kaspersky

Kaspersky Endpoint Security

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 12.12.0.522

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 17.02.2026

Обозначение документа: 643.46856491.00100-10 90 01

© 2026 АО "Лаборатория Касперского"

https://www.kaspersky.ru
https://help.kaspersky.com/ru
https://support.kaspersky.ru

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

kaspersky

Содержание

Об этом документе 11
Источники информации о программе 12
О программе 13
Требования 14
Аппаратные и программные требования 14
Указания по эксплуатации и требования к среде 17
Установка программы с помощью мастера 19
Активация программы с помощью мастера активации программы 25
Удаление приложения 27
Процедура приемки 28
Безопасное состояние 28
Проверка работоспособности. Тестовый файл EICAR 28
Проверка работоспособности Защиты от веб-угроз 28
Проверка работоспособности Защиты от файловых угроз 30
Проверка работоспособности антивирусной проверки 31
Проверка работоспособности функции контроля запуска программ 32
Проверка работоспособности функции контроля подключения устройств 33
Разделение доступа к функциям программы по пользовательским ролям 36
Управление приложением через Консоль администрирования Kaspersky Security Center 38
О плагине управления Kaspersky Endpoint Security для Windows 38
Особенности использования защищенных протоколов для взаимодействия с внешними службами 39
Настройка локальных параметров приложения 40
Управление задачами 41
Управление политиками 44
Создание политики 45
Индикатор уровня защиты 49
Интерфейс приложения 51
Значок приложения в области уведомлений 53
Упрощенный интерфейс приложения 55
Настройка отображения интерфейса приложения 55
Запуск и остановка Kaspersky Endpoint Security 57
Приостановка и возобновление защиты и контроля компьютера 60
Поиск вредоносного ПО 62
Проверка компьютера 63
Проверка съемных дисков при подключении к компьютеру 70
Фоновая проверка 72
Проверка из контекстного меню 73
Проверка целостности приложения 77

Формирование области проверки ... 78
Запуск проверки по расписанию ... 80
Запуск проверки с правами другого пользователя ... 83
Оптимизация проверки ... 83
Обновление баз и модулей программы ... 86
Схема обновления с серверного хранилища ... 87
Запуск и остановка задачи обновления ... 90
Запуск задачи обновления с правами другого пользователя ... 91
Выбор режима запуска для задачи обновления ... 91
Добавление источника обновлений ... 92
Обновление модулей приложения ... 95
Использование прокси-сервера при обновлении ... 96
Откат последнего обновления ... 99
Обновление антивирусных баз в ручном режиме ... 100
Устранение уязвимостей и установка критических обновлений в приложении ... 101
Технология лечения активного заражения ... 102
Лечение активных угроз на рабочих станциях ... 104
Лечение активных угроз на серверах ... 105
Устранение необработанных угроз ... 106
Kaspersky Security Network ... 109
Включение и выключение использования Kaspersky Security Network ... 110
Ограничения работы с Локальным KSN ... 110
Включение и выключение облачного режима для компонентов защиты ... 111
Проверка репутации файла в Kaspersky Security Network ... 112
Анализ поведения ... 115
Защита от шифрования ... 117
Включение и выключение защиты папок общего доступа от внешнего шифрования ... 118
Настройка периода блокировки недоверенного компьютера ... 119
Формирование области защиты ... 119
Добавление доверенных компьютеров для внешнего шифрования данных ... 120
Откат вредоносных действий ... 122
Защита от эксплойтов ... 124
Включение и выключение Защиты от эксплойтов ... 124
Защита памяти системных процессов ... 126
Предотвращение вторжений ... 127
Включение и выключение Предотвращения вторжений ... 128
Работа с группами доверия приложений ... 129
Изменение группы доверия для приложения ... 129
Настройка прав группы доверия ... 130
Выбор группы доверия для приложений, запускаемых до Kaspersky Endpoint Security ... 131

