл журнала. Для просмотра файла журнала откройте [главное окно программы](#) > **Настройка > Сеть > Показать журналы**.

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

- Дата и время события.
- имя события;
- источник;
- сетевой адрес целевого объекта;
- сетевой протокол связи;
- Примененное правило или имя червя (если определено).
- Путь и имя приложения.
- Хэш
- Пользователь.
- Лицо, подписавшее приложение (издатель).
- Имя пакета
- Имя службы.

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

## Использование уязвимости в системе безопасности

**i** 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.

# Решение проблем с функцией защиты сети ESET

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

Для решения проблем с Защитой сети ESET см. следующие темы:

- [Устранение неполадок с доступом к сети](#)
- [Ведение журнала и создание правил и исключений на основе журнала](#)
- [Расширенное ведение журналов для защиты сети](#)
- [Решение проблем со сканером сетевого трафика](#)

# Ведение журнала и создание правил и исключений на основе журнала

По умолчанию фаервол ESET не вносит в журнал все блокируемые соединения. Если вы хотите видеть, что заблокировала функция защиты сети, откройте раздел [Расширенные параметры](#) > **Инструменты** > **Диагностика** > **Расширенное ведение журналов** и включите параметр **Включить расширенное ведение журналов для защиты сети**. Если в журнале есть элемент, который фаерволу 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 Защита сети блокировала 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 Antivirus 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 Antivirus следует настроить следующим образом:

1. Установите минимальную степень детализации журнала **Диагностика**, последовательно выбрав [Дополнительные настройки](#) > **Служебные программы** > **Файлы журнала**.
2. Включите параметр **Уведомлять о входящих атаках, которые используют бреши в системе безопасности** в разделе [Расширенные параметры](#) > **Защита** > **Защита доступа к сети** > **Защита от сетевых атак** > **Расширенные параметры** > **Обнаружение вторжений**.

## 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. Открыть [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 Security\Diagnostics\*

## **Решение проблем со сканером сетевого трафика**

Если возникают проблемы с браузером или почтовым клиентом, сначала следует определить, не является ли причиной этому сканер сетевого трафика. Для этого временно отключите сканер сетевого трафика в разделе [Расширенные параметры](#) > **Модуль обнаружения** > **Сканер сетевого трафика** (обязательно снова 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 включен параметр [SSL/TLS](#), попробуйте временно его отключить. Если помогло, значит, можно продолжать использовать SSL/TLS и выполнять обновления.  
Отключить SSL/TLS 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 [защиты доступа в интернет](#) (исключение браузера или почтового клиента оставило бы вас незащищенным). Любое приложение, в отношении которого выполнялась в прошлом фильтрация соединений, должно быть в списке, предоставляемом при добавлении исключений. Поэтому не должно возникнуть необходимости добавлять исключения вручную.

### **Проблема с доступом к устройству в сети**

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

## Проблемы с определенным веб-сайтом

Исключить определенные веб-сайты из [защиты доступа в Интернет](#) можно с помощью управления URL-адресами. Например, если не удастся 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 SSL/TLS программа ESET Endpoint Antivirus выполняет фильтрацию протокола SSL так, что установленные программы доверяют ее действиям (происходит импорт сертификата в их хранилище сертификатов). Для импорта сертификата некоторым приложениям может потребоваться перезапуск. 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 отключите параметр SSL/TLS и снова включите его. Будет выполнена повторная попытка импорта.

## Сетевая угроза заблокирована

Такая ситуация может произойти, когда, например, приложение на компьютере пытается направить вредоносный трафик на другое устройство или сеть, используя брешь в системе безопасности, или при обнаружении попытки сканирования портов системы.

Тип угрозы и IP-адрес соответствующего устройства отображаются в уведомлении. Щелкните **Изменить способ обработки этой угрозы**, чтобы отобразились следующие опции.

**Продолжить блокировать:** обнаруженные угрозы блокируются. Чтобы больше не получать уведомления об угрозах этого типа с определенного удаленного адреса, выберите переключатель **Не уведомлять**, а затем щелкните **Продолжить блокировать**. При этом будет создано [правило службы обнаружения вторжений \(Intrusion Detection Service, IDS\)](#) со следующей конфигурацией: **Блокировать** — по умолчанию, **Уведомить** — нет, **Записать в журнал** — нет.

**Разрешить:** создается [правило службы обнаружения вторжений \(Intrusion Detection Service, IDS\)](#), разрешающее обнаруженную угрозу. Выберите одну из следующих опций, чтобы указать настройки правила, и щелкните **Разрешить**.

- **Уведомлять только тогда, когда эта угроза блокируется** — конфигурация правила: **Блокировать** — нет, **Уведомить** — нет, **Записать в журнал** — нет.
- **Уведомлять всегда, когда эта угроза появляется** — конфигурация правила: **Блокировать** — нет, **Уведомить** — по умолчанию, **Записать в журнал** — по умолчанию.
- **Не уведомлять** — конфигурация правила: **Блокировать** — нет, **Уведомить** — нет,




Записать в журнал — нет.

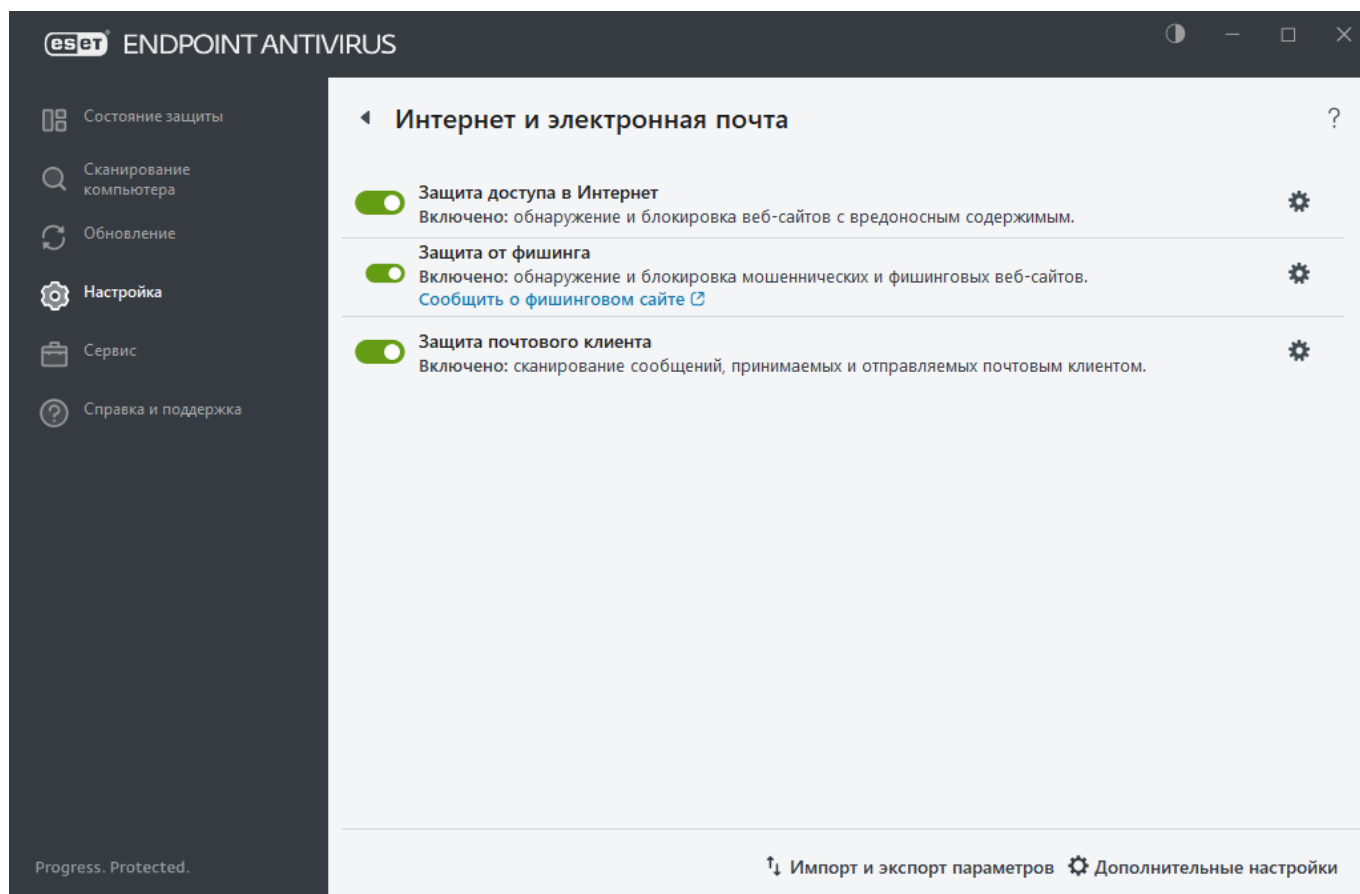
Отображаемая в этом окне информация зависит от типа обнаруженной угрозы. Для получения дополнительных сведений об угрозах и других связанных терминах см. раздел о [типах удаленных атак](#) или [типах обнаруженных угроз](#). Сведения о том, как разрешить событие **Дублирующиеся IP-адреса в сети**, можно найти в [статье базы знаний ESET](#).


## Интернет и электронная почта

Подключение к Интернету стало стандартной функцией персонального компьютера, но Интернет также стал и основной средой распространения вредоносного кода. Чтобы настроить функции ESET Endpoint Antivirus, которые повышают защиту Интернета, откройте [главное окно программы](#) > **Настройка** > **Интернет и электронная почта**.

Чтобы приостановить или отключить отдельные модули защиты, щелкните значок переключателя .

 Отключение модулей может привести к снижению уровня защиты вашего компьютера.



Щелкните значок шестеренки  рядом с модулем защиты, чтобы получить доступ к его расширенным настройкам.

[Защита доступа в Интернет](#) сканирует обмен данными по протоколу HTTP/HTTPS на наличие вредоносных программ и фишинга. Отключать защиту доступа в Интернет следует только для устранения неполадок.



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

**Сообщить о фишинговом сайте:** отправьте сведения о фишинговом или вредоносном веб-сайте в ESET для 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](#).

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

## Защита от фишинга

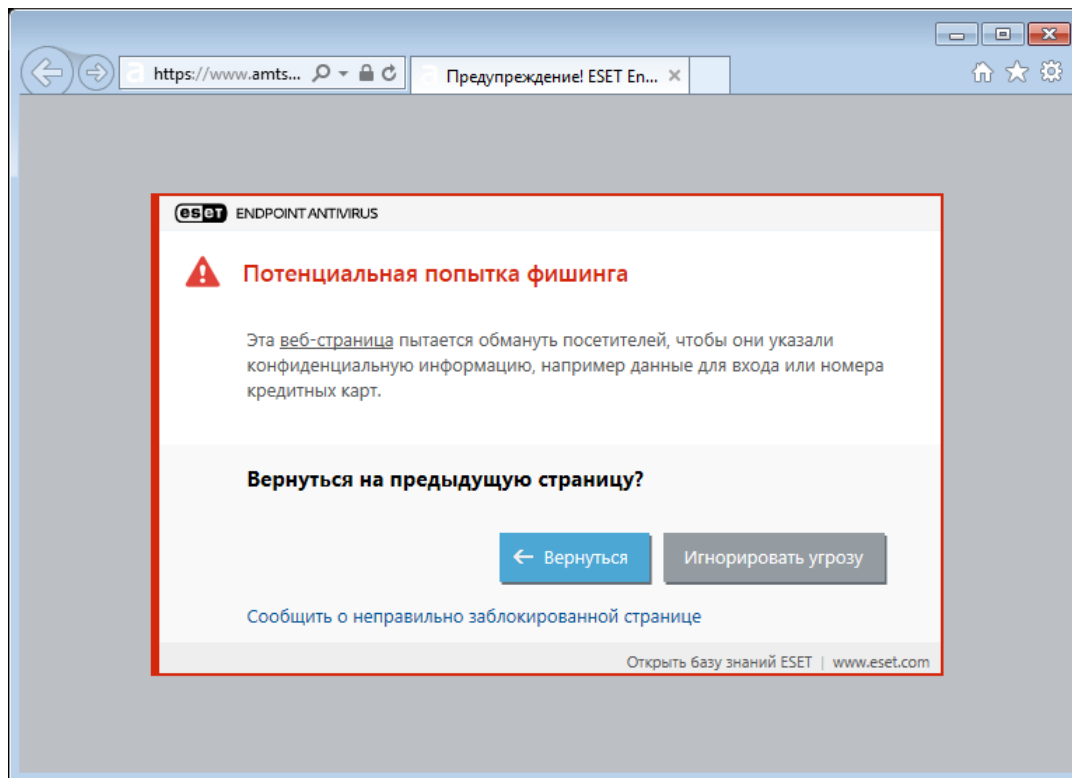
Фишинг — это преступная деятельность с использованием социальной инженерии (манипулирование пользователями для получения конфиденциальной информации). Фишинг используется для получения таких конфиденциальных данных, как номера банковских счетов, PIN-коды и т. д. Дополнительные сведения можно найти в [гlossарии](#). Программа ESET Endpoint Antivirus обеспечивает защиту от фишинга, блокируя веб-страницы, о которых известно, что они распространяют такой тип содержимого.

Защита от фишинга включена по умолчанию. Этот параметр можно настроить в разделе [Расширенные параметры](#) > **Защита** > **Защита доступа в Интернет**.

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

## Доступ к фишинговому веб-сайту

При доступе к известному фишинговому веб-сайту в вашем веб-браузере отобразится следующее диалоговое окно. Если вы все равно хотите открыть этот веб-сайт, щелкните элемент **Игнорировать угрозу** (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 > Защиты > Защита доступа в Интернет > Управление URL-адресами > Список адресов > Изменить** и добавьте необходимый веб-сайт в список.

## Сообщить о фишинговом сайте

С помощью ссылки **Сообщить о неправильно заблокированной странице** можно сообщить о веб-сайте, который неправильно определен как угроза.

Или же адрес веб-сайта можно отправить по электронной почте. Отправьте письмо на адрес [samples@eset.com](mailto: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.).

## Импорт и экспорт параметров

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

**Иллюстрированные инструкции**  
Иллюстрированные инструкции на английском и еще нескольких языках приведены в разделе **Импорт и экспорт конфигурации ESET с помощью XML-файла**.

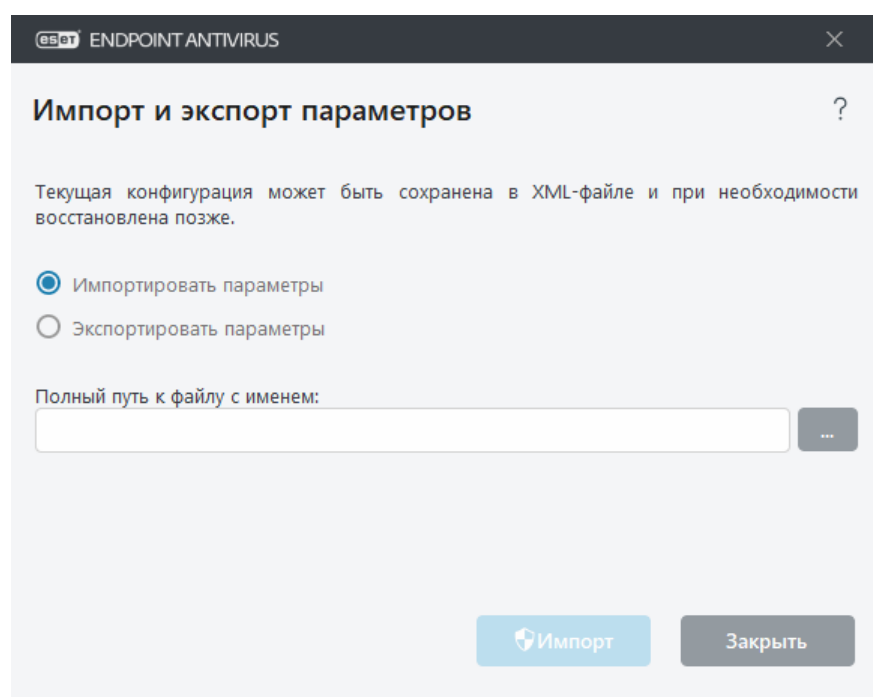
Импорт и экспорт файлов конфигурации можно применять, если нужно создать резервную копию текущей конфигурации программы ESET Endpoint Antivirus для использования в будущем. Экспорт параметров также удобен, если необходимо использовать предпочитаемую

конфигурацию на нескольких компьютерах. Файл .xml можно импортировать для переноса нужных параметров.

Чтобы импортировать конфигурацию, в [главном окне программы](#) щелкните **Настройка > Импорт и экспорт параметров** и выберите **Импортировать параметры**. Введите имя файла конфигурации или нажмите кнопку ..., чтобы выбрать файл конфигурации, который следует импортировать.

Чтобы экспортировать конфигурацию, в [главном окне программы](#) щелкните **Настройка > Импорт и экспорт параметров**. Выберите **Экспортировать параметры** и введите полный путь к файлу с именем. Щелкните ..., чтобы перейти в расположение на вашем компьютере, в котором необходимо сохранить файл конфигурации.

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

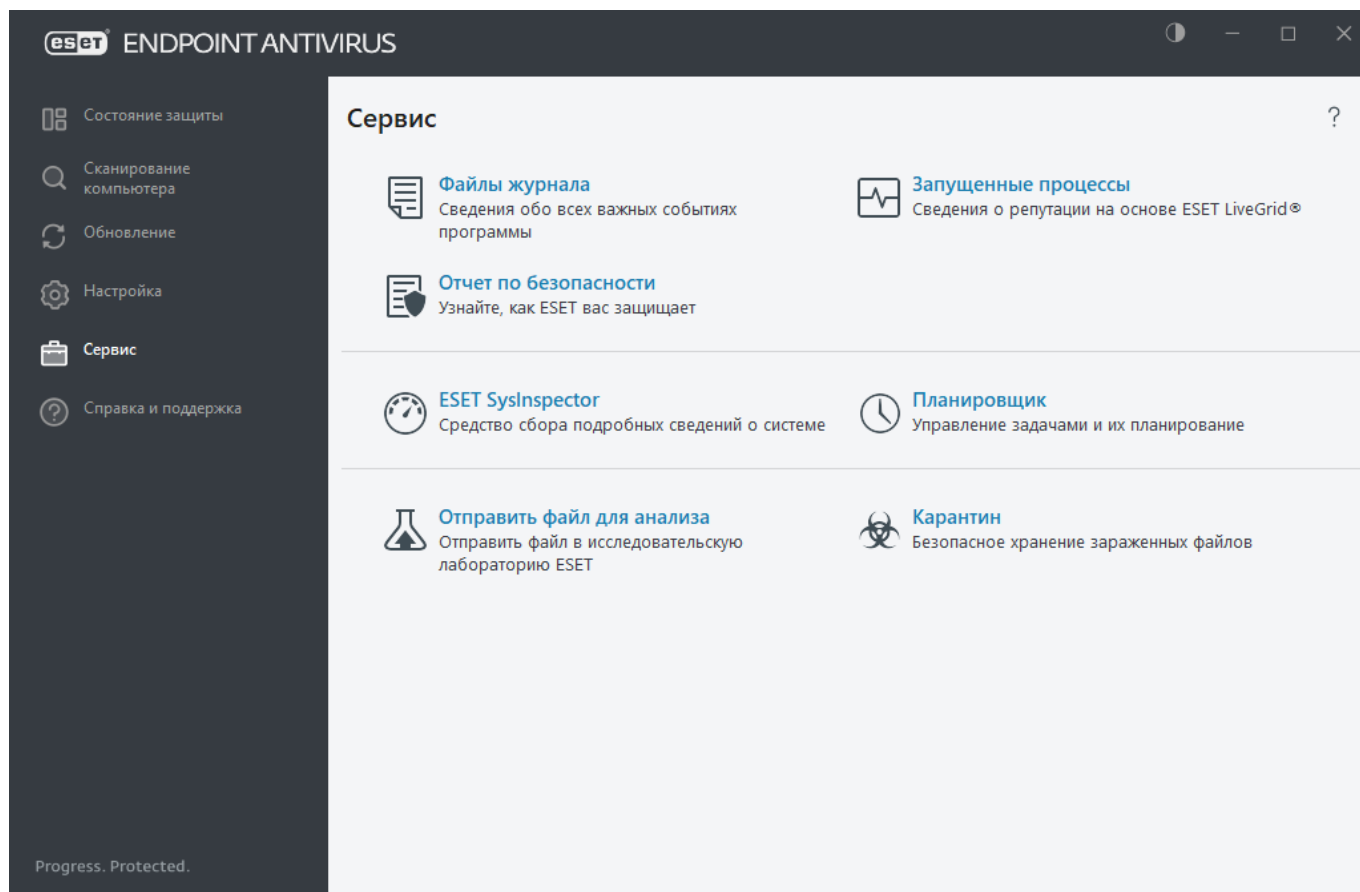


## Служебные программы

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

- [Файлы журнала](#)
- [Запущенные процессы](#) (если использование системы ESET LiveGrid® включено в ESET Endpoint Antivirus)
- [Отчет по безопасности](#) (для неуправляемых конечных точек)
- [ESET SysInspector](#)
- [Планировщик](#)
- [Отправка образца на анализ](#). Возможность отправить подозрительный файл на анализ в исследовательскую лабораторию ESET (может быть недоступна в зависимости от конфигурации ESET LiveGrid®).

- [Карантин](#)



## Файлы журнала

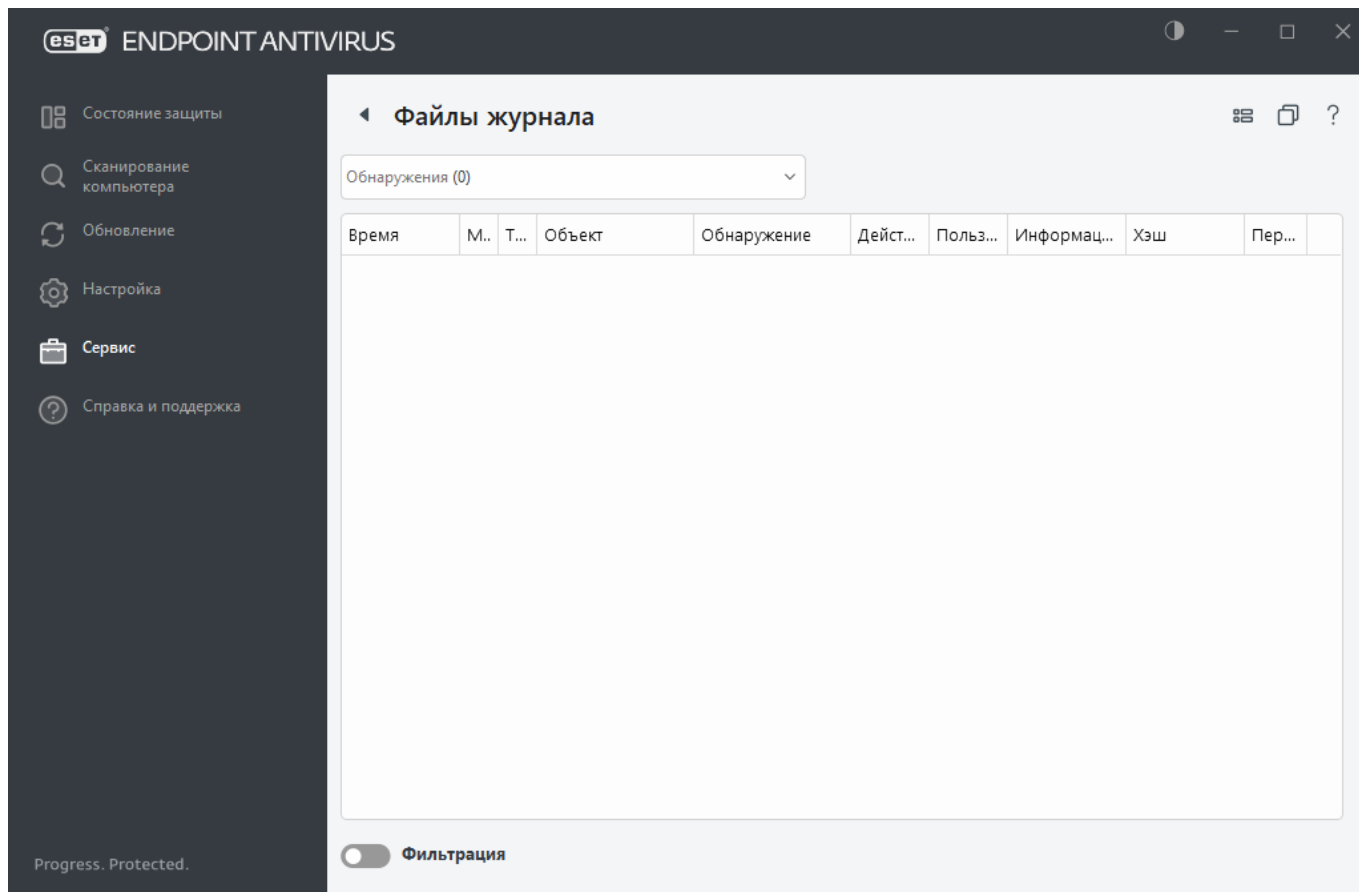
Файлы журнала содержат информацию о важных программных событиях и предоставляют сводные сведения об обнаруженных угрозах. Журналы являются важнейшим элементом анализа, обнаружения угроз и устранения неполадок. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии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

Получить доступ к файлам журнала можно из главного окна программы с помощью команды **Службные 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 Antivirus. 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 Antivirus. 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. Дополнительные сведения см. в [интерактивном руководстве пользователя ESET Enterprise Inspector](#).
- **Отправленные файлы.** Содержит записи о файлах, отправленных в ESET LiveGrid® или [ESET LiveGuard](#) 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 все удаленные атаки, обнаруженные [защитой от сетевых атак](#). 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 защиты сети может помочь своевременно обнаружить попытки заражения компьютера, чтобы предотвратить несанкционированный доступ. Дополнительные сведения о сетевых атаках см. в разделе [IDS и расширенные параметры](#).
- **Отфильтрованные веб-сайты:** этот список полезен, если вы хотите просмотреть список веб-сайтов, заблокированных [защитой доступа в Интернет](#). В этих журналах отображается время, URL-адрес, пользователь и приложение, с помощью которого установлено соединение с конкретным веб-сайтом.
- **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 можно задать критерии фильтрации для определенных записей журнала в [окне «Фильтрация 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.
- **Копировать ячейку:** копирование содержимого ячейки по ее щелчку правой кнопкой мыши.
- **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 следующее/Найти ранее:** щелкнув этот параметр, можно определить критерии фильтрации, чтобы выделить определенную запись в окне «Фильтрация журнала».

- **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 **ОК**, 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**.

## 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.

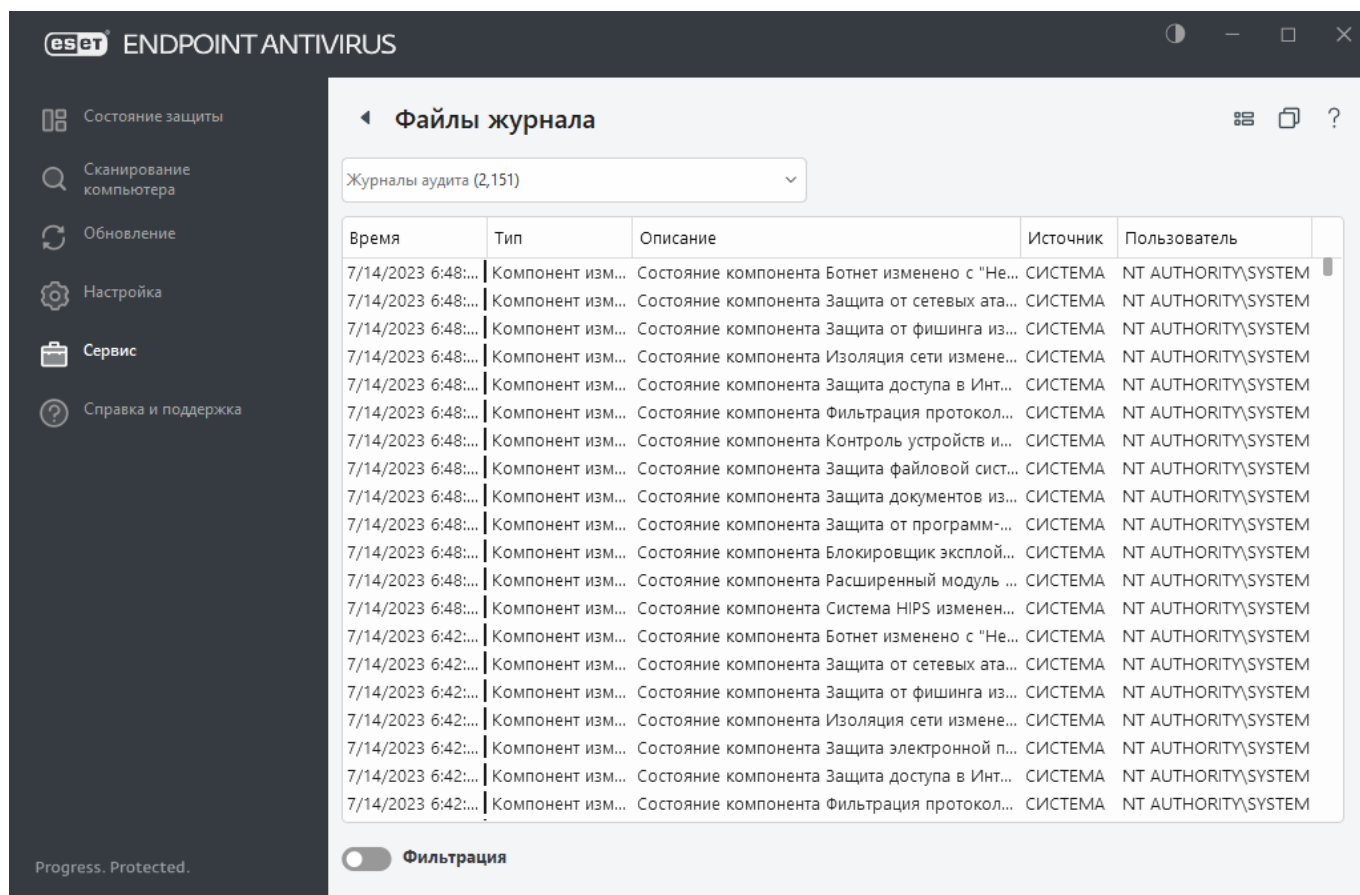
Журнал аудита — это новый тип ведения журнала, который помогает определить причину проблемы. В журнал аудита заносятся изменения в конфигурации или состоянии защиты и записываются моментальные снимки для последующего изучения.

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.





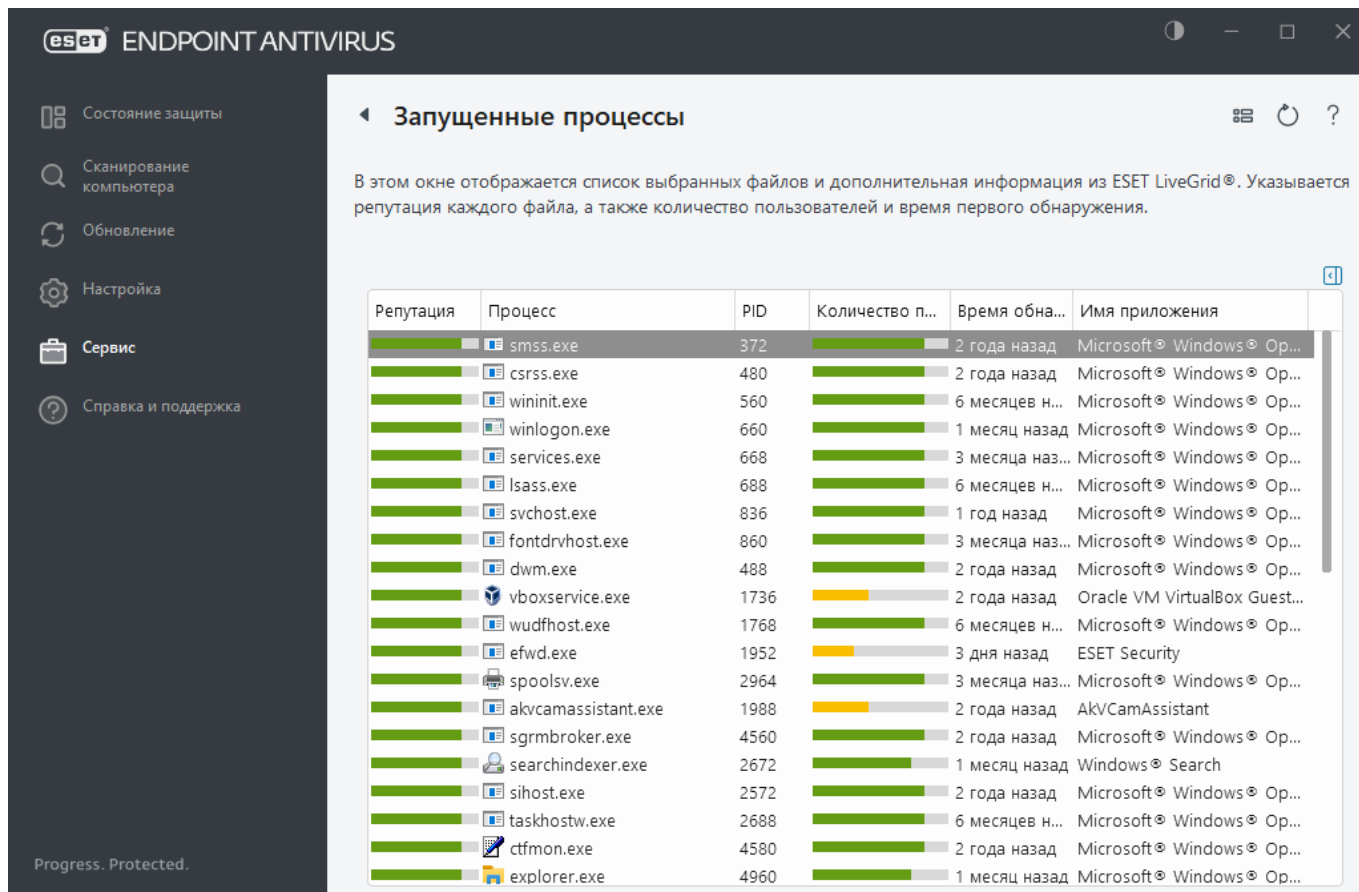
В окне «Файлы журнала» щелкните правой кнопкой мыши любой тип в разделе **Параметры изменены** журнала аудита и выберите в контекстном меню пункт **Показать изменения**, чтобы просмотреть подробные сведения о внесенном изменении. Кроме того, вы можете отменить изменение параметров, выбрав в контекстном меню пункт **Восстановить** (недоступен для продуктов под управлением 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.

## 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 Antivirus предоставляет подробные сведения о запущенных процессах для защиты пользователей с помощью технологии [ESET LiveGrid®](#).



**Репутация:** в большинстве случаев ESET Endpoint Antivirus и технология ESET LiveGrid® присваивают объектам (файлам, процессам, разделам реестра и т. п.) уровни риска на основе наборов эвристических правил, которые изучают характеристики каждого объекта и затем оценивают вероятность их вредоносной деятельности. На основе такого эвристического анализа объектам присваивается уровень 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.

**i** 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®.

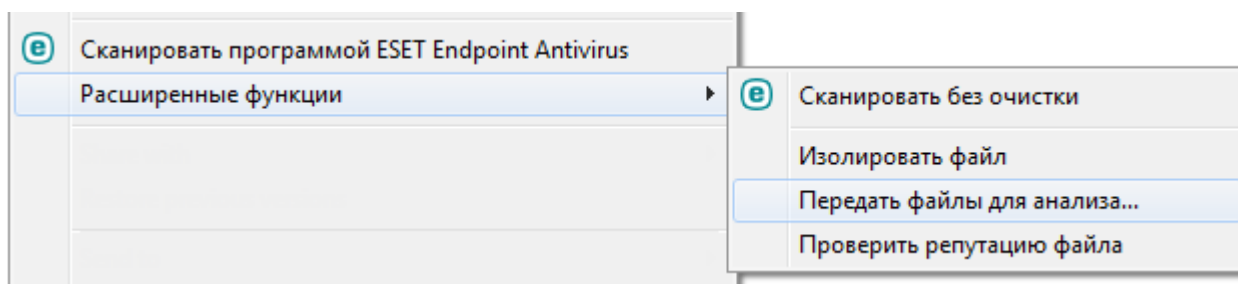
**i** Если для приложения выбран уровень безопасности Неизвестно (оранжевый), оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в безопасности файла, воспользуйтесь функцией [отправки на анализ](#), чтобы отправить файл в вирусную лабораторию ESET.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

**Имя приложения:** конкретное имя программы или процесса.

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

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

**i** 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:

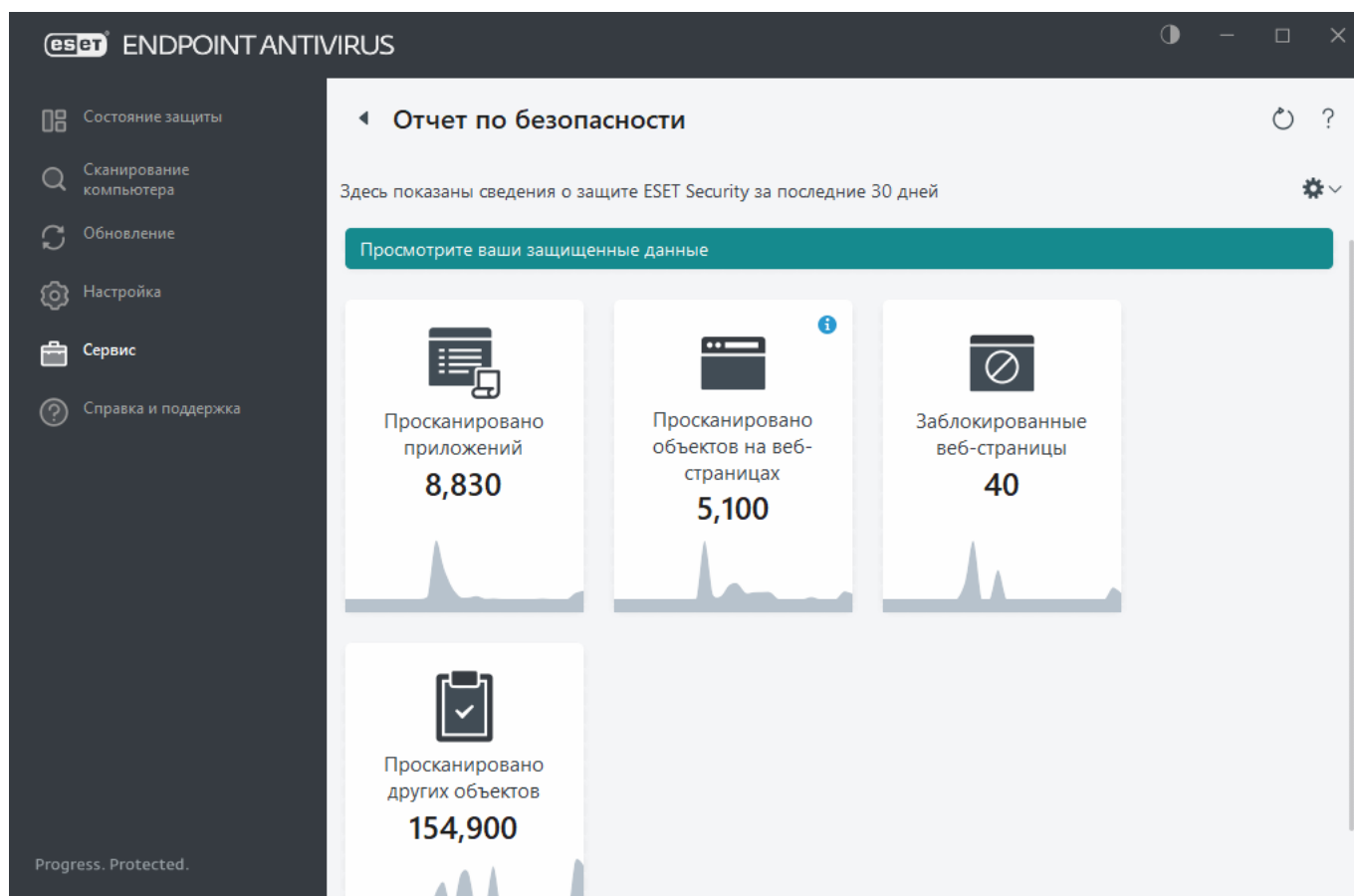
- **Заблокированные веб-страницы:** отображает количество заблокированных веб-страниц (URL-адрес внесен в «черный» список потенциально нежелательных приложений, фишинговый сайт, взломанный маршрутизатор, IP-адрес или сертификат).
- **Обнаружены зараженные объекты электронной почты:** отображается количество обнаруженных зараженных [объектов](#) электронной почты.
- **Обнаружено потенциально нежелательное приложение:** отображается количество [потенциально нежелательных приложений](#).
- **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.

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 Antivirus 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](#) > **Уведомления** > **Интерактивные предупреждения** > **Подтверждения**.

## 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. Чтобы узнать, как использовать ESET SysInspector, см. интерактивную справку [ESET SysInspector](#).

В окне ESET SysInspector отображаются следующие сведения о журналах:

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

Доступны перечисленные далее действия.

- **Показать** — открывает выбранный журнал в ESET SysInspector. Вы также можете щелкнуть файл журнала правой кнопкой мыши и выбрать в контекстном меню пункт **Показать**.
- **Создать:** создание журнала. Прежде чем пытаться открыть журнал, подождите, пока не сгенерируется ESET SysInspector (состояние **Создано**). Журнал сохраняется в папке C:\ProgramData\ESET\ESET Security\SysInspector.
- **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).
- **Создать:** создание журнала. Прежде чем пытаться открыть журнал, подождите, пока не сгенерируется ESET SysInspector (состояние **Создано**).
- **Удалить:** удаление выделенных журналов из списка.
- **Удалить все:** удаление всех журналов.
- **Экспорт:** экспорт журнала в файл или архив в формате XML.

## Планировщик

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

Планировщик можно открыть из главного окна программы ESET Endpoint Antivirus, щелкнув элемент **Сервис > Планировщик**. Здесь приведен полный список запланированных задач и параметры их запуска (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.

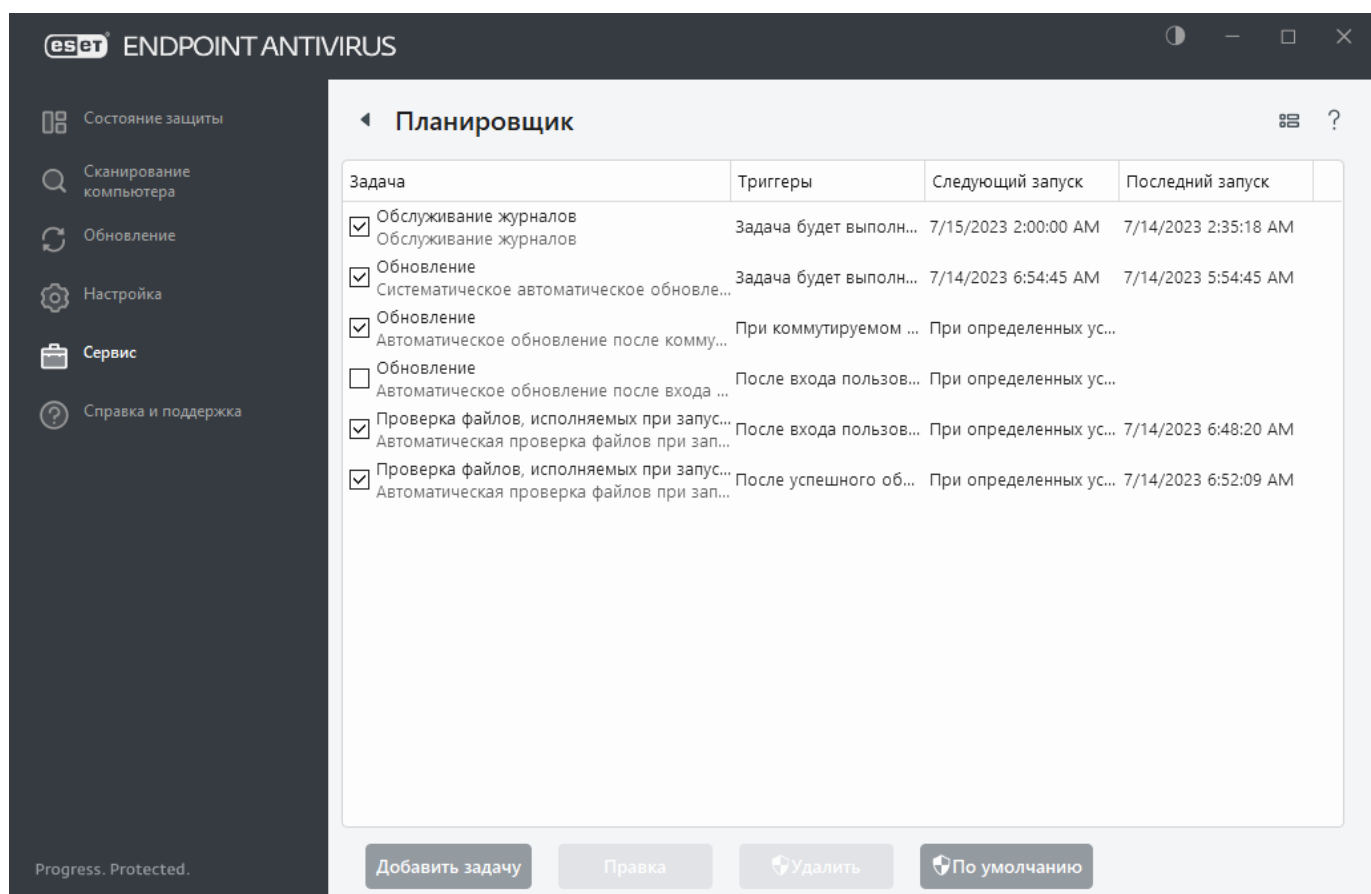
По умолчанию в **планировщике** отображаются следующие запланированные задачи.

- **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)

**i** Функция ESET PROTECT: произвольная задержка выполнения задачи позволяет снизить нагрузку на сервер при выполнении задач, особенно в крупных сетях. Она дает возможность задать промежуток времени, в течение которого задача может быть выполнена по всей сети (в отличие от выполнения задачи сразу на всех рабочих станциях в сети). При запуске задачи заданное время произвольно делится, благодаря чему каждой рабочей станции в сети выделяется уникальное время выполнения задачи. Это позволяет избежать перегрузки серверов и сопутствующих проблем (например, некоторые серверы могут сообщать о [DoS-атаках](#) при выполнении массового обновления сразу на всех рабочих станциях в сети).

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 из них.
  - **Сканирование компьютера по требованию:** сканирование файлов и папок на компьютере.
  - **Обновление:** планирование задачи обновления, в рамках которой обновляется модуль обнаружения и программные модули.
4. Активируйте кнопку **Включено** при необходимости активировать задачу (это можно сделать позже, установив/сняв флажок в списке запланированных задач), нажмите кнопку **Далее** и выберите один из режимов времени выполнения:
- **Однократно:** задача будет выполнена однократно в указанные дату и время.
  - **Многократно:** задача будет выполняться регулярно через указанный промежуток времени.
  - **Ежедневно:** задача будет многократно выполняться каждые сутки в указанное время.
  - **Еженедельно:** задача будет выполняться в выбранный день недели в указанное время.
  - **При определенных условиях:** задача будет выполнена при возникновении указанного события.
5. Установите флажок **Пропускать задачу, если устройство работает от аккумулятора**, чтобы свести к минимуму потребление системных ресурсов, когда ноутбук работает от аккумулятора. Задача будет выполняться в день и время, указанные в полях области **Выполнение задачи**. Если задача не могла быть выполнена в отведенное ей время, можно указать, когда будет предпринята следующая попытка запуска задачи.
- **В следующее запланированное время**
  - **Как можно скорее**
  - **Незамедлительно, если с момента последнего запуска прошло больше времени, чем указано** (интервал можно указать с помощью параметра **Время с момента последнего запуска**).

Чтобы просмотреть запланированную задачу, щелкните ее правой кнопкой мыши и выберите **Показать информацию о задаче**.

## Параметры сканирования по расписанию

В этом окне можно задать расширенные параметры для запланированных задач сканирования компьютера.

Чтобы выполнить сканирование без очистки, щелкните **Дополнительные параметры** и выберите **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.

Действие, которое нужно автоматически выполнить после сканирования, можно выбрать в раскрывающемся меню.

- **Ничего не предпринимать:** после сканирования действия предприниматься не будут.
- **Выключить:** после сканирования компьютер отключается.
- **Перезагрузить:** после сканирования открытые программы закрываются, а компьютер перезагружается.
- **Перезагрузка при необходимости:** компьютер перезагружается, только если нужно завершить очистку обнаруженных угроз.
- **Принудительная перезагрузка:** все открытые программы принудительно закрываются, не дожидаясь вмешательства пользователя, и компьютер перезапускается после завершения сканирования.
- **Принудительная перезагрузка при необходимости:** компьютер перезагружается, только если нужно завершить очистку обнаруженных угроз.
- **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.

**i** Доступность действий **Сон** и **Гибернация** зависит от параметров питания и спящего режима операционной системы и возможностей вашего ноутбука или компьютера. Не забывайте, что компьютер в спящем режиме все же работает. Компьютер выполняет основные функции и потребляет электричество, когда работает от аккумулятора. Чтобы сохранить время работы батареи (например, если вы находитесь в пути), рекомендуется перевести компьютер в режим гибернации.

Выберите элемент **Сканирование не может быть отменено**, чтобы пользователи, не обладающие нужными правами, не могли отменить действия, которые выполняются после сканирования.

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

См. также [Ход сканирования](#).

## Обзор запланированных задач

В данном диалоговом окне отображается подробная информация о выбранной запланированной задаче, если дважды щелкнуть настраиваемую задачу или щелкнуть правой кнопкой мыши настраиваемую задачу планировщика и выбрать команду **Показать информацию о задаче**.

## Сведения о задаче

Введите **имя задачи**, выберите **тип задачи** и щелкните **Далее**.

- **Запуск внешнего приложения:** планирование выполнения внешнего приложения.
- **Обслуживание журнала** - в файлах журнала также содержатся остатки удаленных



записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.

- **Проверка файлов при загрузке системы:** проверка файлов, исполнение которых разрешено при запуске или входе пользователя в систему.
- **Создать снимок состояния компьютера:** создание снимка состояния компьютера в [ESET SysInspector](#), для которого собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого из них.
- **Сканирование компьютера по требованию:** сканирование файлов и папок на компьютере.
- **Обновление:** планирование задачи обновления путем обновления модулей.

## Время задачи

Задача будет выполняться регулярно через указанный промежуток времени. Выберите один из следующих параметров.

- **Однократно:** задача будет выполнена однократно в установленные дату и время.
- **Многократно:** задача будет выполняться регулярно через указанный промежуток времени (в часах).
- **Ежедневно:** задача будет выполняться раз в сутки в указанное время.
- **Еженедельно:** задача будет выполняться один или несколько раз в неделю в указанные дни и время.
- **При определенных условиях:** задача будет выполнена при возникновении указанного события.

**Пропускать задачу, если устройство работает от аккумулятора:** задача не запустится, если на момент планируемого запуска задачи компьютер работает от аккумулятора. Это также относится к компьютерам, работающим от источника бесперебойного питания.

## Время выполнения задачи: однократно

**Выполнение задачи:** указанная задача будет выполнена однократно в указанные дату и время.

## Время выполнения задачи: ежедневно

Задача будет выполняться раз в сутки в указанное время.

## Время выполнения задачи: еженедельно

Задача будет выполняться каждую неделю в указанные день и время.

## Время выполнения задачи: при

# определенных условиях

Задача запускается в случае возникновения одного из перечисленных далее событий.

- **Каждый раз при запуске компьютера**
- **Каждые сутки при первом запуске компьютера**
- **При коммутируемом подключении к Интернету/VPN**
- **После успешного обновления модуля**
- **После успешного обновления программы**
- **Вход пользователя**
- **Обнаружение угроз**

При планировании задачи по событию пользователь может указать минимальный интервал между двумя окончаниями выполнения задачи. Например, если пользователь входит в систему несколько раз в день, выберите 24 часа, чтобы задача выполнялась только при первом входе в систему за сутки, а затем только на следующий день.

## Пропущенная задача

Задача может быть [пропущена, если компьютер выключен или работает от аккумулятора](#). Выберите среди этих вариантов, когда должна быть запущена пропущенная задача, и нажмите кнопку **Далее**.

- **В следующее запланированное время** — задание будет запущено, если компьютер будет включен в следующее запланированное время.
- **Как можно скорее** — задание будет запускаться при включении компьютера.
- **Немедленно, если время с момента последнего запланированного запуска превышает (часы)** — представляет время, прошедшее с момента первого пропущенного запуска задания. Если это время превышено, задание будет запущено незамедлительно.

### Немедленно, если время с момента последнего запланированного запуска превысит (ч) – примеры

Для примера задания настроен повторный запуск каждый час. Выбрана опция **Немедленно, если время, прошедшее с момента последнего запланированного запуска, превышает (часы)**, а для превышенного времени установлено два часа.

✓ Задание запускается в 13:00, и по его завершении компьютер переходит в спящий режим:

- Компьютер выходит из спящего режима в 15:30. Первый пропущенный запуск задания был в 14:00. С 14:00 прошло всего 1,5 часа, поэтому задание будет запущено в 16:00.
- Компьютер выходит из спящего режима в 16:30. Первый пропущенный запуск задачи был в 14:00. С 14:00 прошло два с половиной часа, поэтому задание будет запущено немедленно.

## Сведения о задаче: обновление

Если нужно иметь возможность обновлять программу с двух серверов обновлений, нужно создать два разных профиля обновления. Если не удастся загрузить файлы обновлений с одного сервера, программа автоматически переключится на другой. Этот вариант подходит,

например, для ноутбуков, которые обычно обновляются с сервера обновлений в локальной сети, но при этом их владельцы часто подключаются к Интернету в других сетях. Таким образом, если с первым профилем возникнет ошибка, файлы обновлений с серверов обновлений ESET автоматически будут загружены через второй профиль.

## Сведения о задаче: запуск приложения

С помощью этой задачи можно запланировать выполнение внешнего приложения.

**Исполняемый файл:** выберите исполняемый файл в дереве каталогов или нажмите кнопку ..., чтобы вручную ввести путь.

**Рабочая папка:** задайте рабочий каталог внешнего приложения. Все временные файлы выбранного в поле **Исполняемый файл** файла будут создаваться в этом каталоге.

**Параметры:** параметры командной строки для приложения (необязательно).

Нажмите кнопку **Готово** для применения задачи.

## 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](mailto:samples@eset.com).
3. Чтобы сообщить о спаме или ложном обнаружении спама, ознакомьтесь с этой [статьей 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**.

**i** 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. Дополнительные сведения об этой деятельности приведены в глоссарии. 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.



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.

## Карантин

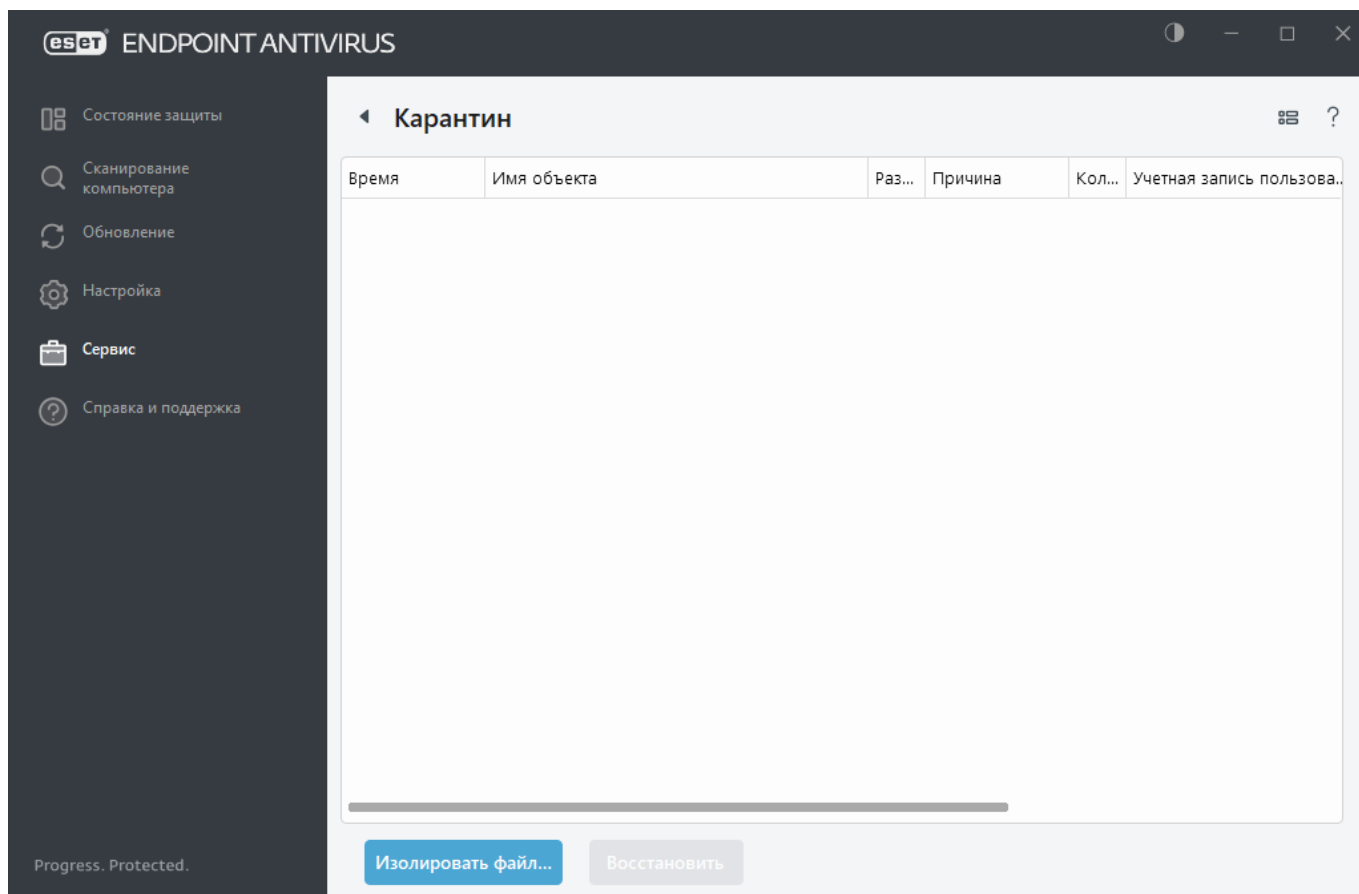
Главная функция карантина — безопасное хранение обнаруженных объектов (например, вредоносных программ, зараженных файлов или потенциально нежелательных приложений).

Карантин можно открыть из главного окна программы ESET Endpoint Antivirus, 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 Antivirus автоматически помещает удаленные файлы на карантин (если пользователь не отключил эту функцию в [окне предупреждения](#)).

Дополнительные файлы следует помещать на карантин, если:

- их нельзя вылечить;
- их нельзя безопасно удалить;
- они отнесены программой ESET Endpoint Antivirus к зараженным по ошибке;
- файл с подозрительной активностью, но не определяется [модулем сканирования](#).

Чтобы поместить файл на карантин, можно использовать несколько приведенных ниже вариантов.

- 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 будет переведено в фоновый режим.
- Щелкните **Переместить в карантин** в главном окне программы.
- 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 щелкните 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](#)
  - [Продукт ESET уведомил меня об обнаружении. Что мне делать?](#)

## Справка и поддержка

Щелкните **Справка и поддержка** в [главном окне программы](#), чтобы отобразить сведения о поддержке и средствах устранения неполадок, которые помогут вам решить проблемы, с которыми вы можете столкнуться.



### Установленный продукт

- [О программе ESET Endpoint Antivirus](#): на экран выводится информация о вашей копии программы ESET Endpoint Antivirus.
- [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 Antivirus.



### [Служба технической поддержки](#)

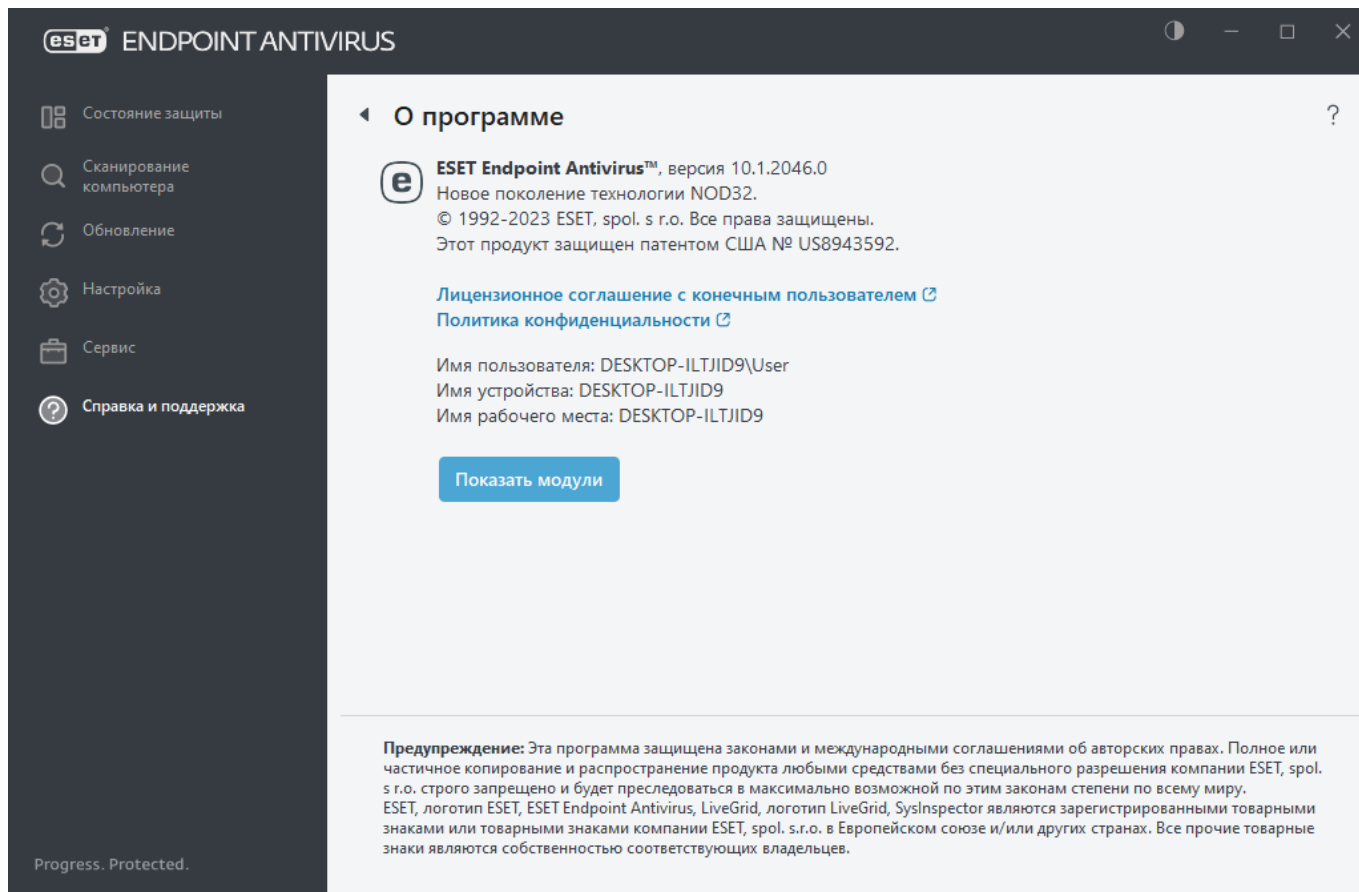


**База знаний**: в [базе знаний ESET](#) содержатся ответы на наиболее часто задаваемые вопросы, а также рекомендуемые решения различных проблем. База знаний регулярно обновляется техническими специалистами ESET, что делает ее самым полезным инструментом для решения разнообразных проблем.

## О программе ESET Endpoint Antivirus

В этом окне содержатся сведения об установленной версии ESET Endpoint Antivirus и о вашем компьютере.





Щелкните **Показать модули**, чтобы просмотреть информацию о списке загруженных модулей программы.

- Чтобы скопировать информацию о модулях в буфер обмена, используйте команду **Копировать**. Это может быть полезно при устранении проблем или обращении в службу технической поддержки.
- Щелкните **Модуль обнаружения** в окне «Модули», чтобы открыть сайт ESET Virus Radar, который содержит информацию о каждой версии модуля обнаружения ESET.

## Отправка данных о конфигурации системы

Чтобы иметь возможность максимально быстро и эффективно оказывать пользователям помощь, компании ESET требуется информация о конфигурации ESET Endpoint Antivirus, 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.

После отправки [веб-формы](#) в ESET будут отправлены данные о конфигурации вашей системы. Установите флажок **Всегда отправлять эти сведения**, если нужно запомнить данное действие для текущего процесса. При отправке [веб-формы](#) без отправки каких-либо данных, щелкните **Не отправлять данные** и продолжите.

Настроить отправку данных о конфигурации системы можно в разделе [Расширенные параметры](#) > **Инструменты** > **Диагностика** > [Служба технической поддержки](#).

**i** Если вы решили отправить данные о конфигурации системы, необходимо заполнить и отправить веб-форму. В противном случае ваша заявка не будет создана, и данные о конфигурации вашей системы будут потеряны. Если данные о конфигурации системы отправить не удастся, заполните веб-форму и дождитесь инструкций от службы технической поддержки.

## Служба технической поддержки

В главном окне программы щелкните **Справка и поддержка > Служба технической поддержки**.

### Обратиться в службу технической поддержки

**Запрос в службу поддержки:** если не удастся 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 Collector здесь](#).

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.

## Дополнительные настройки

В разделе «Расширенные параметры» можно детально настроить ESET Endpoint Antivirus в соответствии с вашими потребностями.

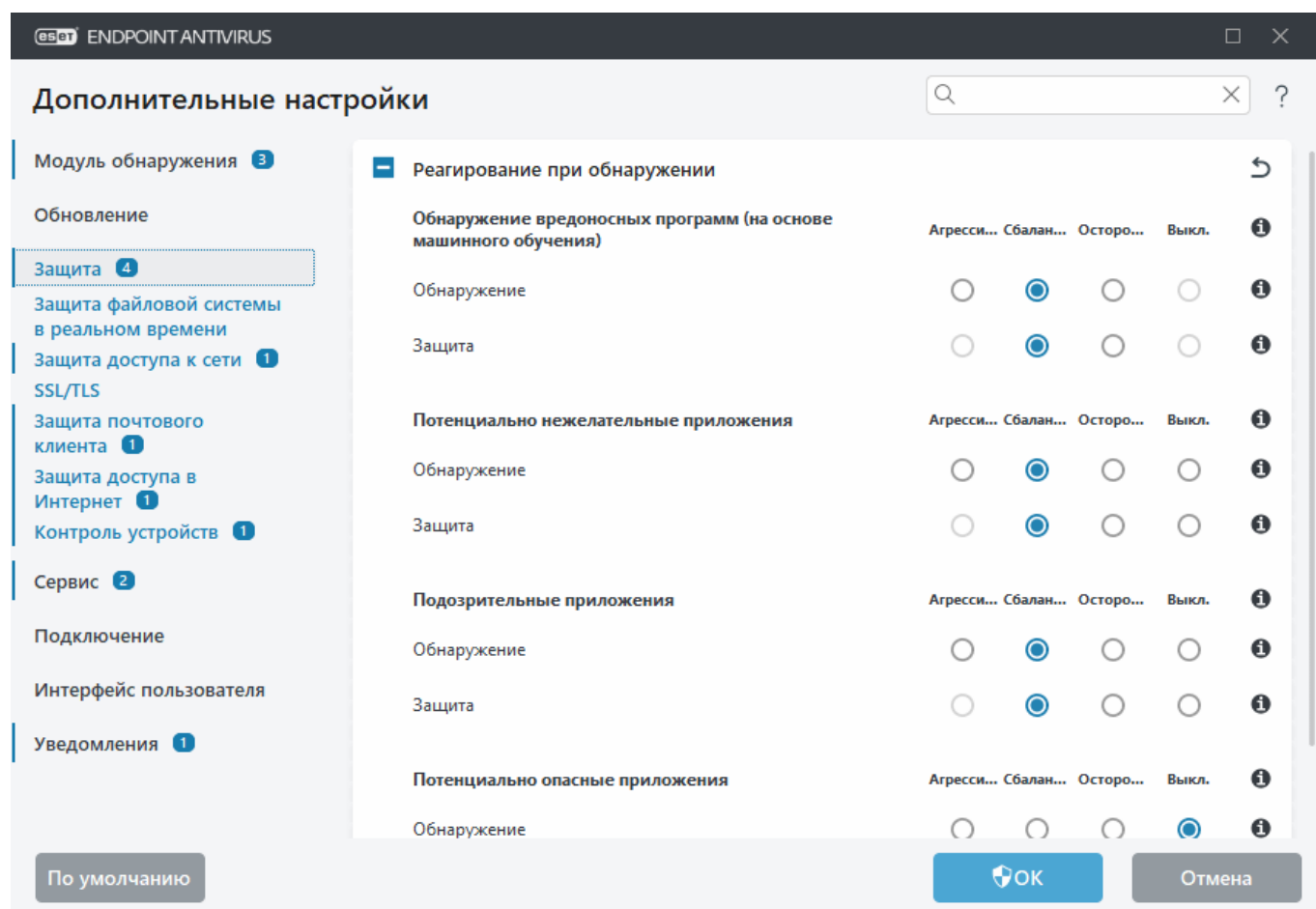
Чтобы получить доступ к расширенным параметрам, откройте [главное окно программы](#) и нажмите клавишу **F5** на клавиатуре или щелкните **Настройка > Расширенные параметры**.

**i** При создании политики из веб-консоли ESET PROTECT 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](#).

**i** В зависимости от [настроек доступа](#) вам может быть предложено ввести пароль, чтобы открыть расширенные параметры.

В расширенных параметрах доступны следующие настройки:

- [Модуль обнаружения](#)
- [обновление;](#)
- [Защита](#)
- [Служебные программы](#)
- [Подключение](#)
- [Интерфейс пользователя](#)
- [Уведомления](#)



## Модуль обнаружения

В разделе [Расширенные параметры](#) > **Модуль обнаружения** можно настроить следующие опции:

- [Исключения](#)

- Расширенные параметры
- [Сканер сетевого трафика](#)

## 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 быстрогодействия](#): исключение файлов и папок из сканирования. Исключения для быстрогодействия полезны для исключения при сканировании игровых приложений на уровне файлов, неправильном поведении системы или повышенной производительности.

[Исключения из обнаружения](#): исключение объектов из очистки по имени, пути или хэшу обнаружения. Они не исключают файлы и папки из сканирования как делают исключения для быстрогодействия. Исключения обнаружения исключают объекты только при их обнаружении модулем обнаружения и если в списке исключений присутствует соответствующее правило.

Не стоит путать с другими типами исключений:

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

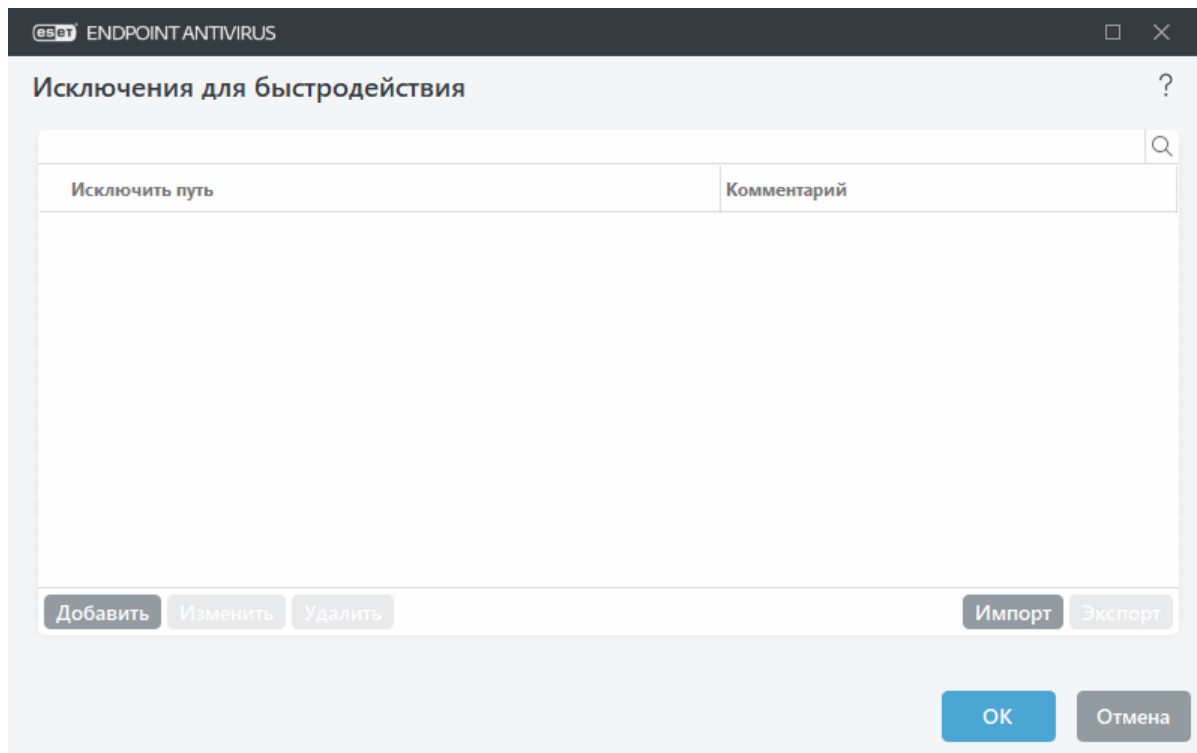
## Исключения для быстрогодействия

Исключения для быстрогодействия позволяют исключить файлы и папки из сканирования.

Мы рекомендуем создавать исключения для быстрогодействия 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](#) > **Модуль обнаружения** > **Исключения** > **Исключения для быстрогодействия** > **Изменить**.

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



**i** 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 быстрого действия 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":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}
```

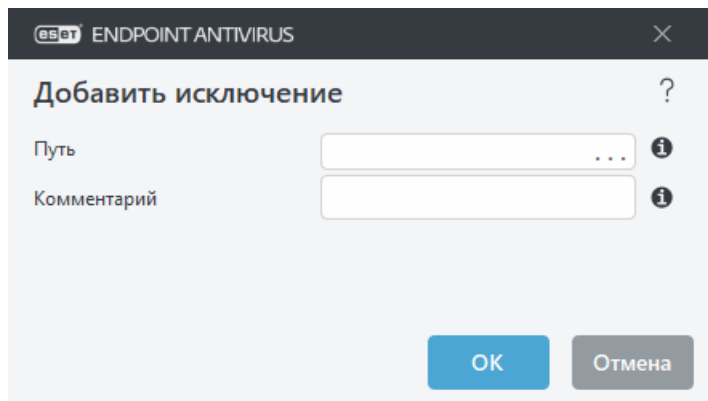
```
C:\Backup\*,custom comment
```

```
C:\pagefile.sys
```

# Добавление или изменение исключений для быстрого действия

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

**i** 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 которой (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:

- 
- Настройка уровня приоритета для исключений с помощью кнопок «В начало» и «В конец» 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 которой (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.

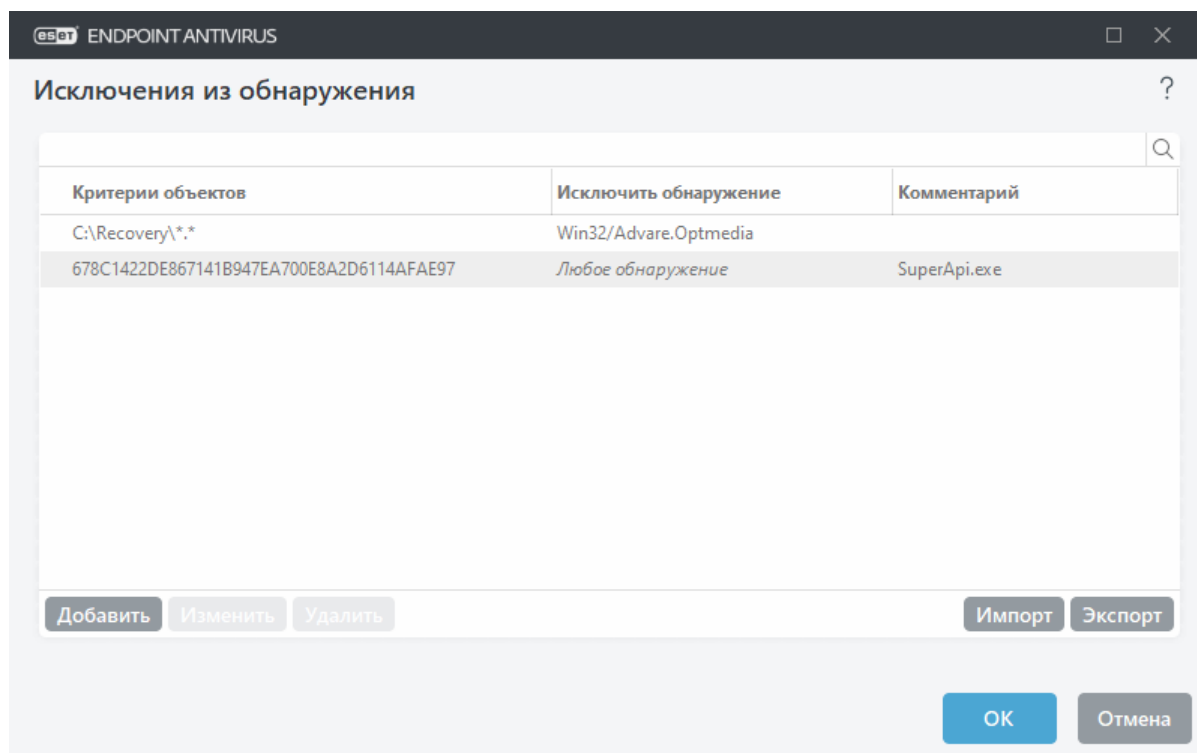
## Исключения из обнаружения

Исключения из обнаружения позволяют исключить объекты из [очистки](#) путем фильтрации имени обнаружения, пути объекта или его хэша.



Исключения из обнаружения не исключают файлы и папки из сканирования, как делают [Исключения для быстрогодействия](#). Исключения обнаружения исключают объекты только при их обнаружении модулем обнаружения и если 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](#) > **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":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}
```