Выбор группы доверия для неизвестных приложений ... 131
Выбор группы доверия для приложений с цифровой подписью ... 132
Работа с правами приложений ... 132
Защита ресурсов ОС и персональных данных ... 135
Удаление информации о неиспользуемых приложениях ... 136
Мониторинг работы Предотвращения вторжений ... 137
Защита доступа к аудио и видео ... 137
Защита от файловых угроз ... 139
Включение и выключение Защиты от файловых угроз ... 139
Автоматическая приостановка Защиты от файловых угроз ... 142
Изменение действия компонента Защита от файловых угроз над зараженными файлами ... 143
Формирование области защиты компонента Защита от файловых угроз ... 144
Использование методов проверки ... 145
Использование технологий проверки в работе компонента Защита от файловых угроз ... 146
Оптимизация проверки файлов ... 147
Проверка составных файлов ... 147
Изменение режима проверки файлов ... 148
Проверка контейнеров ... 149
Защита от веб-угроз ... 151
Включение и выключение Защиты от веб-угроз ... 152
Настройка методов обнаружения вредоносных веб-адресов ... 154
Анти-Фишинг ... 156
Формирование списка доверенных веб-адресов ... 157
Защита от почтовых угроз ... 158
Включение и выключение Защиты от почтовых угроз ... 159
Изменение действия над зараженными сообщениями электронной почты ... 162
Формирование области защиты компонента Защита от почтовых угроз ... 163
Проверка составных файлов, вложенных в сообщения электронной почты ... 164
Фильтрация вложений в сообщениях электронной почты ... 165
Защита от сетевых угроз ... 167
Включение и выключение Защиты от сетевых угроз ... 167
Блокирование атакующего компьютера ... 168
Настройка адресов исключений из блокирования ... 170
Настройка Защиты от сетевых угроз по типам ... 171
Защита от атак BadUSB ... 173
Включение и выключение Защиты от атак BadUSB ... 174
Использовании экранной клавиатуры при авторизации USB-устройств ... 174
Авторизация сканеров штрихкода ... 175
AMSI-защита ... 177
Включение и выключение AMSI-защиты ... 178

Оптимизация проверки файлов AMSI-защитой 179
Проверка защищенных соединений 181
Включение проверки защищенных соединений 181
Установка доверенных корневых сертификатов 185
Проверка защищенных соединений с недоверенным сертификатом 186
Добавление сертификата "Лаборатории Касперского" в собственное хранилище сертификатов 187
Исключение защищенных соединений из проверки 188
Контроль приложений 191
Ограничения функциональности Контроля приложений 195
Включение режима блокирования только запрещенных приложений 196
Контроль приложений на основе эталонного компьютера 198
Действия с правилами Контроля приложений в интерфейсе приложения 201
Добавление правила Контроля приложений 203
Добавление условия срабатывания в правило Контроля приложений 204
Изменение статуса правила Контроля приложений 205
Тестирование правил Контроля приложений 206
Мониторинг активности приложений 206
Правила формирования масок имен файлов или папок 207
Изменение шаблонов сообщений Контроля приложений 208
Контроль устройств 210
Контроль доступа к устройствам по типу 213
О правилах доступа 214
Разграничение прав доступа пользователей к устройствам 216
Контроль доступа к устройствам по шине подключения 216
Контроль доступа к мобильным устройствам 217
Контроль доступа к Bluetooth-устройствам 221
Контроль печати 222
Контроль подключения к Wi-Fi 226
Мониторинг использования съемных дисков 229
Изменение периода кеширования 231
Добавление устройства в список доверенных из интерфейса приложения 232
Получение доступа к заблокированному устройству 232
Онлайн-режим предоставления доступа 234
Офлайн-режим предоставления доступа 235
Изменение шаблонов сообщений Контроля устройств 237
Анти-Бриджинг 239
Включение Анти-Бриджинга 240
Изменение статуса правила установки соединений 240
Изменение приоритета правила установки соединений 240

Адаптивный контроль аномалий 241
Обучение Адаптивного контроля аномалий 244
Включение и выключение правила Адаптивного контроля аномалий 245
Изменение действия при срабатывании правила Адаптивного контроля аномалий 245
Создание исключения для правила Адаптивного контроля аномалий 246
Применение обновлений для правил Адаптивного контроля аномалий 248
Изменение шаблонов сообщений Адаптивного контроля аномалий 248
Мониторинг работы Адаптивного контроля аномалий 249
Веб-Контроль 252
Добавление правила доступа к веб-ресурсам 254
Фильтр по содержанию веб-ресурсов 258
Фильтр по адресам веб-ресурсов 261
Проверка работы правил доступа к веб-ресурсам 262
Мониторинг активности пользователей в интернете 264
Изменение шаблонов сообщений Веб-Контроля 268
Правила формирования масок адресов веб-ресурсов 270
Контроль сетевых портов 273
Включение контроля всех сетевых портов 273
Формирование списка контролируемых сетевых портов 274
Формирование списка приложений, для которых контролируются все сетевые порты 275
Контроль целостности системы 277
О правилах Контроля целостности системы 278
Контроль целостности системы в режиме реального времени 280
Проверка целостности системы по запросу 283
Просмотр отчетов о работе Контроля целостности системы 289
Сброс статуса целостности системы 290
Анализ журналов 291
Настройка предустановленных правил 292
Добавление пользовательских правил 293
Endpoint Detection and Response Optimum 295
Интеграция с Kaspersky Endpoint Detection and Response 295
Поиск индикаторов компрометации (стандартная задача) 298
Расширенный сбор телеметрии для поиска IOC 303
Помещение файла на карантин 304
Получение файла 306
Удаление файла 308
Запуск процесса 309
Завершение процесса 311
Запрет запуска объектов 312
Сетевая изоляция компьютера 315