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

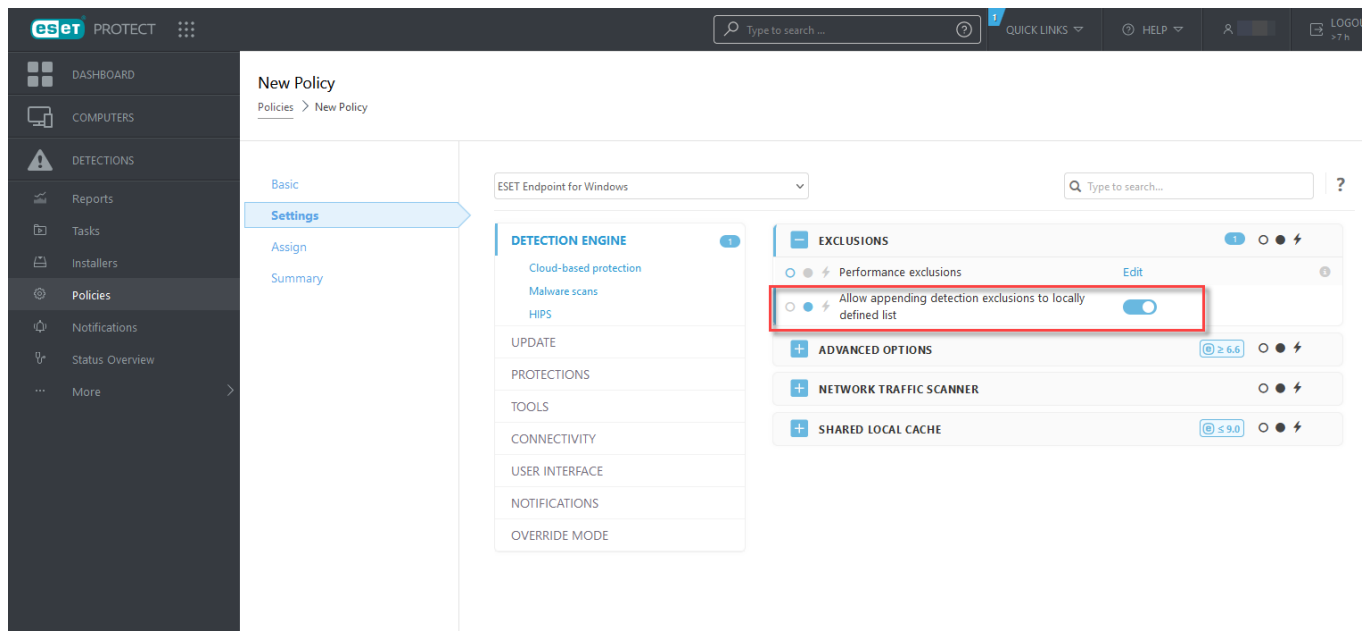
```
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

## Настройка исключений из обнаружения в ESET PROTECT

[Мастер управления исключениями из обнаружения](#) ESET PROTECT — создание исключения из обнаружения и применение его к большому 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 исключения из обнаружения из ESET PROTECT будет работать, как и ожидалось.

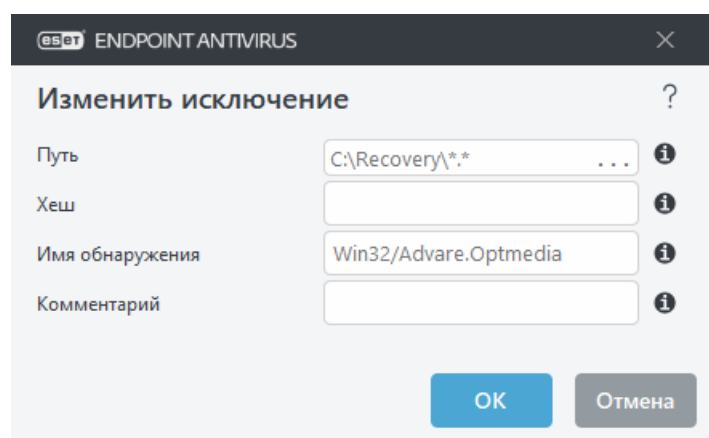


# Добавление или изменение исключений из обнаружения

## 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 Antivirus. 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.

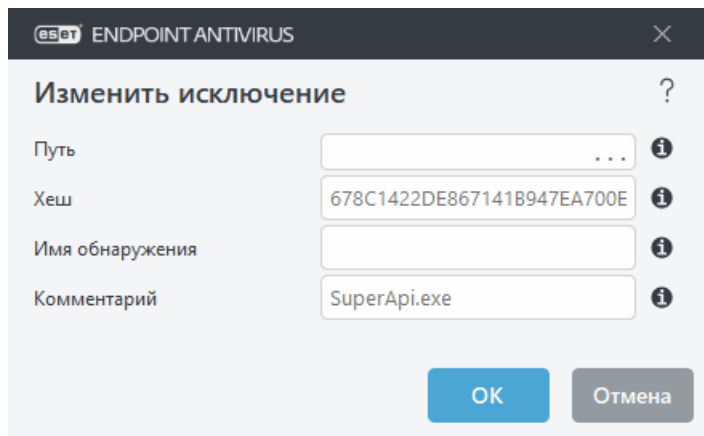
См. также [Формат исключения пути](#).



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 Antivirus 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.

## Модуль обнаружения расширенных параметров

**Включить расширенное сканирование с помощью AMSI** — это средство Microsoft Antimalware Scan Interface, которое дает возможность сканировать сценарии PowerShell, сценарии, выполняемые сервером Windows Script Host, а также данные, которые сканируются с помощью пакета SDK AMSI.

## Сканер сетевого трафика

Сканер сетевого трафика обеспечивает для протоколов приложений защиту от вредоносных программ, которая объединяет множество передовых методов сканирования на наличие вредоносных программ. Сканер сетевого трафика автоматически сканирует протоколы HTTP(S), POP3(S) и IMAP(S) независимо от используемого интернет-браузера или почтового клиента. Вы можете включить и отключить сканер сетевого трафика в разделе [Расширенные параметры](#) > **Модуль обнаружения** > **Сканер сетевого трафика**.

**Включить сканер сетевого трафика:** если эту опцию отключить, протоколы HTTP(S), POP3(S) и IMAP(S) сканироваться не будут. Обратите внимание, что для следующих функций ESET Endpoint Antivirus сканер сетевого трафика должен быть включен:

- [Защита доступа в Интернет](#)
- [SSL/TLS](#)
- [Защита от фишинга](#)
- [Защита почтового клиента](#)

## Защита на основе облака

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

Доступны указанные ниже варианты.

## Вариант 1. Включить систему репутации ESET LiveGrid®

Система репутации ESET LiveGrid® работает на основе облачных белых и черных списков.

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

## Вариант 3. Не включать ESET LiveGrid®

Функциональность программного обеспечения при этом не ограничивается, но в некоторых случаях ESET Endpoint Antivirus может быстрее реагировать на новые угрозы, чем обновление модулей обнаружения, когда система ESET LiveGrid® включена.

 Дополнительную информацию о ESET LiveGrid® см. в [гlossарии](#).  
См. наши [иллюстрированные инструкции](#) на английском и еще нескольких языках по включению и отключению ESET LiveGrid® в ESET Endpoint Antivirus.

## Настройка облачной защиты в окне расширенных параметров

Чтобы получить доступ к настройкам ESET LiveGrid®, откройте раздел [Расширенные параметры](#) > **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.

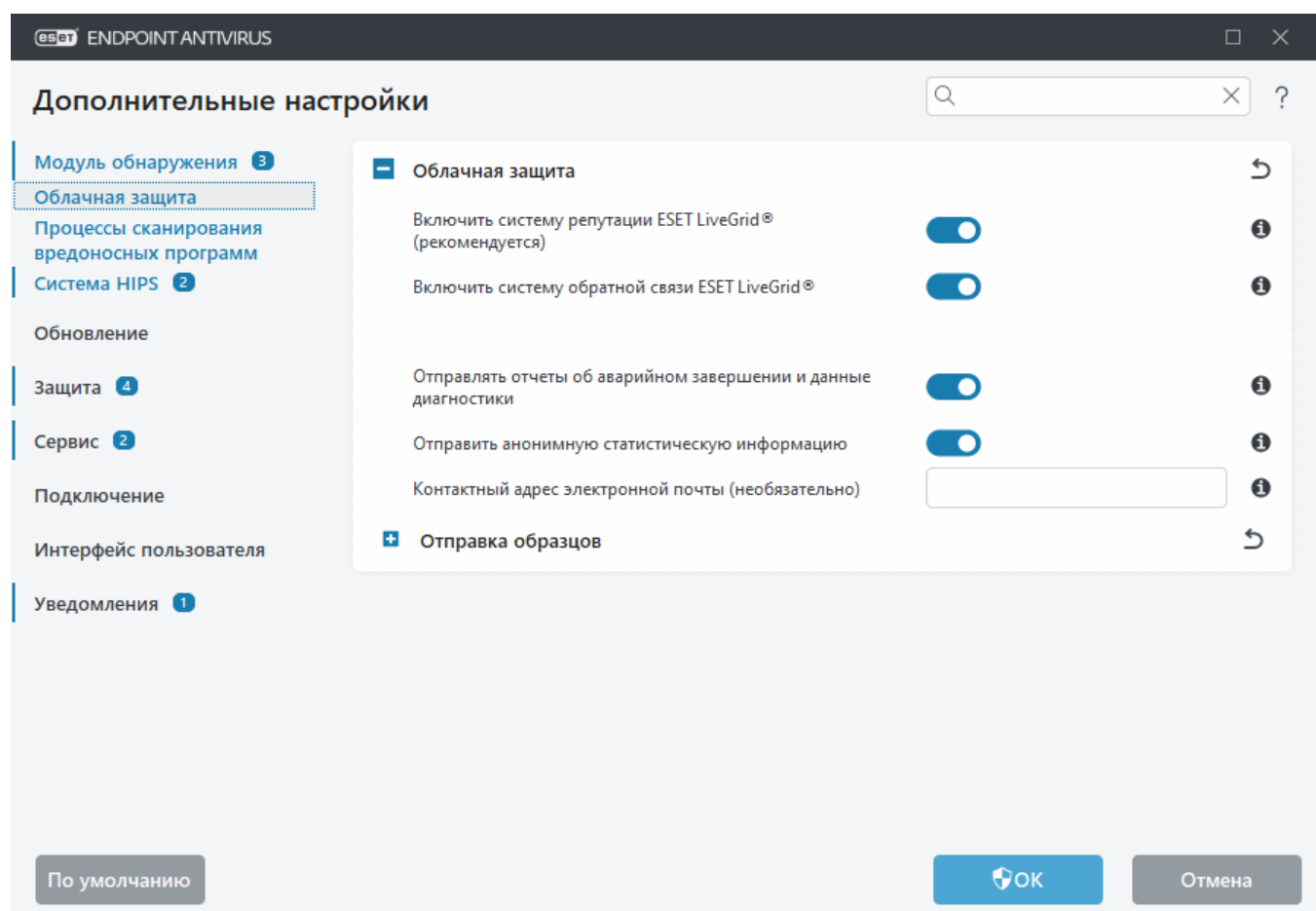
**Включить ESET LiveGuard** ([ESET LiveGuard](#) — это дополнительная функция, продаваемая компанией ESET и недоступная по умолчанию). ESET LiveGuard — это платная служба,

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 [Сервис](#).

## Автоматическая отправка обнаруженных образцов

Укажите, какие образцы будут отправляться в компанию ESET для анализа и совершенствования механизмов обнаружения. Доступны указанные ниже 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 отправляться в ESET, если модуль обнаружения их не обнаруживает. Например, образцы, которые почти попали под обнаружение, признаны подозрительными одним из [модулей защиты](#) ESET Endpoint Antivirus 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 сможете 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](#)

ACCEDB, 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\*.

**Максимальный размер образцов (МБ):** определяет максимальный размер автоматически отправляемых образцов (1-64 МБ).




## ESET LiveGuard

Чтобы включить службу ESET LiveGuard на клиентском компьютере с помощью веб-консоли ESET PROTECT, воспользуйтесь информацией в разделе [Настройка ESET LiveGuard для ESET Endpoint Antivirus](#).

Если система ESET LiveGrid® использовалась ранее, но была отключена, могут оставаться некоторые 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, щелкните [Расширенные параметры](#) > **Модуль обнаружения** > **Облачная защита** > **Отправка образцов** > **Исключения** и добавьте исключение \*download.domain.com\*.

## Процессы сканирования вредоносных программ

В разделе [Расширенные параметры](#) > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** можно настроить параметры сканирования для профилей сканирования.

### Сканирование по требованию

**Выбранный профиль** – конкретный набор параметров, используемых сканером по запросу. Чтобы создать новый профиль, нажмите **Изменить** возле элемента **Список профилей**. Дополнительные сведения см. в разделе [Профили сканирования](#).

После выбора профиля сканирования можно настроить следующие опции:

**Объекты сканирования:** чтобы просканировать определенный объект или группу объектов, щелкните **Изменить** рядом с параметром **Объекты сканирования** и выберите вариант в структуры папок (дерева). Дополнительные сведения см. в разделе [Объекты сканирования](#).

**Защита по требованию и на основе машинного обучения:** можно настроить уровни отчетности и защиты для каждого профиля сканирования. По умолчанию профили

сканирования используют настройки, указанные в разделе [Защита файловой системы в реальном времени](#). Отключите переключатель рядом с элементом **Использовать настройки защиты в реальном времени** для настройки пользовательских уровней отчетности и защиты. Подробные сведения об уровнях отчетности и защиты см. в разделе [Защита](#).

**ThreatSense** — расширенные параметры, например расширения файлов, которые нужно контролировать, и используемые методы обнаружения. Для получения дополнительных сведений см. раздел [ThreatSense](#).

## Профили сканирования

В ESET Endpoint Antivirus 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).

Чтобы создать профиль, откройте раздел [Расширенные параметры](#) > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Сканирование по требованию** > **Список профилей** > **Изменить**. 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 [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 **Всегда исправлять обнаружение**. Введите имя нового профиля в окне **Диспетчер профилей** и нажмите кнопку **Добавить**. Выберите новый профиль в раскрывающемся меню **Выбранный профиль** и настройте остальные параметры в соответствии со своими требованиями, а затем нажмите кнопку **ОК**, чтобы сохранить новый профиль.

# Объекты сканирования

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 [гlossарии](#).
- **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 объекту сканирования (файлу или папке), введите его путь в текстовом поле под древовидной структурой. Путь вводится с учетом регистра. Чтобы включить объект в сканирование, установите его флажок в древовидной структуре.

## 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

Включите переключатель рядом с элементом **Включить сканирование в состоянии простоя**, чтобы включить эту функцию. Когда компьютер находится в состоянии простоя, автоматически выполняется сканирование компьютера на всех жестких дисках.

По умолчанию сканирование в состоянии простоя не работает, если компьютер (ноутбук) работает от батареи. Этот параметр можно изменить, включив ползунок рядом с элементом **Сканировать даже в случае работы компьютера от аккумулятора** в разделе «Расширенные параметры».

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](#).

**ThreatSense** — расширенные параметры, например расширения файлов, которые нужно контролировать, и используемые методы обнаружения. Дополнительные сведения см. в разделе [ThreatSense](#).

## Сканирование в состоянии простоя

Настройки сканирования в состоянии простоя можно изменить в меню [Расширенные параметры](#) > **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:

- **Выключенный экран или заставка**
- **блокировка компьютера;**
- **Выход пользователя**

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

## сканирование при запуске

При загрузке компьютера и обновлении модуля обнаружения автоматически проверяются файлы, исполняемые при запуске системы. Это сканирование зависит от [конфигурации и задач планировщика](#).

Сканирование файлов, исполняемых при запуске системы, входит в задачу планировщика **Проверка файлов, исполняемых при запуске системы**. Для изменения ее настроек перейдите в раздел **Инструменты > Планировщик**, щелкните элемент **Автоматическая проверка файлов при запуске системы**, а затем — **Изменить**. На последнем этапе отобразится окно [Автоматическая проверка файлов при запуске системы](#). Более подробные инструкции по созданию задач в планировщике и управлению ими см. в разделе [Создание новой задачи](#).

**ThreatSense** — расширенные параметры, например расширения файлов, которые нужно контролировать, и используемые методы обнаружения. Дополнительные сведения см. в разделе [ThreatSense](#).

# 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 файлов, которые нужно просканировать, являются фиксированными для каждой вышеприведенной группы. Если выбрать меньшую глубину сканирования для файлов, исполняемых при запуске системы, файлы, которые не были просканированы, будут сканироваться при открытии или исполнении.

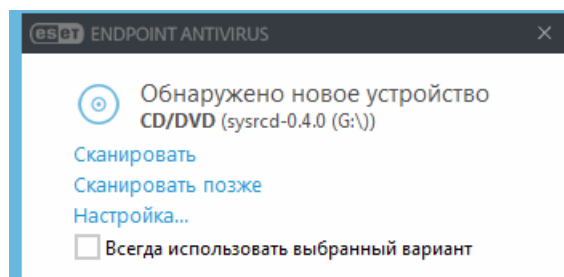
**Приоритет сканирования:** уровень приоритетности, используемый для определения условий начала сканирования.

- **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.

## Съемные носители

ESET Endpoint Antivirus 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 разделе [Расширенные параметры](#) > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Съемные носители** включен параметр **Показать параметры сканирования**, то при подключении съемного носителя отображается следующее диалоговое окно:



Параметры этого диалогового окна:

- **Сканировать сейчас:** запуск сканирования съемного носителя.
- **Не сканировать:** съемные носители сканироваться не будут.
- **Настройка:** вызов [расширенных параметров](#).
- **Всегда использовать выбранный вариант:** если установить этот флажок, выбранное действие будет выполняться каждый раз, когда вставляется съемный носитель.

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

---

Чтобы изменить настройки сканирования съемных носителей, последовательно выберите элементы [Расширенные параметры](#) > **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.
- **Принудительное сканирование устройства:** выполняется сканирование подключенного к компьютеру съемного носителя без возможности отмены.
- **Показать параметры сканирования:** переход в раздел, где настраиваются действия со съемными носителями.

## 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 [Расширенные параметры \( \)](#) > **Модуль обнаружения** > **Процессы сканирования вредоносных программ** > **Защита документов** и щелкните ползунок рядом с элементом **Включить защиту документов**.

**ThreatSense** — расширенные параметры, например расширения файлов, которые нужно контролировать, и используемые методы обнаружения. Дополнительные сведения см. в разделе [ThreatSense](#).

**i** Эта функция активируется приложениями, в которых используется Microsoft Antivirus API (например, Microsoft Office 2000 и более поздних версий или Microsoft Internet Explorer 5.0 и более поздних версий).

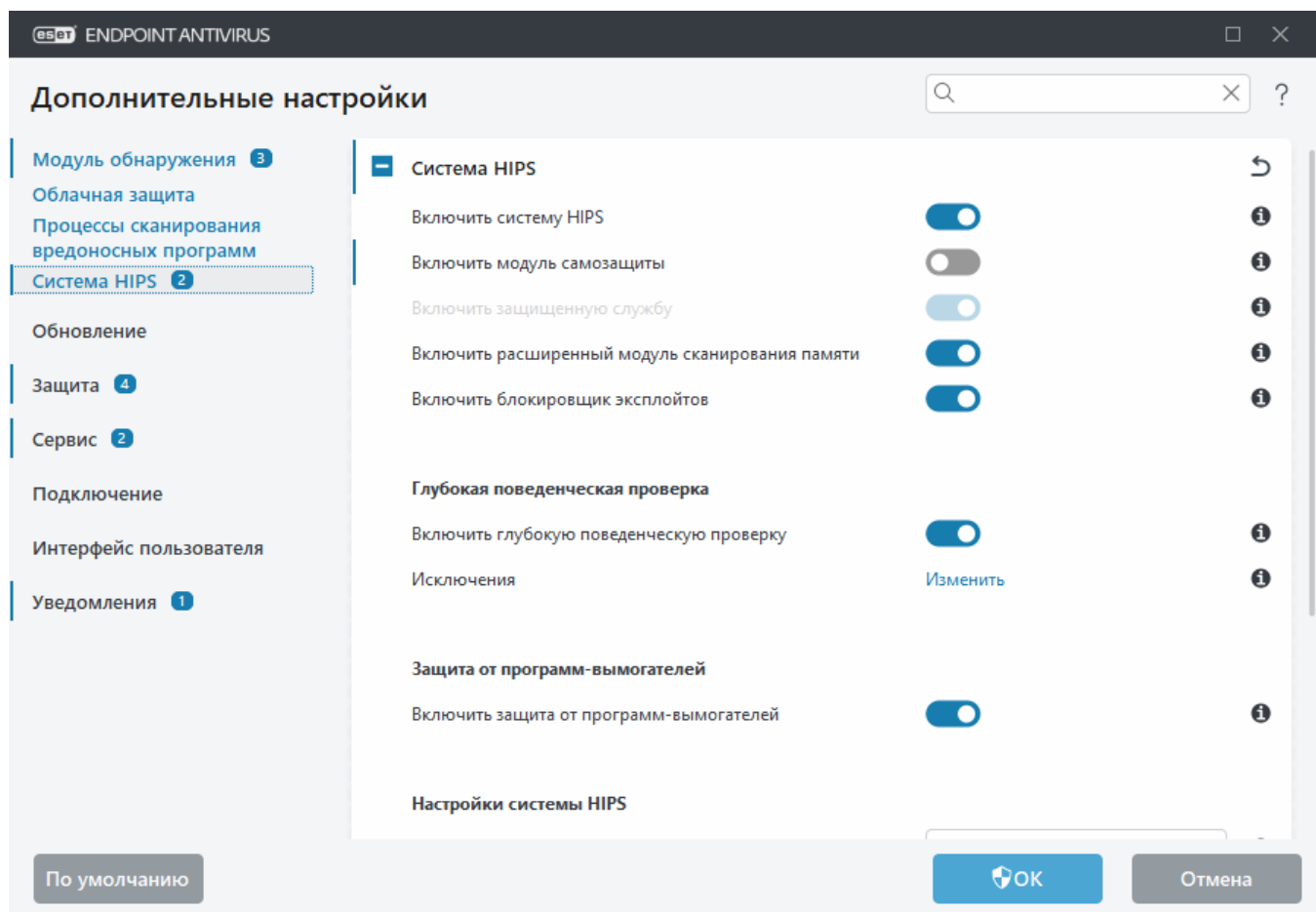
## Система HIPS (система предотвращения вторжений на узел)

**!** 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 системы HIPS можно настроить в разделе [Расширенные параметры](#) > **Модуль обнаружения** > **Система HIPS** > **Система HIPS**. Состояние HIPS (включено/отключено) отображается в [главном окне программы](#) ESET Endpoint Antivirus, в разделе **Настройка** > **Компьютер**.





## Система HIPS

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

**Включить модуль самозащиты** — В ESET Endpoint Antivirus 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 [гlossарии](#).

**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 [гlossарии](#).



## 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.](#)

**Включить Intel® Threat Detection Technology:** помогает обнаруживать атаки программ-вымогателей, используя уникальную телеметрию процессора Intel для повышения эффективности обнаружения, уменьшения количества ложных предупреждений об угрозах и расширения возможностей противодействия передовым методам уклонения от обнаружения. См. информацию о [поддерживаемых процессорах](#).

**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 Antivirus. Этот параметр доступен только в редакторе конфигурации политики ESET PROTECT.

## Настройки системы HIPS

**Режим фильтрации** можно выполнять в одном из следующих режимов:

| Режим фильтрации                | Описание   |
|---------------------------------|--|
| <b>Автоматический режим</b>     | Включены все операции за исключением тех, которые заблокированы предварительно заданными правилами, защищающими компьютер. |
| <b>Интеллектуальный режим</b>   | Пользователь будет получать уведомления только об очень подозрительных событиях.   |
| <b>Интерактивный режим</b>      | Пользователь будет получать запросы на подтверждение операций.   |
| <b>Режим на основе политики</b> | блокируются все операции, кроме тех, что разрешены определенным правилом.  |

| Режим фильтрации      | Описание   |
|-----------------------|--|
| <b>Режим обучения</b> | Операции включены, и после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в редакторе <b>Правила NIPS</b> , но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. При выборе элемента <b>Режим обучения</b> в раскрывающемся меню <b>Режим фильтрации</b> становится доступным параметр <b>Режим обучения завершится</b> . Выберите длительность для режима обучения. Максимальная длительность — 14 дней. Когда указанный период завершится, вам будет предложено изменить правила, созданные системой NIPS 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 этот режим фильтрации, который будет действовать по окончании использования режима обучения. Чтобы после завершения режима обучения изменить режим фильтрации NIPS на **Спросить пользователя**, нужны права администратора.

Система NIPS 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 NIPS**. В этом окне можно выбирать, создавать, изменять и удалять правила. Дополнительные сведения о создании правил и операциях системы NIPS см. в разделе [Изменение правила системы предотвращения вторжений на узел](#).

## Исключения системы NIPS

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

Чтобы изменить исключения системы NIPS, откройте раздел [Расширенные параметры](#) > **Модуль обнаружения** > **Система NIPS** > **Система NIPS** > **Исключения** > **Изменить**.

**i** Не следует путать эту функцию с другими возможностями исключения — [Исключенные расширения файлов](#), [Исключения из обнаружения](#), [Исключения для быстрого действия](#) или [Исключения для процессов](#).

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

## Расширенные параметры NIPS

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. Используйте эту функцию только при устранении неполадок или по запросу службы технической поддержки ESET, так как она может создать очень большой файл журнала и замедлить работу компьютера.

**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.

**i** 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.

**i** После установки список драйверов пуст. ESET Endpoint Antivirus заполняет список автоматически с течением времени.

**i** Драйверы, которые всегда разрешены к загрузке, специфичны для каждого устройства и не могут быть изменены с помощью политики ESET PROTECT. После установки список драйверов пуст. ESET Endpoint Antivirus заполняет список автоматически с течением времени.

## 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.

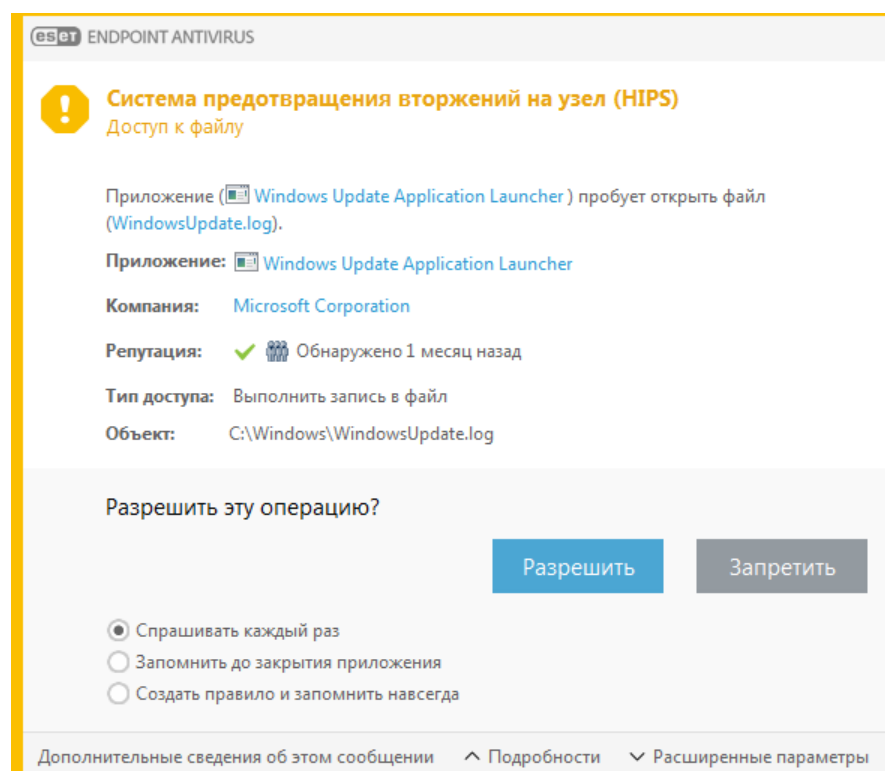
Если выбрать параметр **Создать правило и запомнить навсегда**, будет создано новое правило HIPS, которое позже можно изменить в разделе [Управление правилами HIPS](#) (нужны права администратора).

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](#) > **Модуль обнаружения** > HIPS > **Основные сведения**.



# Потенциальное поведение Программ-вымогателей обнаружено

При обнаружении потенциального поведения, характерного для программы-шантажиста, отображается диалоговое окно. Для операции также можно выбрать другие действия:

**Запретить** или **Разрешить**.

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 отображается уведомление.

### Элементы управления

**Добавить:** создание правила.

**Изменить:** изменение выделенных записей.

**Удалить.** Удаление выбранных записей.

## Приоритетность для правил HIPS

Настройка уровня приоритета для правил системы HIPS с помощью кнопок «В начало» и «В конец» 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 переключатель, если правило нужно оставить в списке, но при этом не применять 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 отображается уведомление.

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.

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

**i** 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.

## 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

- i** 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. Щелкните **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 **ОК**. 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.



## Добавление пути к приложению или реестру для системы HIPS

Выберите путь к файлу приложения, нажав .... При выборе папки все расположенные в ней приложения будут включены.

Параметр **Открыть редактор реестра** запускает редактор реестра Windows (regedit). При добавлении пути реестра нужно правильно ввести расположение в поле **Значение**.

Примеры пути к файлу или реестру:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY\_LOCAL\_MACHINE\system\ControlSet*

## Обновление

Опции настройки обновления доступны в разделе [Расширенные параметры](#) > **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).

### Обновление

Текущий профиль обновления отображается в раскрывающемся меню **Выбрать профиль обновления по умолчанию**.

Чтобы создать профиль, см. сведения в разделе [Профили обновления](#).

**Настроить уведомления об обновлениях:** щелкните Изменить, чтобы выбрать, какие [уведомления приложения](#) будут отображаться. Можно выбрать, нужно ли их показывать на рабочем столе и/или отправлять по электронной почте.

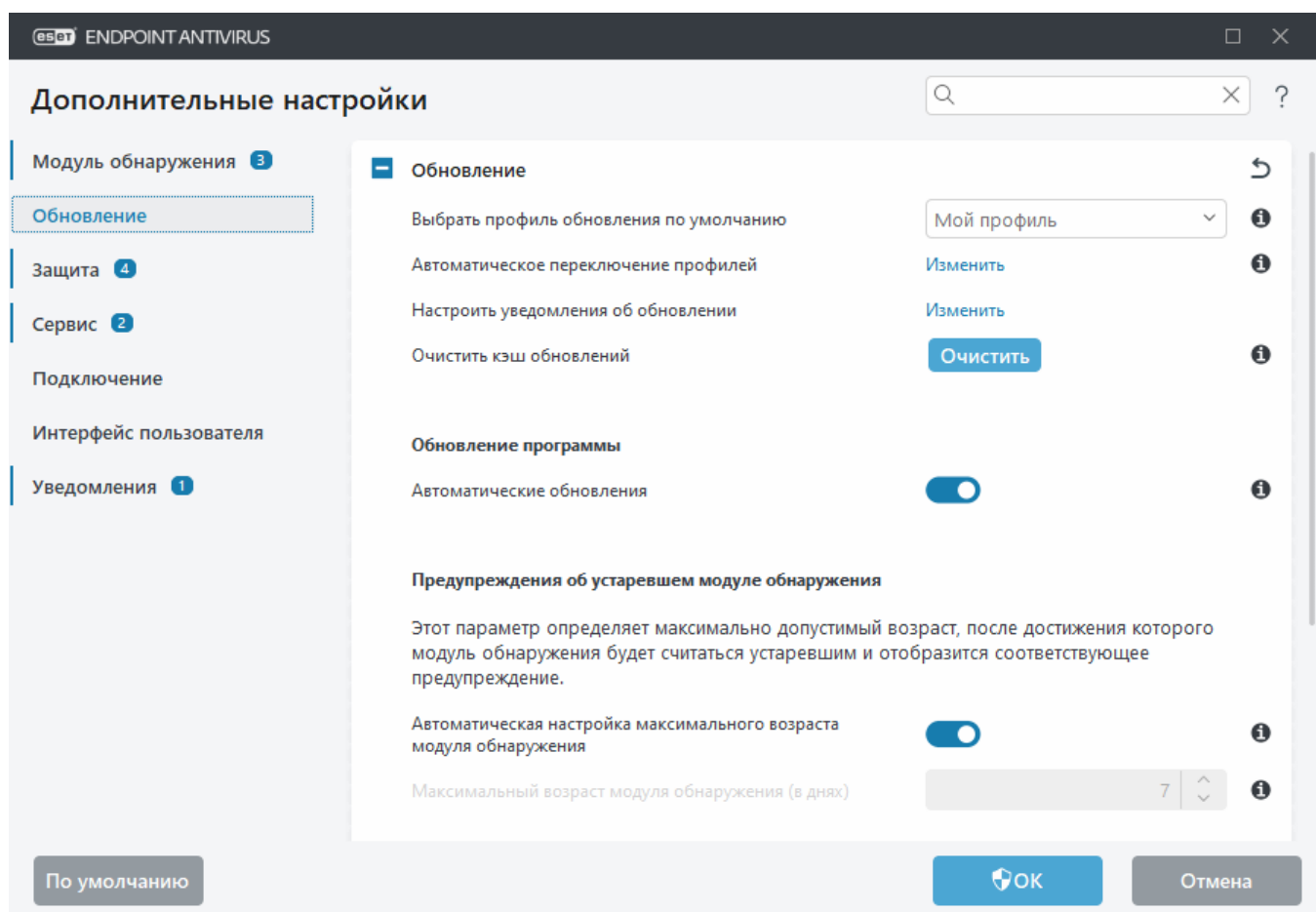
Если во время загрузки обновлений модуля обнаружения возникли проблемы, рядом с параметром **Очистить кэш обновлений** щелкните **Очистить**, чтобы удалить временные файлы обновлений (очистить кэш).

## 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**.

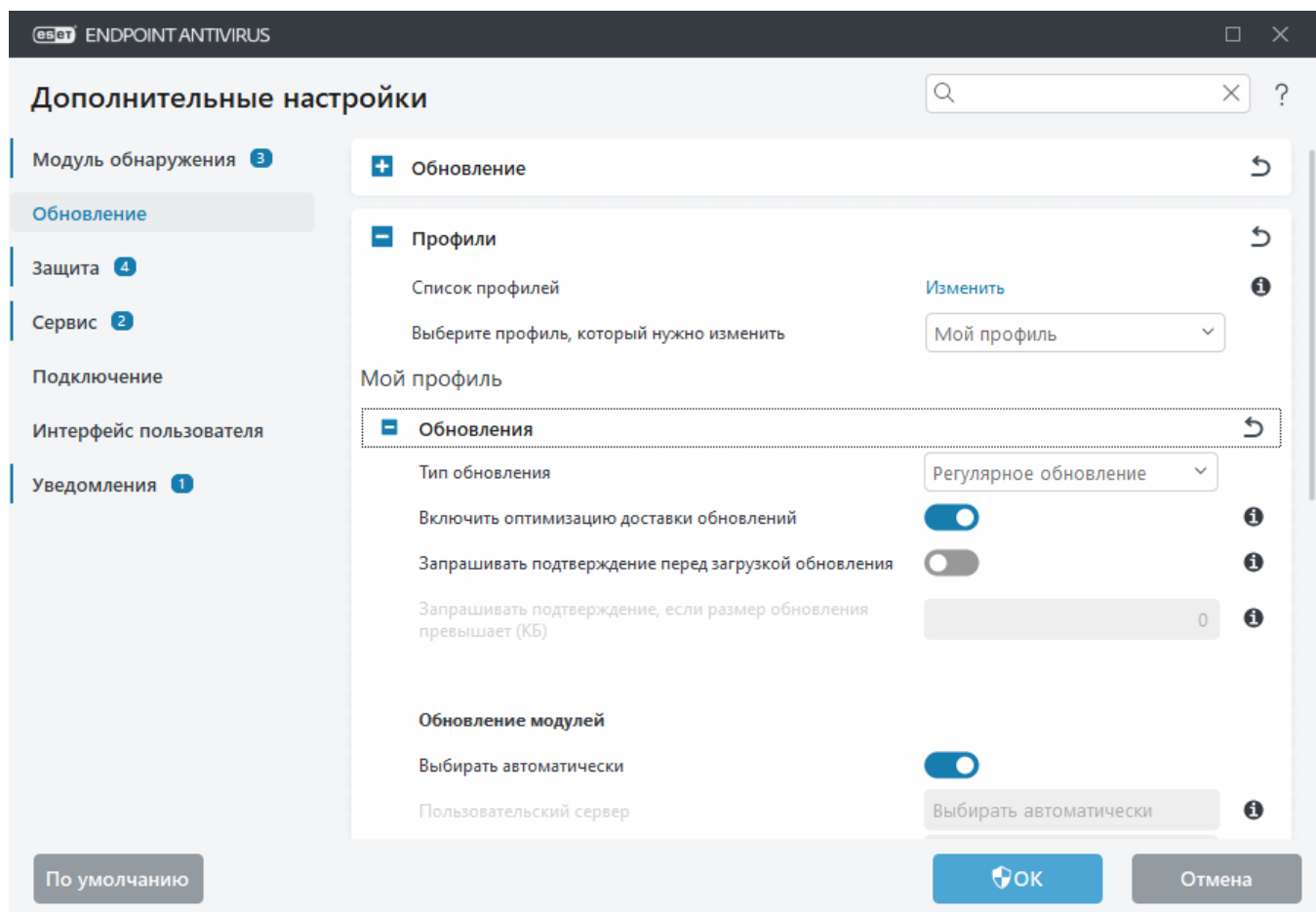
Чтобы создать профиль, рядом с элементом **Список профилей** щелкните **Изменить**, введите **имя профиля** и нажмите кнопку **Добавить**.

## 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. Тестовые обновления (параметр **Тестовое обновление**) — это обновления, которые уже прошли полное внутреннее тестирование и в ближайшее время будут доступны всем пользователям. Преимущество их использования заключается в том, что у вас появляется доступ к новейшим методам обнаружения и исправлениям. Однако такие обновления иногда могут быть недостаточно стабильны и НЕ ДОЛЖНЫ использоваться на производственных серверах и рабочих станциях, где необходимы максимальные работоспособность и стабильность. 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:** в программе отобразится уведомление, в котором можно подтвердить или отклонить загрузку 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 размер файла обновления задан равным 0 КБ, диалоговое окно подтверждения в программе будет отображаться в любом случае.



## 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:** будет уменьшен интервал обновления сигнатур обнаружения. Отключение этого параметра может негативно отразиться на скорости обнаружения.

**Разрешить обновление модуля со съемных носителей:** позволяет выполнять 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 программы

См. раздел [Обновление программы](#).

## Параметры подключения

См. раздел [Параметры подключения](#).

## Зеркало обновлений

См. раздел [Зеркало обновлений](#).

# Откат обновления

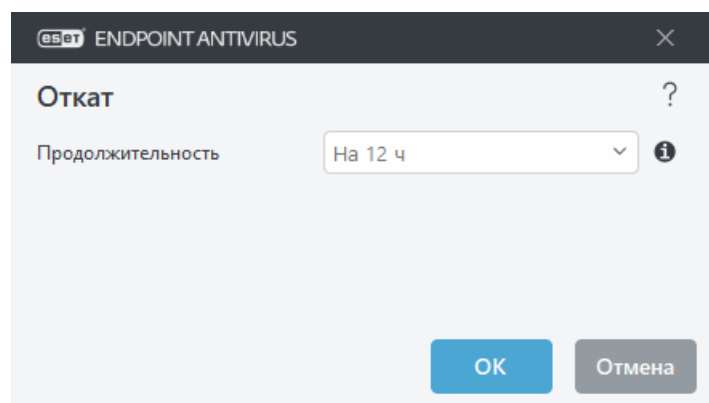
Если вы подозреваете, что последнее обновление модуля обнаружения или новые модули программы повреждены или работают нестабильно, вы можете выполнить откат до предыдущей версии и временно отключить обновления. Или же можно включить ранее отключенные обновления, если они отложены на неопределенный период времени.

Программа ESET Endpoint Antivirus 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 Antivirus откатывает версии обновления модуля обнаружения и модуля программы до самого старого снимка.

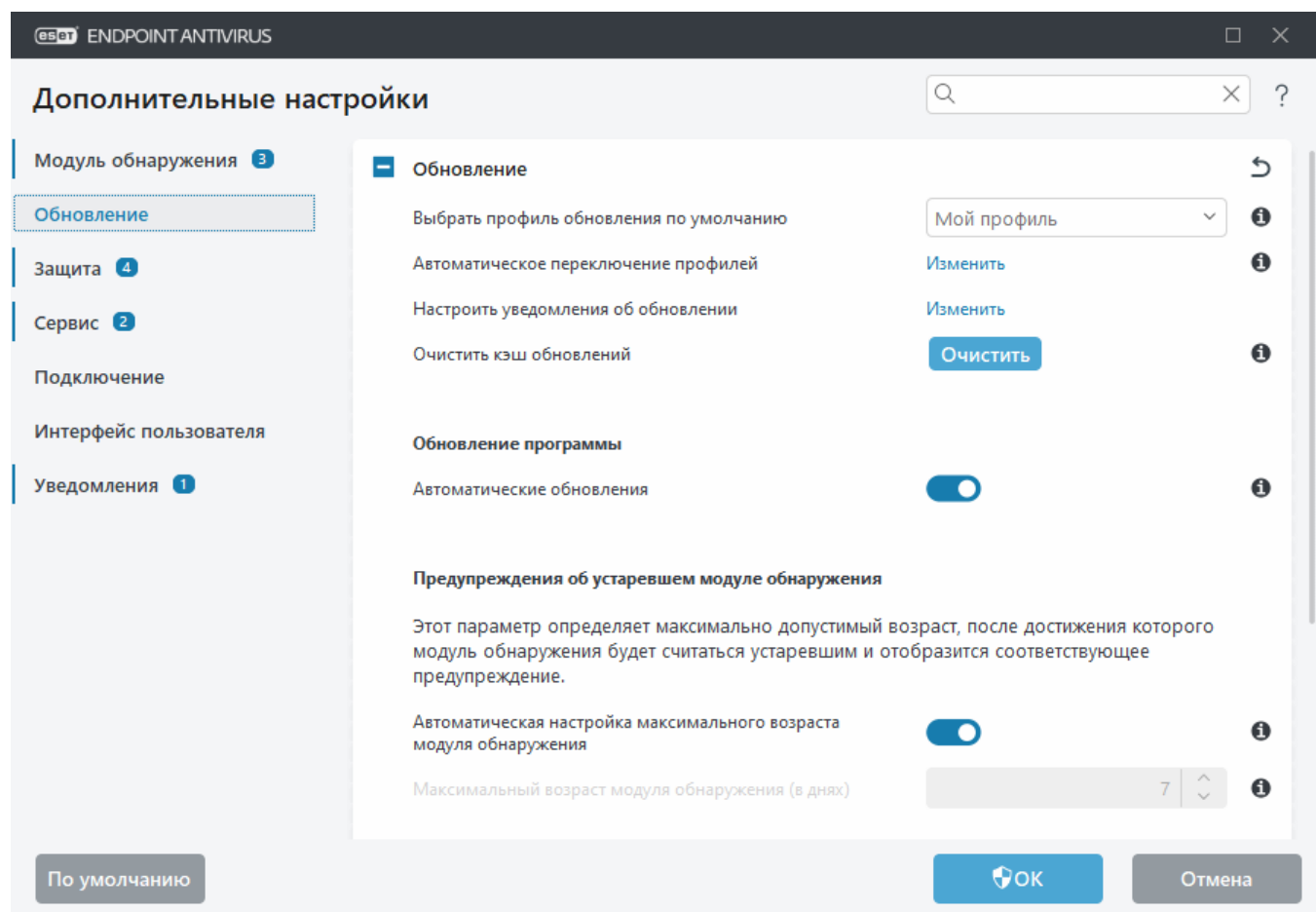
Откройте раздел [Расширенные параметры](#) > **Обновление** > **Обновление** > **Откат модуля** > **Откат** и выберите временной интервал в раскрывающемся меню **Длительность**.



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 программы

Раздел **Обновление программы** содержит параметры, связанные с обновлением программы. Пользователь может предварительно настроить поведение программы в тех случаях, когда появляются обновления для нее.

Обновления программы добавляют новые функции или вносят изменения в уже существующие. Обновление может выполняться как в автоматическом режиме без вмешательства пользователя, так и с отображением уведомления для пользователя. После установки обновления программы может потребоваться перезапуск компьютера.

**Автоматические обновления:** приостановка автоматического обновления для определенных профилей обновления временно отключает автоматическое обновление программы при

подключении к Интернету с помощью других сетей или лимитных подключений. Чтобы иметь постоянный доступ к новейшим функциям и обеспечить максимально высокую защиту, следует включить этот параметр. Дополнительные сведения об автоматическом обновлении можно найти в разделе [Вопросы и ответы по автоматическому обновлению](#).

По умолчанию обновления программы загружаются с серверов репозитория ESET. В больших или автономных средах трафик можно распределить, используя внутреннее кэширование файлов продукта.

#### [Определение пользовательского сервера для обновления компонентов программы](#)

1. Задайте путь к обновлению 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 программы, выполнив стандартное обновление ESET Endpoint Antivirus.

**i** 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 стать причиной значительного ущерба для компании.

## Параметры подключения

Чтобы получить доступ к опциям настройки прокси-сервера для определенного профиля обновления, откройте раздел [Расширенные параметры](#) > **Обновление** > **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 глобальные параметры прокси-сервера**, чтобы использовать конфигурацию прокси-сервера, уже заданную в разделе [Расширенные параметры](#) > **Подключение** > **Прокси-сервер**.

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

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

- Для обновления ESET Endpoint Antivirus 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 Antivirus будет подключаться к прокси-серверу для получения обновлений.
- Компьютер подключается к Интернету через прокси-сервер. Параметры берутся из браузера 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.

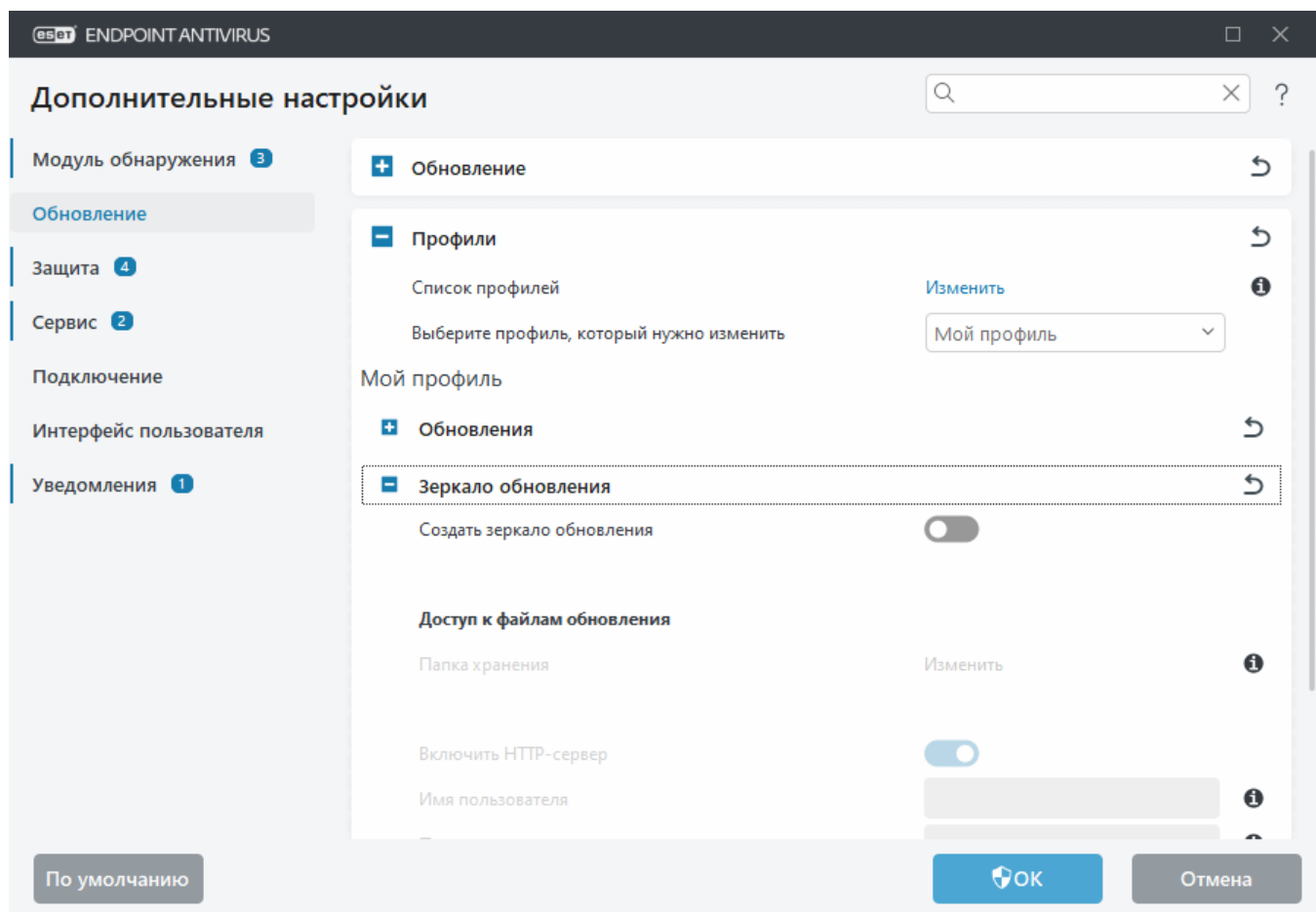
## Зеркало обновлений

ESET Endpoint Antivirus 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.

На зеркале обновлений создаются копии файлов обновления, которые можно использовать для обновления рабочих станций с решением ESET Endpoint Antivirus для Windows того же поколения (например, ESET Endpoint Antivirus для Windows версии 10.x создает файлы обновления только для версии 10.x решений ESET Endpoint Antivirus для Windows и ESET Endpoint Security для Windows).

Чтобы свести к минимуму интернет-трафик в сетях, в которых ESET PROTECT используется для управления большим количеством клиентов, рекомендуем использовать решение ESET Bridge, а не настраивать клиент как зеркало. Решение ESET Bridge можно установить вместе с ESET PROTECT с помощью комплексного установщика или как отдельный компонент. Дополнительные сведения и описание различий между ESET Bridge, прокси-сервером Apache HTTP, средством «Зеркало» и прямым подключением можно найти на [странице онлайн-справки ESET PROTECT](#).

Настроить локальный сервер зеркала можно в разделе [Расширенные параметры](#) > **Обновление** > **Профили** > **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 Antivirus\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 следует вводить в формате домен/пользователь или рабочая группа/пользователь. Не забудьте ввести соответствующие пароли.

# 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 указанные ниже варианты. 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.

 На зеркале обновлений создаются копии файлов обновления, которые можно использовать для обновления рабочих станций с решением ESET Endpoint Antivirus для Windows того же поколения (например, ESET Endpoint Antivirus для Windows версии 10.x создает файлы обновления только для версии 10.x решений ESET Endpoint Antivirus для Windows и ESET Endpoint Security для Windows).

## 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 указанные ниже варианты. 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 Antivirus, 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 в меню [Расширенные параметры](#) и щелкните **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 Antivirus 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 раздел [Расширенные параметры](#) 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 [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`.

**i** 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/ep10`

Последний раздел предназначен для управления компонентами программы (PCU). По умолчанию загруженные компоненты программы подготовлены для копирования в локальное зеркало. Если активирована функция **Обновление программы**, не нужно щелкать **Обновить**, поскольку файлы автоматически копируются в локальное зеркало, когда они доступны. Дополнительные сведения об обновлении 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 Antivirus 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 **ОК**. На экран должно быть выведено содержимое папки.

**ESET Endpoint Antivirus 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 Antivirus к серверу зеркала:** подключение к порту, указанному для доступа к HTTP-версии зеркала, блокируется.

**ESET Endpoint Antivirus ошибка при подключении при загрузке файлов обновлений:** обычно происходит при указании неправильных данных сервера обновлений (сетевое пути к папке зеркала), с которого рабочие станции загружают обновления.

## Защита

Защита предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и связи через Интернет. Например, при обнаружении объекта, который классифицируется как «вредоносная программа» начнется процесс исправления. Функция защиты может устранить угрозу, сначала заблокировав его, а затем очистив, удалив или переместив в карантин.

Чтобы детально настроить защиту, откройте раздел [Расширенные параметры](#) > **Защита**.



Изменения в параметры защиты должны вносить только опытные пользователи. Неправильная настройка этих параметров может привести к снижению уровня защиты.

В этом разделе:

- [Реагирование при обнаружении](#)
- [Настройка обнаружения](#)
- [Настройка защиты](#)

---

## Реагирование при обнаружении

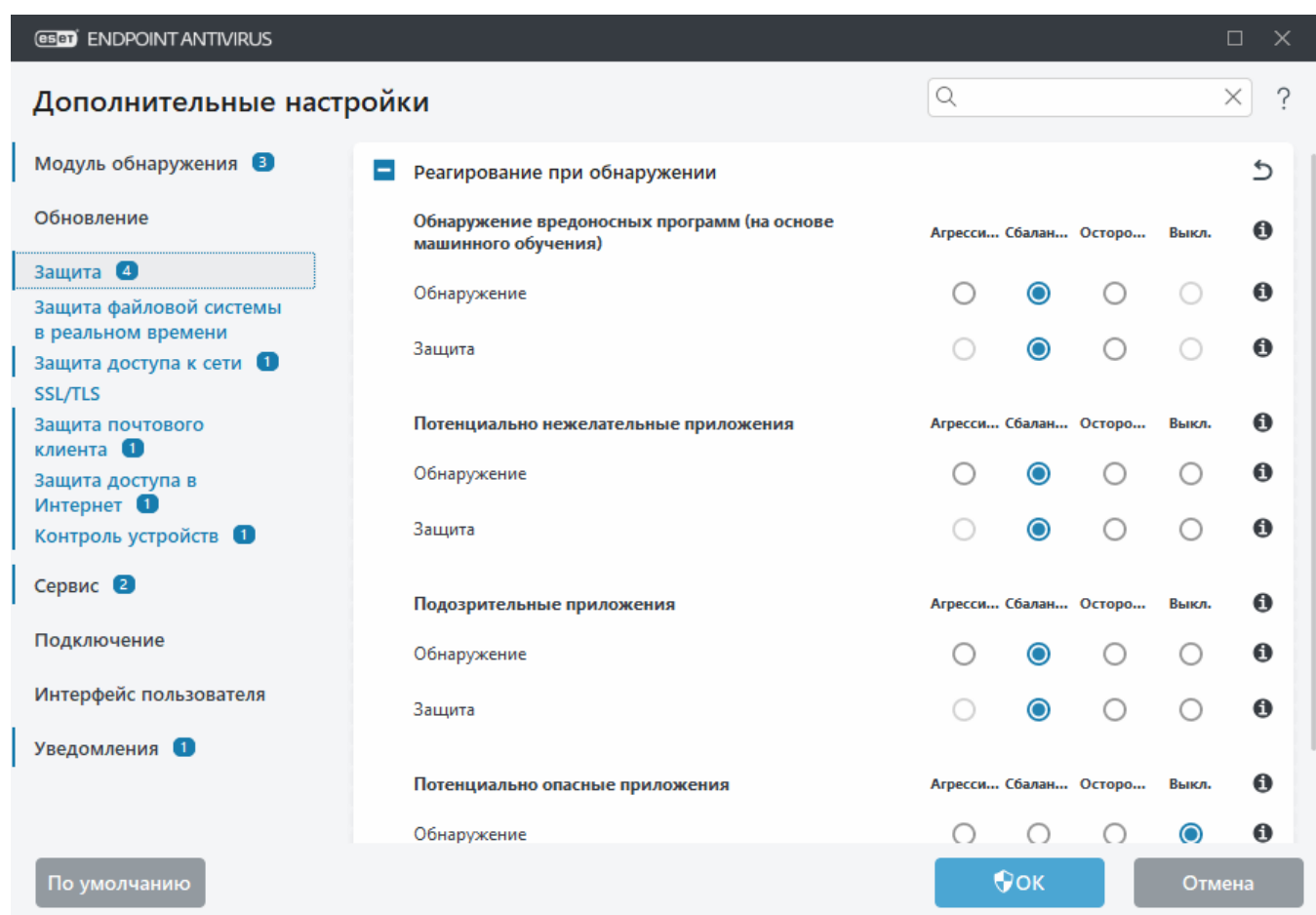
В разделе «Реагирование при обнаружении» можно настроить уровни отчетности и защиты для следующих категорий:

- **Обнаружение вредоносных программ (на основе машинного обучения)** –  
Компьютерный вирус — это фрагмент вредоносного кода, который добавляется в начало



или конец файлов на 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 [гlossарии](#).

- **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, таких как вирусы или троянские программы. 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 [гlossарии](#).
- К **подозрительным приложениям** относятся программы, сжатые с помощью [программ-упаковщиков](#) или средств защиты. Средства защиты такого типа часто используются злоумышленниками, чтобы избежать обнаружения.
- **Потенциально опасные приложения:** это определение относится к законному коммерческому программному обеспечению, которое может быть использовано для причинения вреда. К потенциально опасным приложениям относятся средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, регистрирующие каждое нажатие пользователем клавиш на клавиатуре). Дополнительную информацию о приложениях этого типа см. в [гlossарии](#).



## Улучшенная защита

- i** Расширенное машинное обучение – это часть защит, к качеству дополнительного уровня защиты на основе машинного обучения, который улучшает работу функции обнаружения. Дополнительную информацию об этом типе защиты см. в [гlossарии](#).

## 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 Antivirus.

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

1. Обнаружение вредоносных программ
2. Потенциально нежелательные приложения
3. Потенциально опасный
4. Подозрительные приложения

Обнаружения выполняются 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   |
|-------------------------|--|
| <b>Агрессивный</b>      | Функция обнаружения КАТЕГОРИИ настроена на максимальную чувствительность. Случаев обнаружения будет больше. При уровне <b>Агрессивный</b> функция может ошибочно считать объекты КАТЕГОРИЯМИ.  |
| <b>Сбалансированный</b> | Установлен сбалансированный уровень функции обнаружения КАТЕГОРИИ. Эта настройка должна обеспечивать оптимальный баланс производительности, точности обнаружения и количества ложных обнаружений.  |
| <b>Осторожный</b>       | 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.  |
| <b>Выкл.</b>            | 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.<br>Значение «Выкл» недоступно для оповещения о вредоносных программах и по умолчанию используется для потенциально опасных приложений. |

 [Доступность модулей защиты ESET Endpoint Antivirus](#)



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

|  | Агрессивный              | Сбалансированный             | Осторожный | Выкл* |
|--|--------------------------|------------------------------|------------|-------|
| Модуль расширенного машинного обучения | ✓<br>(агрессивный режим) | ✓<br>(консервативный модуль) | X          | X     |
| Модуль обнаружения                     | ✓                        | ✓                            | ✓          | X     |
| Другие модули защиты                   | ✓                        | ✓                            | ✓          | X     |

\* Не рекомендуется.

### [Определение версии продукта, версий модуля программы и даты сборки](#)

1. Щелкните элемент **Справка и поддержка** > **О продукте ESET Endpoint Antivirus**.
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 рекомендуется для сред, в которых приоритетом является минимизация количества объектов, ложно выявленных программой защиты.
- 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 Antivirus 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  |
|-------------------------|---|
| <b>Агрессивный</b>      | 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. |
| <b>Сбалансированный</b> | Обнаружения сбалансированного (или более низкого) уровня блокируются, после чего запускается автоматическое исправление (т. е. очистка).  |
| <b>Осторожный</b>       | Обнаружения осторожного уровня блокируются, и запускается автоматическое исправление (т. е. очистка).   |
| <b>Выкл.</b>            | Полезно для идентификации и исключения ложных сообщений об объектах.<br>Значение «Выкл» недоступно для защиты вредоносных программ и по умолчанию используется для потенциально опасных приложений.   |

## 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

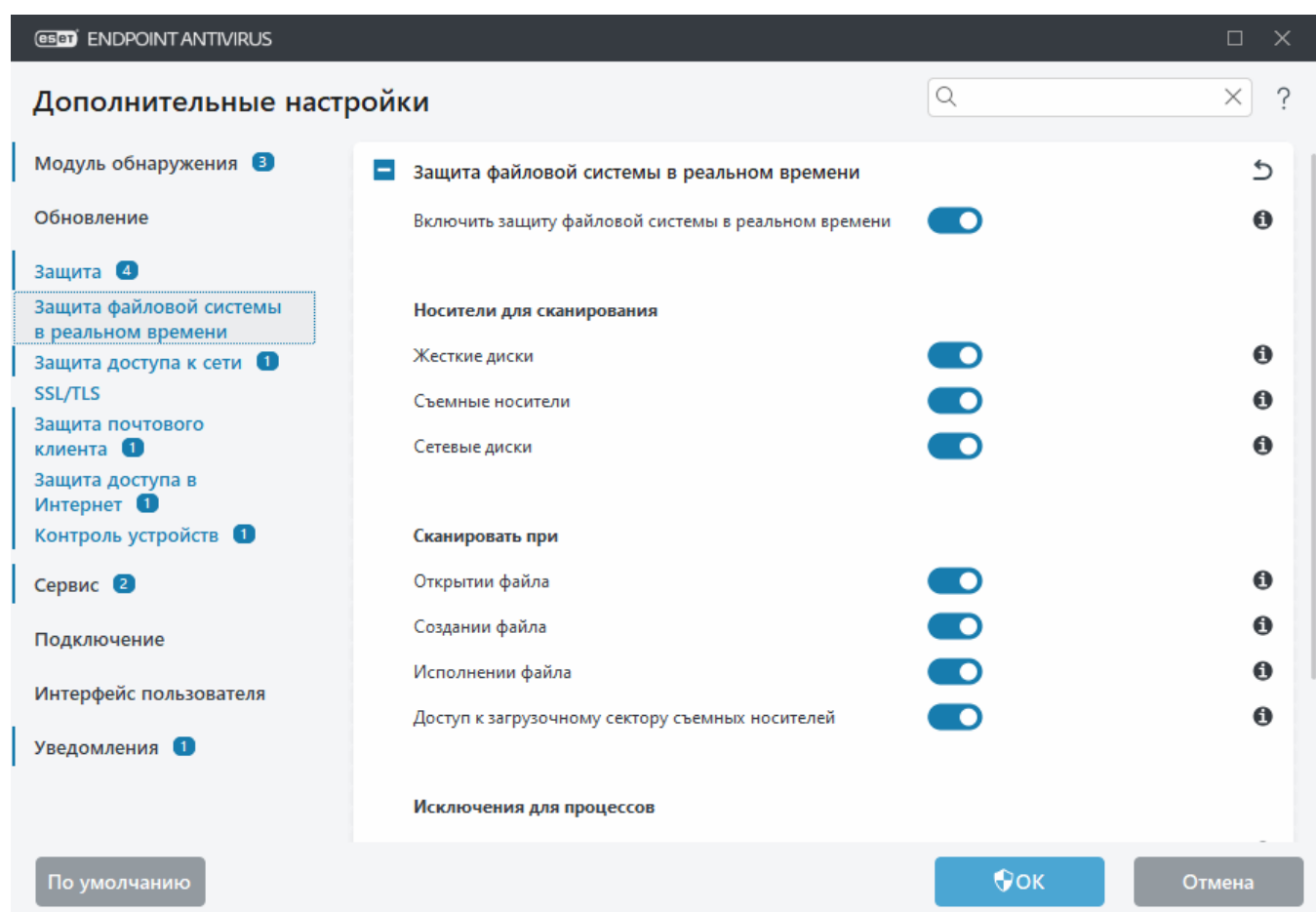
- Внедрите «производственную фазу» в некоторые рабочие станции в качестве тестовой (не для всех рабочих станций в сети).

### 3. Производственная фаза

- Настройте все пороговые значения **Защиты** на **Сбалансированный**.
- При удаленном управлении используйте соответствующую [предопределённую политику](#) защиты от вирусов для ESET Endpoint Antivirus.
- **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.

## 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 отключать параметр **Включить защиту файловой системы в реальном времени** в разделе [Расширенные параметры](#) > **Защита** > **Защита файловой системы в реальном времени** > **Защита файловой системы в реальном времени**.

## 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 выполнении. 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 ThreatSense.

## Исключения для процессов

[Исключения для процессов.](#)

### ThreatSense

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 [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. Чтобы изменить

эту настройку, откройте раздел [Расширенные параметры](#) > **Защита** > **Защита файловой системы в реальном времени**. Последовательно щелкните элементы ThreatSense > **Другое** и снимите или установите флажок **Включить интеллектуальную оптимизацию**.

Защита файловой системы в реальном времени также позволяет настраивать [дополнительные параметры ThreatSense](#).

## 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. 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.

 Не следует путать эту функцию с другими возможностями исключения — [Исключенные расширения файлов](#), [Исключения системы NIPS](#), [Исключения из обнаружения](#) или [Исключения для быстрого действия](#).

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 исключенных процессов можно в разделе [Расширенные параметры](#) > **Защита** > **Защита файловой системы в реальном времени** > **Защита файловой системы в реальном 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 Antivirus 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 NIPS](#) может выдавать сообщения об ошибке.

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

**i** [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 Antivirus 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.

## Момент изменения конфигурации защиты в режиме реального времени

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

После установки ESET Endpoint Antivirus все параметры оптимизированы для максимальной защиты системы. Чтобы восстановить настройки по умолчанию, щелкните  рядом с элементом [Расширенные параметры](#) > **Защита** > **Реагирование при обнаружении**.

## Проверка модуля защиты в режиме

## реального времени

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

Файл доступен для загрузки с веб-сайта <http://www.eicar.org/download/eicar.com>.

После ввода этого URL-адреса в браузере вы должны увидеть сообщение об удалении угрозы.

## 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 **Компьютер > 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 убедиться, что эта опция включена, откройте раздел [Расширенные параметры > Защита > Защита файловой системы в реальном времени](#).

### Защита в режиме реального времени не обнаруживает и не очищает заражения

Убедитесь, 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.

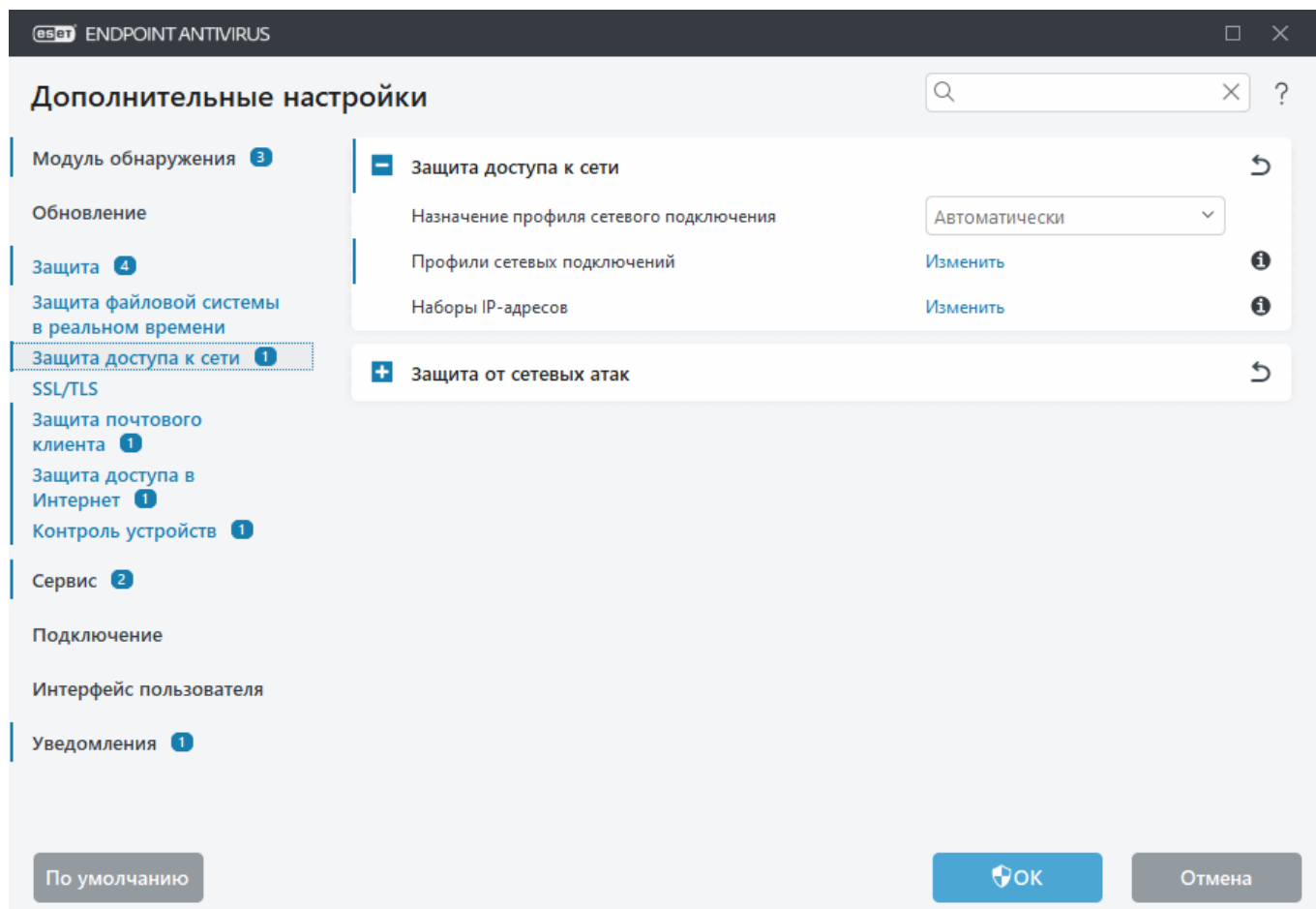
### Защита в режиме реального времени не запускается

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 решить эту проблему, [создайте журнал ESET SysInspector и отправьте его в службу технической поддержки ESET для анализа](#).



# Защита доступа к сети

В разделе «Защита доступа к сети» можно настроить все сетевые подключения. По умолчанию в ESET Endpoint Antivirus включен максимальный уровень защиты доступа к сети. Однако для определенных сред может потребоваться пользовательская настройка. Изменять настройки по умолчанию должны только опытные пользователи.



В разделе [Расширенные параметры](#) > **Защита** > **Защита доступа к сети** можно настроить указанные ниже параметры. (Щелкайте ссылки ниже для получения подробного описания каждой опции защиты доступа к сети.)

## Защита доступа к сети

[Профили сетевых подключений](#): профили можно использовать, чтобы управлять защитой доступа к сети для определенных сетевых подключений.

[Наборы IP-адресов](#): можно определить наборы IP-адресов, объединенных в одну логическую группу, которые затем можно добавить как доверенную зону или исключить из [защиты от сетевых атак](#).

[Защита от сетевых атак](#)




# Профили сетевых подключений

С помощью профилей можно управлять поведением защиты доступа к сети в ESET Endpoint Antivirus для определенного сетевого подключения. При создании или изменении [правил IDS](#), правил [защиты от атак методом подбора](#) их можно назначать определенному профилю или применять ко всем профилям. Когда определенный профиль действует для сетевого подключения, к нему применяются только глобальные правила (правила без указания профиля) и правила, назначенные этому профилю.

Настроить профили сетевого подключения и назначения можно в разделе [Расширенные параметры](#) > **Защита** > **Защита доступа к сети** > **Защита доступа к сети**.

**Назначение профиля сетевого подключения:** позволяет выбрать, будет ли вновь обнаруженным сетевым подключениям автоматически (выберите **Автоматически** в раскрывающемся меню) назначаться предварительно заданный или пользовательский профиль согласно [активаторам](#), настроенным в профилях сетевых подключений, или программа должна отображать запрос (выберите **Запросить** в раскрывающемся меню) о необходимости [настроить защиту сети](#) и назначить профиль вручную при каждом обнаружении нового сетевого подключения.

Кроме того, вы можете вручную назначить определенный профиль сетевого подключения в [главном окне программы](#) в разделе **Настройка** > **Сеть** > **Сетевые подключения**. Наведите курсор на конкретное сетевое подключение и щелкните значок меню  > **Изменить**, чтобы открыть окно [Настройка защиты сети](#) и выбрать профиль.

**Профили сетевых подключений:** щелкните **Изменить**, чтобы [добавить или изменить профили сетевых подключений](#).

Следующие профили предварительно заданы и не могут быть изменены или удалены:

**Конфиденциально** — для доверенной сети (домашней или офисной сети). Ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также системные ресурсы доступны другим пользователям сети (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Этот параметр рекомендуется использовать при доступе к безопасной локальной сети. Этот профиль автоматически назначается сетевому подключению, если оно настроено как доменная или частная сеть в Windows.

**Общедоступная** — для недоверенных (общедоступных) сетей. Файлы и папки в вашей системе не являются общими для других пользователей в сети, и другие пользователи сети их не видят, а общий доступ к системным ресурсам отключен. Этот параметр рекомендуется использовать при доступе к беспроводным сетям. Этот профиль автоматически назначается любому сетевому подключению, которое не настроено как доменная или частная сеть в Windows.

При переключении сетевого подключения на другой профиль в правом нижнем углу экрана отображается уведомление.


# Добавление и изменение профилей сетевых подключений

Добавлять или изменять [профили сетевых подключений](#) можно в разделе [Расширенные параметры](#) > **Защита** > **Защита доступа к сети** > **Защита доступа к сети** > **Профили сетевых подключений** > **Изменить**. Чтобы изменить профиль, его необходимо выбрать из списка в окне **Профили сетевых подключений**.

Следующие профили предварительно заданы и не могут быть изменены или удалены:

**Конфиденциально** — для доверенной сети (домашней или офисной сети). Ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также системные ресурсы доступны другим пользователям сети (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Этот параметр рекомендуется использовать при доступе к безопасной локальной сети. Этот профиль автоматически назначается сетевому подключению, если оно настроено как доменная или частная сеть в Windows.

**Общедоступная** — для недоверенных (общедоступных) сетей. Файлы и папки в вашей системе не являются общими для других пользователей в сети, и другие пользователи сети их не видят, а общий доступ к системным ресурсам отключен. Этот параметр рекомендуется использовать при доступе к беспроводным сетям. Этот профиль автоматически назначается любому сетевому подключению, которое не настроено как доменная или частная сеть в Windows.

**В начало/Вверх/Вниз/В конец**  : позволяет настроить уровень приоритета для профилей сетевых подключений. (Профили сетевых подключений оцениваются и применяются согласно их приоритету. Всегда применяется первый соответствующий профиль.)

## Добавление или изменение профиля

Пользовательский профиль сетевого подключения позволяет применять правила [защиты от атак методом подбора](#) и задавать дополнительные настройки для определенных сетевых подключений. Указать, каким сетевым подключениям будет назначен пользовательский профиль, можно в разделе [Активаторы](#).

Чтобы открыть редактор профиля, в окне **Профили сетевых подключений** выполните следующие действия:

- Нажмите кнопку **Добавить**.
- Выберите один из существующих профилей и щелкните **Изменить**.
- Выберите один из существующих профилей и щелкните **Копировать**.

**Имя:** пользовательское имя для вашего профиля.

**Описание:** описание профиля, помогающее его идентифицировать.

**Дополнительные доверенные адреса:** адреса, указанные здесь, добавляются в доверенную зону сетевого подключения, к которому применяется этот профиль (независимо от типа защиты сети).

**Доверенное подключение:** ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также системные ресурсы доступны другим пользователям сети (доступ к общим файлам и принтерам включен, входящее подключение RPC включено, общий доступ к удаленному рабочему столу предоставлен). Рекомендуем использовать эту настройку при создании профиля для безопасного подключения к локальной сети. Все напрямую подключенные сетевые подсети также считаются доверенными. Например, если сетевой адаптер подключен к этой 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 такой сети. Если у адаптера есть больше адресов/подсетей, все они будут доверенными.

**Сообщать о слабом шифровании Wi-Fi:** ESET Endpoint Antivirus отобразит [уведомление на рабочем столе](#) при подключении к незащищенной беспроводной сети или сети со слабой защитой.

**Активаторы:** пользовательские условия, которые должны быть выполнены для назначения сетевому подключению этого профиля. Подробное объяснение см. в разделе [Активаторы](#).

## Активаторы

Активаторы — это пользовательские условия, которые должны быть выполнены, чтобы [профиль сетевого подключения](#) был назначен сетевому подключению. Если атрибуты подключенной сети совпадают с атрибутами, которые определены в активаторах для профиля подключенной сети, такой профиль будет применен к сети. У профиля сетевого подключения может быть один или несколько активаторов. При наличии нескольких активаторов применяется логика ИЛИ (должно быть выполнено хотя бы одно условие). Определять активаторы можно в [редакторе профилей сетевых подключений](#). Создавать пользовательские профили сетевых подключений должны опытные пользователи.

Доступны следующие активаторы:

### [Адаптер](#)

**Тип адаптера:** применить профиль, если сетевое подключение установлено на выбранном типе адаптера.

**Имя адаптера:** применить профиль, если совпадает имя сетевого адаптера.

**IP-адрес адаптера:** применить профиль, если совпадает IP-адрес сетевого адаптера.

### [DNS](#)

**DNS-суффикс:** применить профиль, если совпадает доменное имя.

**IP-адрес DNS:** применить профиль, если совпадает IP-адрес DNS-сервера.

### [WINS](#)

Применить профиль, если совпадает сопоставленный IP-адрес Windows Internet Name Service (WINS).

### [DHCP](#)

**IP-адрес DHCP:** совпадение IP-адреса DHCP-сервера.

### [Шлюз по умолчанию](#)

**IP-адрес:** применить профиль, если совпадает IP-адрес шлюза по умолчанию.  
**MAC-адрес:** применить профиль, если совпадает MAC-адрес шлюза по умолчанию.

### [Wi-Fi](#)

**SSID:** применить профиль, если совпадает SSID (имя сети Wi-Fi).

**Имя профиля:** применить профиль, если совпадает имя профиля Wi-Fi.

**Тип защиты:** применить профиль, если тип защиты совпадает с типом, который выбран с помощью раскрывающегося меню. (Если необходимо совпадение с несколькими типами, создайте еще один активатор.)

**Тип шифрования:** применить профиль, если тип шифрования совпадает с типом, который выбран с помощью раскрывающегося меню. (Если необходимо совпадение с несколькими типами, создайте еще один активатор.)

**Безопасность сети:** применить профиль, если сеть **открыта/защищена**.

### [Профиль Windows](#)

Применить профиль, если сеть настроена в Windows как **доменная/частная/общедоступная**.

### [Аутентификация](#)

В рамках аутентификации сети выполняется поиск определенного сервера в сети, а для аутентификации сервера используется асимметричное шифрование (RSA). Имя сети, для которой проводится аутентификация, должно совпадать с именем, заданным в настройках сервера аутентификации. Имя вводится с учетом регистра. Имя сервера может быть введено как IP-адрес, DNS-имя или NetBIOS-имя.

[Загрузите сервер аутентификации ESET.](#)

Открытым ключом может быть файл одного из указанных ниже типов.

- Открытый ключ с шифрованием PEM (.pem). Этот ключ можно создать с помощью сервера аутентификации ESET.
- 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.

## Наборы IP-адресов

Набор IP-адресов — это ряд IP-адресов, создающих одну логическую группу, которая может быть полезна при повторном использовании одного и того же набора адресов в нескольких правилах [защиты от атак методом подбора](#). Кроме того, ESET Endpoint Antivirus содержит

предварительно заданные наборы IP-адресов, к которым применяются внутренние правила. Примером такой группы является **доверенная зона**. Доверенная зона представляет собой группу сетевых адресов, где ваш компьютер и общие файлы, хранящиеся на нем, видны для других пользователей сети, а также другим пользователям сети доступны системные ресурсы.

Чтобы добавить набор IP-адресов, выполните следующие действия.

1. Откройте раздел [Расширенные параметры](#) > **Защита** > **Защита доступа к сети** > **Наборы IP-адресов** > **Изменить**.
2. Щелкните **Добавить**, введите **имя** и **описание** зоны и укажите удаленный IP-адрес в поле **Адрес удаленного компьютера (IPv4, IPv6, диапазон, маска)**.
3. Нажмите кнопку **ОК**.

Дополнительные сведения см. в разделе [Изменение наборов IP-адресов](#).

## Редактирование наборов IP-адресов

Дополнительные сведения о наборах IP-адресов см. в разделе [Наборы IP-адресов](#).

### Столбцы

**Имя:** имя группы удаленных компьютеров.

**Описание:** общее описание группы.

**IP-адреса:** удаленные IP-адреса, которые принадлежат набору IP-адресов.

### Элементы управления

При **добавлении** или **изменении** набора IP-адресов доступны следующие поля.

**Имя:** имя группы удаленных компьютеров.

**Описание:** общее описание группы.

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

**Удалить:** удаление зоны из списка.

**i** Предварительно заданные наборы IP-адресов не могут быть удалены.

### Примеры IP-адресов

Добавить адрес IPv4:

**Один адрес:** добавляет IP-адрес отдельного компьютера (например, *192.168.0.10*).

**Диапазон адресов:** введите начальный и конечный IP-адреса, чтобы задать диапазон IP-адресов нескольких компьютеров (например, *192.168.0.1–192.168.0.99*).

✓ **Подсеть:** подсеть (группа компьютеров), заданная IP-адресом и маской. Например, *255.255.255.0* — это маска сети для подсети *192.168.1.0*. Чтобы исключить всю подсеть, введите *192.168.1.0/24*.

Добавить адрес IPv6:

**Один адрес:** добавляет IP-адрес отдельного компьютера (например, *2001:718:1c01:16:214:22ff:fec9:ca5*).

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

## Защита от сетевых атак (IDS)

Защита от сетевых атак (IDS) улучшает обнаружение эксплойтов для известных уязвимостей. Дополнительные сведения о защите от сетевых атак см. в [гlossарии](#). Чтобы настроить защиту от сетевых атак, откройте раздел [Расширенные параметры](#) > **Защита** > **Защита доступа к сети** > **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 [гlossарии](#).

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

Все важные события, обнаруженные защитой сети, сохраняются в файле журнала. Дополнительные сведения см. в [журнале защиты сети](#).

## 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.

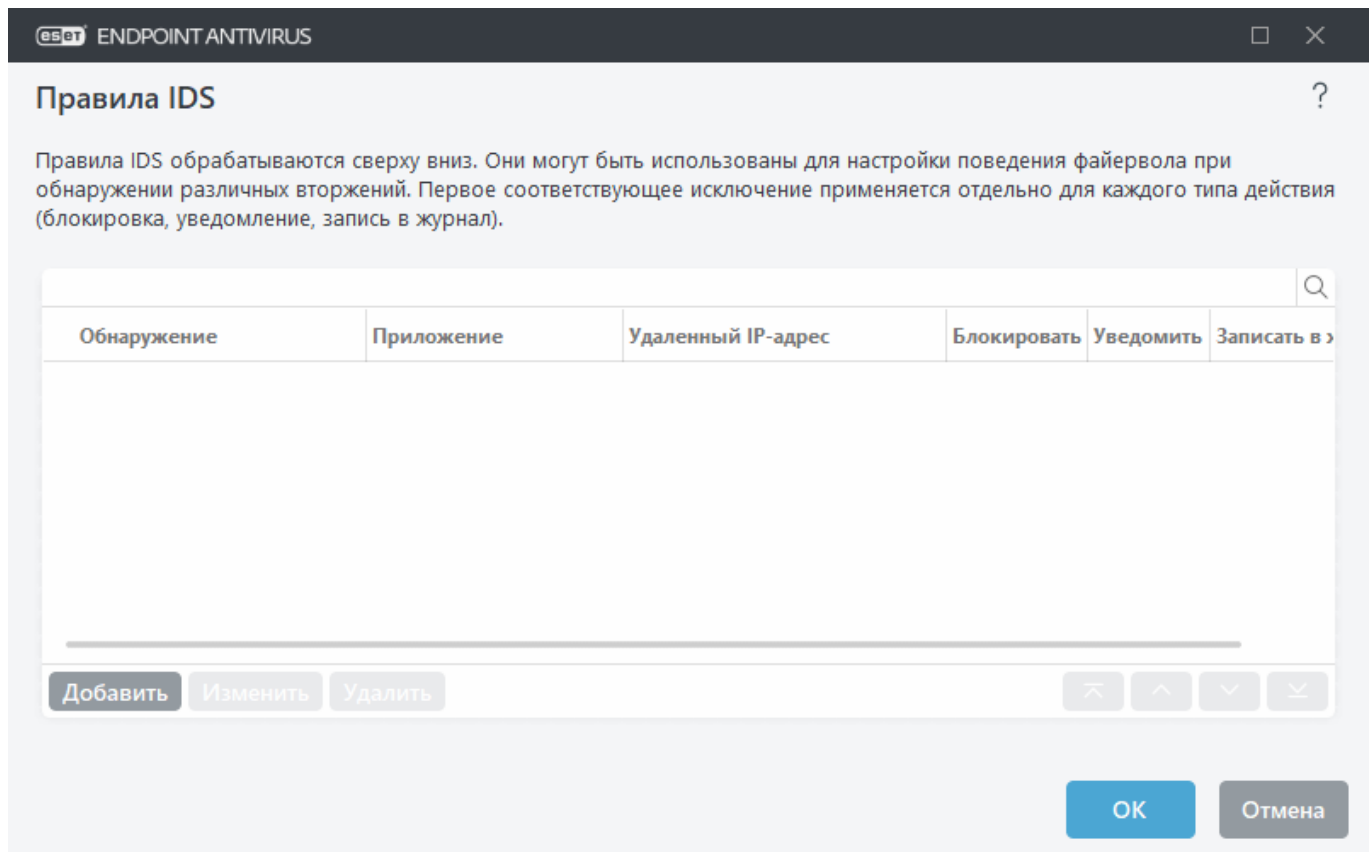


Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:

- [Создание правил IDS на рабочих станциях клиента в ESET Endpoint Antivirus](#)
- [Создание правил IDS для рабочих станций клиента в ESET PROTECT](#)

## Управление правилами IDS

- **Добавить:** нажмите для создания нового правила IDS.
- **Изменить:** нажмите для изменения существующего правила IDS.
- **Удалить:** выберите и щелкните для удаления правила IDS из списка исключений.
-     **В начало/Вверх/Вниз/В конец:** настройка приоритетности правил (исключения обрабатываются сверху вниз).



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.

## Редактор правил

**Обнаружение:** тип обнаружения.

**Имя угрозы:** можно указать имя угрозы для некоторых доступных обнаружений.

**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). Несколько адресов следует разделять запятой.

**Профиль.** Можно выбрать [профиль сетевого подключения](#), к которому применяется это правило.

## Действие

**Блокировать.** Каждый системный процесс имеет свое поведение по умолчанию и назначенное действие (блокировать или разрешить). Для изменения поведения ESET Endpoint Antivirus 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 Antivirus](#). Выберите **Нет**, чтобы отключить запись. Доступные значения: **По умолчанию, Да, Нет.**

The screenshot shows the 'Добавить правило IDS' (Add IDS Rule) dialog box in the ESET Endpoint Antivirus interface. The dialog has a title bar with the ESET logo and 'ENDPOINT ANTIVIRUS'. The main area contains several configuration options:

- Обнаружение** (Detection): A dropdown menu set to 'Любое обнаружение' (Any detection).
- Имя угрозы** (Threat name): A text input field.
- Направление** (Direction): A dropdown menu set to 'Оба' (Both).
- Приложение** (Application): A text input field with a dropdown arrow.
- Удаленный IP-адрес:** (Remote IP address): A large text input field with an information icon.
- Профиль** (Profile): A text input field with an information icon. Below it are 'Добавить' (Add) and 'Удалить' (Remove) buttons.
- Действие** (Action): A section with three dropdown menus:
  - Блокировать** (Block): Set to 'По умолчанию' (By default).
  - Уведомить** (Notify): Set to 'По умолчанию' (By default).
  - Записать в журнал** (Log): Set to 'По умолчанию' (By default).

At the bottom right, there are 'ОК' (OK) and 'Отмена' (Cancel) buttons.



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 Antivirus.
5. Выберите в раскрывающихся меню **Уведомить** и **Записать в журнал** значения **Да**.
6. Щелкните **ОК**, 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 оповещение в раскрывающемся меню **Обнаружение**, например **Сеанс SMB без расширений безопасности**.
- ✓ 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 **ОК**, чтобы сохранить это уведомление.

## Защита от атак методом подбора

Защита от атак методом подбора блокирует атаки, которые предусматривают угадывание пароля и направлены на службы RDP или SMB. Атака методом подбора — это способ определения пароля, при котором происходит систематический перебор всех комбинаций букв, цифр и символов. Чтобы настроить защиту от атак методом подбора, откройте раздел [Расширенные параметры](#) > **Защита** > **Защита доступа к сети** > **Защита от сетевых атак** > **Защита от атак методом подбора**.

**Включить защиту от атак методом подбора:** ESET Endpoint Antivirus проверяет содержимое сетевого трафика и блокирует попытки атак, которые предусматривают угадывание пароля.





**Правила:** вы можете создавать, изменять и просматривать правила для входящих и исходящих сетевых подключений. Дополнительные сведения см. здесь [Правила](#).

**Исключения:** список исключаемых обнаружений, определенных с помощью IP-адреса или пути приложения. Исключения можно создавать и изменять в ESET PROTECT. Дополнительные сведения см. здесь [Исключения](#).

## Правила

**Правила:** вы можете создавать, изменять и просматривать правила для входящих и исходящих сетевых подключений. Предварительно заданные правила нельзя изменить или удалить.

# Управление правилами защиты от атак методом подбора

- **Добавить:** щелкните для создания правила защиты от атак методом подбора.
- **Изменить:** щелкните для изменения существующего правила защиты от атак методом подбора.
- **Удалить:** выберите и щелкните для удаления правила IDS из списка исключений.
-     **В начало/Вверх/Вниз/В конец:** настройка приоритетности правил.

eset ENDPOINT ANTIVIRUS

Правила

?





Определите входящие и исходящие сетевые подключения, используемые защитой от атак методом подбора. Правила оцениваются сверху вниз, и применяется действие первого подходящего правила.

| Имя                         | Включено                            | Протокол    | Действие  | Профиль       | Наборы IP-адресов источника    | Макс. кол-в |
|-----------------------------|-------------------------------------|-------------|-----------|---------------|--------------------------------|-------------|
| Блокировать атаку мето...   | <input checked="" type="checkbox"/> | Протокол... | Запретить | Любой профиль | Локальные адреса, Частные а... | 12          |
| Блокировать атаку мето...   | <input checked="" type="checkbox"/> | Протокол... | Запретить | Любой профиль |                                | 10          |
| Игнорировать попытку вхо... | <input checked="" type="checkbox"/> | Протокол... | Разрешить | Любой профиль | Локальные адреса, Частные а... |             |
| Блокировать атаку мето...   | <input checked="" type="checkbox"/> | Протокол... | Запретить | Любой профиль |                                | 40          |

Добавить

Изменить

Удалить

OK

Отмена



Чтобы обеспечить максимальную защиту, применяется правило блокировки с наименьшим значением параметра **Макс. кол-во попыток**, даже если это правило находится ниже в списке правил, когда условиям обнаружения соответствует несколько правил блокировки.

## Редактор правил

**Имя:** имя правила.

**Включено:** отключите этот переключатель, если правило нужно оставить в списке, но при этом не применять его.

**Действие:** выберите, следует ли **запретить** или **разрешить** подключение, если выполняются параметры правила.

**Протокол:** протокол связи, который будет проверяться этим правилом.

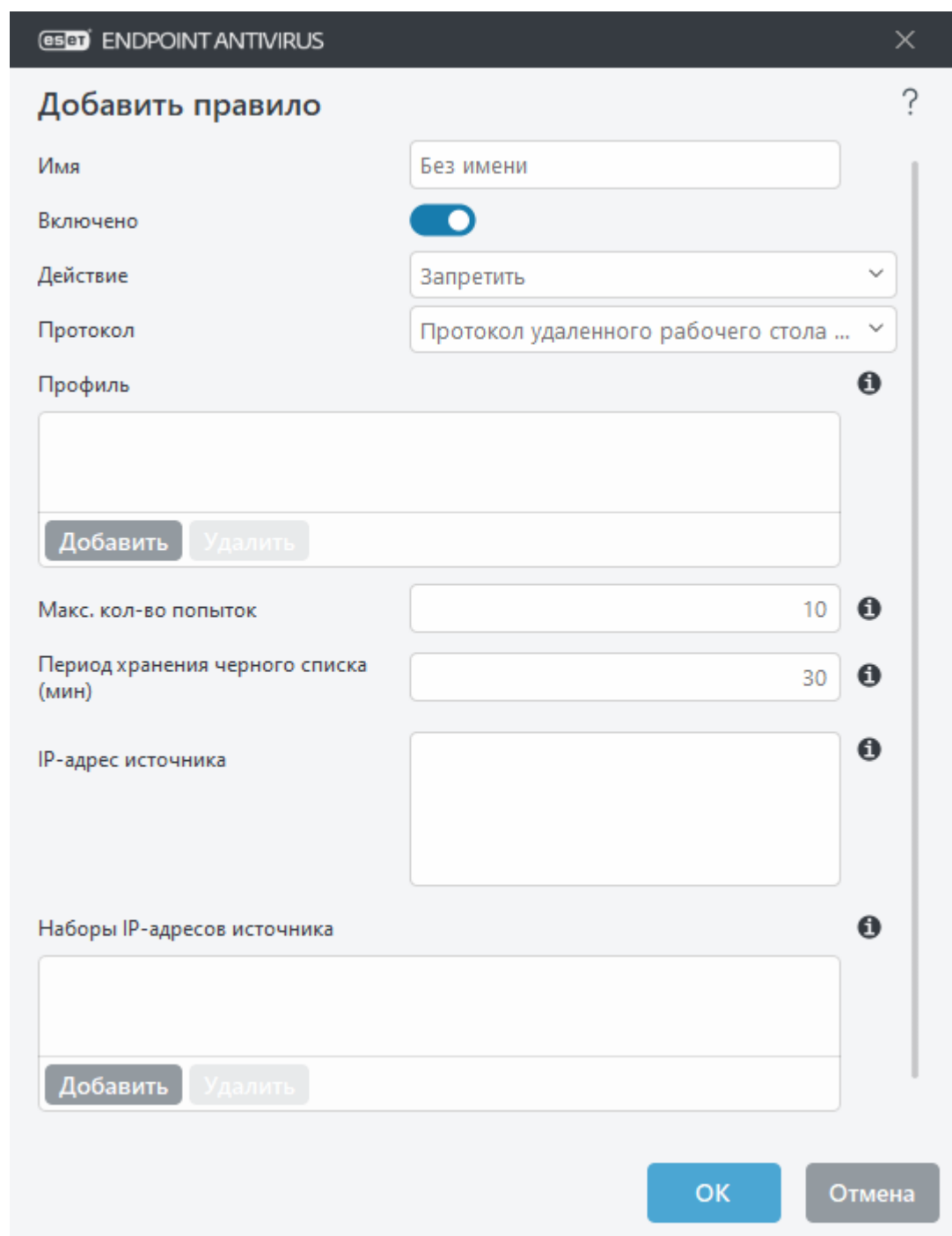
**Профиль.** Можно выбрать [профиль сетевого подключения](#), к которому применяется это правило.

**Макс. кол-во попыток** — Максимальное количество разрешенных попыток повторения атаки, по достижении которого IP-адрес будет заблокирован и добавлен в черный список.

**Период хранения черного списка (мин):** установка времени, по истечении которого адрес будет исключен из черного списка.

**IP-адрес источника:** список IP-адресов, диапазонов или подсетей. Несколько адресов следует разделять запятой.

**Наборы IP-адресов источника:** набор IP-адресов, который вы уже задали в разделе [Наборы IP-адресов](#).



The screenshot shows the 'Добавить правило' (Add Rule) window in ESET Endpoint Antivirus. The window has a dark header with the ESET logo and 'ENDPOINT ANTIVIRUS' text. The main area contains several configuration fields:

- Имя** (Name): A text box containing 'Без имени' (No name).
- Включено** (Enabled): A toggle switch that is currently turned on.
- Действие** (Action): A dropdown menu set to 'Запретить' (Prohibit).
- Протокол** (Protocol): A dropdown menu set to 'Протокол удаленного рабочего стола ...' (Remote Desktop Protocol ...).
- Профиль** (Profile): A large empty text box with 'Добавить' (Add) and 'Удалить' (Remove) buttons below it.
- Макс. кол-во попыток** (Max. number of attempts): A text box containing '10'.
- Период хранения черного списка (мин)** (Blacklist storage period (min)): A text box containing '30'.
- IP-адрес источника** (Source IP address): A large empty text box.
- Наборы IP-адресов источника** (Source IP address sets): A large empty text box with 'Добавить' (Add) and 'Удалить' (Remove) buttons below it.

Information icons (i) are present next to the Profile, Max. number of attempts, Blacklist storage period, Source IP address, and Source IP address sets fields. A question mark icon (?) is in the top right corner. At the bottom right are 'ОК' (OK) and 'Отмена' (Cancel) buttons.

# Исключения

Исключения для атак методом подбора можно использовать, чтобы подавлять обнаружение атак методом подбора при наличии определенных условий. Эти исключения создаются в ESET PROTECT на основе обнаружений атак методом подбора.

## 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). Несколько адресов следует разделять запятой.


## Управление исключениями

Исключения будут отображаться, если администратор [создал исключения для атак методом подбора в веб-консоли ESET PROTECT](#). Исключения могут содержать только разрешающие правила и оцениваются перед правилами IDS.

## Расширенные параметры

В разделе [Расширенные параметры](#) > **Защита** > **Защита доступа к сети** > **Защита от сетевых атак** > **Расширенные параметры** можно включить или отключить обнаружение нескольких типов атак и эксплойтов, которые могут нанести вред компьютеру.

 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 этом окне зависит от типа или версии программы ESET и модуля файервола, а также от версии операционной системы.

## ■ 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).
- **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. Вы можете определить **срок хранения черного списка**, который устанавливает время, на которое будет заблокирован адрес после обнаружения атаки.
- **Уведомлять об обнаружении атаки:** включение уведомлений в области уведомлений Windows в правом нижнем углу экрана.
- **Показывать уведомление при обнаружении атаки, использующей брешу в системе безопасности:** показывает уведомления, если обнаруживается атака, использующая брешу в системе безопасности, или если опасный объект пытается войти в систему через брешь.

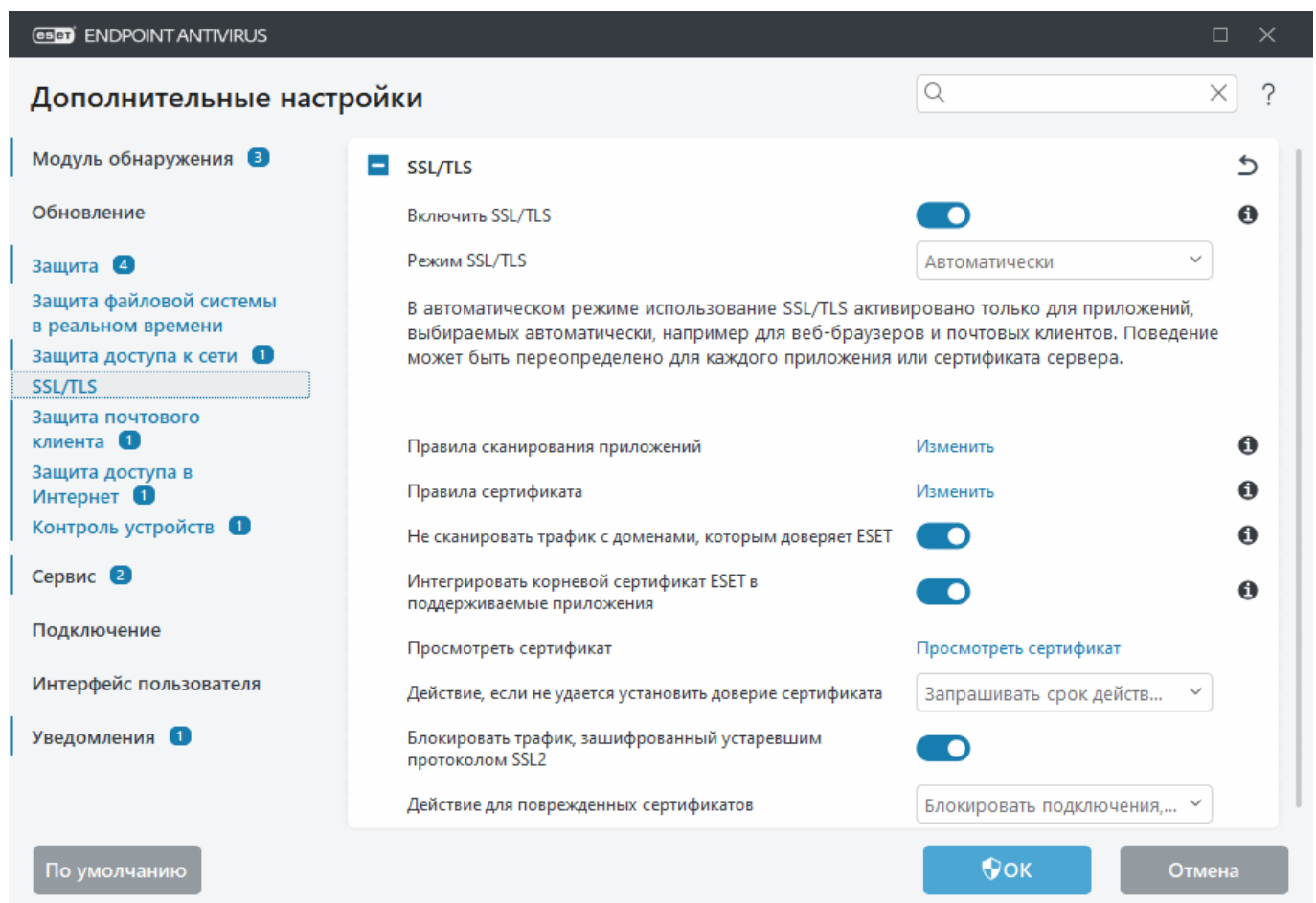
## ■ Проверка пакетов

- **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.
- **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:** другие службы MSRPC. 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\_ip). 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»).

## SSL/TLS

ESET Endpoint Antivirus может выполнять проверку на наличие угроз при обмене данными, которые используют протокол SSL. Можно использовать различные режимы фильтрации для защищенных SSL-соединений, для которых используются доверенные сертификаты, неизвестные сертификаты или сертификаты, исключенные из проверки защищенных SSL-соединений. Чтобы изменить настройки SSL/TLS, откройте раздел [Расширенные параметры](#) > **Защита** > **SSL/TLS**.



**Включить SSL/TLS:** если этот параметр отключен, ESET Endpoint Antivirus не будет сканировать обмен данными по протоколу SSL/TLS.

**режим SSL/TLS** доступен со следующими параметрами:

| Режим фильтрации          | Описание   |
|---------------------------|--|
| <b>Автоматический</b>     | Используемый по умолчанию режим, в котором сканируются только соответствующие приложения, такие как веб-браузеры и почтовые клиенты. Вы можете переопределить его, выбрав приложения, в которых обмен данными следует сканировать.   |
| <b>Интерактивно</b>       | При выполнении входа на новый защищенный SSL-сайт (с неизвестным сертификатом) на экран выводится <a href="#">диалоговое окно выбора действия</a> . Этот режим позволяет создавать список сертификатов SSL и приложений, исключаемых из сканирования.  |
| <b>На основе политики</b> | 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. |

**Правила сканирования приложений:** позволяет настроить поведение ESET Endpoint Antivirus для определенных приложений.

**Правила сертификата:** позволяет настроить поведение ESET Endpoint Antivirus для конкретных сертификатов SSL.

**Не сканировать трафик с доменами, которым доверяет ESET:** если этот параметр включен, обмен данными с доверенными доменами будет исключен из сканирования. Надежность домена определяется управляемым компанией ESET встроенным белым списком.

**Интегрировать корневой сертификат ESET в поддерживаемые приложения** — Для нормальной работы SSL-подключений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET в список известных корневых сертификатов (издателей). При включении этого параметра ESET Endpoint Antivirus автоматически добавляет сертификат ESET SSL Filter CA в известные браузеры (например, Opera). Для браузеров, использующих системное хранилище сертификатов, сертификат добавляется автоматически. Например, Firefox автоматически настроен для доверия корневым центрам в хранилище сертификатов системы.

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

**Действие, если не удастся установить доверие сертификата:** в некоторых случаях сертификат веб-сайта не может быть проверен с помощью хранилища доверенных корневых центров сертификации (TRCA) (например, сертификат с истекшим сроком действия, недоверенный сертификат, сертификат, недействительный для определенного домена, или подпись, которую можно проанализировать, но которая неправильно подписывает сертификат). Законный веб-сайт всегда использует доверенный сертификат. Если он его не предоставляет, это может означать, что злоумышленник расшифровывает ваш обмен данными или веб-сайт испытывает технические трудности.



Если установлен флажок **Запрашивать срок действия сертификата** (он установлен 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 подключения, использующие данный сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтом, использующим недоверенный сертификат.

**Блокировать трафик, зашифрованный устаревшим протоколом SSL2:** обмен данными с использованием более ранней версии протокола SSL будет автоматически блокироваться.

**Действие для поврежденных сертификатов:** поврежденный сертификат означает, что сертификат использует формат, который не распознается решением ESET Endpoint Antivirus, или сертификат был получен поврежденным (например, перезаписан случайными данными). 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](#)
- [«Зашифрованный сетевой трафик: ненадежный сертификат» отображается при посещении веб-страниц](#)

## Правила сканирования приложений

Параметр **Правила сканирования приложений** может использоваться для настройки поведения ESET Endpoint Antivirus в отношении определенных приложений, а также для запоминания выбранных действий, если для параметра **Режим SSL/TLS** выбран **интерактивный режим**. Список можно просмотреть и изменить в разделе [Расширенные параметры](#) > **Защита** > **SSL/TLS** > **Правила сканирования приложений** > **Изменить**.

Окно **Правила сканирования приложений** состоит из следующих элементов.

### Столбцы

**Приложение:** выберите исполняемый файл в дереве каталогов или нажмите кнопку ..., чтобы вручную ввести путь.

**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 приложение, которое нужно настроить, и нажмите кнопку **Изменить**.

**Удалить:** выберите приложение, которое нужно удалить, и нажмите кнопку **Удалить**.

**Импорт/Экспорт:** импорт приложений из файла или сохранение текущего списка приложений в файл.

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

## Правила сертификата

Параметр **Правила сертификата** может использоваться для настройки поведения ESET Endpoint Antivirus в отношении определенных сертификатов SSL, а также для запоминания выбранных действий, если для параметра **Режим SSL/TLS** выбран **интерактивный режим**. Список можно просмотреть и изменить в разделе [Расширенные параметры](#) > **Защита** > **SSL/TLS** > **Правила сертификата** > **Изменить**.

Окно **Правила сертификата** состоит из следующих элементов.

### 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. Чтобы сканировать в автоматическом режиме и запрашивать действия в интерактивном, выберите элемент **Автоматически**. Выберите **Запрашивать**, чтобы всегда запрашивать действия пользователя.

## Элементы управления

**Добавить** — выбор нового сертификата и настройка его параметров, связанных с доступом и сканированием.

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

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

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

## Зашифрованный сетевой трафик

Если в системе настроено сканирование протокола SSL/TLS, 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 Antivirus 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 **SSL/TLS режима** 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 Antivirus должна SSL-трафик **игнорировать**.

### Примеры с иллюстрациями

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:



- [Уведомления касательно сертификатов в продуктах ESET для Windows](#)
- [«Зашифрованный сетевой трафик: ненадежный сертификат» отображается при посещении веб-страниц](#)

В каждом из этих случаев пользователь может сохранить в системе выбранное действие. Сохраненные действия хранятся в разделе [Правила сертификата](#).

## Защита почтового клиента

Чтобы настроить защиту почтового клиента, откройте раздел [Расширенные параметры](#) > **Защита** > **Защита почтового клиента** и сделайте выбор среди следующих опций конфигурации:

- [Защита транспортного уровня](#)
- [Защита почтового ящика](#)
- [ThreatSense](#)

## Защита транспортного уровня

IMAP(S) и POP3(S) — самые распространенные протоколы, используемый для получения электронной почты в почтовых клиентах. Они используются для обмена данными по электронной почте с помощью приложения почтового клиента. Протокол IMAP — это еще один 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 передавать 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 Antivirus 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 IMAP, не сканируются. Но связь с сервером Microsoft Exchange может сканировать [модуль интеграции](#) в почтовых клиентах, таких как Microsoft Outlook.

**i** ESET Endpoint Antivirus также поддерживает сканирование протоколов IMAPS (585, 993) и POP3S (995), которые для передачи информации между сервером и клиентом используют зашифрованный канал. ESET Endpoint Antivirus проверяет соединения, использующие методы шифрования SSL и TLS. Зашифрованные соединения сканируются по умолчанию. Чтобы просмотреть настройки модуля сканирования, откройте раздел [Расширенные параметры](#) > **Защита** > [SSL/TLS](#).

Чтобы настроить защиту почтового транспорта, откройте раздел [Расширенные параметры](#) > **Защита** > **Защита почтового клиента** > **Защита почтового транспорта**.

**Включить защиту почтового транспорта:** если этот параметр включен, обмен данными почтового транспорта будет сканироваться решением ESET Endpoint Antivirus.

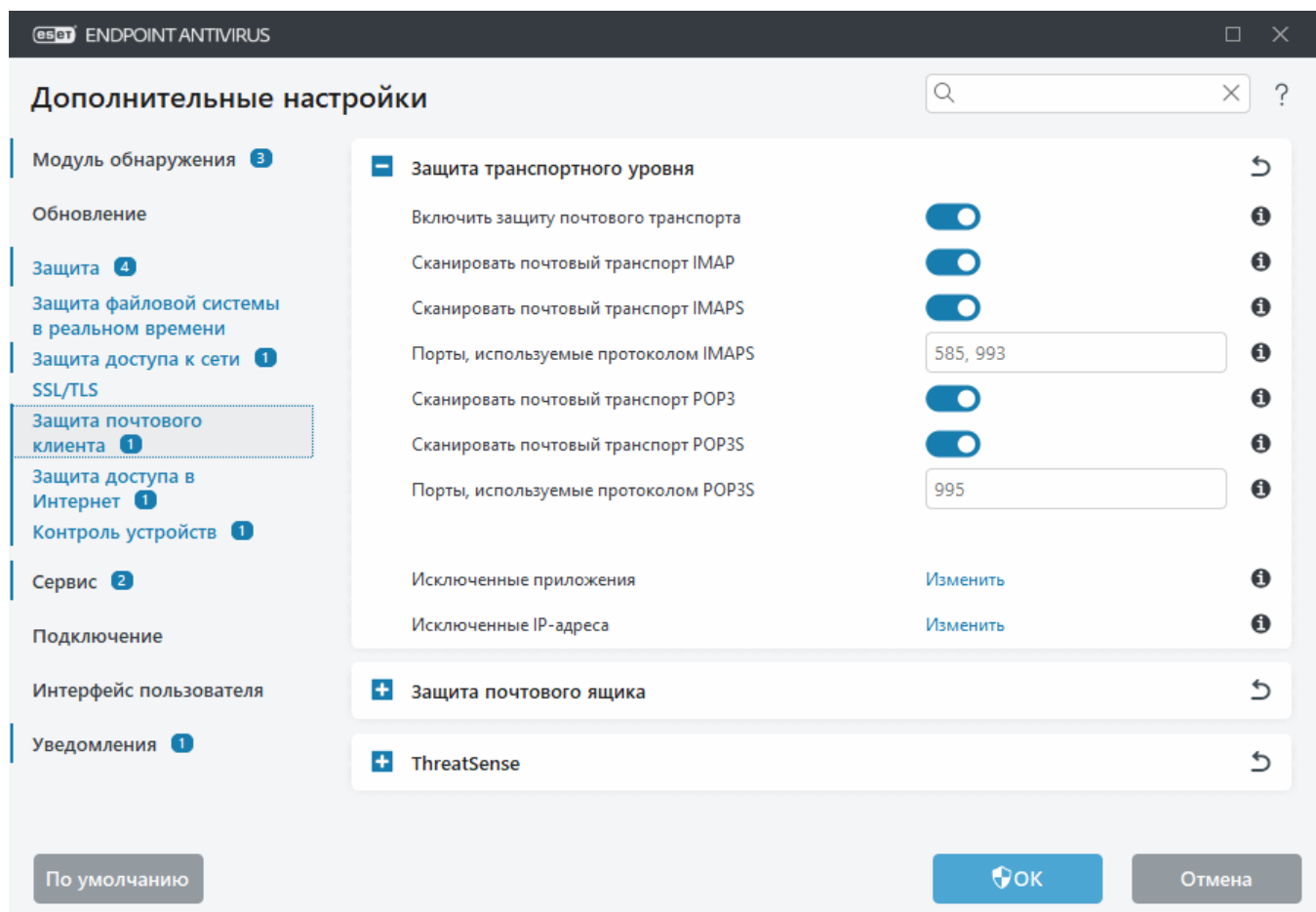
Вы можете выбрать, какие протоколы почтового транспорта будут сканироваться, щелкнув переключатель рядом со следующими опциями (по умолчанию включено сканирование всех протоколов):

- **Сканировать почтовый транспорт IMAP**
- **Сканировать почтовый транспорт IMAPS**
- **Сканировать почтовый транспорт POP3**
- **Сканировать почтовый транспорт POP3S**

По умолчанию ESET Endpoint Antivirus сканирует обмен данными по протоколам IMAPS и POP3S на стандартных портах. Чтобы добавить пользовательские порты для протоколов IMAPS и POP3S, добавьте их в текстовое поле рядом с элементом **Порты, используемые протоколом IMAPS** или **Порты, используемые протоколом POP3S**. Номера портов следует разделять запятой.

[Исключенные приложения:](#) позволяет исключить определенные приложения из сканирования функцией защиты почтового транспорта. Это полезно, когда защита доступа в Интернет вызывает проблемы совместимости.

[Исключенные IP-адреса:](#) позволяет исключить определенные удаленные адреса из сканирования функцией защиты почтового транспорта. Это полезно, когда защита доступа в Интернет вызывает проблемы совместимости.



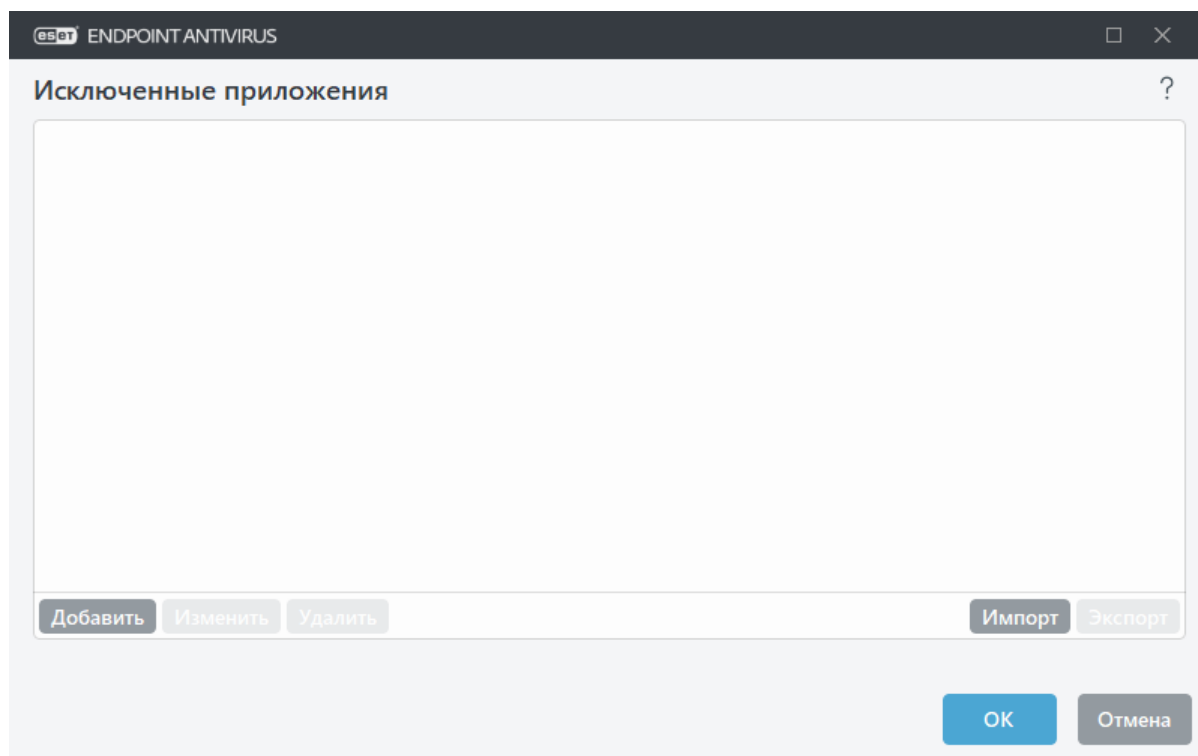
## Исключенные приложения

Чтобы исключить сканирование обмена данными для определенных приложений, добавьте их в список. Соединения выделенных приложений по протоколам HTTP(S)/POP3(S)/IMAP(S) не будут проверяться на наличие угроз. Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Запуск приложений и служб будет доступен здесь автоматически, когда вы щелкните элемент **Добавить**. Щелкните ... и перейдите к приложению, чтобы добавить исключение вручную.

**Изменить:** изменение выбранных в списке записей.

**Удалить:** удаление выбранных записей из списка.



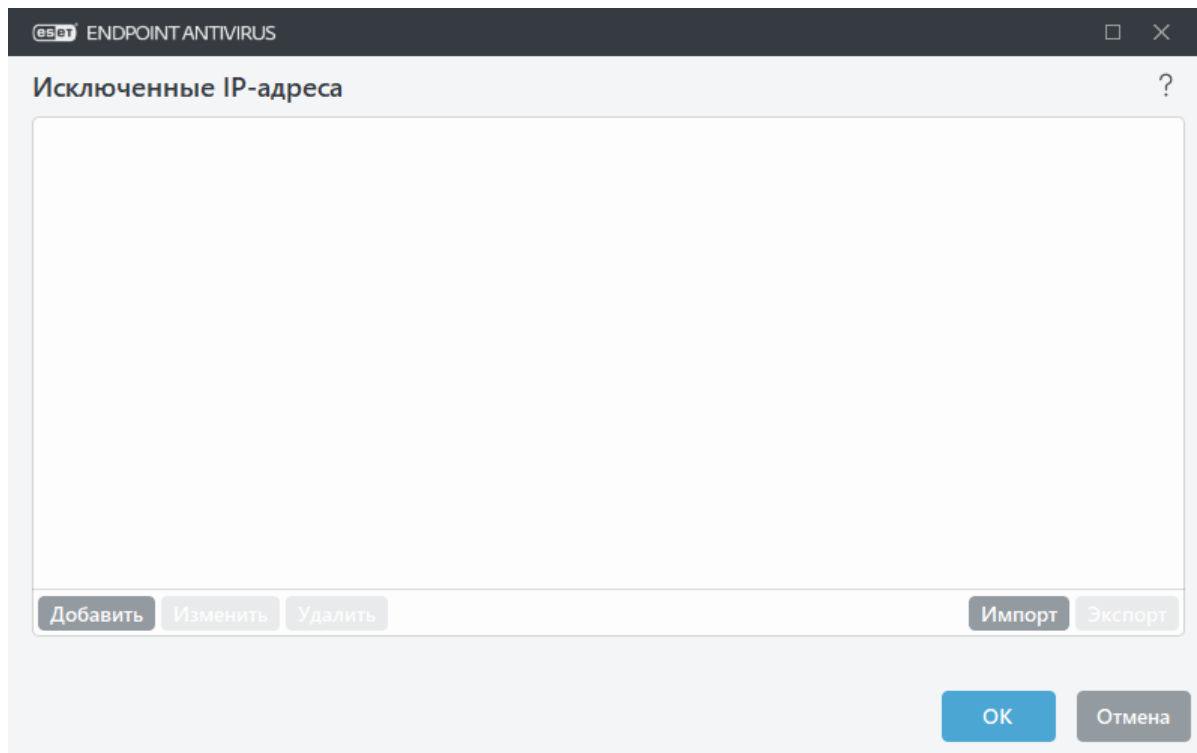
## Исключенные IP-адреса

Записи в списке будут исключены из сканирования. Соединения по протоколам HTTP(S)/POP3(S)/IMAP(S), 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.



### Примеры IP-адресов

Добавить адрес IPv4:

**Один адрес:** добавляет IP-адрес отдельного компьютера (например, *192.168.0.10*).

**Диапазон адресов:** введите начальный и конечный IP-адреса, чтобы задать диапазон IP-адресов нескольких компьютеров (например, *192.168.0.1–192.168.0.99*).

✓ **Подсеть:** подсеть (группа компьютеров), заданная IP-адресом и маской. Например, *255.255.255.0* — это маска сети для подсети *192.168.1.0*. Чтобы исключить всю подсеть, введите *192.168.1.0/24*.

Добавить адрес IPv6:

**Один адрес:** добавляет IP-адрес отдельного компьютера (например, *2001:718:1c01:16:214:22ff:fec9:ca5*).

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