Доверенная зона 320
Создание исключения из проверки 320
Создание исключения по типу обнаруживаемых объектов 326
Формирование списка доверенных приложений 326
Работа с приложениями, подписанными доверенной цифровой подписью 331
Работа с резервным хранилищем 332
Настройка максимального срока хранения файлов в резервном хранилище 332
Настройка максимального размера резервного хранилища 333
Восстановление файлов из резервного хранилища 334
Удаление резервных копий файлов из резервного хранилища 335
Работа с карантином 336
Настройка максимального размера карантина 336
Передача данных о файлах на карантине в Kaspersky Security Center 337
Восстановление файлов из карантина 338
Служба уведомлений 339
Настройка параметров журналов событий 339
Настройка отображения и доставки уведомлений 340
Настройка отображения предупреждений о состоянии приложения в области уведомлений 341
Работа с отчетами 342
Просмотр отчетов 344
Настройка максимального срока хранения отчетов 344
Настройка максимального размера файла отчета 345
Сохранение отчета в файл 345
Удаление информации из отчетов 346
Самозащита Kaspersky Endpoint Security 347
Включение и выключение механизма самозащиты 348
Включение и выключение поддержки AM-PPL 349
Защита служб приложения от внешнего управления 351
Обеспечение работы приложений удаленного администрирования 352
Защита паролем 352
Включение Защиты паролем 356
Предоставление разрешений для отдельных пользователей или групп 357
Использование временного пароля для предоставления разрешений 358
Отзыв временного пароля 360
Особенности разрешений Защиты паролем 361
Сброс пароля KLAdmin 363
Защита подключения к Серверу администрирования 364
Производительность Kaspersky Endpoint Security и совместимость с другими приложениями 369
Включение и выключение режима энергосбережения 370
Включение и выключение режима передачи ресурсов другим приложениям 372

Создание и использование конфигурационного файла ... 373
Восстановление параметров приложения по умолчанию ... 375
Работа с приложением из командной строки ... 376
Setup. Установка приложения ... 376
Setup /x. Удаление приложения ... 385
msiexec /i. Восстановление приложения ... 386
Команды AVP ... 387
SCAN. Поиск вредоносного ПО ... 389
UPDATE. Обновление баз и модулей приложения ... 393
ROLLBACK. Откат последнего обновления ... 395
TRACES. Трассировка ... 396
START. Запуск профиля ... 397
STOP. Остановка профиля ... 398
STATUS. Статус профиля ... 399
STATISTICS. Статистика выполнения профиля ... 399
RESTORE. Восстановление файлов из резервного хранилища ... 400
EXPORT. Экспорт параметров приложения ... 401
IMPORT. Импорт параметров приложения ... 402
ADDKEY. Применение файла ключа ... 403
LICENSE. Лицензирование ... 404
RENEW. Приобретение лицензии ... 406
EXIT. Завершение работы приложения ... 406
EXITPOLICY. Выключение политики ... 407
STARTPOLICY. Включение политики ... 407
DISABLE. Выключение защиты ... 407
SPYWARE. Обнаружение шпионского ПО ... 407
KSN. Переключение KSN / KPSN ... 408
SERVERBINDINGDISABLE. Выключение защиты подключения к серверу ... 409
Команды KESCLI ... 410
Scan. Поиск вредоносного ПО ... 411
GetScanState. Статус выполнения проверки ... 412
GetLastScanTime. Определения времени выполнения проверки ... 412
GetThreats. Получение данных об обнаруженных угрозах ... 412
UpdateDefinitions. Обновление баз и модулей приложения ... 416
GetDefinitionState. Определение даты и времени последнего обновления баз ... 416
EnableRTP. Включение защиты ... 416
GetRealTimeProtectionState. Статус Защиты от файловых угроз ... 417
Version. Определение версии приложения ... 417
Команды управления Detection and Response ... 417
PREVENTION. Управление Запретом запуска объектов ... 418

ISOLATION. Управление Сетевой изоляцией 419
RESTORE. Восстановление файлов из карантина 419
IOCSCAN. Поиск индикаторов компрометации (IOC) 420
Сообщения об ошибках 428
Коды возврата 431
Коды ошибок 437
Использование профилей задач 443
Профили приложения 444
Действия после сбоя или неустранимой ошибки в работе приложения 446
Способы получения технической поддержки 447
Техническая поддержка через Kaspersky CompanyAccount 447
Обращение в Службу технической поддержки 448
О составе и хранении файлов трассировки 449
Трассировка работы приложения 452
Трассировка производительности приложения 453
Запись дампов 454
Защита файлов дампов и трассировок 455
Глоссарий 457
Информация о стороннем коде 463
Соответствие терминов 464
Приложение 1. Значения параметров программы в сертифицированной конфигурации 465
Приложение 2. Группы доверия приложений 469
Приложение 3. Расширения файлов для быстрой проверки съемных дисков 470
Приложение 4. Типы файлов для фильтра вложений Защиты от почтовых угроз 473
Приложение 5. Сетевые параметры для взаимодействия с внешними службами 476
Приложение 7. Поддерживаемые расширения файлов для Запрета запуска объектов 481
Приложение 8. Поддерживаемые интерпретаторы скриптов для Запрета запуска объектов 483
Приложение 9. Область поиска IOC в реестре (RegistryItem) 485
Приложение 10. Требования к IOC-файлам 486
Приложение 11. Учетные записи пользователей в правилах компонентов приложения 489
Приложение 12. Скрипт для создания папки Endpoint Agent 491