## Защита почтового ящика

Интеграция ESET Endpoint Antivirus с почтовым клиентом увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты.

Чтобы настроить защиту почтового ящика, откройте раздел [Расширенные параметры](#) >

**Защита > Защита почтового клиента > Защита почтового ящика.**

**Включить защиту электронной почты с помощью подключаемых модулей клиента:**

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

Выберите письма для сканирования:

- Полученные сообщения
- Отправленные сообщения
- Прочитанные сообщения

- **Измененное сообщение электронной почты**

**i** 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 [Защита почтового транспорта](#) (IMAP/IMAPS и POP3/POP3S).

**Интеграции:** позволяет интегрировать защиту почтового ящика в почтовый клиент. Дополнительные сведения см. в разделе [Интеграции](#).

**Реагирование:** позволяет настроить обработку спам-сообщений. Дополнительные сведения см. в разделе [Реагирование](#).

## Интеграции

Интеграция ESET Endpoint Antivirus с почтовым клиентом увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если ваш почтовый клиент поддерживается, в ESET Endpoint Antivirus можно включить интеграцию. При этом панель инструментов ESET Endpoint Antivirus вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты. Чтобы изменить настройки интеграции, откройте раздел [Расширенные параметры](#) > **Защита** > **Защита почтового клиента** > **Защита почтового ящика** > **Интеграция**.

**Интеграция с Microsoft Outlook:** В настоящее время единственным поддерживаемым почтовым клиентом является [Microsoft Outlook](#). Защита электронной почты работает как плагин. 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 версий Microsoft Outlook см. в этой [статье базы знаний ESET](#).

**Расширенная обработка почтового клиента:** обработка дополнительных [событий Outlook Messaging API \(MAPI\)](#) — «Объект изменен» (fnevObjectModified) и «Объект создан» (fnevObjectCreated). Если при работе с почтовым клиентом наблюдается снижение быстродействия системы, отключите этот параметр.

## Панель инструментов Microsoft Outlook

Защита Microsoft Outlook работает в виде плагина. После установки ESET Endpoint Antivirus эта панель инструментов, содержащая опции защиты от вирусов, добавляется в Microsoft Outlook:

**ESET Endpoint Antivirus:** дважды щелкните значок, чтобы открыть главное окно ESET Endpoint Antivirus.

**Повторное сканирование сообщения:** позволяет запустить проверку электронной почты вручную. Можно указать сообщения, которые будут проверяться, и активировать повторное сканирование полученных сообщений. Дополнительные сведения см. в разделе [Защита почтового ящика](#).

**Настройки модуля сканирования:** отображаются опции для настройки [защиты почтового ящика](#).

# 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 Antivirus, 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.

## Реагирование

На основании результатов сканирования сообщений решение ESET Endpoint Antivirus может перемещать просканированные сообщения или добавлять пользовательский текст в тему. Эти параметры можно настроить в разделе [Расширенные параметры](#) > **Защита** > **Защита почтового клиента** > **Защита почтового ящика** > **Реагирование**.

Если есть сообщение, содержащее обнаружение, по умолчанию ESET Endpoint Antivirus пытается очистить сообщение. Если сообщение не может быть очищено, можно выбрать вариант для параметра **Предпринимаемое действие, если очистка невозможна**:

- **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.

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 следующие варианты:

- **Никогда:** уведомления не добавляются.
- **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 полученных и прочитанных сообщений электронной почты/Изменять тему отправленных сообщений электронной почты:** включите эту опцию, чтобы добавлять в сообщения пользовательский текст, указанный ниже.

**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.

## ThreatSense

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

Для модуля ThreatSense можно настроить несколько параметров сканирования:

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

Чтобы открыть окно параметров, щелкните **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 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.** 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 следующие 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 Antivirus при очистке объектов.

## Исключения

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

## Другое

При настройке 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 оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

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

## Ограничения

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

## Параметры объектов

**Максимальный размер объекта:** определяет максимальный размер объектов, подлежащих сканированию. Данный модуль защиты от вирусов будет сканировать только объекты меньше указанного размера. Этот параметр рекомендуется менять только опытным пользователям, у

которых есть веские основания для исключения из сканирования больших объектов. Значение по умолчанию: Не ограничено.

**Максимальная продолжительность сканирования объекта (с):** определяет максимальное значение времени для сканирования файлов в объекте-контейнере (например, в архиве RAR/ZIP или в электронном письме 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-контейнере. Если речь идет об архиве с большими файлами, сканирование будет прекращено не раньше, чем произойдет извлечение файла из архива (например, когда пользователь задал значение в 3 секунды, но извлечение файла занимает 5 секунд). По истечении этого времени остальные файлы в архиве сканироваться не будут. Чтобы ограничить время сканирования, в том числе для архивов большого 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. Максимальное значение — 3 ГБ.

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

## Защита доступа в Интернет

В разделе «Защита доступа в Интернет» можно настроить расширенные параметры модуля [Защита Интернета](#). В разделе [Расширенные параметры](#) > **Защита** > **Защита доступа в Интернет** > **Защита доступа в Интернет** доступны следующие параметры:

**Включить защиту доступа в Интернет:** когда этот параметр отключен, защита доступа в интернет и [защита от фишинга](#) не осуществляются.

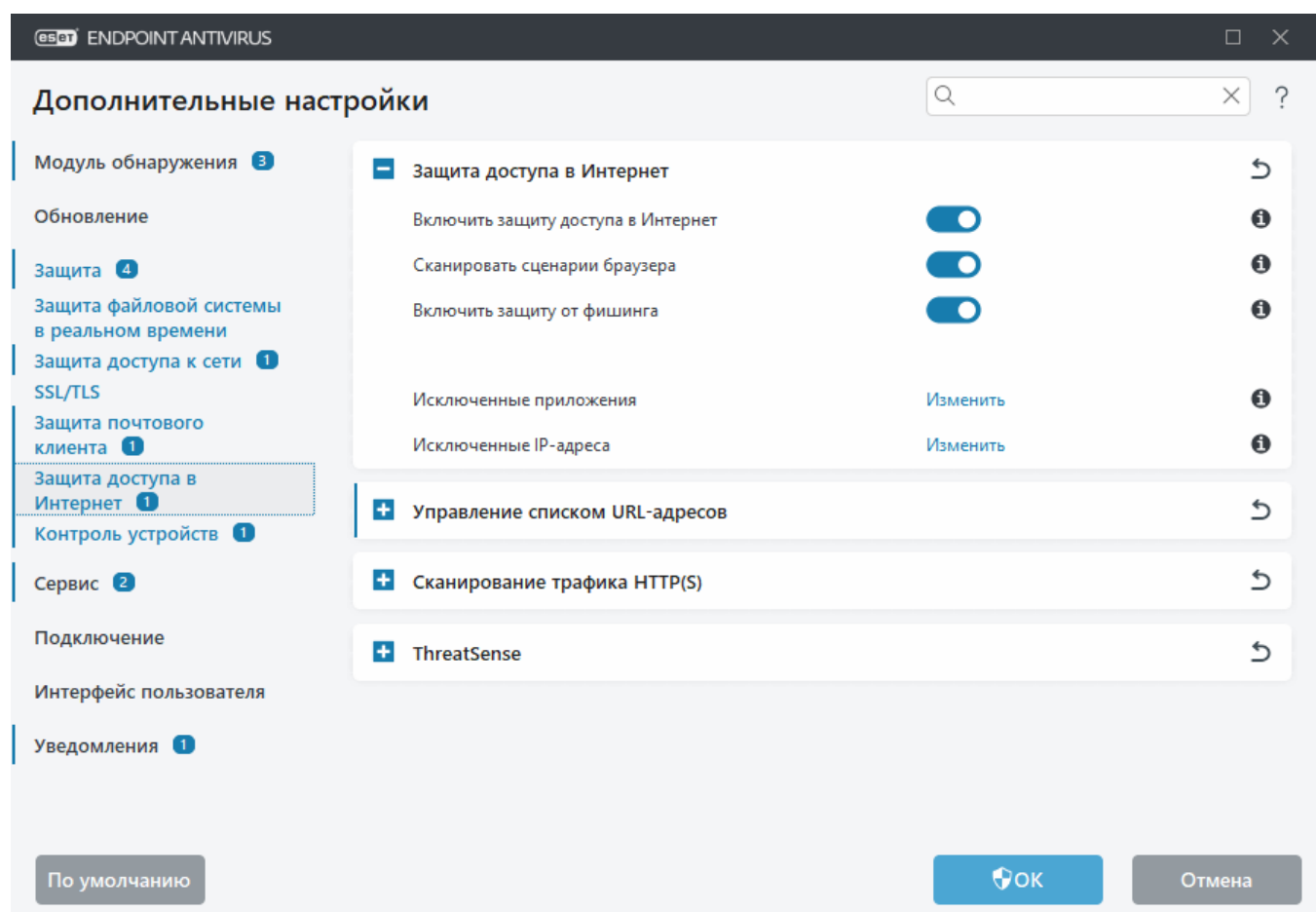
**i** Настоятельно рекомендуем оставить включенной защиту доступа в Интернет и не исключать никакие приложения или IP-адреса по умолчанию.

**Сканировать сценарии браузера:** если этот параметр включен, модуль обнаружения проверяет все программы JavaScript, выполняемые веб-браузерами.

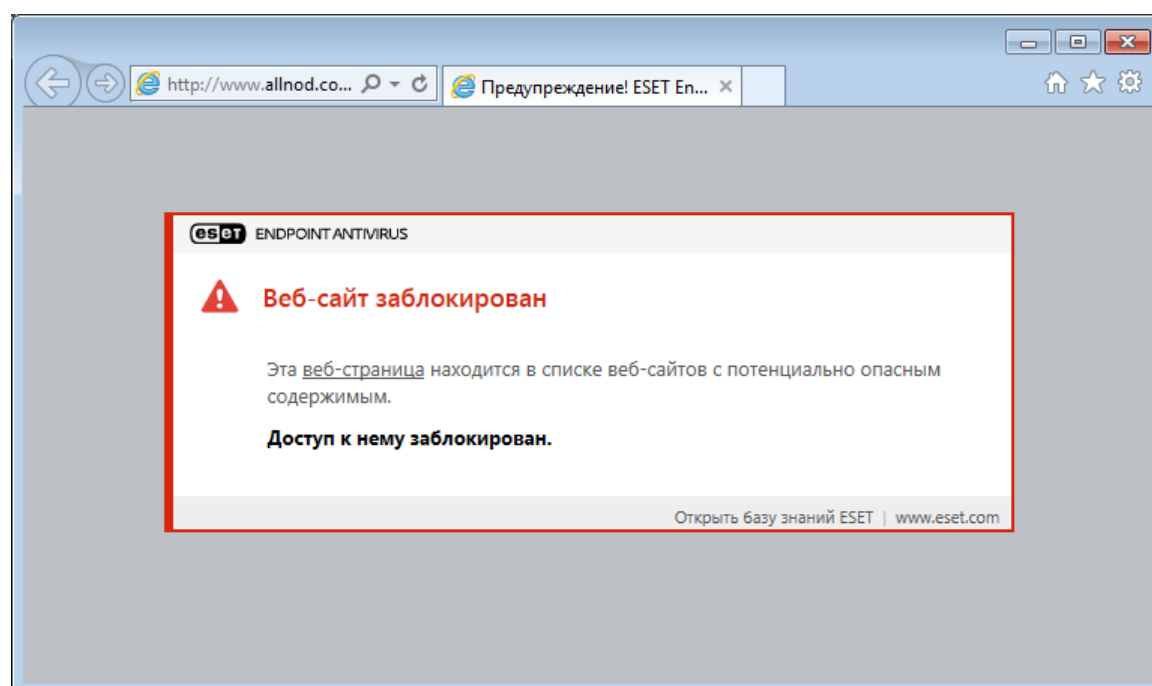
**Включить защиту от фишинга:** если этот параметр включен, фишинговые веб-страницы блокируются. Для получения дополнительных сведений см. раздел [Защита от фишинга](#).

[Исключенные приложения:](#) позволяет исключить определенные приложения из сканирования функцией защиты доступа в Интернет. Это полезно, когда защита доступа в Интернет вызывает проблемы совместимости.

Исключенные IP-адреса: позволяет исключить определенные удаленные адреса из сканирования функцией защиты доступа в Интернет. Это полезно, когда защита доступа в Интернет вызывает проблемы совместимости.



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 Antivirus](#)

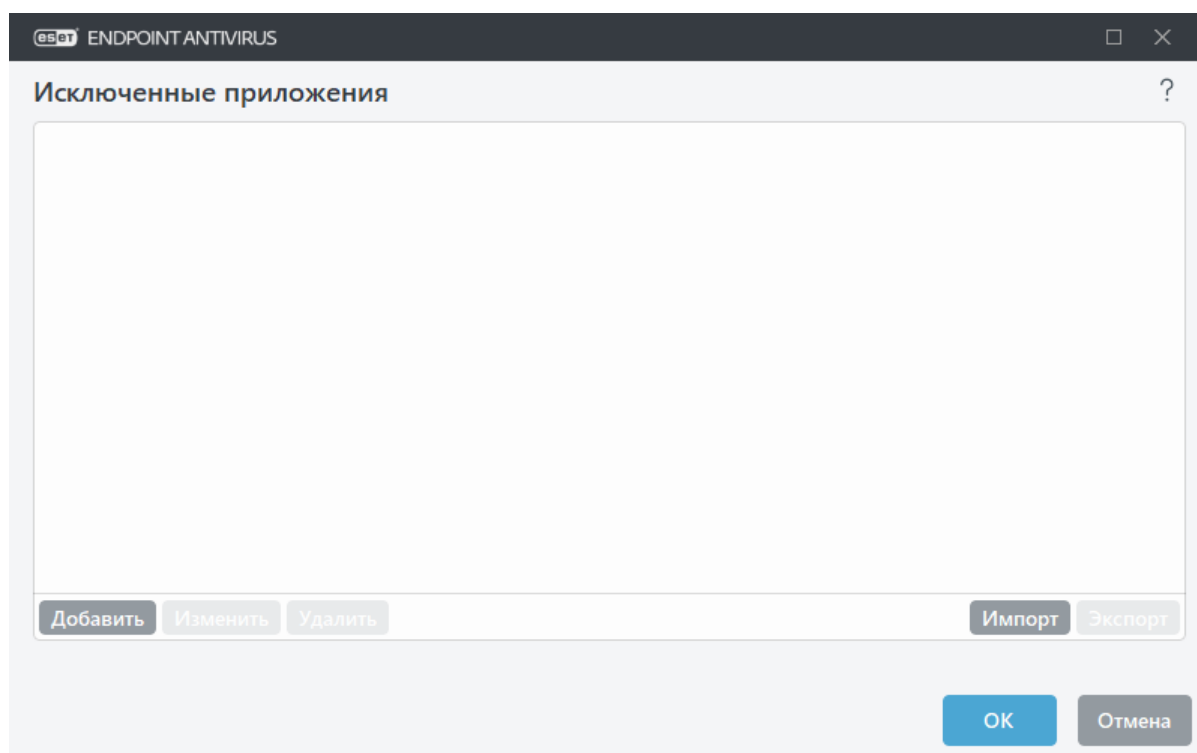
## Исключенные приложения

Чтобы исключить сканирование обмена данными для определенных приложений, добавьте их в список. Соединения выделенных приложений по протоколам HTTP(S)/POP3(S)/IMAP(S) не будут проверяться на наличие угроз. Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Запуск приложений и служб будет доступен здесь автоматически, когда вы щелкните элемент **Добавить**. Щелкните ... и перейдите к приложению, чтобы добавить исключение вручную.

**Изменить:** изменение выбранных в списке записей.

**Удалить:** удаление выбранных записей из списка.



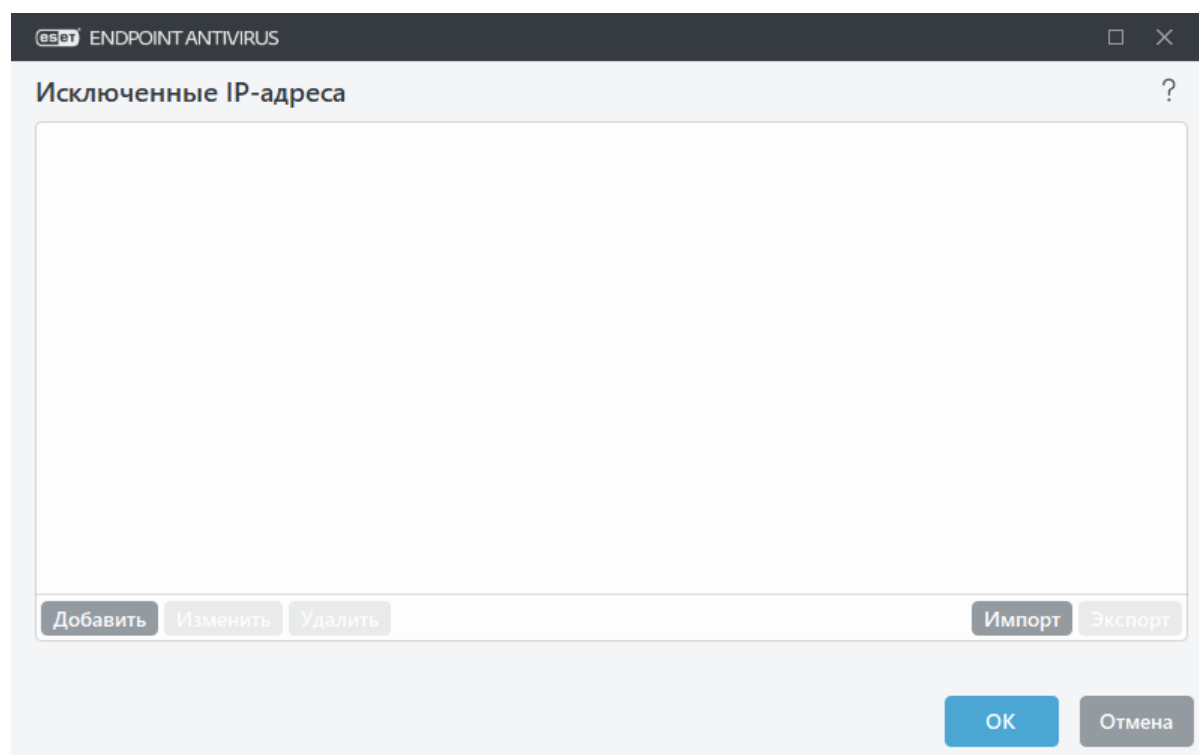
## Исключенные IP-адреса

Записи в списке будут исключены из сканирования. Соединения по протоколам HTTP(S)/POP3(S)/IMAP(S), 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.



### Примеры IP-адресов

Добавить адрес IPv4:

**Один адрес:** добавляет IP-адрес отдельного компьютера (например, *192.168.0.10*).

**Диапазон адресов:** введите начальный и конечный IP-адреса, чтобы задать диапазон IP-адресов нескольких компьютеров (например, *192.168.0.1–192.168.0.99*).

✓ **Подсеть:** подсеть (группа компьютеров), заданная IP-адресом и маской. Например, *255.255.255.0* — это маска сети для подсети *192.168.1.0*. Чтобы исключить всю подсеть, введите *192.168.1.0/24*.

Добавить адрес IPv6:

**Один адрес:** добавляет IP-адрес отдельного компьютера (например, *2001:718:1c01:16:214:22ff:fec9:ca5*).

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

## Управление списком URL-адресов

С помощью параметра **Управление списком URL-адресов** в разделе [Расширенные параметры](#) > **Защита** > **Защита доступа в Интернет** можно указать адреса HTTP, которые следует блокировать, разрешить или исключить из сканирования содержимого.

Протоколы [SSL/TLS](#) должны быть включены, если нужно фильтровать адреса HTTPS в дополнение к HTTP. В противном случае в список будут добавлены только посещенные вами домены HTTPS-сайтов, а не полный URL-адрес.

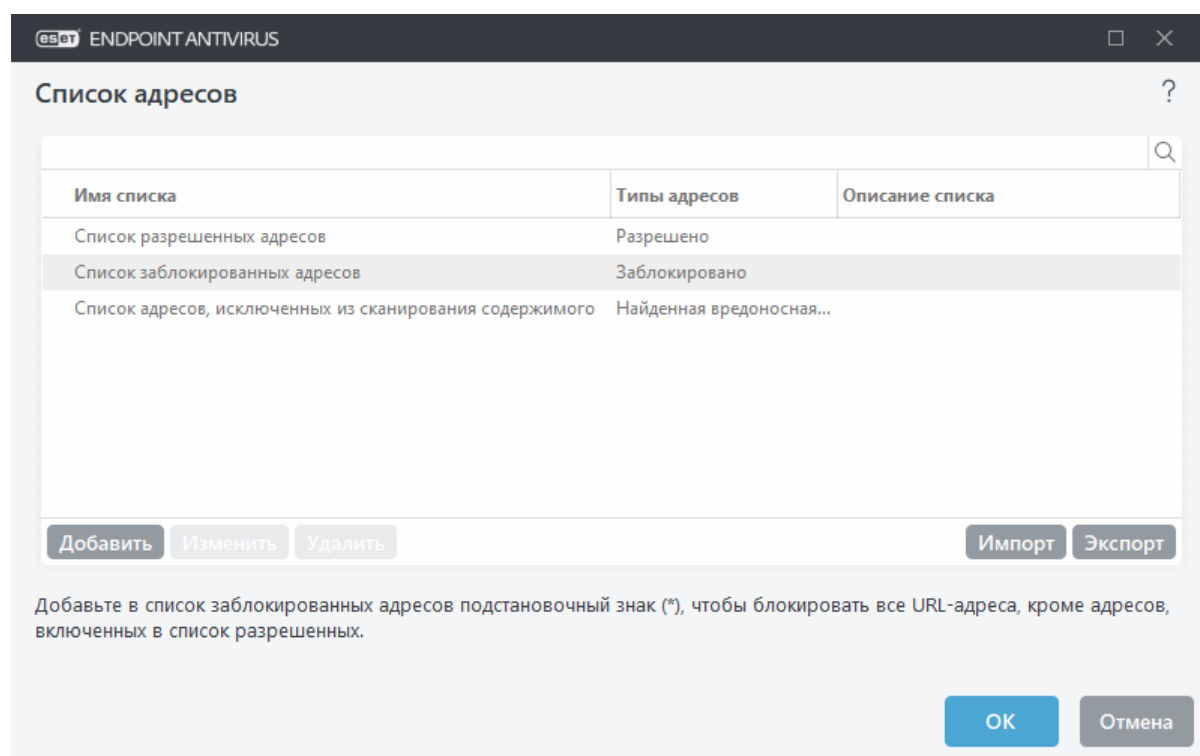
Посещение веб-сайтов, добавленных в **список заблокированных адресов** невозможно, кроме случаев, когда их адреса также добавлены в **список разрешенных адресов**. Веб-сайты из **списка адресов, для которых отключено сканирование содержимого**, загружаются без проверки на вредоносный код.

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. Будьте внимательны при указании адресов, исключенных из проверки, поскольку этот список должен включать в себя 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**.

### Адреса, которым доверяет ESET

**i** Если параметр **Не сканировать трафик с доменами, которым доверяет ESET** включен в разделе [SSL/TLS](#), на домены в белом списке, которым управляет ESET, не будет распространяться конфигурация управления списком URL-адресов.



## 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.

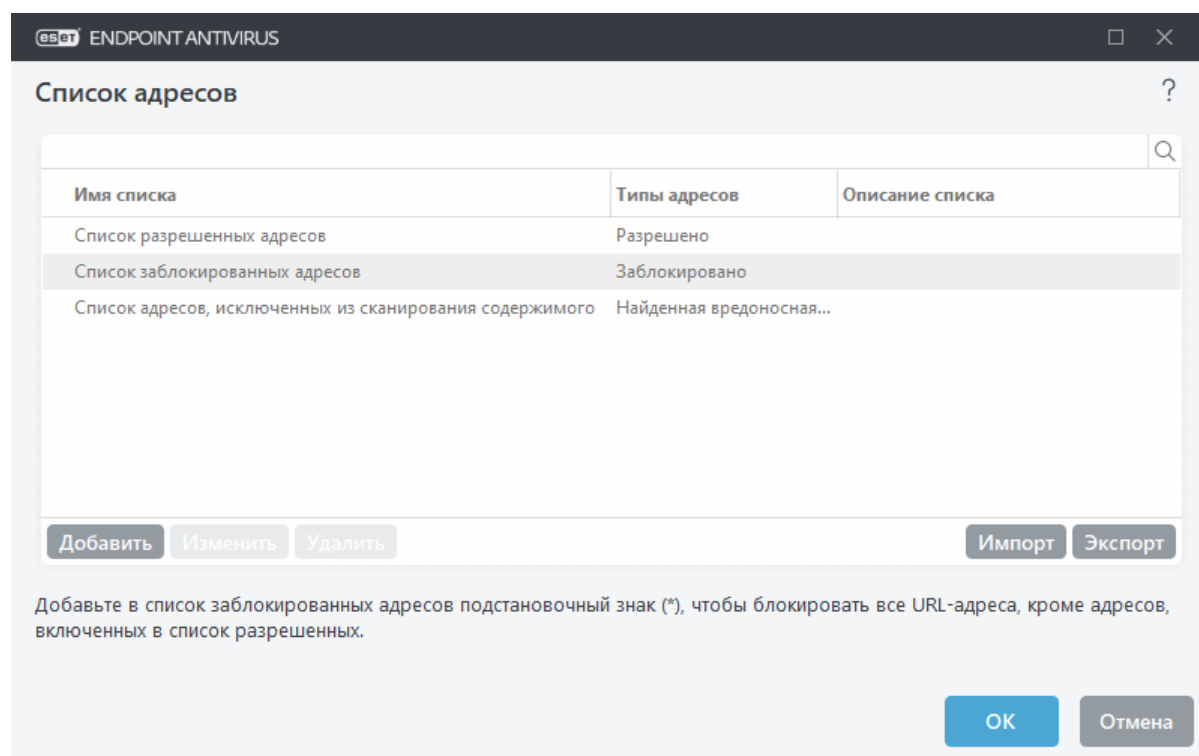
## Список адресов

В этом разделе можно указать списки HTTP(S)-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 Antivirus](#)

Дополнительные сведения см. в разделе [Управление URL-адресами](#).

# Создание списка адресов

В этом диалоговом окне можно настроить новый [список URL-адресов и масок](#), которые будут блокироваться, разрешаться или исключаться из проверки.

Можно конфигурировать следующие опции.

**Тип списка адресов.** Доступны три типа списков:

- **Найденная вредоносная программа пропущена.** Все добавленные в этот список адреса не будут проверяться на наличие вредоносного кода.
- **Заблокировано.** Доступ к адресам, указанным в этом списке, будет заблокирован.
- **Разрешено.** Доступ к адресам, указанным в этом списке, будет разрешен. Адреса в этом списке разрешены, даже если они включены в список заблокированных адресов.

**Имя списка:** здесь указывается имя списка. Это поле будет недоступно при редактировании одного из предварительно заданных списков.

**Описание списка:** здесь указывается краткое описание списка (необязательно). Этот параметр недоступен при редактировании одного из предварительно заданных списков.

Чтобы активировать его, рядом со списком щелкните элемент **Список активен**. Если необходимо получать уведомление, когда при доступе к веб-сайтам используется определенный список, выберите **Уведомлять о применении**. Например, вы получите уведомление, когда доступ к веб-сайту будет заблокирован или разрешен по причине присутствия его адреса в списке заблокированных или разрешенных адресов. На рабочем столе отобразится соответствующее уведомление.

**Серьезность регистрируемых событий.** Выберите уровень серьезности в раскрывающемся меню. Записи с уровнем детализации «Предупреждение» могут собираться средством ESET PROTECT.

Уровни детализации журнала «Информация» и «Предупреждение» доступны только для правил, которые содержат как минимум два компонента без подстановочных знаков в домене. Например:

- \*.domain.com/\*
- \*www.domain.com/\*

## Элементы управления

**Добавить.** Добавление нового URL-адреса в список (несколько адресов следует указывать через запятую).

**Изменить.** Изменение существующего адреса в списке. Доступно только для адресов, созданных с помощью функции **Добавить**.

**Удалить:** удаление существующих адресов из списка. Доступно только для адресов, созданных с помощью функции **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 инструкциями в этом диалоговом окне.

ESET Endpoint Antivirus позволяет пользователям блокировать доступ к указанным веб-узлам и предотвращать отображение их содержимого в веб-браузере. Кроме того, можно 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 «с», заканчивается буквой «m» и содержит любой символ между ними (.com, .cam и т. д.).

Например, маска \*x? обозначает все адреса с предпоследним символом «х». Если необходимо полное соответствие домена, укажите его в формате \*.domain.com/\*. Указывать префикс протокола (http://, https://) в маске необязательно. Если его не указать, маска будет соответствовать любому протоколу. 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 в том, что «\*.» в этом особом случае также соответствует пустой строке. Это позволяет обозначить одной маской целый домен, включая возможные поддомены. Например, маска \*.domain.com также соответствует *http://domain.com*. Использовать маску \*domain.com было бы неверно, поскольку она также совпала бы с *http://anotherdomain.com*.

 Уровни детализации журнала «Информация» и «Предупреждение» доступны только для правил, которые содержат как минимум два компонента без подстановочных знаков в домене. Например:

- \*.domain.com/\*
- \*www.domain.com/\*

## Сканирование трафика HTTP(S)

По умолчанию ESET Endpoint Antivirus сканирует трафик HTTP и HTTPS, который используется интернет-браузерами и другими приложениями. Отключать сканирование трафика следует только в том случае, если у вас возникли проблемы со сторонним программным обеспечением и вам нужно знать, вызвана ли проблема решением ESET Endpoint Antivirus.

**Включить сканирование трафика HTTP** — HTTP-трафик отслеживается для всех портов и приложений.

**Включить сканирование трафика HTTPS** — для передачи трафика HTTPS между сервером и клиентом используется зашифрованный канал. ESET Endpoint Antivirus проверяет обмен данными с помощью протоколов SSL и TLS. Программа сканирует только те порты, которые указаны в параметре **Порты, используемые протоколом HTTPS**, вне зависимости от версии операционной системы (вы можете добавить порты к предварительно заданным 443 и 0-65535).

## ThreatSense

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

Для модуля ThreatSense можно настроить несколько параметров сканирования:

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

Чтобы открыть окно параметров, щелкните **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 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.** 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 следующие 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 Antivirus при очистке объектов.

## Исключения

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

## Другое

При настройке 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 оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

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

## Ограничения

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

## Параметры объектов

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

**Максимальная продолжительность сканирования объекта (с):** определяет максимальное значение времени для сканирования файлов в объекте-контейнере (например, в архиве RAR/ZIP или в электронном письме 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-контейнере. Если речь идет об архиве с большими файлами, сканирование будет прекращено не раньше, чем произойдет извлечение файла из архива (например, когда пользователь задал значение в 3 секунды, но извлечение

файла занимает 5 секунд). По истечении этого времени остальные файлы в архиве сканироваться не будут. Чтобы ограничить время сканирования, в том числе для архивов большого 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. Максимальное значение — 3 ГБ.

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

## Контроль устройств

ESET Endpoint Antivirus обеспечивает автоматический контроль устройств (компакт-дисков, DVD-дисков, USB и т. д.). Данный модуль позволяет блокировать или изменять расширенные фильтры и разрешения, а также указывать, может ли пользователь получать доступ к конкретному устройству и работать с ним. Это может быть удобно, если администратор компьютера хочет предотвратить использование устройств с нежелательным содержанием.

### Поддерживаемые внешние устройства:

- Дисковый накопитель (жесткий диск, съемный USB-диск)
- Компакт-/DVD-диск
- Принтер USB
- FireWire Хранилище
- Bluetooth Устройство
- Устройство чтения смарт-карт
- Устройство обработки изображений
- Модемы
- LPT/COM порт
- Портативное устройство (устройства от аккумулятора, такие как мультимедийный проигрыватель, смартфоны, самонастраивающиеся устройства и т. д.)
- Все типы устройств

Параметры контроля устройств можно изменить в разделе [Дополнительные настройки](#) > **Защиты > Контроль устройств**.

Щелкните переключатель **Включить контроль устройств**, чтобы включить функцию контроля устройств в ESET Endpoint Antivirus. Чтобы это изменение вступило в силу, необходимо перезапустить компьютер. После включения контроля устройств можно настроить **правила** в окне [Редактор правил](#).



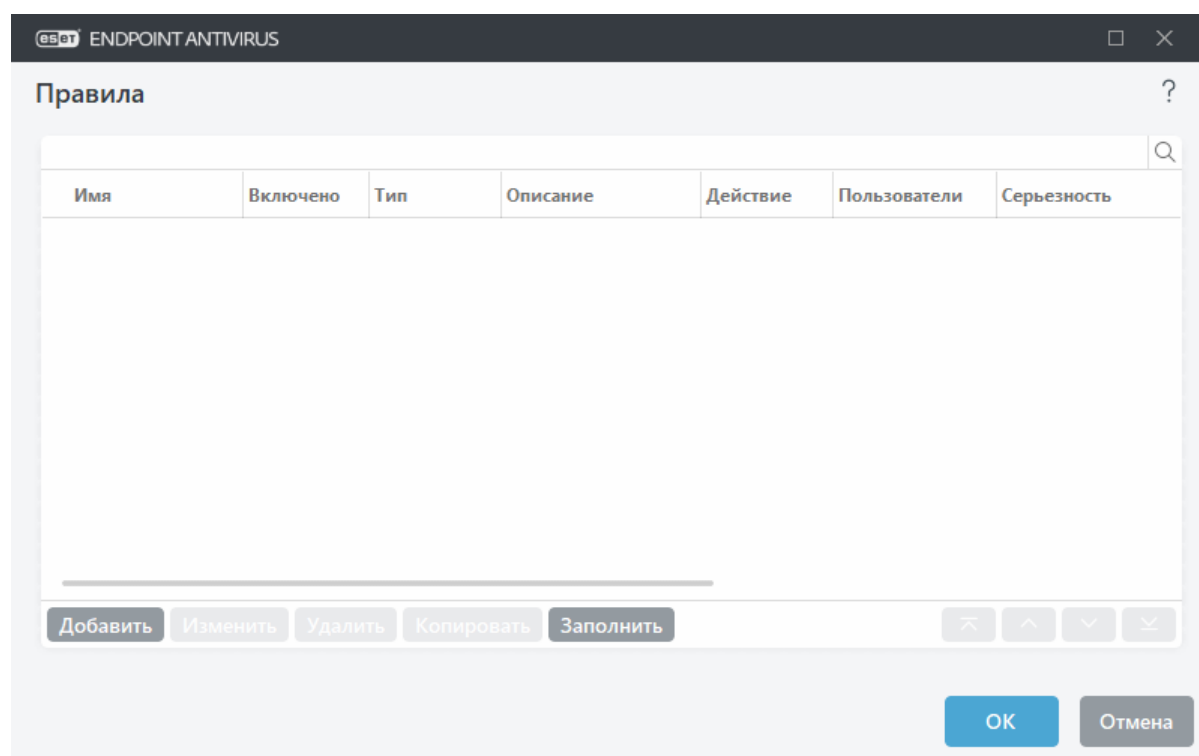
**i** Группу контроля устройств с правилами можно импортировать из XML-файла с помощью планировщика. Дополнительные сведения и пошаговое руководство можно найти в [статье базы знаний ESET](#).

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 статью [Добавление правил контроля устройств](#).

**i** 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 Antivirus 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).

Выберите устройство в списке обнаруженных устройств и нажмите кнопку **ОК**, чтобы [добавить правило контроля устройств](#) с предварительно заданной информацией (все параметры можно настраивать).

Устройства в режиме низкого энергопотребления (спящем режиме) отмечены значком предупреждения . Чтобы активировать кнопку **ОК** и добавить правило для этого устройства, сделайте следующее:

- Повторно подключите устройство.
- Используйте устройство (например, запустите приложение «Камера» в Windows, чтобы активировать веб-камеру).

## Добавление правил контроля устройств

Правилом контроля устройств определяется действие, выполняемое при подключении к компьютеру устройств, которые соответствуют заданным критериям.

**Добавить правило** ?

Имя: Без имени

Правило включено: ☒

Применять во время: Всегда

Тип устройства: Дисковый накопитель

Действие: Разрешить

Тип критериев: Устройство

Производитель:

Модель:

Серийный номер:

Серьезность регистрируемых событий: Всегда

Список пользователей: [Изменить](#)

Уведомить пользователя: ☒

OK

Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить это правило, щелкните ползунок 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 для 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.

- **Разрешить** — будет разрешен полный доступ к устройству.
- **Блокировать** — доступ к устройству будет заблокирован.
- **Блокировка записи** — 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 (разрешений) доступен не для всех типов устройств. Если устройство относится к типу хранилищ, будут доступны все четыре действия. Если устройство не предназначено для хранения данных, доступны будут только три действия. Например, право **Блокировка записи** 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 правила для разных устройств. Во всех параметрах учитывается регистр и поддерживаются подстановочные знаки (\*, ?):

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



Если для этих параметров не заданы значения, во время сопоставления правило игнорирует эти поля. Параметры фильтрации во всех текстовых полях учитывают регистр и поддерживают подстановочные знаки (вопросительный знак (?) обозначает один символ, а звездочка (\*) — строку длиной ноль символов и более).



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.

### Ограничения для списка пользователей

Список пользователей нельзя определить для правил с указанными [типами устройств](#):

- USB-принтер
- Устройство Bluetooth
- Устройство чтения смарт-карт
- Устройство обработки изображений
- Модемы
- LPT/COM-порты

**Уведомить пользователя** — при подключении устройства, заблокированного существующим правилом, отобразится окно оповещения.

## 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 для отображения устройств 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 **ОК**, чтобы добавить их в группу.

## Элементы управления

**Добавить.** Позволяет добавить группу, введя ее имя, или устройство в существующую группу (в зависимости от того, в какой части окна нажата кнопка).

**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).



Группу контроля устройств с правилами можно импортировать из XML-файла с помощью планировщика. Дополнительные сведения и пошаговое руководство можно найти в [статье базы знаний ESET](#).

## Добавить устройство

Щелкните Добавить в правом окне, чтобы добавить устройство в существующую группу. С помощью указанных ниже дополнительных параметров можно точно настраивать правила для разных устройств. Во всех параметрах учитывается регистр и поддерживаются подстановочные знаки (\*, ?):

- **Производитель:** фильтрация по имени или ID производителя.
- **Модель** — имя устройства.
- **Серийный номер** — у внешних устройств обычно есть серийные номера. Когда речь идет о CD- или DVD-диске, то это серийный номер конкретного носителя, а не дисковода CD-дисков.
- **Описание** — ваше описание устройства.



Если для этих параметров не заданы значения, во время сопоставления правило игнорирует эти поля. Параметры фильтрации во всех текстовых полях учитывают регистр и поддерживают подстановочные знаки (вопросительный знак (?) обозначает один символ, а звездочка (\*) — строку длиной ноль символов и более).

Для сохранения изменений щелкните **ОК**. Чтобы закрыть окно **Группы устройств** без сохранения изменений, нажмите кнопку **Отмена**.



После создания группы устройств необходимо для созданной группы устройств [добавить новое правило контроля устройств](#) и выбрать выполняемое действие.

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

# ThreatSense

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

Для модуля ThreatSense можно настроить несколько параметров сканирования:

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

Чтобы открыть окно параметров, щелкните **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 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.** 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 следующие 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 Antivirus при очистке объектов.

## Исключения

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

## Другое

При настройке 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 оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

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

## Ограничения

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

## Параметры объектов

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

**Максимальная продолжительность сканирования объекта (с):** определяет максимальное значение времени для сканирования файлов в объекте-контейнере (например, в архиве RAR/ZIP или в электронном письме 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-контейнере. Если речь идет об архиве с большими файлами, сканирование будет прекращено не раньше, чем произойдет извлечение файла из архива (например, когда пользователь задал значение в 3 секунды, но извлечение файла занимает 5 секунд). По истечении этого времени остальные файлы в архиве сканироваться не будут. Чтобы ограничить время сканирования, в том числе для архивов большого 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. Максимальное значение — 3 ГБ.

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

## Уровни очистки

Чтобы изменить настройки уровня очистки для нужного модуля защиты, разверните элемент **ThreatSense** (например, **Защита файловой системы в реальном времени**), а затем выберите в раскрывающемся меню пункт **Уровень очистки**.

ThreatSense имеет такие уровни исправления проблем (т. е. очистки):

### Исправление в ESET Endpoint Antivirus

| Уровень очистки   | Описание   |
|---|--|
| <b>Всегда исправлять обнаружения</b>  | Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, с системными файлами), если обнаружение не удастся исправить, обнаруженный объект оставляется в исходном расположении. Функция <b>Всегда исправлять обнаружения</b> является рекомендуемой настройкой по умолчанию в <a href="#">управляемой среде</a> . |
| <b>Исправлять обнаружения, если это безопасно, в другом случае оставить</b>   | Пытаться исправлять обнаружения при очистке <a href="#">объектов</a> без вмешательства конечного пользователя. В некоторых случаях (например, системные файлы или архивы, которые содержат и чистые, и зараженные файлы), если обнаружение не удастся исправить, обнаруженный объект остается в исходном расположении.   |
| <b>Исправлять обнаружения, если это безопасно, в другом случае спрашивать</b> | 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.   |
| <b>Всегда спрашивать у конечного пользователя</b>                             | 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

Исключенные расширения файлов относятся к [ThreatSense](#). Чтобы настроить исключенные расширения файлов, щелкните **ThreatSense** в окне [«Расширенные параметры»](#) для любого

[модуля, который использует технологию ThreatSense.](#)

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

**i** Не следует путать эту функцию с другими возможностями исключения — [Исключения для процессов](#), [Исключения системы HIPs](#) или [Исключения файлов/папок](#).

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 **ОК**. 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`).

**i** Чтобы увидеть расширение файла (при наличии расширения) в операционной системе Windows, необходимо установить флажок **Расширения имен файлов** в проводнике Windows на вкладке **Вид**.

## Дополнительные параметры ThreatSense

Чтобы изменить эти настройки, откройте раздел [Расширенные параметры](#) > **Защита** > **Защита файловой системы в реальном времени** > **Дополнительные параметры ThreatSense**.

### Дополнительные параметры ThreatSense для только что созданных и измененных файлов

Вероятность заражения только что созданных или измененных файлов выше по сравнению с аналогичным показателем для существующих файлов. Именно поэтому программа проверяет эти файлы с использованием дополнительных параметров сканирования. ESET Endpoint Antivirus вместе с обычными методами сканирования, основанными на сигнатурах, применяет расширенный эвристический анализ, что делает возможным обнаружение новых угроз еще до выпуска обновлений модуля обнаружения.

В дополнение к только что созданным файлам выполняется также сканирование **самораспаковывающихся архивов** (`.sfx`) и **программ-упаковщиков среды выполнения** (исполняемых файлов с внутренним сжатием). По умолчанию архивы сканируются до 10-го уровня вложенности независимо от их фактического размера. Для изменения параметров проверки архивов снимите флажок **Параметры сканирования архивов по умолчанию**.

## Дополнительные параметры ThreatSense для исполняемых файлов

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

**Расширенный эвристический анализ при запуске файлов со съемных носителей:** прежде чем разрешить запуск кода со съемного носителя, система расширенного эвристического анализа эмулирует код в виртуальной среде и оценивает его поведение.

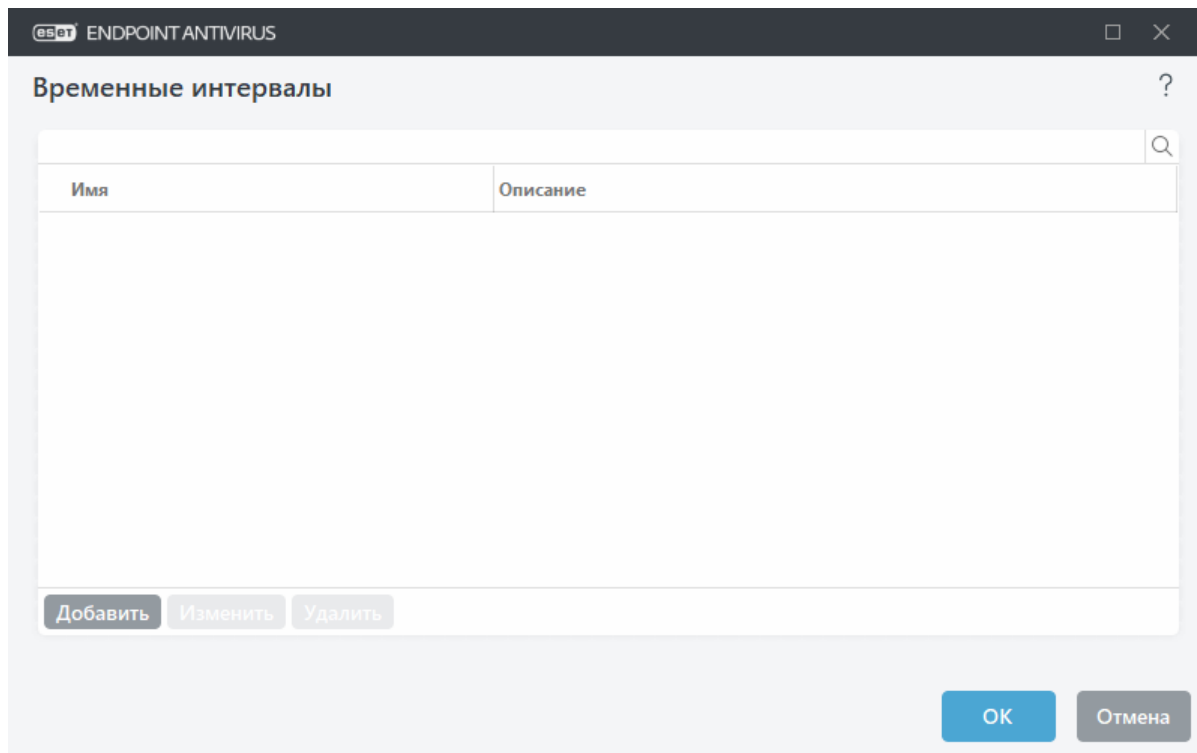
## Служебные программы

Вы можете настроить дополнительные параметры для функций, которые обеспечивают дополнительную безопасность и упрощают администрирование ESET Endpoint Antivirus, в разделе [Расширенные параметры](#) > **Инструменты**.

- [Временные интервалы](#)
- [Центр обновления Microsoft Windows®](#)
- [ESET CMD](#)
- [Удаленный мониторинг и управление](#)
- [Проверка лицензии с интервалом](#)
- [Файлы журнала](#)
- [Режим презентации](#)
- [Диагностика](#)

## Временные интервалы

Можно создавать временные интервалы, а затем назначать их правилам для **контроля устройств**. 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 временный 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. Щелкните **ОК**, чтобы подтвердить.

Один временный 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](#).

## 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 Antivirus уведомляет пользователя об отсутствующих обновлениях в соответствии с выбранным уровнем. Доступны следующие уровни:

- **Без обновлений:** запросы на загрузку обновлений системы не отображаются.
- **Необязательные обновления:** отображаются запросы на загрузку обновлений с низким и более высоким уровнем приоритета.
- **Рекомендуемые обновления:** отображаются запросы на загрузку обновлений с обычным и более высоким уровнем приоритета.
- **Важные обновления:** отображаются запросы на загрузку обновлений, помеченных как важные и с более высоким уровнем приоритета.
- **Критические обновления:** пользователю предлагается загрузить только критические обновления.

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

## Диалоговое окно — обновление операционной системы

Если для вашей операционной системы доступны какие-либо обновления, на домашней странице ESET Endpoint Antivirus отобразится уведомление. Щелкните **Дополнительные сведения**, чтобы открыть окно обновлений системы.

В окне «Обновления системы» представлен список доступных обновлений, готовых для загрузки и установки. Тип обновления отображается рядом с его названием.

Дважды щелкните любую строку обновления, чтобы отобразить окно [Информация об обновлениях](#), содержащее дополнительную информацию.

Щелкните **Запустить обновление системы**, чтобы загрузить и установить все перечисленные обновления операционной системы.

## Информация об обновлениях

В окне «Обновления системы» представлен список доступных обновлений, готовых для загрузки и установки. Уровень приоритета обновления отображается справа от его названия.

Нажмите **Запустить обновление системы**, чтобы начать загрузку и установку обновлений операционной системы.

Щелкните правой кнопкой мыши любую строку обновления и нажмите **Показать информацию**, чтобы вывести на экран новое окно с дополнительными сведениями.

## ESET CMD


Эта функция включает расширенные команды escmd. С помощью командной строки можно экспортировать и импортировать настройки (escmd.exe). До недавнего времени экспортировать параметры можно было только через [графический интерфейс пользователя](#). Конфигурацию ESET Endpoint Antivirus 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, конфигурация не будет импортирована.

После включения ESET CMD можно использовать командную строку для импорта и экспорта конфигураций программы ESET Endpoint Antivirus. Это можно сделать вручную или создать сценарий с целью автоматизации.


 Для использования расширенных команд `escmd` необходимо выполнять их с правами администратора или же открыть командную строку Windows (`cmd`) в режиме **Запуск от имени администратора**. В противном случае появится сообщение **Error executing command**. Кроме того, во время экспорта конфигурации должна существовать папка назначения. Команда экспорта работает даже при отключенном параметре ESET CMD.

 Расширенные команды `escmd` можно выполнять только локально. Приостановку команд `escmd` можно выполнить только с помощью клиентской задачи **Выполнение команды** с использованием ESET PROTECT.

 Команда экспорта параметров:  
`escmd /getcfg c:\config\settings.xml`  
Команда импорта параметров:  
`escmd /setcfg c:\config\settings.xml`

Для подписания файла конфигурации в формате XML (*.xml*) выполните следующие действия.

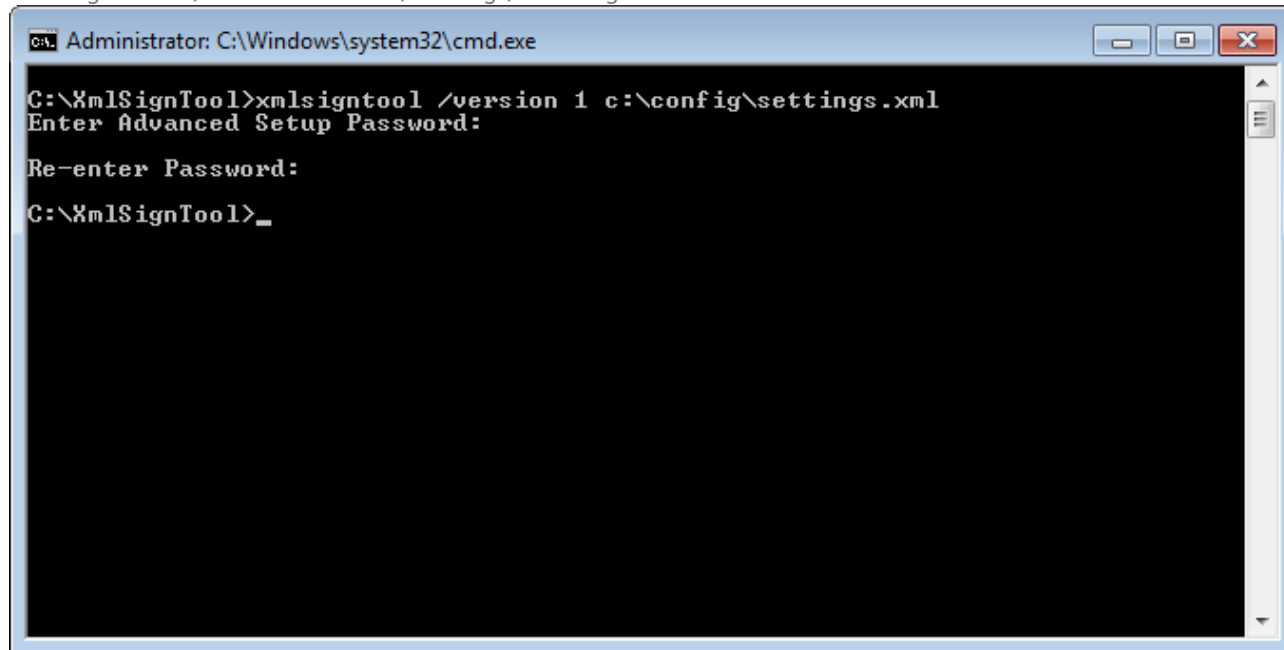
1. Загрузите исполняемый файл [XmlSignTool](#).
2. Откройте командную строку Windows (`cmd`) с помощью команды **Запуск от имени администратора**.
3. Перейдите в расположение файла `xmlsigntool.exe`.
4. Выполните команду для подписания файла конфигурации в формате XML (*.xml*).  
Использование: `xmlsigntool /version 1|2 <xml_file_path>`

 Значение параметра `/version` зависит от версии ESET Endpoint Antivirus. 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 Antivirus 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 Antivirus 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 escmd

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 | escmd /setfeature onaccess pause     | escmd /setfeature onaccess enable     |
| Защита документов                                  | escmd /setfeature document pause     | escmd /setfeature document enable     |
| Контроль устройств                                 | escmd /setfeature devcontrol pause   | escmd /setfeature devcontrol enable   |
| Режим презентации                                  | escmd /setfeature presentation pause | escmd /setfeature presentation enable |

| Функция системы безопасности      | Команда временной приостановки      | Команда включения                    |
|-----------------------------------|-------------------------------------|--------------------------------------|
| Персональный фаервол              | 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 почтового клиента от спама | ecmd /setfeature antispam pause     | ecmd /setfeature antispam enable     |
| Защита от фишинга                 | ecmd /setfeature antiphishing pause | ecmd /setfeature antiphishing enable |

## 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 Antivirus, используемая по умолчанию, содержит файл `ermmm.exe` в каталоге приложения Endpoint:  
`C:\Program Files\ESET\ESET Security\ermmm.exe`
- `ermmm.exe` — это программа командной строки, которая позволяет управлять продуктами для конечных точек и обмениваться данными с любым плагином RMM.
- `ermmm.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 управления ESET Endpoint Antivirus](#)

## 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](#)

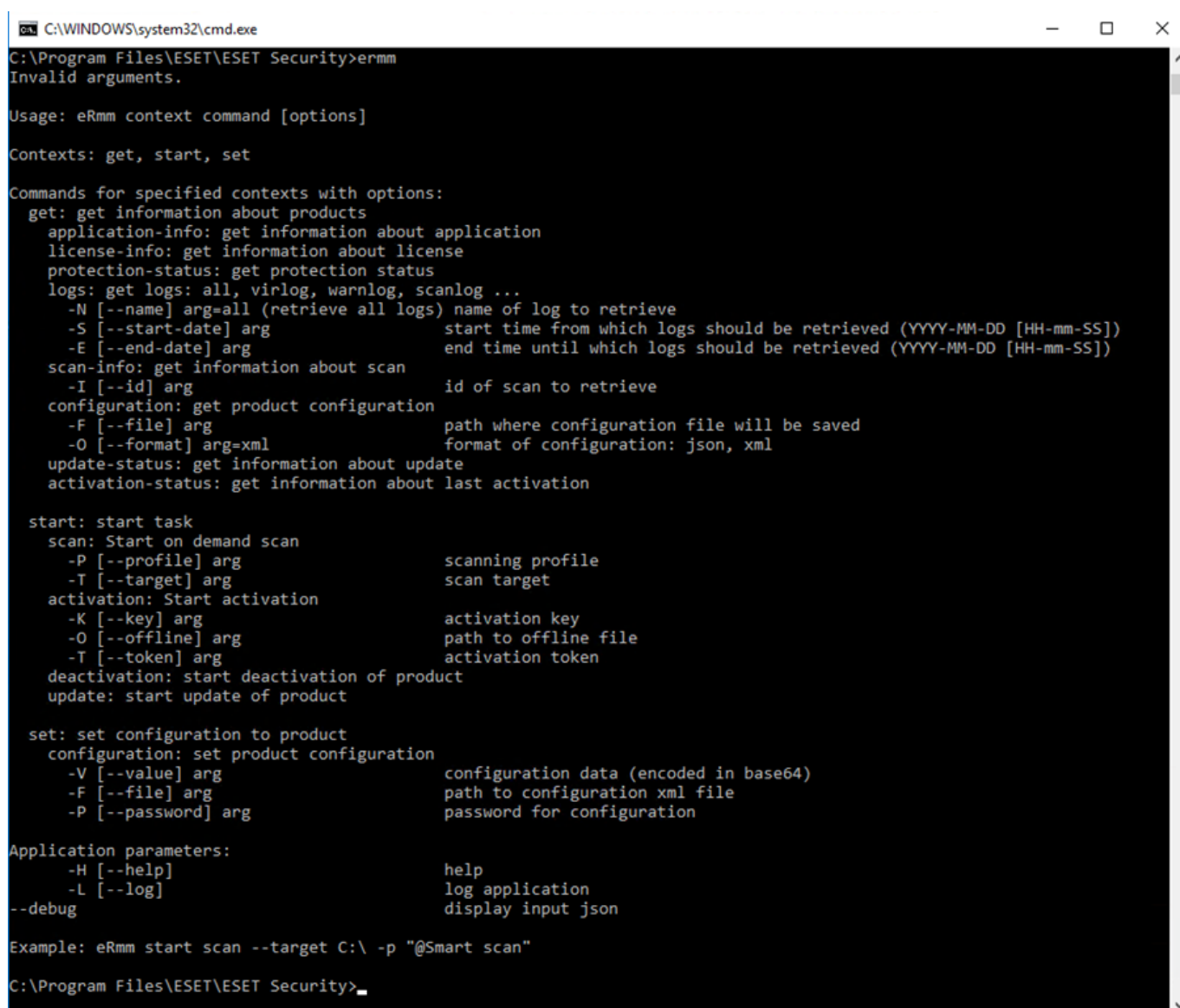
## Командная строка ERMM

Управление удаленным мониторингом выполняется с помощью интерфейса командной строки. Установка ESET Endpoint Antivirus, используемая по умолчанию, содержит файл ermm.exe в каталоге приложения Endpoint: *c:\Program Files\ESET\ESET Security*.

Запустите командную строку (cmd.exe) от имени администратора и перейдите к упомянутому пути (чтобы открыть командную строку, нажмите клавиши Windows + R на клавиатуре, введите cmd в окне «Выполнить» и нажмите клавишу ВВОД).

Синтаксис команды: `ermm context command [options]`

В параметрах журнала учитывается регистр.



```

C:\WINDOWS\system32\cmd.exe
C:\Program Files\ESET\ESET Security>ermm
Invalid arguments.

Usage: eRmm context command [options]

Contexts: get, start, set

Commands for specified contexts with options:
get: get information about products
  application-info: get information about application
  license-info: get information about license
  protection-status: get protection status
  logs: get logs: all, virlog, warnlog, scanlog ...
    -N [--name] arg=all (retrieve all logs) name of log to retrieve
    -S [--start-date] arg start time from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
    -E [--end-date] arg end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
scan-info: get information about scan
  -I [--id] arg id of scan to retrieve
configuration: get product configuration
  -F [--file] arg path where configuration file will be saved
  -O [--format] arg=json 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>_
  
```

В ermm.exe используются три основных контекста: получение, запуск и настройка. В таблице ниже приведены примеры синтаксиса команд. Щелкните ссылку в столбце «Команда» для просмотра дополнительных опций, параметров и примеров использования. После успешного выполнения команды на экране появятся выводимые данные (результат). Для просмотра

введенных данных добавьте параметр - `-debug` в конце команды.

| Контекст     | Команда                           | Описание                                      |
|--------------|-----------------------------------|---|
| <b>get</b>   |                                   | <b>Получить информацию о продуктах</b>        |
|              | <a href="#">application-info</a>  | Получить информацию о продукте                |
|              | <a href="#">license-info</a>      | Получить информацию о лицензии                |
|              | <a href="#">protection-status</a> | Получить данные о состоянии защиты            |
|              | <a href="#">logs</a>              | Получить журналы                              |
|              | <a href="#">scan-info</a>         | Получить информацию о запущенном сканировании |
|              | <a href="#">configuration</a>     | Получить конфигурацию продукта                |
|              | <a href="#">update-status</a>     | Получить информацию об обновлении             |
|              | <a href="#">activation-status</a> | Получить информацию о последней активации     |
| <b>start</b> |                                   | <b>Запустить задачу</b>                       |
|              | <a href="#">scan</a>              | Запустить сканирование по требованию          |
|              | <a href="#">activation</a>        | Запустить активацию продукта                  |
|              | <a href="#">deactivation</a>      | Запустить деактивацию продукта                |
|              | <a href="#">update</a>            | Запустить обновление продукта                 |
| <b>set</b>   |                                   | <b>Настроить параметры для продукта</b>       |
|              | <a href="#">configuration</a>     | Настроить конфигурацию для продукта           |

В выводимом результате каждой команды первая отображаемая информация — это идентификатор результата. Чтобы лучше понять информацию результата, ознакомьтесь с таблицей идентификаторов ниже.

| Идентификатор ошибки | Ошибка                                     | Описание   |
|----------------------|--|--|
| <b>0</b>             | Success                                    |  |
| <b>1</b>             | Command node not present                   | Узел «Команда» отсутствует в введенных данных json   |
| <b>2</b>             | Command not supported                      | Команда не поддерживается  |
| <b>3</b>             | General error executing the command        | Ошибка при выполнении команды  |
| <b>4</b>             | Task already running                       | Запрашиваемая задача уже выполняется и не была запущена  |
| <b>5</b>             | Invalid parameter for command              | Пользователь ввел неверные данные  |
| <b>6</b>             | Command not executed because it's disabled | Управление удаленным мониторингом не включено в расширенных настройках или не запущено от имени администратора |

## Список команд ERM JSON

- [get protection-status](#)
- [get application-info](#)

- [get license-info](#)
- [get logs](#)
- [get activation-status](#)
- [get scan-info](#)
- [get configuration](#)
- [get update-status](#)
- [start scan](#)
- [start activation](#)
- [start deactivation](#)
- [start update](#)
- [set configuration](#)

## get protection-status

Get the list of application statuses and the global application status

### Командная строка

```
ermm.exe get protection-status
```

### Параметры

None

### Пример

#### call

```
{
  "command": "get_protection_status",
  "id": 1,
  "version": "1"
}
```

#### result

```
{
  "id": 1,
  "result": {
    "statuses": [{
      "id": "EkrrnNotActivated",
      "status": 2,
      "priority": 768,
      "description": "Product not activated"
    }],
    "status": 2,
    "description": "Security alert"
  },
  "error": null
}
```

# get application-info

Get information about the installed application

## Командная строка

```
ermm.exe get application-info
```

## Параметры

None

## Пример

**call**

```
{
  "command": "get_application_info",
  "id": 1,
  "version": "1"
}
```

**result**

```

{
  "id":1,
  "result":{
    "description":"ESET Endpoint Antivirus",
    "version":"6.6.2018.0",
    "product":"eea",
    "lang_id":1033,
    "modules":[{
      "id":"SCANNER32",
      "description":"Detection engine",
      "version":"15117",
      "date":"2017-03-20"
    },{
      "id":"PEGASUS32",
      "description":"Rapid Response module",
      "version":"9734",
      "date":"2017-03-20"
    },{
      "id":"LOADER32",
      "description":"Update module",
      "version":"1009",
      "date":"2016-12-05"
    },{
      "id":"PERSEUS32",
      "description":"Antivirus and antispysware scanner module",
      "version":"1513",
      "date":"2017-03-06"
    },{
      "id":"ADVHEUR32",
      "description":"Advanced heuristics module",
      "version":"1176",
      "date":"2017-01-16"
    },{
      "id":"ARCHIVER32",
      "description":"Archive support module",
      "version":"1261",
      "date":"2017-02-22"
    },{
      "id":"CLEANER32",
      "description":"Cleaner module",
      "version":"1132",
      "date":"2017-03-15"
    },{
      "id":"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

### Командная строка

```
ermm.exe get license-info
```

### Параметры

None

### Пример

#### 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

### Командная строка

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

### Параметры

| 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]) |
|----------|---|

## Пример

### 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, running, failure }

## Командная строка

```
ermm.exe get activation-status
```

## Параметры

None

## Пример

### call

```
{
  "command": "get_activation_status",
  "id": 1,
  "version": "1"
}
```

### result

```
{
  "id": 1,
  "result": {
    "status": "success"
  },
  "error": null
}
```

## get scan-info

Получить информацию о запущенном сканировании.

## Командная строка

```
ermm.exe get scan-info
```

## Параметры

Нет

## Пример

### ВЫЗОВ

```
{
  "command": "get_scan_info",
  "id": 1,
  "version": "1"
}
```

### результат



```
{
  "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 }

## Командная строка

```
ermmm.exe get configuration --file C:\\tmp\\conf.xml --format xml
```

## Параметры

| Name   | Value   |
|--------|---|
| file   | the path where the configuration file will be saved       |
| format | format of configuration: json, xml. Default format is xml |

## Пример

```
call
```

```
{
  "command": "get_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml"
  }
}
```

#### result

```
{
  "id": 1,
  "result": {
    "configuration": "PD94bWwgdGVyc2lvbj0iMS4w=="
  },
  "error": null
}
```

## get update-status

Get information about the update. Result of status may be { success, error }

## Командная строка

ermm.exe get update-status

## Параметры

None

## Пример

#### 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

### Командная строка

```
ermm.exe start scan --profile "profile name" --target "path"
```

### Параметры

| Name    | Value  |
|---------|--|
| profile | Profile name of On-demand computer scan defined in product |
| target  | Path to be scanned   |

### Пример

#### 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

### Командная строка

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

### Параметры

| Name | Value          |
|------|----------------|
| key  | Activation key |

|         |                      |
|---------|----------------------|
| offline | Path to offline file |
|---------|----------------------|

## Пример

### 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

## Командная строка

ermm.exe start deactivation

## Параметры

None

## Пример

### 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

### Командная строка

```
ermm.exe start update
```

### Параметры

None

### Пример

#### 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 }

### Командная строка

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

### Параметры

| 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) |

## Пример

### call