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Endpoint Security для Windows" (далее также "Kaspersky Endpoint Security", "приложение").

Подготовительные процедуры изложены в разделах "Подготовка к установке приложения", "Установка приложения", "Подготовка приложения к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки приложения, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки приложения.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование приложения, а также инструкции и указания по безопасному использованию приложения.

В документе также содержатся разделы с дополнительной информацией о приложении.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Endpoint Security, а также поддержка организаций, использующих Kaspersky Endpoint Security.

kaspersky

Источники информации о программе

Указанные источники информации о приложении (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Endpoint Security:

- страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Endpoint Security в Базе знаний;
- электронная справка.

Страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security (http://www.kaspersky.ru/business-security/endpoint-windows) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Endpoint Security в Базе знаний (https://support.kaspersky.ru/kes12) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

Электронная справка входит в состав программы Kaspersky Endpoint Security. Вы можете открыть справку по кнопке  или по клавише **F1**. В электронной справке вы можете найти описание параметров Kaspersky Endpoint Security.

kaspersky

О программе

Программное изделие "Kaspersky Endpoint Security для Windows" представляет собой средство антивирусной защиты (САВЗ) типов "Б", "В", "Г" второго класса защиты и средство контроля подключения съемных машинных носителей информации (СКН) второго класса защиты, с функциями аутентификации администратора безопасности и ограничения программной среды.

Объект оценки представляет собой программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации, предназначенное для применения на серверах или АРМ информационных систем, а также на автономных АРМ. Также в программном изделии реализованы функции для обеспечения контроля использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации для конкретных пользователей информационной системы.

Основными угрозами, для противостояния которым используется Kaspersky Endpoint Security, являются:

- угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и / или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ);
- угрозы, связанные с установкой на узлы информационной системы внутренними и внешними нарушителями незарегистрированного (неучтенного) потенциально вредоносного программного обеспечения;
- угрозы, связанные с подключением к информационной системе внутренними и внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей несанкционированной записью (передачей) на эти носители защищаемой информации из информационной системы или загрузкой в информационную систему с этих съемных машинных носителей информации вредоносного программного обеспечения.

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению ОО;
- управление работой ОО;
- управление параметрами ОО;
- управление установкой обновлений (актуализации) БД ПКВ ОО;
- аудит безопасности ОО;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация ОО;
- идентификация и аутентификация администратора безопасности;
- ограничение программной среды (управление запуском компонентов ПО, контроль доступа к веб-ресурсам);
- контроль подключения съемных машинных носителей информации.

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы приложения, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования 14

Указания по эксплуатации и требования к среде 17

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- 2 ГБ свободного места на жестком диске;
- процессор:
  - рабочая станция – 1 ГГц;
  - сервер – 1.4 ГГц;
  - поддержка инструкций SSE2.

  Архитектура Arm не поддерживается.
- оперативная память:
  - рабочая станция (x86) – 1 ГБ;
  - рабочая станция (x64) – 2 ГБ;
  - сервер – 2 ГБ;
  - сервер для установки приложения со встроенным агентом для интеграции с Kaspersky Anti Targeted Attack Platform – 8 ГБ.
- Microsoft .NET Framework 4 или выше.
- для установки приложения необходимо владеть правами администратора на компьютере.

Рабочие станции

Поддерживаемые операционные системы для рабочих станций:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;

- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise / Enterprise multi-session;
- Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise.

Операционные системы Windows, начиная с версии 11 24H2, поддерживают технологию UDP Receive Segment Coalescing Offload (URO). Технология включена по умолчанию, если на компьютере установлены совместимая сетевая карта и драйверы. Отключение URO на компьютере пользователя может значительно снизить производительность приложения.
Для корректной работы Kaspersky Endpoint Security на компьютере пользователя должна быть запущена служба Windows Security Center (wscsvc).
Приложение Kaspersky Endpoint Security не может быть установлено на Microsoft Windows 7, если не установлены обновления операционной системы KB4490628 (обновление от 12 марта 2019) и KB4474419 (обновление от 23 сентября 2019). Подробнее см. в базе знаний Службы технической поддержки https://support.kaspersky.ru/common/error/installation/11004#block8.
Особенности поддержки операционной системы Microsoft Windows 10 вы можете узнать в базе знаний Службы технической поддержки https://support.kaspersky.ru/common/compatibility/13036.
Особенности поддержки операционной системы Microsoft Windows 11 вы можете узнать в базе знаний Службы технической поддержки https://support.kaspersky.ru/common/compatibility/15778.

Серверы

Kaspersky Endpoint Security поддерживает работу основных компонентов приложения на компьютерах под управлением операционной системы Windows для серверов. Вы можете использовать Kaspersky Endpoint Security для Windows вместо Kaspersky Security для Windows Server на серверах и кластерах организации (англ. Cluster Mode). Также приложение поддерживает режим основных серверных компонентов (англ. Server Core Mode) (см. известные ограничения https://support.kaspersky.com/help/KESWin/12.12/ru-RU/201943.htm).

Поддерживаемые операционные системы для серверов:

- Windows Small Business Server 2011 Essentials / Standard (64-разрядная);

  Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
- Windows Web Server 2008 R2 Service Pack 1 и выше;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core);
- Windows Server 2025 Standard / Datacenter.

Приложение Kaspersky Endpoint Security не может быть установлено на Microsoft Windows Server 2008 R2, если не установлены обновления операционной системы KB4490628 (обновление от 12 марта 2019) и KB4474419 (обновление от 23 сентября 2019).
Особенности поддержки операционной системы Microsoft Windows Server 2016 и Microsoft Windows Server 2019 вы можете узнать в базе знаний Службы технической поддержки https://support.kaspersky.ru/common/compatibility/13036.
Особенности поддержки операционной системы Microsoft Windows Server 2022 вы можете узнать в базе знаний Службы технической поддержки https://support.kaspersky.ru/common/compatibility/15778.

Неподдерживаемые операционные системы для серверов:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Microsoft Small Business Server 2008 Standard / Premium SP2 или выше.

Виртуальные платформы

Поддерживаемые виртуальные платформы для работы приложения в стандартном режиме:

- VMware Workstation Pro 17.6.4;
- VMware ESXi 8.0 Update 3g;
- Windows Server 2025;
- Citrix Virtual Apps and Desktops 7 2503;
- Citrix Provisioning 2503.1;
- XenServer 8.4.

Виртуальные машины для установки Легкого агента

BIOS на защищаемой виртуальной машине должен поддерживать спецификацию SMBIOS версии 2.1 или выше.

На виртуальных машинах для установки Легкого агента должны быть установлены следующие пакеты и утилиты:

- При использовании Microsoft Hyper-V – пакет служб интеграции (Integration Services).
- При использовании VMware vSphere – пакет VMware Tools.
- При использовании XenServer – пакет XenTools.
- При использовании HUAWEI FusionSphere – пакет HUAWEI Tools.
- При использовании KVM, OpenStack, VK Private Cloud, Облачная платформа ТИОНИКС, Astra Linux, Альт Сервер Виртуализации, Базис, Базис.DynamiX и Базис Dynamix Standard – QEMU Guest Agent.

Требования к виртуальной инфраструктуре для работы приложения в режиме Легкого агента см. в справке Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/help/KSVLA/6.1/ru-RU/254038.htm.

- Для корректной работы приложения необходимо использовать виртуализированный сетевой интерфейс с полосой пропускания не менее 100 Мбит/сек.

Поддержка Kaspersky Security Center

Kaspersky Endpoint Security поддерживает работу со следующими версиями Kaspersky Security Center:

- Kaspersky Security Center 14;
- Kaspersky Security Center 14.1;
- Kaspersky Security Center 14.2;
- Kaspersky Security Center Linux 14.2;
- Kaspersky Security Center Linux 15;
- Kaspersky Security Center Windows 15.1;
- Kaspersky Security Center Linux 15.1;
- Kaspersky Security Center Linux 15.2;
- Kaspersky Security Center Linux 15.3;
- Kaspersky Security Center Linux 15.4;
- Kaspersky Security Center Linux 16;
- Kaspersky Security Center Linux 16.1.

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление приложением должны осуществляться в соответствии с эксплуатационной документацией.
2. Приложение должно эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации приложения необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ приложения ко всем объектам информационной системы, которые необходимы приложению для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость приложения с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы приложения со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлено приложение.

8. Должна быть обеспечена синхронизация по времени между компонентами приложения, а также между приложением и средой его функционирования.
9. Персонал, ответственный за функционирование приложения, должен обеспечивать надлежащее функционирование приложения, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между приложением и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование приложения должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности приложения.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности приложения.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным приложения, должно предоставляться только уполномоченным ролям (администраторам приложения и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

Установка программы с помощью мастера

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы.

► *Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы,*

скопируйте файл setup_kes.exe, входящий в комплект поставки, на компьютер пользователя и запустите его.

Запустится мастер установки программы.