```
{
  "command": "set_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml",
    "password": "pass"
  }
}
```

### result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

## Проверка лицензии с интервалом

Программе ESET Endpoint Antivirus необходимо автоматически подключаться к серверам лицензий ESET. Ограничить количество подключений к серверу лицензий ESET можно в разделе [Расширенные параметры](#) > **Средства** > **Лицензия**. По умолчанию для параметра **Проверка с интервалом** установлено значение **Автоматически**, и соединение устанавливается несколько раз в час. Если сетевой трафик станет слишком большим, измените значение параметра **Проверка с интервалом** на **Ограничено**, чтобы уменьшить нагрузку. Если выбрано значение **Ограничено**, ESET Endpoint Antivirus 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 Antivirus связанных с лицензией изменений, внесенных с помощью ESET HUB/ESET MSP Administrator, может уйти до одного дня.

## Файлы журнала

Конфигурация ведения журнала ESET Endpoint Antivirus находится в разделе [Расширенные параметры](#) > **Средства** > **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.
- **Критические:** регистрируются только критические ошибки (ошибки запуска защиты от вирусов и 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 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 средстве ESET Log Collector см. в [статье базы знаний ESET](#).

# Режим презентации

Режим презентации — это функция для пользователей, которым нужно избежать перерывов при использовании своих программ и появления отвлекающих уведомлений или предупреждений, а также свести к минимуму нагрузку на процессор (CPU). Его также можно использовать во время проведения презентаций, которые нельзя прерывать деятельностью модуля защиты от вирусов. При включении этой функции отключаются все всплывающие окна, а работа планировщика полностью останавливается. Защита системы по-прежнему работает в фоновом режиме, но не требует какого-либо вмешательства со стороны пользователя.

Включение и отключение режима презентации осуществляется в [главном окне программы](#) в разделе **Настройка > Компьютер**, где необходимо щелкнуть  или  рядом с элементом **Режим презентации**. Включая режим презентации вы подвергаете систему угрозе, поэтому значок состояния защиты на панели задач станет оранжевым, чтобы тем самым предупредить вас. Кроме того, данное предупреждение будет отображаться в [главном окне программы](#), где оранжевым цветом будет написано **Режим презентации активен**.

Активируйте параметр **Автоматически включать режим презентации при выполнении приложений в полноэкранном режиме** в разделе [Расширенные параметры](#) > **Сервис** > **Режим презентации**, чтобы режим презентации включался при запуске любого приложения в полноэкранном режиме и выключался при выходе из приложения.

Активируйте параметр **Автоматически отключать режим презентации через** для указания времени, через которое режим презентации будет автоматически отключен.

## 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 Antivirus.

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 дампы диагностики:** нажмите кнопку **Создать**, чтобы создать в **целевом каталоге** файлы дампа диагностики.

## Расширенное ведение журналов

**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 Direct Cloud** — Запись всех сообщений, которыми обмениваются продукт и серверы Direct Cloud.

**Включить расширенное ведение журнала защиты документов:** запись всех событий, которые происходят в модуле защиты документов, для диагностики и устранения проблем.

**Включить расширенное ведение журналов защиты почтового клиента** — запись всех событий, происходящих в защите почтового клиента и плагине почтового клиента, для диагностики и решения проблем.

**Включить расширенное ведение журнала ядра:** запись всех событий, которые происходят в службе ядра ESET (ekrn). Это помогает выявлять и исправлять проблемы.

**Включить расширенное ведение журнала для лицензирования:** запись всего обмена данными между серверами лицензирования 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 фаервол в формате PCAP. Это помогает разработчикам выявлять и устранять проблемы, связанные с фаерволом.

**Включить расширенное ведение журнала для сканера сетевого трафика:** запись всех данных, проходящих через сканер сетевого трафика в формате PCAP. Это помогает разработчикам выявлять и устранять проблемы, связанные со сканером сетевого трафика.

**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 журналов для обмена push-сообщениями** — Запись всех событий, происходящих во время обмена push-сообщениями, для обеспечения диагностики и устранения проблем.

**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 управления уязвимостями и исправлениями:** запись всех событий для функции [Управление уязвимостями и исправлениями](#). Этот параметр отображается только в том случае, если в вашей среде включено управление уязвимостями и исправлениями (включено в ESET PROTECT Cloud).

Файлы журнала находятся в папке `C:\ProgramData\ESET\ESET Security\Diagnostics\`.

## Служба технической поддержки

При [обращении в службу технической поддержки ESET](#) из программы ESET Endpoint Antivirus можно отправить данные о конфигурации системы. Выберите **Отправлять всегда** в раскрывающемся меню **Отправка данных о конфигурации системы** для автоматической отправки данных или выберите **Запрашивать подтверждение перед отправкой**, чтобы получать запрос перед отправкой данных.

## Подключение

В определенных сетях подключение компьютеров к Интернету может осуществляться через прокси-сервер. Если вы используете прокси-сервер, вам необходимо задать следующие настройки. В противном случае решение ESET Endpoint Antivirus и его модули не смогут обновляться автоматически. В ESET Endpoint Antivirus настройка прокси-сервера доступна в двух разных разделах [расширенных параметров](#).

Глобальные настройки прокси-сервера можно конфигурировать в разделе [Расширенные параметры](#) > **Подключение** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для программы ESET Endpoint Antivirus в целом. Они используются всеми модулями программы, которым требуется подключение к Интернету.

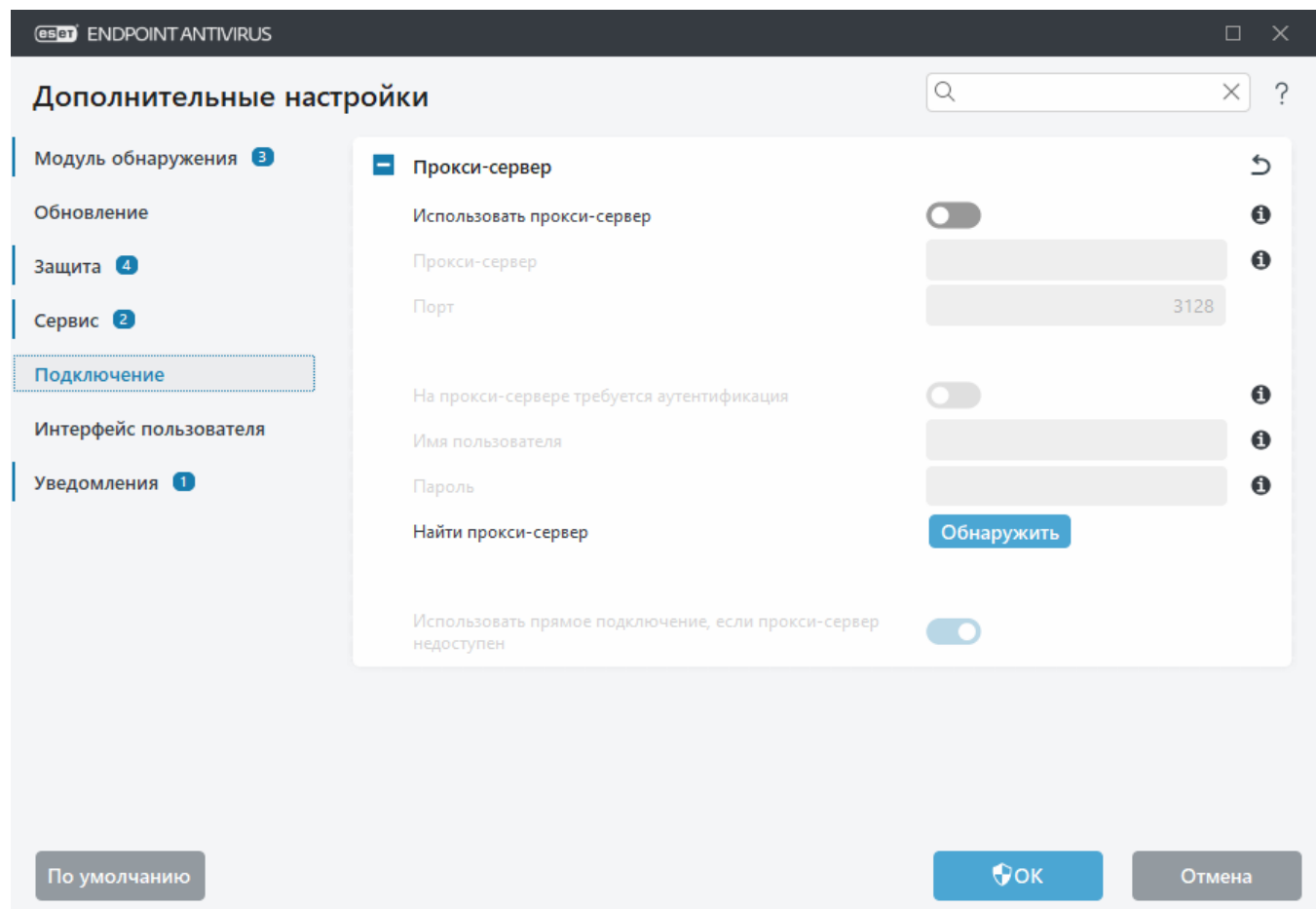
Чтобы задать глобальные настройки прокси-сервера, включите параметр **Использовать прокси-сервер** и введите адрес **прокси-сервера**, а также его номер **порта**.

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. Чтобы найти настройки прокси-сервера в операционной системе, нажмите сочетание клавиш **Windows + I** и выберите **Сеть и Интернет** > **Прокси-сервер**. ESET Endpoint Antivirus скопирует параметры подключения к Интернету, указанные для Internet Explorer или Google Chrome.

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

**Использовать прямое подключение, если прокси-сервер недоступен:** если в ESET Endpoint Antivirus настроено подключение через прокси-сервер, а он недоступен, ESET Endpoint Antivirus будет обходить прокси-сервер и подключаться к серверам ESET напрямую.

Параметры прокси-сервера также можно настроить в области [Дополнительные настройки](#) > **Обновление** > **Профили** > **Обновления** > **Параметры подключения** и в раскрывающемся списке **Режим прокси-сервера** выберите элемент **Подключение через прокси-сервер**). Эта конфигурация применяется только для обновлений и рекомендуется для ноутбуков, получающих обновления модулей из удаленных расположений. Дополнительные сведения см. в разделе [Дополнительные настройки обновления](#).



## Интерфейс пользователя

Чтобы настроить поведение графического интерфейса программы, откройте раздел [Расширенные параметры](#) > **Интерфейс**.

В окне [Элементы интерфейса](#) расширенных параметров можно настроить внешний вид программы и используемые эффекты.

Чтобы обеспечить максимальную защиту для программы безопасности, можно запретить удаление программы или внесение несанкционированных изменений, защитив параметры паролем с помощью служебной программы [Настройка доступа](#).

**i** Сведения о том, как настроить системные уведомления, предупреждения об обнаружении и состояния приложения, см. в разделе [Уведомления](#).

[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 Antivirus интерфейс](#) (полезен для управляемых сред).

## Элементы интерфейса пользователя

Параметры интерфейса пользователя в ESET Endpoint Antivirus позволяют настроить рабочую среду в соответствии с конкретными требованиями. Эти параметры конфигурации доступны, если последовательно открыть **Расширенные параметры (F5) > Интерфейс > Элементы интерфейса**.

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.

**i** 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 Antivirus от имени администратора. Это также можно сделать в ESET PROTECT, применив соответствующую [политику](#).

**Режим цвета:** выберите в раскрывающемся меню цветовую схему интерфейса ESET Endpoint Antivirus.

- **Соответствовать цвету системы:** цветовая схема ESET Endpoint Antivirus задается согласно настройкам операционной системы.
- **Темная:** выбор темной цветовой схемы для ESET Endpoint Antivirus (темный режим).
- **Светлая:** выбор стандартной (светлой) цветовой схемы для ESET Endpoint Antivirus.

**i** Кроме того, цветовую схему графического интерфейса ESET Endpoint Antivirus можно выбрать в правом верхнем углу [главного окна программы](#).

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

Если вы хотите, чтобы программа ESET Endpoint Antivirus 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 Antivirus в контекстное меню.

## Информация о лицензии

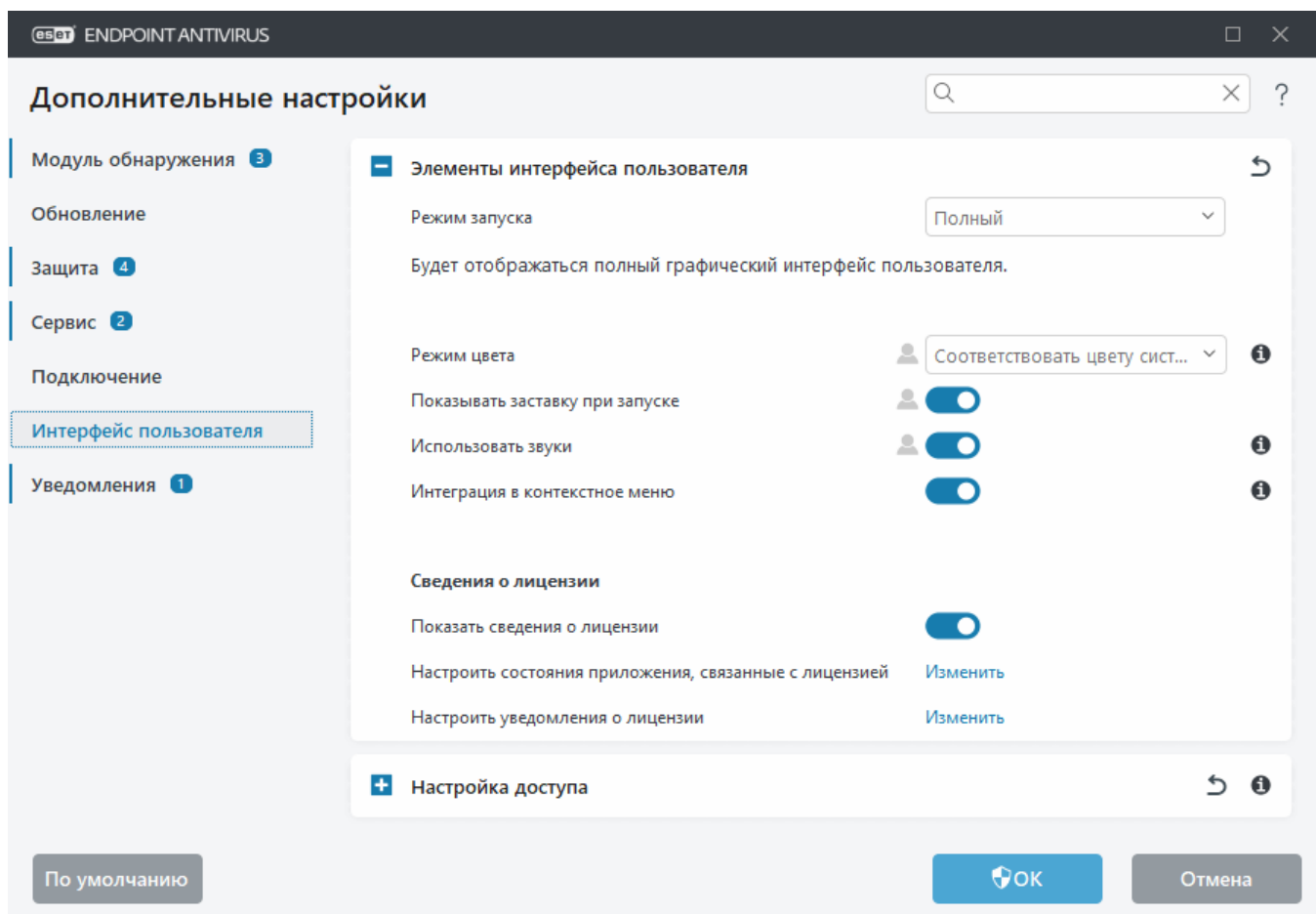
**Показать сведения о лицензии.** Если этот параметр отключен, дата истечения срока действия лицензии не будет отображаться в окнах **Состояние защиты** и **Справка и поддержка**.

**Настроить состояния приложения, связанные с лицензией.** Открывает список [СОСТОЯНИЙ приложения](#), связанных с лицензией.

**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 Antivirus активирован с помощью лицензии MSP.



## Настройка доступа

Настройки ESET Endpoint Antivirus являются важной составной частью вашей политики безопасности. Несанкционированное изменение параметров может нарушить стабильность работы системы и ослабить ее защиту. Для предотвращения несанкционированного изменения параметры настройки и возможность удаления приложения ESET Endpoint Antivirus можно защитить паролем. Доступ можно настроить в разделе [Расширенные параметры](#) > **Интерфейс** > **Настройка доступа**.

Чтобы установить пароль для защиты параметров настройки и функции удаления приложения

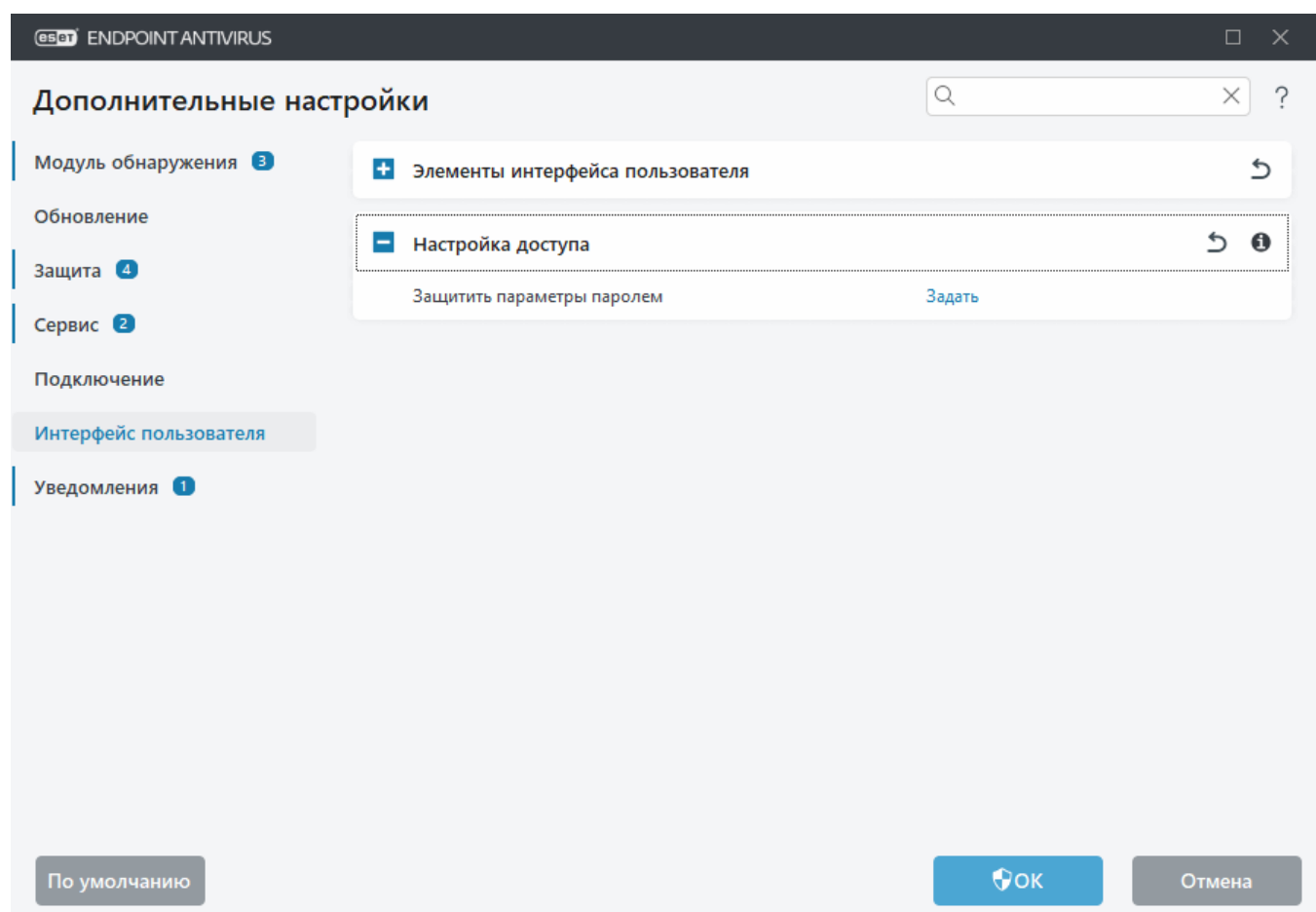
ESET Endpoint Antivirus, щелкните **Задать** рядом с полем **Защитить параметры паролем**.

Чтобы изменить пароль, щелкните **Изменить пароль** рядом с полем **Защитить параметры паролем**.

Чтобы удалить пароль, щелкните **Удалить** рядом с полем **Защитить параметры паролем**.

## Управляемые среды

Администратор может создать политику защиты параметров паролем для ESET Endpoint Antivirus на подключенных клиентских компьютерах. Указания по созданию новой политики см. в разделе [Защищенные паролем параметры](#).



## Пароль для доступа к расширенным параметрам

Чтобы защитить расширенные параметры ESET Endpoint Antivirus и избежать их несанкционированного изменения, введите новый пароль в поля **Новый пароль** и **Подтвердите пароль**. Нажмите кнопку **ОК**.

## Управляемые среды

Администратор может создать политику защиты параметров паролем для ESET Endpoint Antivirus 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 **ОК**.

Теперь для внесения каких-либо изменений в ESET Endpoint Antivirus нужно будет указать этот пароль.

Если вы забудете пароль, см. раздел [Разблокировка пароля для настроек в продуктах ESET для конечных точек](#).

Чтобы восстановить потерянный лицензионный ключ ESET, данные о дате окончания срока действия вашей лицензии или другие сведения о лицензии ESET Endpoint Antivirus, см. раздел [Действия в случае потери имени пользователя и пароля либо лицензионного ключа](#).

## Пароль

Для предотвращения несанкционированного изменения параметры ESET Endpoint Antivirus можно защитить паролем.

## Безопасный режим

В том случае, когда графический интерфейс ESET Endpoint Antivirus запущен в безопасном режиме, на экран выводится диалоговое окно, сообщающее о необходимости запустить приложение в безопасном режиме. Так как работа всех программ в безопасном режиме ограничена, запустить графический интерфейс ESET Endpoint Antivirus так же, как в обычном режиме, не удастся.

В появившемся окне можно запустить сканирование компьютера. Для того чтобы проверить компьютер на наличие вредоносного кода, выберите **Да**.

После этого сканирование запустится в отдельном окне с теми же параметрами, что в профиле сканирования компьютера по умолчанию, которые применяются после установки ESET Endpoint Antivirus.

Выберите **Нет**, чтобы закрыть это диалоговое окно. ESET Endpoint Antivirus не будет выполнять никаких действий.

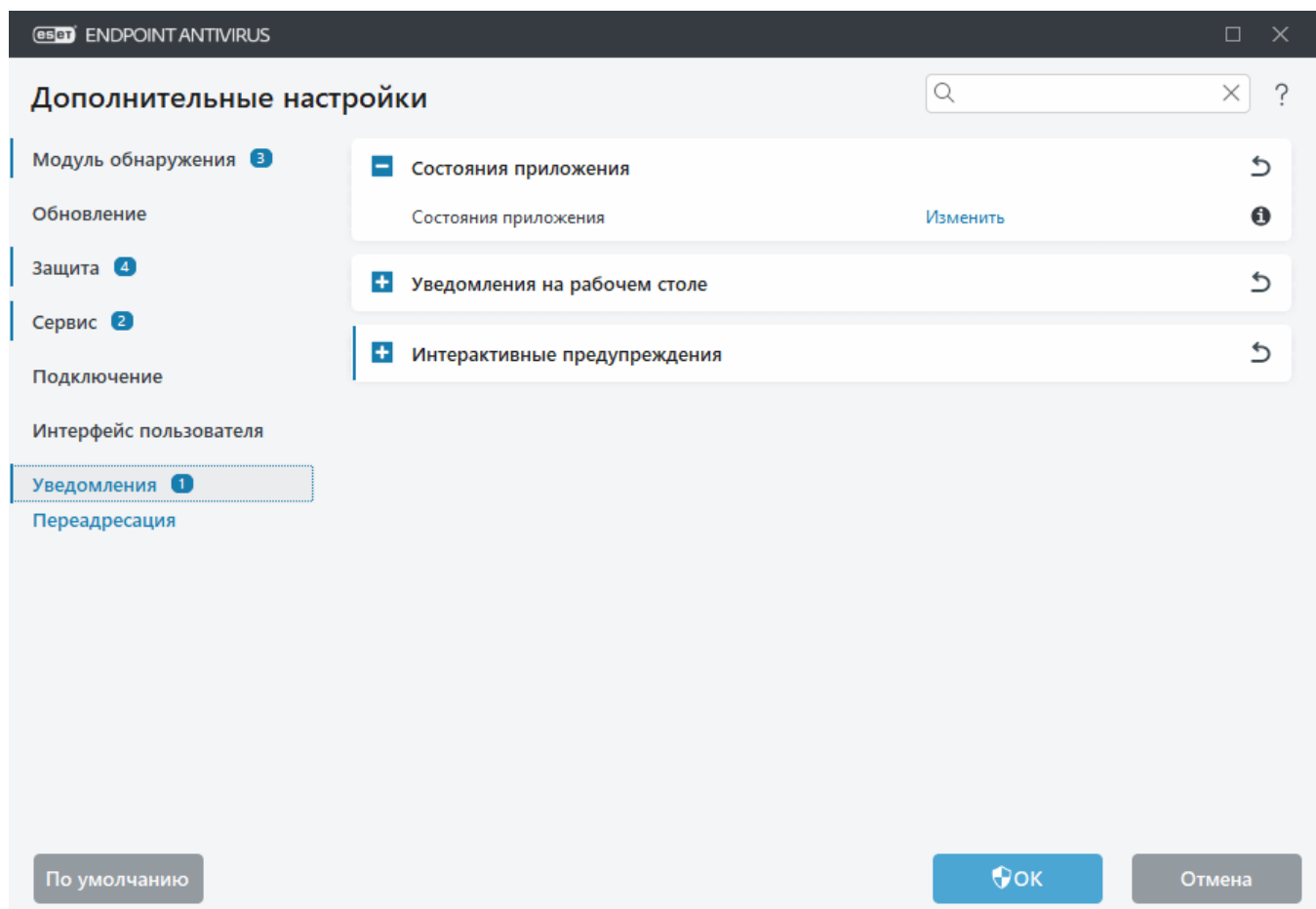
## Уведомления

Чтобы управлять уведомлениями ESET Endpoint Antivirus, откройте раздел [Расширенные параметры](#) > **Уведомления**. Можно настроить следующие типы уведомлений.

- Состояния приложения: уведомления, отображаемые на домашней странице [главного](#)

[окна программы.](#)

- [Уведомления на рабочем столе](#): небольшие окна уведомления рядом с системной панелью задач.
- [Интерактивные предупреждения](#): окна и сообщения с предупреждениями, которые требуют вмешательства пользователя.
- [Переадресация](#) (уведомления по электронной почте): уведомления отправляются на указанный адрес электронной почты.
- [Настройка уведомлений](#): добавьте произвольное сообщение к, например, уведомлению на рабочем столе.



## Состояния приложения

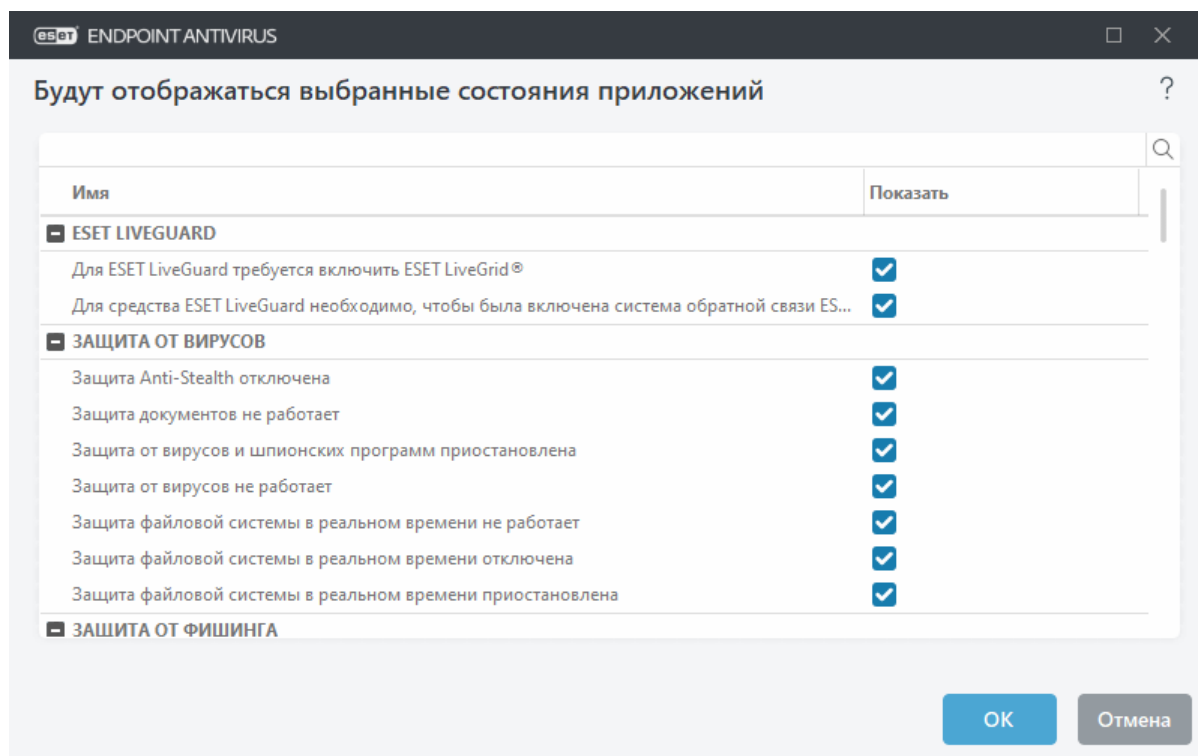
**Состояния приложения:** щелкните **Изменить**, чтобы выбрать, какие состояния приложения будут отображаться на домашней странице главного окна программы.

## Состояния приложения

Для настройки того, какие состояния приложения будут отображаться (например, при приостановке защиты от вирусов и шпионских программ или включении режима презентации), откройте раздел [Расширенные параметры](#) > **Уведомления** и щелкните **Изменить** рядом с элементом **Состояния приложения**.

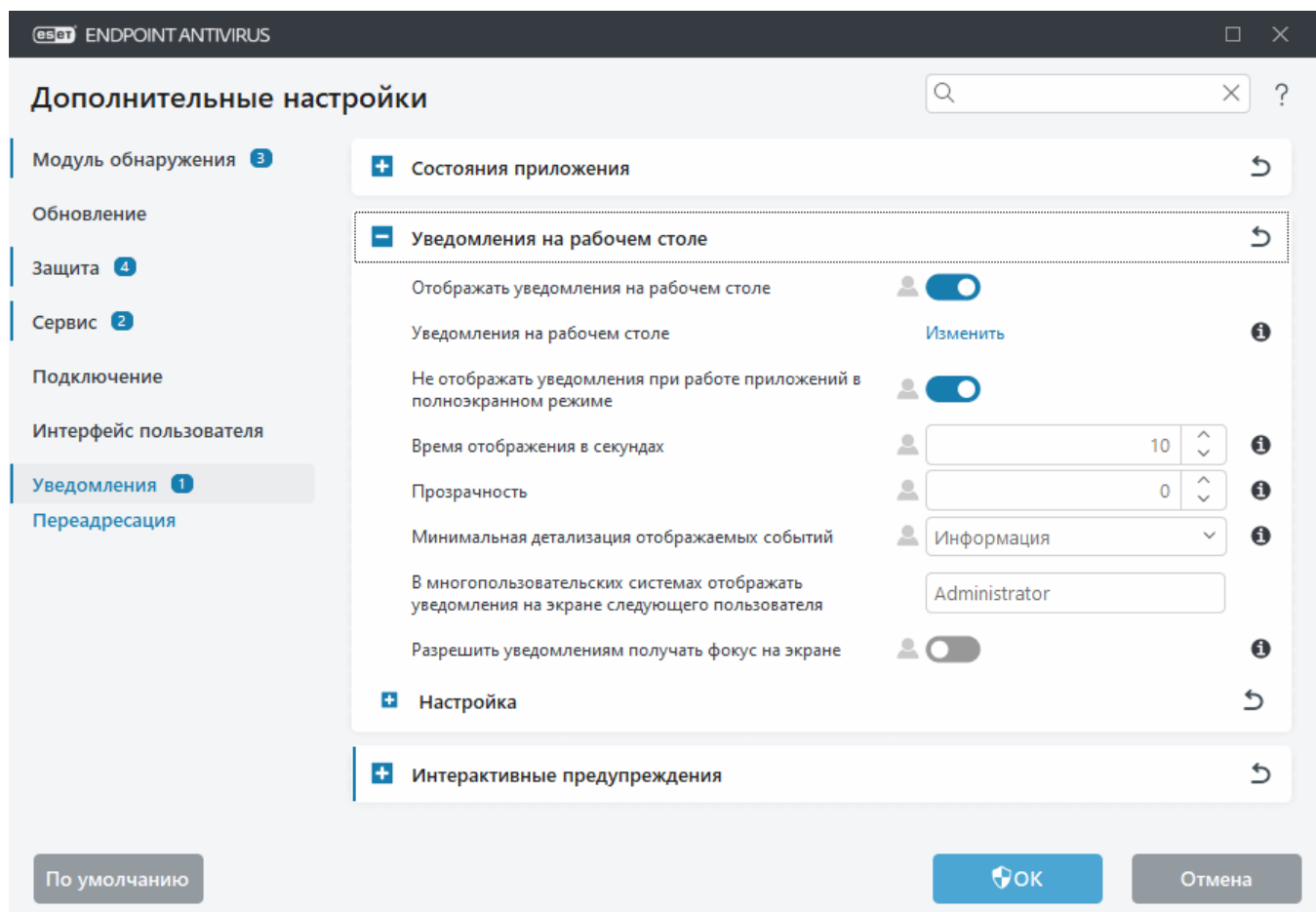
Кроме того, состояние приложения будет отображаться, если продукт не активирован или срок действия лицензии истек. Эту настройку можно изменить с помощью [ПОЛИТИК ESET PROTECT](#).





## Уведомления на рабочем столе

Уведомление на рабочем столе представляет собой небольшое окно уведомления возле системной панели задач. По умолчанию оно отображается в течение 10 секунд, затем медленно исчезает. Это основной способ, с помощью которого программа ESET Endpoint Antivirus сообщает пользователю об обновлении программы, подключении новых устройств, завершении задач сканирования на наличие вирусов и об обнаружении новых угроз.



**Отображать уведомления на рабочем столе:** рекомендуем не выключать этот параметр, чтобы продукт мог сообщать вам о новых событиях.

**Уведомления на рабочем столе:** щелкните **Изменить**, чтобы включить или отключить определенные [уведомления на рабочем столе](#).

**Не отображать уведомления при работе приложений в полноэкранном режиме:** скрывание всех неинтерактивных уведомлений, когда запущены приложения в полноэкранном режиме.

**Время ожидания (сек.):** настройка продолжительности отображения уведомлений. Значение должно быть от 3 до 30 секунд.

**Прозрачность:** настройка процента прозрачности уведомлений. Поддерживаются значения от 0 (без прозрачности) до 80 (очень высокая прозрачность).

**Минимальная детализация отображаемых событий:** настройка начального уровня серьезности уведомлений, которые следует отображать. В раскрывающемся меню можно выбрать следующие параметры.

- **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:** в журнал вносится информация обо всех критических ошибках и предупреждениях (например, о невыполненном обновлении).

- **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:** можно разрешить выбранным учетным записям получать уведомления на рабочем столе. Например, если учетная запись администратора не используется, введите полное имя учетной записи, и уведомления на рабочем столе будут отображаться для указанной учетной записи. Получать уведомления на рабочем столе может только одна учетная запись пользователя.

**Разрешить уведомлениям получать фокус на экране:** уведомления будут получать фокус на экране. К ним можно будет перейти нажатием клавиш Alt+Tab.

## 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.

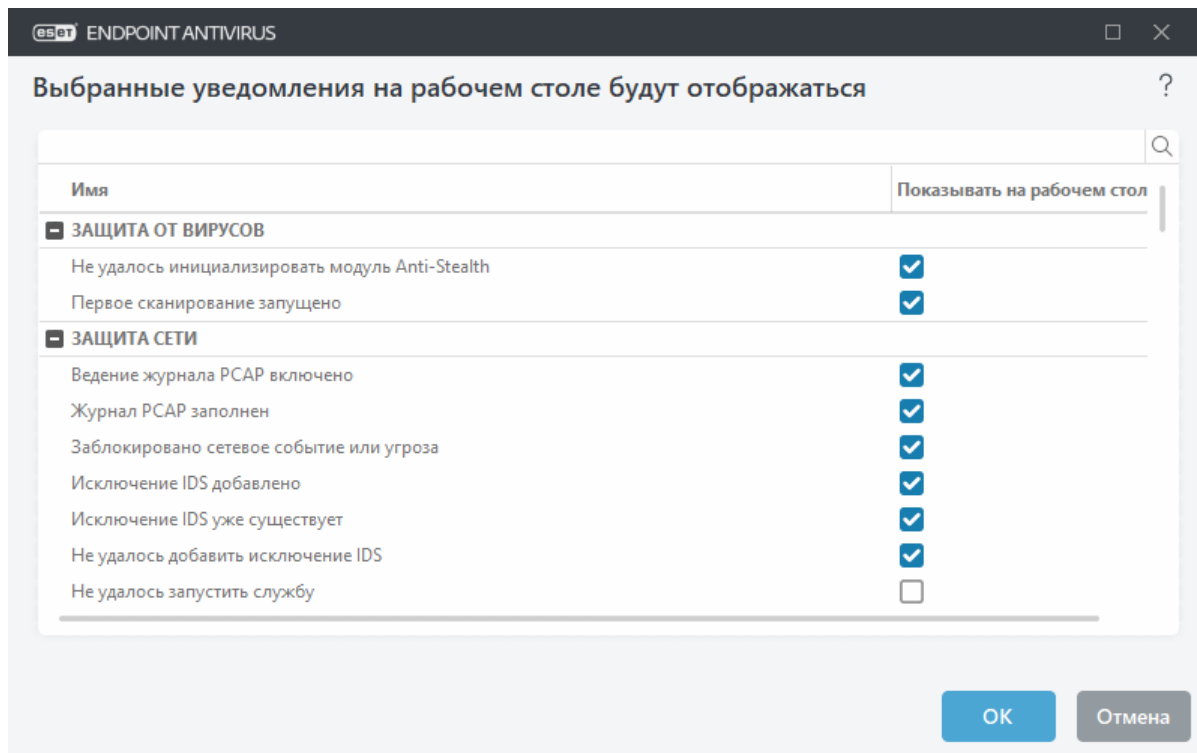
### Обнаружения

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 уведомления об обнаружении** введите собственный текст.

## Диалоговое окно «Уведомления на рабочем столе»

Чтобы изменить видимость уведомлений на рабочем столе (отображаются в правом нижнем углу экрана), откройте раздел [Расширенные параметры](#) > **Уведомления** > **Уведомления на рабочем столе**. Щелкните **Изменить** рядом с элементом **Уведомления на рабочем столе** и установите флажок **Показывать на рабочем столе**.



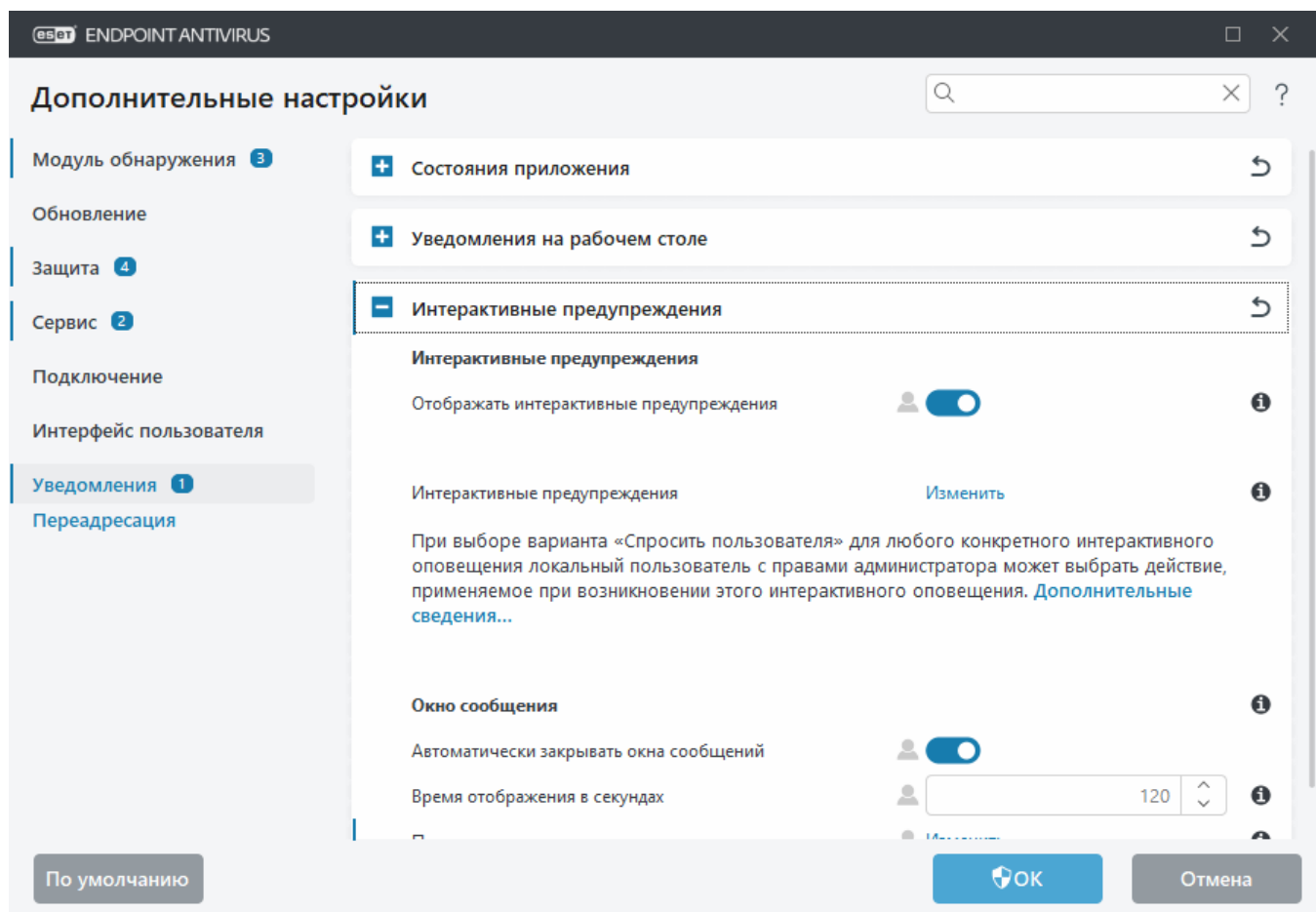
**И** Если вы хотите настроить уведомления **Файл проанализирован** и **Файл не проанализирован** при использовании ESET LiveGuard, для параметра [Проактивная защита](#) нужно задать значение **Заблокировать исполнение до получения результата анализа**.

## Интерактивные предупреждения

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](#)
- [Файл заблокирован из-за анализа](#)

Раздел **Интерактивные предупреждения**, который можно открыть, выбрав [Расширенные параметры](#) > **Уведомления**, позволяет конфигурировать способ обработки в программе ESET Endpoint Antivirus окон с сообщениями и интерактивных предупреждений об обнаружениях, в которых требуется принятие решения пользователем (например, о потенциальных фишинговых веб-сайтах).



## Интерактивные предупреждения

Если отключить параметр **Отображать интерактивные предупреждения**, окна предупреждений и диалоговые окна браузера выводиться на экран не будут. Такой подход следует использовать только для ограниченного количества особых ситуаций.

- 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](#).

**Интерактивные предупреждения:** щелкните **Изменить**, чтобы выбрать, какие [интерактивные предупреждения](#) будут отображаться.

## Окно сообщения

Чтобы окна сообщений 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.

**Время ожидания (сек.):** настройка продолжительности отображения предупреждения. Значение должно быть от 10 до 999 секунд.

**Подтверждения:** щелкните **Изменить**, чтобы открыть [список подтверждений](#), для которых

можно включить или отключить отображение.

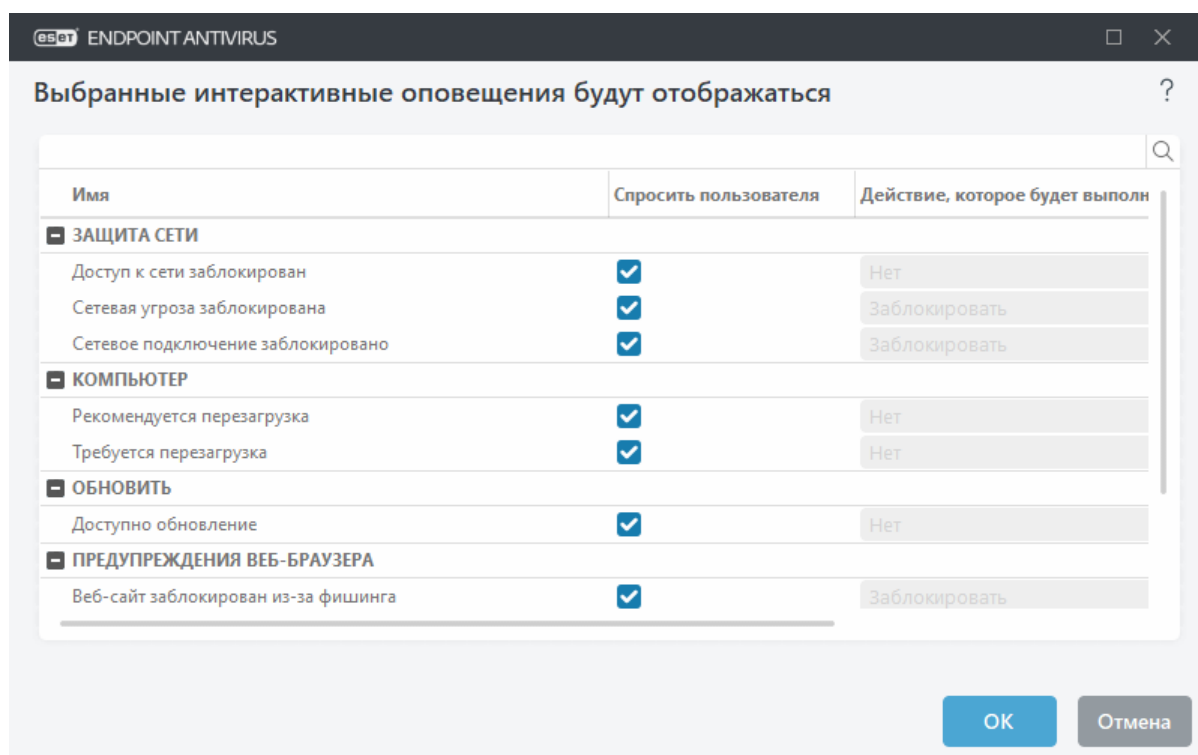
## Список интерактивных предупреждений

В данном разделе описаны несколько окон интерактивных предупреждений, которые ESET Endpoint Antivirus будут отображаться перед выполнением каких-либо действий.

Чтобы настроить поведение настраиваемых интерактивных предупреждений, откройте [Расширенные параметры](#) > **Уведомления** > **Интерактивные предупреждения** и щелкните **Изменить** рядом с параметром **Интерактивные предупреждения**.



Полезно для управляемых сред, где администратор может отменить выбор **Спросить пользователя** и выбрать заранее определенное действие, применяемое при отображении окон интерактивных предупреждений.



Дополнительные сведения о конкретном окне интерактивного предупреждения см. в следующих разделах справки:

## Съемные носители

- [Обнаружено новое устройство](#)

## 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

При наличии этих предупреждений изменится цвет интерфейса:

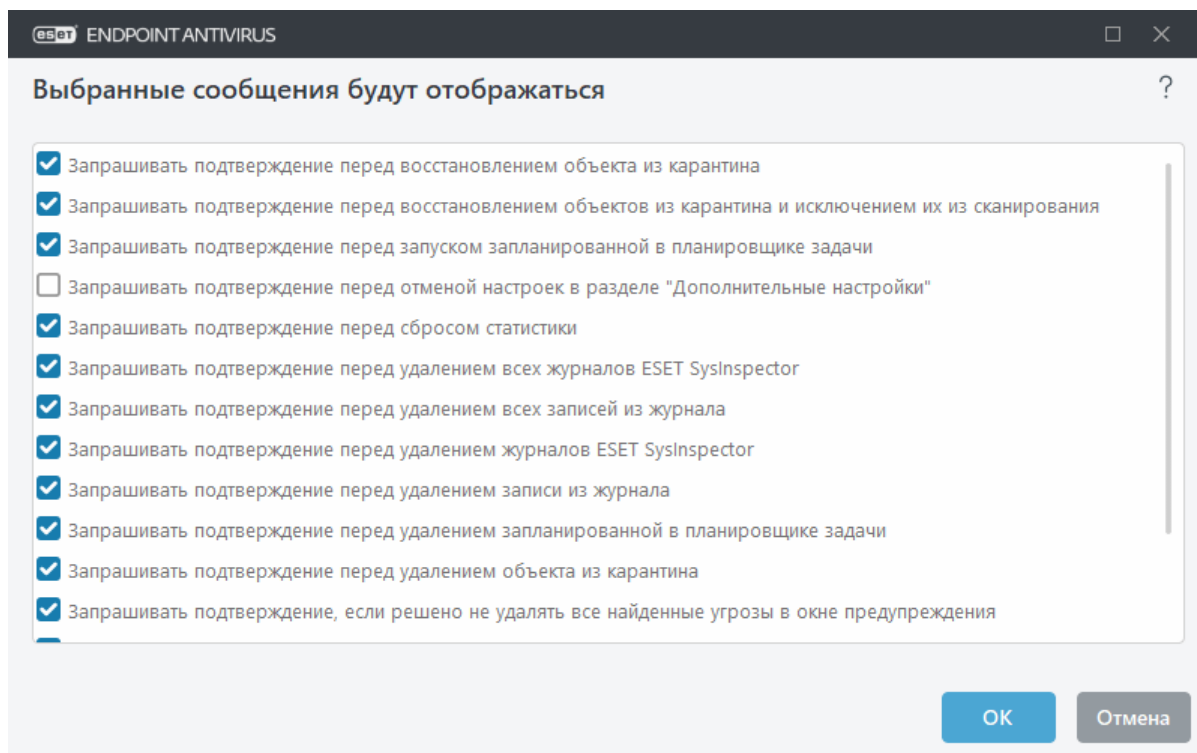
- [Перезагрузить компьютер \(обязательно\)](#)
- [Перезагрузить компьютер \(рекомендуется\)](#)



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 [Расширенные параметры](#) > **Уведомления** > **Интерактивные предупреждения**, а затем щелкните **Изменить** рядом с элементом **Подтверждения**.



В этом диалоговом окне отображаются подтверждения, выводимые ESET Endpoint Antivirus 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 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 HIPS) и пользователь одновременно создадут правила в интерактивном режиме или режиме обучения.



Рекомендуется изменить режим фильтрации на **Автоматический режим** по умолчанию, если вы хотите создавать собственные правила. См. дополнительные сведения о [системе HIPS и режимах фильтрации HIPS](#).

## Требуется перезагрузка

После обновления ESET Endpoint Antivirus до новой версии или применения исправлений к приложениям с помощью функции [управления уязвимостями и исправлениями](#) требуется перезапуск компьютера. Новые версии ESET Endpoint Antivirus выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическими обновлениями модулей программы.

Нажмите кнопку **Перезапустить сейчас**, чтобы перепустить компьютер. Если вы планируете перезапустить компьютер позже, нажмите кнопку **«Напомнить позже»**. Позже можно будет перезапустить компьютер вручную из раздела **Состояние защиты** в главном окне программы.

Чтобы отключить предупреждения «Необходим перезапуск» или «Рекомендуется перезапуск», выполните приведенные ниже действия.

1. Откройте **Расширенные параметры (F5) > Уведомления > Интерактивные предупреждения**.
2. Щелкните **Изменить** рядом с элементом **Интерактивные предупреждения**. В разделе **Компьютер** снимите флажок с пункта **Перезагрузить компьютер (обязательно)** и **Перезагрузить компьютер (рекомендовано)**.



3. Нажмите **ОК**, 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 Antivirus, в [окне состояний приложений](#) снимите флажок с пункта **Необходима перезагрузка компьютера и Рекомендовано перезагрузить компьютер**.

## Рекомендуется перезагрузка

После обновления ESET Endpoint Antivirus до новой версии требуется перезапуск компьютера. Новые версии ESET Endpoint Antivirus выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическими обновлениями модулей программы.

Нажмите кнопку **Перезапустить сейчас**, чтобы перепустить компьютер. Если вы планируете перезапустить компьютер позже, нажмите кнопку **«Напомнить позже»**. Позже можно будет перезапустить компьютер вручную из раздела **Состояние защиты** в главном окне программы.

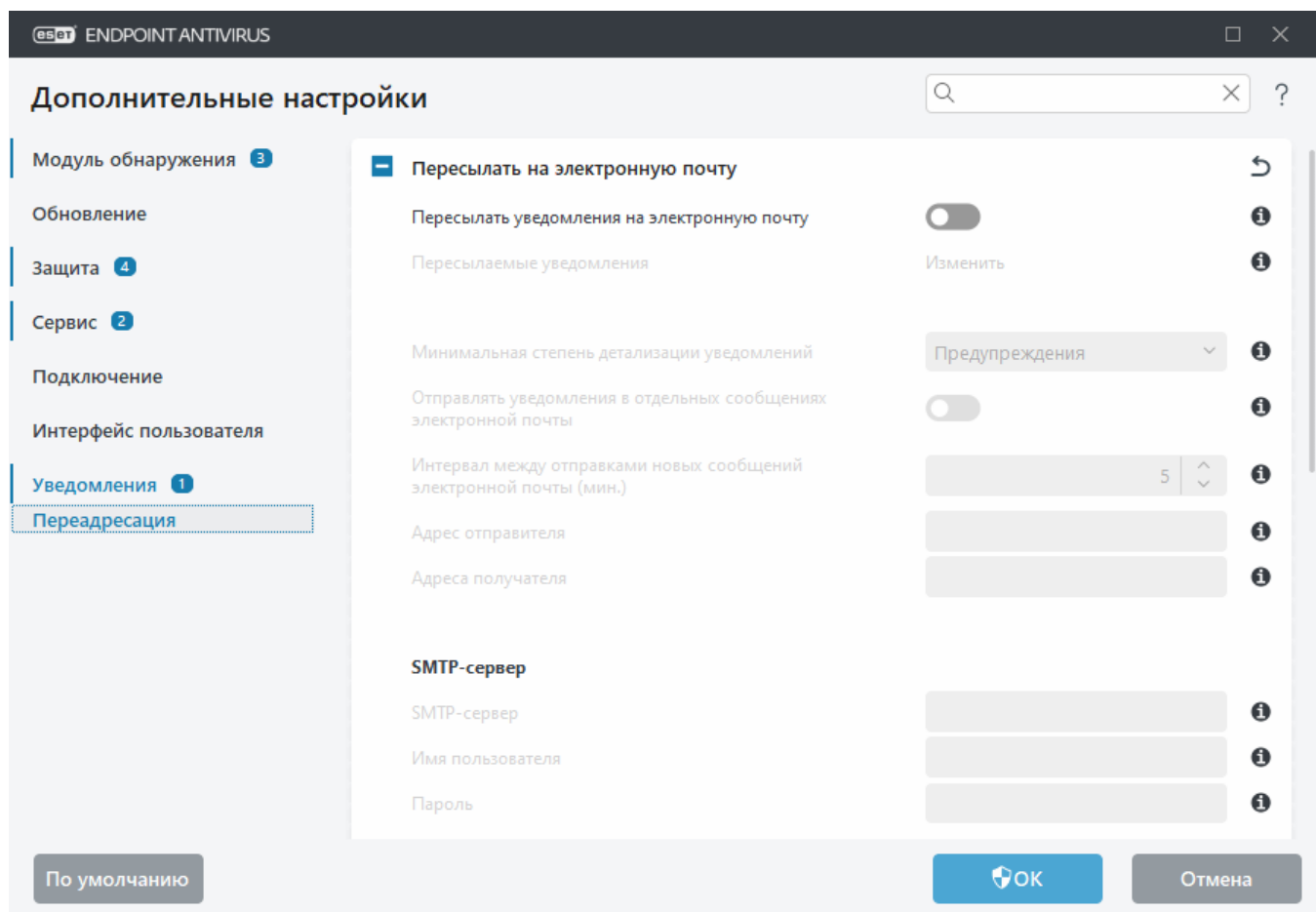
Чтобы отключить предупреждения «Необходим перезапуск» или «Рекомендуется перезапуск», выполните приведенные ниже действия.

1. Откройте **Расширенные параметры (F5) > Уведомления > Интерактивные предупреждения**.
2. Щелкните **Изменить** рядом с элементом **Интерактивные предупреждения**. В разделе **Компьютер** снимите флажок с пункта **Перезагрузить компьютер (обязательно)** и **Перезагрузить компьютер (рекомендовано)**.
3. Нажмите **ОК**, 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 Antivirus, в [окне состояний приложений](#) снимите флажок с пункта **Необходима перезагрузка компьютера и Рекомендовано перезагрузить компьютер**.

## Переадресация

ESET Endpoint Antivirus поддерживает отправку сообщений электронной почты при возникновении событий с заданной степенью детализации. Чтобы активировать эту функцию, в разделе [Расширенные параметры](#) > **Уведомления** > **Переадресация** > **Пересылать на электронную почту** включите параметр **Пересылать уведомления на электронную почту**.

**Пересылаемые уведомления:** выберите, какие уведомления на рабочем столе будут пересылаться на электронную почту.



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:** в журнал вносится информация обо всех критических ошибках и предупреждениях (например, о невыполненном обновлении).
- **Ошибки:** записываются ошибки (не активирована защита документов) и критические ошибки.
- **Критические ошибки:** запись в журнал только сведений о критических ошибках (например, об ошибках при запуске защиты от вирусов или об обнаружении угроз).

**Отправлять уведомления в отдельных сообщениях электронной почты:** если этот параметр активирован, получатель будет получать каждое уведомление в 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.

**Адрес отправителя:** выбор адреса отправителя, который будет отображаться в заголовке сообщений электронной почты с уведомлением.

**Адреса получателя:** указание адресов получателей, которые будут отображаться в заголовке

сообщений электронной почты с уведомлением. Можно указать несколько адресов. В качестве разделителя используйте точку с запятой.

## SMTP-сервер

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

 ESET Endpoint Antivirus 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.

## 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.

## Восстановление всех параметров по умолчанию

Нажмите **По умолчанию** в [расширенных параметрах](#), 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 NIPS 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.

## Сканер командной строки

Модуль защиты от вирусов ESET Endpoint Antivirus 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 [ПАРАМЕТРЫ..] ФАЙЛЫ..
```

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

### Параметры

|                           |   |
|---------------------------|---|
| /base-dir=ПАПКА           | загрузить модули из ПАПКИ                                   |
| /quar-dir=ПАПКА           | ПАПКА карантина   |
| /exclude=МАСКА            | исключить из сканирования файлы, соответствующие МАСКЕ      |
| /subdir                   | сканировать вложенные папки (по умолчанию)                  |
| /no-subdir                | не сканировать вложенные папки                              |
| /max-subdir-level=УРОВЕНЬ | максимальная степень вложенности папок для сканирования     |
| /symlink                  | следовать по символическим ссылкам (по умолчанию)           |
| /no-symlink               | пропускать символические ссылки                             |
| /ads                      | сканировать ADS (по умолчанию)                              |
| /no-ads                   | не сканировать ADS  |
| /log-file=ФАЙЛ            | вывод журнала в ФАЙЛ  |
| /log-rewrite              | перезаписывать выходной файл (по умолчанию — добавлять)     |
| /log-console              | вывод журнала в окно консоли (по умолчанию)                 |
| /no-log-console           | не выводить журнал в консоль                                |
| /log-all                  | регистрировать также незараженные файлы                     |
| /no-log-all               | не регистрировать незараженные файлы (по умолчанию)         |
| /auid                     | 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.<br><br>Доступны указанные ниже варианты. <ul style="list-style-type: none"> <li>• none (по умолчанию) автоматическая очистка не выполняется.</li> <li>• standard — Приложение ecls.exe попытается автоматически очистить или удалить зараженные файлы.</li> <li>• Тщательная: приложение ecls.exe попытается автоматически очистить или удалить зараженные файлы без вмешательства пользователя (вам не будет предложено подтвердить удаление файлов).</li> <li>• «Наиболее тщательная». Приложение ecls.exe удалит все файлы независимо от их типа без очистки.</li> <li>• Удаление: приложение ecls.exe удалит без проведения очистки все файлы, кроме важных, таких как системные файлы Windows.</li> </ul> |
| /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.