Подготовка к установке

В сертифицированной конфигурации Kaspersky Endpoint Security перед установкой программы вам нужно создать папку `%AllUsersProfile%\Application Data\Kaspersky Lab\Endpoint Agent\`. Далее вам необходимо предоставить доступ к новой папке только для учетной записи SYSTEM. Запретите удаление этой папки и изменение прав доступа. Перед установкой программы убедитесь, что права на чтение и запись в эту папку имеет только учетная запись SYSTEM. Для автоматической настройки прав доступа к папке вы можете использовать скрипт, который приведен в Приложении 12.

Перед установкой Kaspersky Endpoint Security на компьютер или обновлением предыдущей версии приложения проверяются следующие условия:

- наличие программного обеспечения, с которым у приложения Kaspersky Endpoint Security могут быть проблемы совместимости (список ПО приведен в файле incompatible.txt в комплекте поставки);
- выполнение аппаратных и программных требований;
- наличие Microsoft .NET Framework;
- наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление. Например, уведомление о наличии несовместимого ПО (см. рис. ниже).

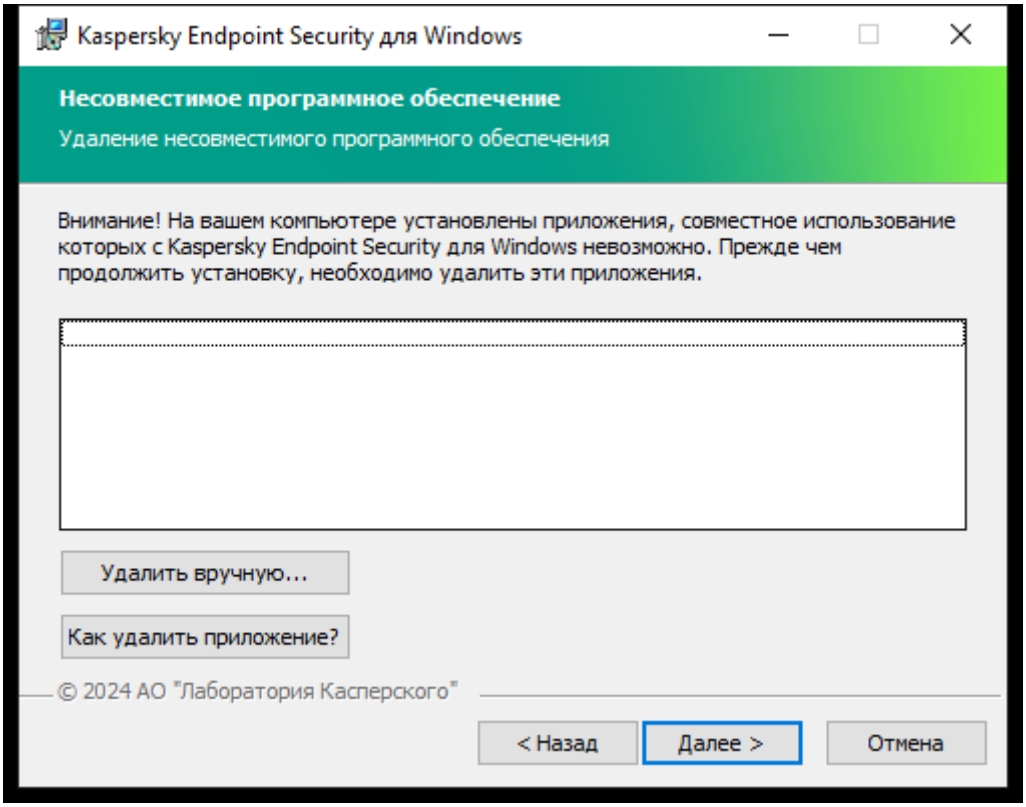


Рисунок 1. Удаление несовместимого обеспечения

Если компьютер соответствует предъявляемым требованиям, мастер установки приложения выполняет поиск приложений "Лаборатории Касперского", одновременная работа которых может привести к возникновению конфликтов. Если такие приложения найдены, вам предлагается удалить их вручную.

Если в числе обнаруженных приложений есть предыдущие версии Kaspersky Endpoint Security, то все данные, которые могут быть мигрированы (например, информация об активации, параметры приложения), сохраняются и используются при установке Kaspersky Endpoint Security 12.12 для Windows, а предыдущая версия приложения автоматически удаляется. Это относится к следующим версиям приложения:

- Kaspersky Endpoint Security для Windows 11.10.0 (сборка 11.10.0.399).
- Kaspersky Endpoint Security для Windows 11.11.0 (сборка 11.11.0.452).
- Kaspersky Endpoint Security для Windows 12.0 (сборка 12.0.0.465).
- Kaspersky Endpoint Security для Windows 12.1 (сборка 12.1.0.506).
- Kaspersky Endpoint Security для Windows 12.2 (сборка 12.2.0.462).
- Kaspersky Endpoint Security для Windows 12.3 (сборка 12.3.0.493).
- Kaspersky Endpoint Security для Windows 12.4 (сборка 12.4.0.467).
- Kaspersky Endpoint Security для Windows 12.5 (сборка 12.5.0.539).
- Kaspersky Endpoint Security для Windows 12.6 (сборка 12.6.0.438).
- Kaspersky Endpoint Security для Windows 12.7 (сборка 12.7.0.533).
- Kaspersky Endpoint Security для Windows 12.8 (сборка 12.8.0.505).
- Kaspersky Endpoint Security для Windows 12.9 (сборка 12.9.0.384).

- Kaspersky Endpoint Security для Windows 12.10 (сборка 12.10.0.466).
- Kaspersky Endpoint Security для Windows 12.11 (сборка 12.11.0.637).

Конфигурация Kaspersky Endpoint Security

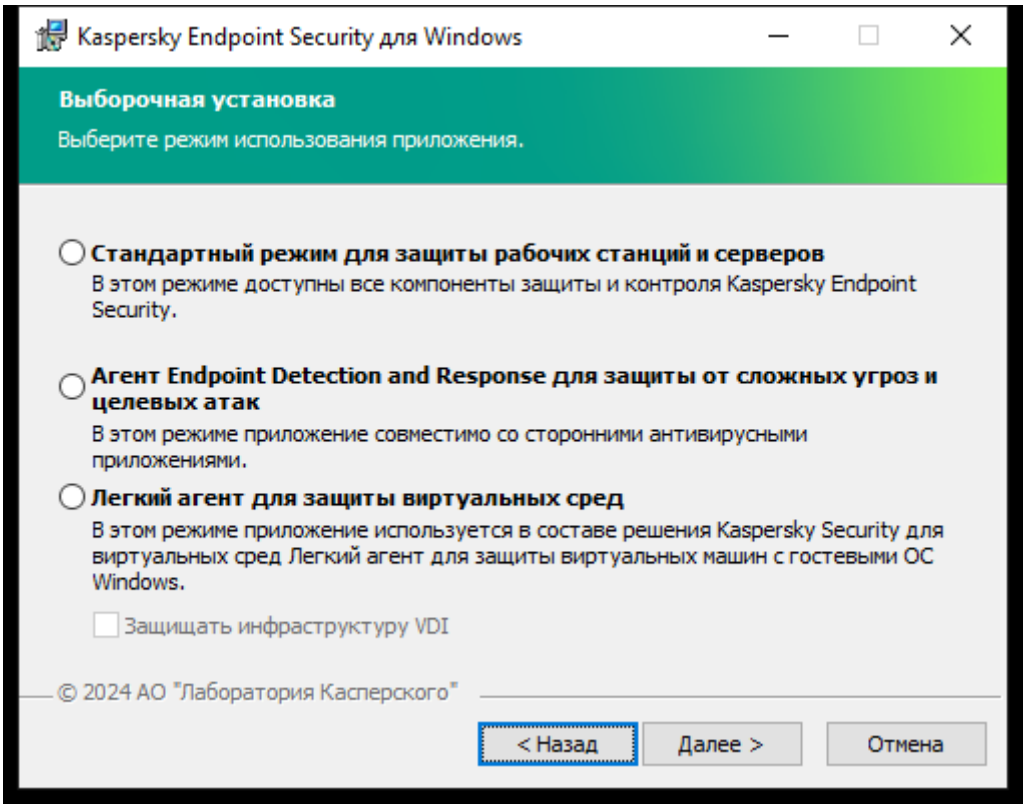


Рисунок 2. Выбор компонентов для установки приложения

Стандартный режим. Конфигурация по умолчанию. В этой конфигурации вам доступны все компоненты приложения, включая компоненты для работы решений Detection and Response. Эта конфигурация нужна для развертывания комплексной защиты компьютера от различного вида угроз, сетевых и мошеннических атак.

Агент Endpoint Detection and Response. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premise), а также KUMA. Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.

В сертифицированной конфигурации приложения интеграция с Kaspersky Managed Detection and Response не поддерживается. Включение интеграции с Kaspersky Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.

Легкий агент для защиты виртуальных сред. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. В этой конфигурации недоступны компоненты шифрования данных и Адаптивный контроль аномалий. Если вы

устанавливаете Легкий агент на шаблон виртуальных машин, из которого вы будете создавать *временные виртуальные машины*, установите флажок **Защищать инфраструктуру VDI** (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин.

Выберите конфигурацию **Стандартный режим**.

Компоненты Kaspersky Endpoint Security

В процессе установки вы можете выбрать компоненты Kaspersky Endpoint Security, которые вы хотите установить.

Для установки сертифицированной конфигурации программы Kaspersky Endpoint Security необходимо исключить установку компонента Сетевой экран (см. рис. ниже).