## 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 Antivirus](#)
- [Активация ESET Endpoint Antivirus](#)
- [Решение ESET Endpoint Antivirus обнаружило угрозу](#)
- [Удаление вируса с компьютера](#)
- [Создание задачи в планировщике](#)
- [Планирование еженедельного сканирования компьютера](#)

- [Управление уведомлениями и интерактивными предупреждениями](#)
- [Подключение продукта к ESET PROTECT](#)
  - [Использование режима переопределения](#)
  - [Применение рекомендуемой политики для ESET Endpoint Antivirus](#)
- [Настройка зеркала](#)
- [Как мне обновить свою систему до Windows 10, если у меня установлен продукт ESET Endpoint Antivirus?](#)
- [Активация удаленного мониторинга и управления](#)
- [Блокировка загрузки файлов определенного типа из Интернета](#)
- [Сведения о свертывании ESET Endpoint Antivirus](#)

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 Antivirus.

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

- [Удаление ESET Endpoint Antivirus](#)
- [Рекомендации по защите от вирусов-шифраторов \(программ-вымогателей\)](#)
- [Вопросы и ответы по ESET Endpoint Security и ESET Endpoint Antivirus](#)
- [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.

## Вопросы и ответы по автоматическому обновлению



Дополнительные сведения об обновлениях программы в ESET Endpoint Antivirus см. в следующей статье базы знаний ESET:

- [Различные типы выпусков и обновлений продуктов ESET](#)

### Будут ли компьютеры обновляться автоматически? Обновление загружается до или после перезапуска?

Загрузка происходит до перезапуска, и на этом этапе выполняется также подготовка обновленных файлов. После перезапуска обновленные файлы все еще находятся в состоянии готовности к использованию, а установленная в данный момент версия обеспечивает непрерывную защиту. Изменения применяются после следующего запуска продукта ESET Endpoint Antivirus.

### У меня примерно 3000 компьютеров. Будут ли все



## **компьютеры загружать обновления одновременно? Можно ли использовать прокси-сервер для автоматического обновления при таком большом количестве компьютеров?**

ESET предлагает средство «Зеркало» и решения прокси-сервера для крупных сетей, поэтому обновления загружаются из Интернета лишь однажды, а затем распространяются локально. Размер обновлений меньше — обычно это 5–10 МБ. В первые несколько недель доступности обновлений компания ESET ограничивает их распространение. Поэтому при прямом подключении к серверам ESET не все клиенты начнут загрузку одновременно.

## **Можно ли указать, какое количество компьютеров или какие компьютеры должны обновляться автоматически? Я хочу делать загрузку не более чем для десяти компьютеров в час; или я хочу обновить только десять компьютеров сейчас, а другие компьютеры через пару дней.**

В управляемых средах есть политика автоматического обновления, в которой можно указать самую последнюю желаемую версию. Кроме того, поддерживаются подстановочные знаки (например, 9.0.2032.\*). Дополнительные сведения см. в главе «Автоматическое обновление» в онлайн-справке для [ESET PROTECT](#) или [ESET PROTECT Cloud](#). К сожалению, на данный момент нет других возможностей ограничить автоматическое обновление. Для нескольких групп можно назначить несколько политик.

## **Настраивается ли автоматическое обновление исключительно с помощью политики? Можно ли отключить политику, если я не хочу, чтобы продукт ESET обновлялся?**

Если для продукта ESET Endpoint появится исправление для обеспечения безопасности и стабильности, продукт будет обновлен даже в том случае, когда автоматическое обновление в нем отключено. Такое условие указано в применяемом лицензионном соглашении. ESET использует [исправления для обеспечения безопасности и стабильности](#), чтобы устранять критические проблемы и обеспечивать максимальную безопасность и стабильность вашего продукта ESET.

Политику автоматического обновления можно назначить любой группе конечных точек вне зависимости от их текущей конфигурации автоматического обновления. В неуправляемых средах пользователь может локально настроить автоматическое обновление на экране «Расширенные параметры» продукта ESET для конечных точек.

## Что, если я настрою в политике использование самой ранней доступной версии? Будет ли ESET обновлять мои продукты даже в таком случае?

Исправления и критические исправления (обновления для обеспечения безопасности и стабильности) относятся к немного разным категориям обновления. Когда настройки пользователя приняты, обычные исправления назначаются для автоматического обновления со стандартной приоритетностью. Критические исправления применяются с наивысшей приоритетностью вне зависимости от настроек пользователя.

## Как обновление будет работать в автономных сценариях? Когда пользователи используют автономный репозиторий?

Автономный репозиторий также содержит файлы с расширениями .dip и .fur. Раздел репозитория должен загружаться с помощью средства «Зеркало», а не обновления модуля. Дополнительные сведения см. в разделе [Автономный репозиторий](#) интернет-справки по ESET PROTECT.

## Откуда в продуктах ESET появляются сведения о необходимости обновления? Из репозитория? Отправляются ли данные на серверы? Если ESET планирует сделать обновление через месяц после выпуска версии, смогут ли серверы ESET справиться со всемирным выпуском?

Продукты ESET загружают автоматические обновления из репозитория. Серверы готовы к этому, так как размер критических обновлений составляет всего несколько килобайт. Компания ESET не ограничивает критические обновления на серверах репозитория. Однако для автоматических обновлений большого размера предусмотрена возможность ограничивать обновления на серверах. В таблице ниже приведены примерные размеры исправлений в случае разностного автоматического обновления.

| Предыдущая версия | Новая версия | Размер  |
|-------------------|--------------|---------|
| 9.0.2032.2        | 9.0.2032.6   | 420 KB  |
| 8.1.2037.2        | 9.0.2032.2   | 6.5 МБ  |
| 8.0.2028.0        | 9.0.2032.2   | 11.5 МБ |

Если разностное автоматическое обновление завершится неудачей, продукт ESET может начать полное обновление. Это все еще автоматическое обновление с гарантией функциональности, но вместо файла .dip будет загружен файл .fur, который имеет больший размер. Для версии 9.0.2032.2 он составляет 27 МБ. Однако такой сценарий встречается редко.

## **Будет ли обновление ESET Endpoint Antivirus выпущено с ограничением? Если да, как долго к обновлению применяется ограничение после выпуска?**

Компания ESET применяет ограничение к обновлениям в течение первых нескольких недель после выпуска новой версии, чтобы снизить нагрузку на наши серверы и равномерно распространить новую версию.

## **Автоматическое обновление станет одним из основных способов обновления. Как оно работает в деталях?**

Компания ESET стремится к тому, чтобы как можно больше клиентов использовали автоматическое обновление. Большое количество более ранних версий сложно поддерживать. Функция автоматического обновления работает просто — при первой проверке на наличие обновления модуля загружаются .dnp-файлы. В процессе обновления продукт находится в полностью рабочем состоянии и защищает компьютер. Новая версия активируется после перезапуска. В решении ESET PROTECT (на стороне сервера) с помощью политики можно указать самую позднюю версию, до которой следует выполнять обновление. Дополнительные сведения см. в главе «Автоматическое обновление» в онлайн-справке для [ESET PROTECT](#) или [ESET PROTECT Cloud](#).

## **Правильно ли, что автоматическое обновление работает с соотношением 1/10? Сейчас я использую решение ESET Endpoint Security 8.0.2028.1. До какой версии оно будет обновлено в случае запуска автоматического обновления?**

Автоматическое обновление продуктов может происходить с задержкой из-за ограничения, применяемого на серверах репозитория. Если обновление программы выпускается с ограничением, оно может стать доступным для автоматического обновления не сразу. Если обновление считается безопасным и стабильным, ограничение может быть сокращено или удалено полностью, чтобы все оставшиеся клиенты могли обновиться.

Процедура ограничения может иметь разную длительность для каждого обновления. Она зависит от того, какое количество клиентов запрашивает обновление, каков трафик на наших серверах, а также от других факторов. Эта процедура постоянно дорабатывается, и все время происходят изменения.

## **Когда начнется автоматическое обновление, если я запускаю компьютер в 8:45 и выключаю его в 17:00?**

Автоматическое обновление начнется при следующем успешном обновлении модуля по расписанию, но не более одного раза каждые 24 часа.

## Когда обновление будет запущено в следующий раз, если компьютер будет выключен во время автоматического обновления?

Обновление будет запущено во время следующего окна обновления по расписанию. Для процедуры автоматического обновления используется надежный отказоустойчивый механизм (ранее — iRSU). После загрузки обновления и перезапуска компьютера обновленные файлы все еще находятся в состоянии готовности к использованию, а установленная в данный момент версия обеспечивает непрерывную защиту. Изменения применяются после следующего запуска продукта ESET Endpoint.

## Каким образом можно незамедлительно запустить автоматическое обновление, не дожидаясь регулярного подключения, которое происходит один раз в сутки? Существует ли альтернатива для функции «Проверить наличие обновлений»?

Процедуру автоматического обновления можно запустить вручную, только открыв главное окно программы и щелкнув **Обновление > Проверить наличие обновлений**. Во всех других способах запуска обновления модулей используется 24-часовая политика планировщика автоматического обновления. Удаленно запустить загрузку автоматического обновления сейчас невозможно. Мы добавим эту функцию в будущем.

## Выполнение обновления ESET Endpoint Antivirus

Обновлять ESET Endpoint Antivirus 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, перейдите в раздел **Инструменты > [Планировщик](#)**.

## 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.

## Создание задачи в планировщике

Чтобы создать новую задачу, выберите **Служебные программы > Планировщик**, а затем нажмите кнопку **Добавить задачу** или щелкните правой кнопкой мыши и в контекстном меню выберите команду **Добавить**. Доступно пять типов задач.

- **Запуск внешнего приложения:** планирование выполнения внешнего приложения.
- **Обслуживание журнала:** в файлах журнала также содержатся остатки удаленных записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.
- **Проверка файлов при загрузке системы:** проверка файлов, исполнение которых разрешено при запуске или входе пользователя в систему.
- **Создать снимок состояния компьютера:** создание снимка состояния компьютера в [ESET SysInspector](#), для которого собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого из них.
- **Сканирование компьютера по требованию:** сканирование файлов и папок на компьютере.
- **Обновление:** планирование задачи обновления путем обновления модулей.

Поскольку **Обновление** - одна из самых часто используемых запланированных задач, ниже описан порядок добавления задачи обновления.

В раскрывающемся меню **Запланированная задача** выберите пункт **Обновление**. Введите имя задачи в поле **Имя задачи** и нажмите кнопку **Далее**. Выберите частоту выполнения задачи. Доступны указанные ниже варианты. **Однократно, Многократно, Ежедневно, Еженедельно и При определенных условиях. Установите флажок Пропускать задачу, если устройство работает от аккумулятора**, чтобы свести к минимуму потребление системных ресурсов, когда ноутбук работает от аккумулятора. Задача будет выполняться в день и время, указанные в полях области **Выполнение задачи**. Затем укажите, какое действие следует предпринимать, если задача не может быть выполнена в установленное время. Доступны указанные ниже варианты.

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

На следующем этапе отображается окно сводной информации о текущей планируемой задаче. После внесения всех необходимых изменений нажмите **Готово**.

На экран будет выведено диалоговое окно, в котором можно выбрать профили, используемые для запланированной задачи. Здесь можно задать основной и вспомогательный профили. Вспомогательный профиль используется, если задачу невозможно выполнить с применением основного профиля. Подтвердите внесенные изменения, нажав кнопку **Готово**, после чего новая задача появится в списке существующих запланированных задач.

# Планирование еженедельного сканирования компьютера

Чтобы запланировать регулярную задачу, откройте [главное окно программы](#) > **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 щелкните **Добавить задачу**.
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 Antivirus к ESET PROTECT

Если после установки ESET Endpoint Antivirus 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 ESET PROTECT 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 Antivirus](#)

## 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.

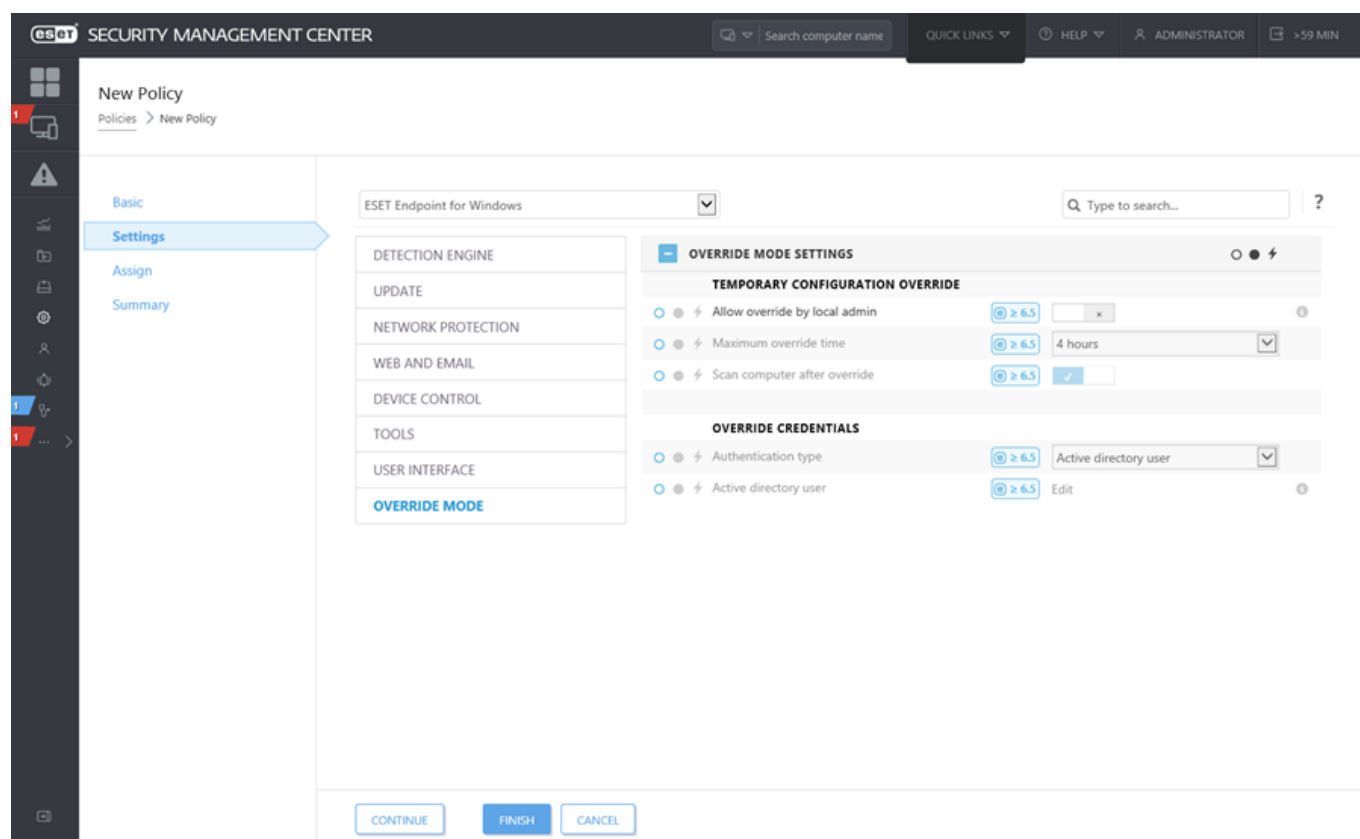
Если режим переопределения включен, его нельзя отключить с помощью веб-консоли ESET PROTECT. Он будет отключен автоматически, когда закончится период времени переопределения. Кроме того, его можно отключить на клиентском компьютере.

**!** Пользователю, который использует режим переопределения, нужно также иметь права администратора Windows. В противном случае пользователь не может сохранить изменения настроек ESET Endpoint Antivirus.

Групповая аутентификация Active Directory поддерживается.

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 ESET PROTECT, 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 ESET PROTECT 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, когда необходимость в ней исчезнет.

## Применение рекомендуемой политики для ESET Endpoint Antivirus

После подключения ESET Endpoint Antivirus к ESET PROTECT лучше всего применить рекомендуемую [политику](#) или пользовательскую политику.

Для ESET Endpoint Antivirus 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 <a href="#">облачную систему репутации и обратной связи ESET LiveGrid®</a> , чтобы улучшить обнаружение новейших угроз и предоставлять сведения о вредоносных и неизвестных потенциальных угрозах для дальнейшего анализа. |




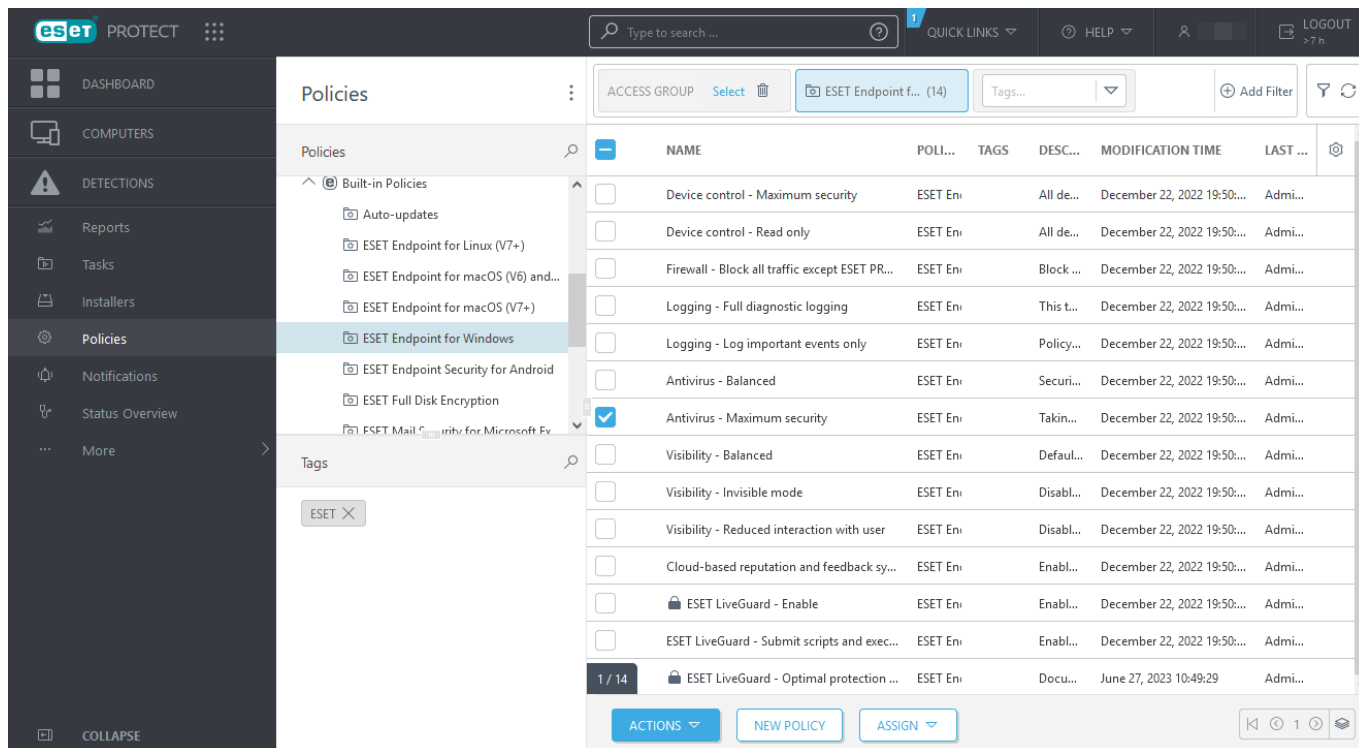
| Политика   | Описание  |
|--|---|
| Контроль устройств — максимальная безопасность                                     | Все устройства блокируются. Когда с устройства инициируется подключение, требуется разрешение администратора.   |
| Контроль устройств — только для чтения   | Все устройства доступны только для чтения. Запись запрещена.  |
| Файервол — блокировать весь трафик, кроме соединения с ESET PROTECT и ESET Inspect | Блокировка всего трафика, кроме подключения к ESET PROTECT и <a href="#">серверу ESET Inspect</a> (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, <a href="#">ThreatSense</a> 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, <a href="#">графический интерфейс</a> , интеграция в контекстное меню не отображаются. Файл <code>egui.exe</code> не запускается. Программа предназначена для управления только через <a href="#">ESET PROTECT Cloud</a> .   |
| 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 Antivirus, установленного на рабочих станциях, выполните следующие действия.

Следующие статьи из базы знаний ESET могут быть доступны только на английском языке:

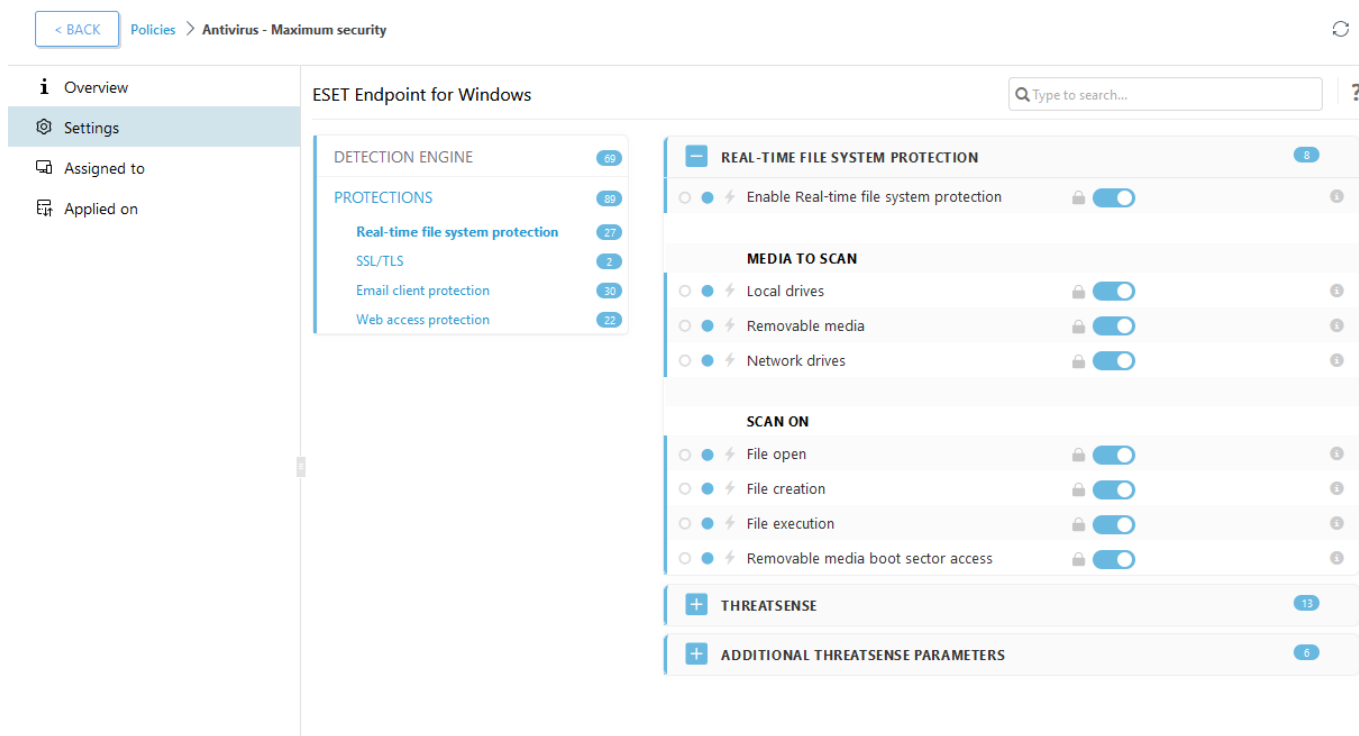
**i** [Применение рекомендуемой или предварительно заданной политики для ESET Endpoint Antivirus с помощью ESET PROTECT](#)

1. Откройте веб-консоль ESET PROTECT.
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 ESET PROTECT см. здесь](#)



# Настройка зеркала


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

 На зеркале обновлений создаются копии файлов обновления, которые можно использовать для обновления рабочих станций с решением ESET Endpoint Antivirus для Windows того же поколения (например, ESET Endpoint Antivirus для Windows версии 10.x создает файлы обновления только для версии 10.x решений ESET Endpoint Antivirus для Windows и ESET Endpoint Security для Windows).

## Настройка ESET Endpoint Antivirus 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. здесь:

-  [Зеркало обновлений](#)
- [Обновление с зеркала](#)

## 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 вам не нужно предоставлять обновления модулей через внутренний HTTP-сервер, отключите параметр **Включить HTTP-сервер**.

## Как мне обновить свою систему до Windows 10, если у меня установлен продукт ESET

# Endpoint Antivirus?



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.

## Версии на других языках:

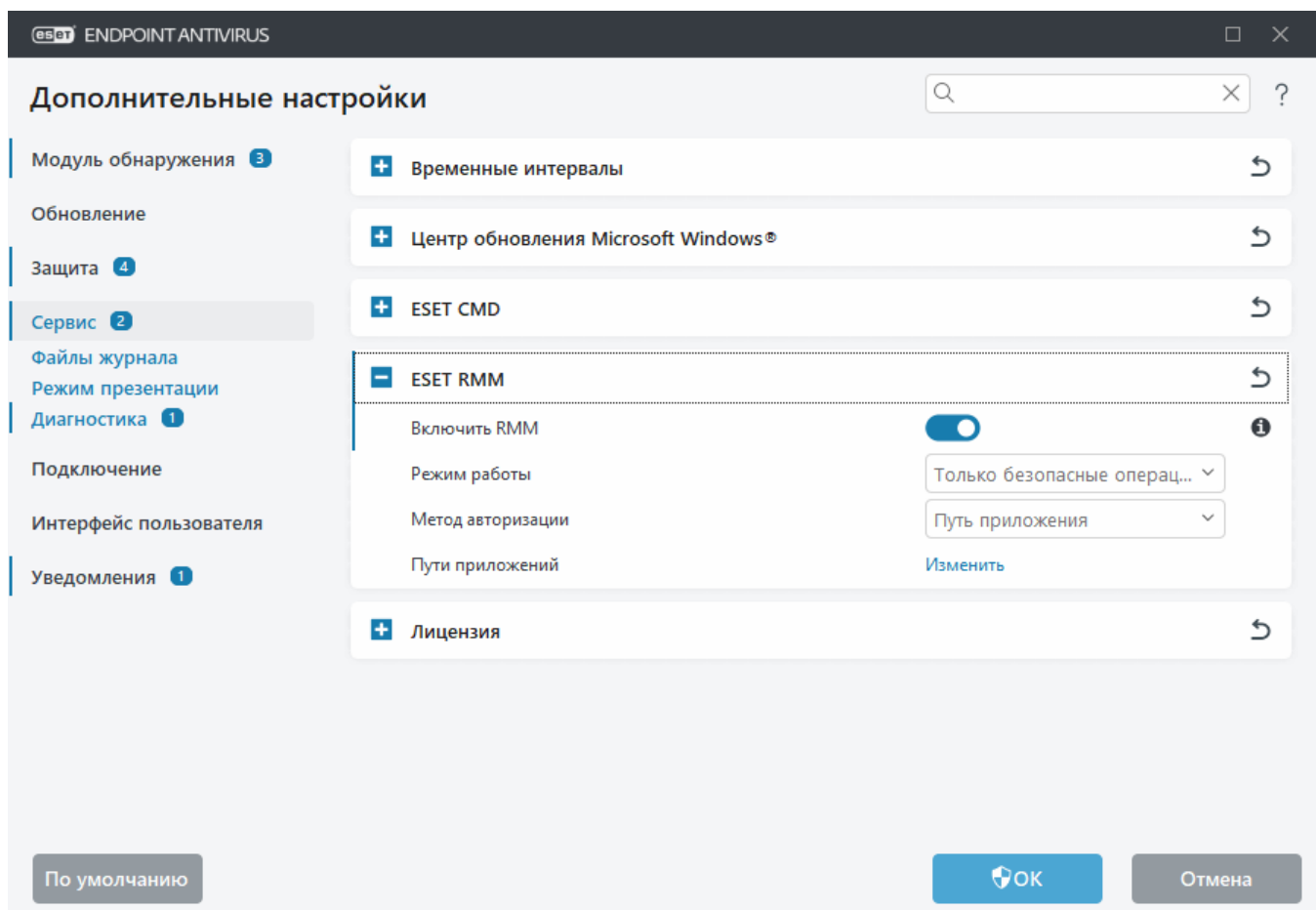
Если вы ищете версию продукта ESET для конечных точек на другом языке, посетите нашу [страницу загрузок](#).



[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 Antivirus начиная с версии 6.6.2028.0.




Компонент ESET RMM по умолчанию отключен. Чтобы включить ESET RMM, откройте раздел [Расширенные параметры](#) > **Средства** > **ESET RMM** и включите переключатель рядом с элементом **Включить RMM**.

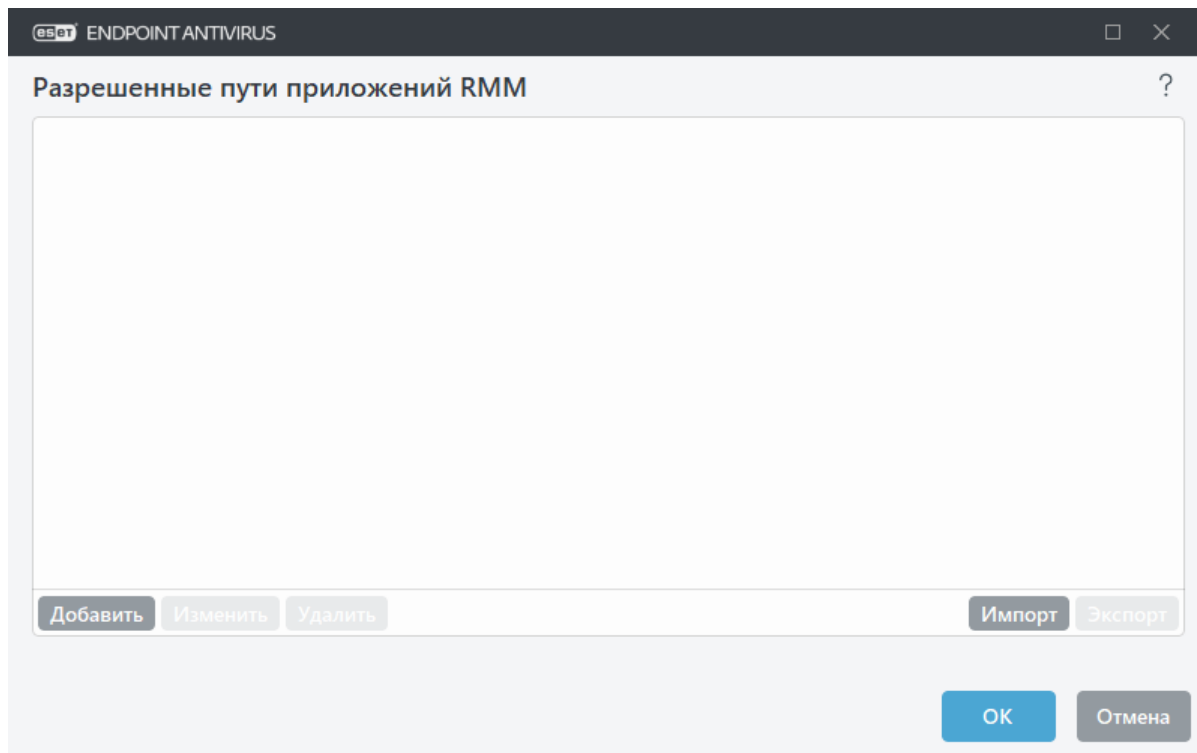
**Режим работы:** выберите **Только безопасные операции**, чтобы разрешить интерфейс RMM только для безопасных операций и операций, которым разрешено только чтение. Выберите **Все операции**, чтобы разрешить интерфейс RMM для всех операций.

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

- `ermm.exe` — это разработанная компанией ESET программа командной строки, которая позволяет управлять продуктами для конечных точек и обмениваться данными с любым подключаемым модулем RMM.
- Подключаемый модуль RMM — это стороннее приложение, работающее локально в системе Endpoint Windows. Он предназначен для обмена данными с определенным агентом RMM (например, только Kaseya) и с исполняемым файлом `ermm.exe`.
- Агент RMM — это стороннее приложение (например, от компании Kaseya), работающее локально в системе Endpoint Windows. Агент обменивается данными с подключаемым модулем RMM и сервером RMM.

## 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 щелкните **Изменить** или **Добавить**, чтобы создать или изменить 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 применении ползунка**. В раскрывающемся меню выберите **серьезность регистрируемых событий**. ESET PROTECT может собирать записи с детализацией **Предупреждение**.



Уровни детализации журнала «Информация» и «Предупреждение» доступны только для правил, которые содержат как минимум два компонента без подстановочных знаков в домене. Например:

- \*.domain.com/\*
- \*www.domain.com/\*

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* блокирует загрузку всех сжатых 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 Antivirus

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](#).

## Лицензионное соглашение с конечным пользователем

Вступает в силу с 19 октября 2021 года.

**ВАЖНО!** Внимательно прочитайте изложенные далее условия использования программного продукта, прежде чем загружать, устанавливать, копировать или использовать его.

**ЗАГРУЖАЯ, УСТАНОВЛИВАЯ, КОПИРУЯ ИЛИ ИСПОЛЬЗУЯ ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВЫ ВЫРАЖАЕТЕ СВОЕ СОГЛАСИЕ С ИЗЛОЖЕННЫМИ УСЛОВИЯМИ И С [ПОЛИТИКОЙ КОНФИДЕНЦИАЛЬНОСТИ](#).**

Лицензионное соглашение с конечным пользователем

Согласно условиям данного Лицензионного соглашения с конечным пользователем («Соглашение»), заключенного компанией ESET, spol. s r. o., зарегистрированной по адресу Einsteinova 24, 85101 Bratislava, Slovak Republic, внесенной в коммерческий регистр окружного суда Bratislava I, раздел Sro, запись № 3586/B, BIN 31333532 (ESET или Поставщик) и вами, физическим или юридическим лицом (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 и Политики конфиденциальности. Если Вы не согласны с каким-либо из условий настоящего Соглашения или Политики конфиденциальности, немедленно выберите вариант отмены, отмените установку или загрузку, уничтожьте или верните Программное обеспечение, установочные носители, сопроводительную документацию, а также квитанцию об оплате Поставщику 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 (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 (Лицензия).

**а) 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.

**б) 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 («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 Конечный пользователь 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.

**с) Выпуск для дома или для бизнеса.** Версия Программного обеспечения для дома должна использоваться исключительно в личной и/или некоммерческой среде и предназначена только для домашнего и семейного использования. Для использования Программного обеспечения в коммерческих средах, а также на почтовых серверах, серверах ретрансляции электронной почты, почтовых шлюзах и шлюзах Интернета необходимо приобрести версию Программного обеспечения для бизнеса.

**д) Срок Лицензии.** Ваше право на использование Программного обеспечения ограничено определенным сроком.

**е) Программное обеспечение, получаемое через изготовителей комплектного оборудования.** Программное обеспечение, классифицированное как OEM (распространяется через изготовителей комплектного оборудования), можно использовать только на том компьютере, на котором оно было получено. Такое программное обеспечение нельзя перенести на другой компьютер.

**ф) 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.

**г) 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 незамедлительно за собственный счет удалить, уничтожить или вернуть Программное обеспечение и все его резервные копии в компанию ESET или в точку продажи, 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.

**а) Обновление Программного обеспечения.** Поставщик имеет право время от времени выпускать обновления Программного обеспечения (далее — «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 Политикой конфиденциальности.

Предоставление любых Обновлений может регулироваться политикой в отношении окончания срока службы (далее — «Политика ОСС»), которая доступна по адресу [https://go.eset.com/eol\\_business](https://go.eset.com/eol_business). После наступления даты окончания срока службы, которая устанавливается политикой ОСС для Программного обеспечения или какой-либо из его функций, Обновления предоставляться не будут.

**б) 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 («Заражения»), и отправляют их Поставщику, в том числе, среди прочего, информацию о процессе установки, о Компьютере и/или платформе, на которых установлено Программное обеспечение, а также информацию об операциях и функциональности Программного обеспечения («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, получают 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.

**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.

а) 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.

б) 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.

с) 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(а). 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. Ваше право на использование Программного обеспечения и любых его функций может регулироваться политикой в отношении окончания срока службы. После наступления даты окончания срока службы, которая устанавливается политикой в отношении окончания срока службы для Программного обеспечения или какой-либо из его функций, ваше право на использование Программного обеспечения прекратится. 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 УСТАНОВКИ, 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. После наступления даты окончания срока службы, которая устанавливается политикой ОСС для Программного обеспечения или какой-либо из его функций, техническая поддержка предоставляться не будет. 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.**

а) 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 («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

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.

(Законодательные акты, упомянутые в пунктах i и ii выше, совместно именуются «Законодательство по регулированию внешней торговли».)

б) 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 а) 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.

с) 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, возвращаемые Программное обеспечение и документация должны быть доставлены по адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, что не ограничивает право ESET сообщать Вам о любых изменениях в настоящем Соглашении, политиках конфиденциальности, политике в отношении окончания срока службы и документации в соответствии со статьей 22 настоящего Соглашения. ESET может отправлять Вам письма по электронной почте и уведомления в Программном обеспечении, а также публиковать сообщения на нашем веб-сайте. Вы соглашаетесь получать юридически значимые сообщения от компании ESET в электронной форме, в том числе любые сообщения об изменении Условий, Специальных условий или Политик конфиденциальности, любые предложения и принятие условий договоров, приглашения вести переговоры о заключении договора, уведомления или другие юридически значимые сообщения. Такие электронные сообщения считаются полученными в письменной форме, если только действующее законодательство не требует другого формата коммуникации.

**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. Настоящее Соглашение составлено на английском языке. В случае подготовки перевода настоящего Соглашения для удобства или любой иной цели либо при наличии любых расхождений между разными языковыми версиями настоящего Соглашения преимуществом обладает версия на английском языке.

Компания ESET оставляет за собой право вносить изменения в Программное обеспечение и пересматривать условия настоящего Соглашения, приложений и дополнений к нему, Политики конфиденциальности, Политики ОСС и документации или какой-либо их части в любое время путем обновления соответствующего документа (а) для отображения изменений в Программном обеспечении либо в способе осуществления деятельности компанией ESET, (б) для соблюдения нормативно-правовых норм или из соображений безопасности либо (в) для недопущения нарушений или нанесения вреда. В случае изменения настоящего Соглашения Вы будете уведомлены с помощью электронной почты, уведомления в приложении или другими электронными средствами. Если Вы не согласны с предлагаемыми изменениями к настоящему Соглашению, Вы можете расторгнуть его в соответствии со статьей 10 в течение 30 дней после получения уведомления об изменении. Если Вы не расторгнете настоящее Соглашение в течение этого срока, предлагаемые изменения будут считаться принятыми и вступят в силу в отношении Вас с даты получения Вами уведомления об изменении.

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.

EULAID: EULA-PRODUCT-LG; 3537.0

## 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 Наши 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:

озараженные 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;

оинформацию об устройствах в локальной сети, например тип, производитель, модель и/или название;

осведения о пользовании Интернетом, например IP-адрес, географическое расположение, пакеты IP, URL-адреса и кадры Ethernet;

офайлы 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