Выберите следующие компоненты для установки:

- Ядро программы;
- Продвинутая защита:
  - Анализ поведения;
  - Защита от эксплойтов;
  - Отказ вредоносных действий;
  - Предотвращение вторжений (только для рабочей станции).
- Базовая защита:
  - Защита от файловых угроз;
  - Защита от почтовых угроз;
  - Защита от веб-угроз;
  - Защита от сетевых угроз;
  - Защита от атак BadUSB;
  - AMSI-защита.
- Контроль безопасности:
  - Веб-Контроль;
  - Контроль приложений;
  - Контроль устройств;
  - Адаптивный контроль аномалий (только для рабочей станции);
  - Анализ журналов (только для серверов);
  - Контроль целостности системы (только для серверов).
- Коннектор к Агенту администрирования.

Для установки сертифицированной конфигурации программы Kaspersky Endpoint Security в составе решения Kaspersky Endpoint Detection and Response Optimum необходимо выбрать компонент Endpoint Detection and Response Optimum.

Вы можете изменить состав компонентов после установки программы. Для этого вам нужно запустить мастер установки повторно и выбрать операцию изменения состава компонентов.

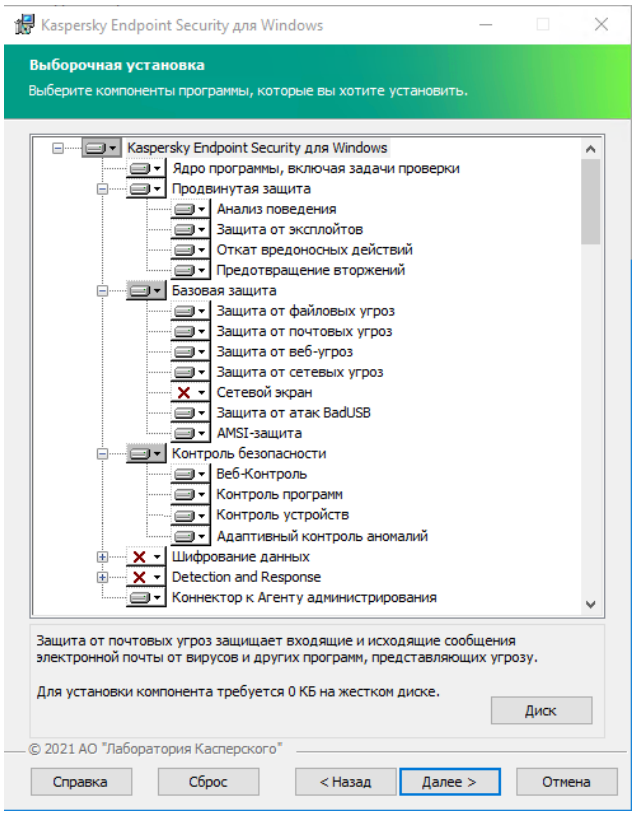


Рисунок 3. Сертифицированная конфигурация программы для рабочей станции

Выбор папки для установки приложения

Вы можете изменить путь установки Kaspersky Endpoint Security на клиентском компьютере. По умолчанию приложение устанавливается в папку `%ProgramFiles(x86)%\Kaspersky Lab\KES.12.12`.

Настройка доверенной зоны

Начиная с версии Kaspersky Endpoint Security для Windows 12.6 в доверенную зону добавлены предустановленные исключения из проверки (см. раздел "Создание исключения из проверки" на стр. 320) и доверенные приложения (см. раздел "Формирование списка доверенных приложений" на стр. 326). Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах.

Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена установка приложения в режиме Легкого агента для защиты виртуальных сред. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMware.

Вы также можете настроить доверенную зону позднее в свойствах политики: исключения из проверки (см. раздел "Создание исключения из проверки" на стр. 320) и доверенные приложения (см. раздел "Формирование списка доверенных приложений" на стр. 326).

Дополнительные параметры

Защищать процесс установки приложения. Защита установки включает в себя защиту от подмены дистрибутива вредоносными приложениями, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами приложения. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку приложения (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).

Обеспечить совместимость с Citrix PVS. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security на виртуальную машину.

Добавить путь к файлу avp.com в системную переменную %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки.

Активация программы с помощью мастера активации программы

Активация программы должна быть выполнена на компьютере с актуальными системными датой и временем. При изменении системных даты и времени после активации программы ключ становится неработоспособным. Программа переходит к режиму работы без обновлений, и Kaspersky Security Network недоступен. Восстановить работоспособность ключа можно только переустановкой операционной системы.

► *Чтобы активировать приложение, выполните следующие действия:*

1. В главном окне приложения перейдите в раздел **Лицензия**.
2. Нажмите на кнопку **Активировать приложение по новой лицензии**.

   Запустится мастер активации приложения. Следуйте указаниям мастера активации приложения.

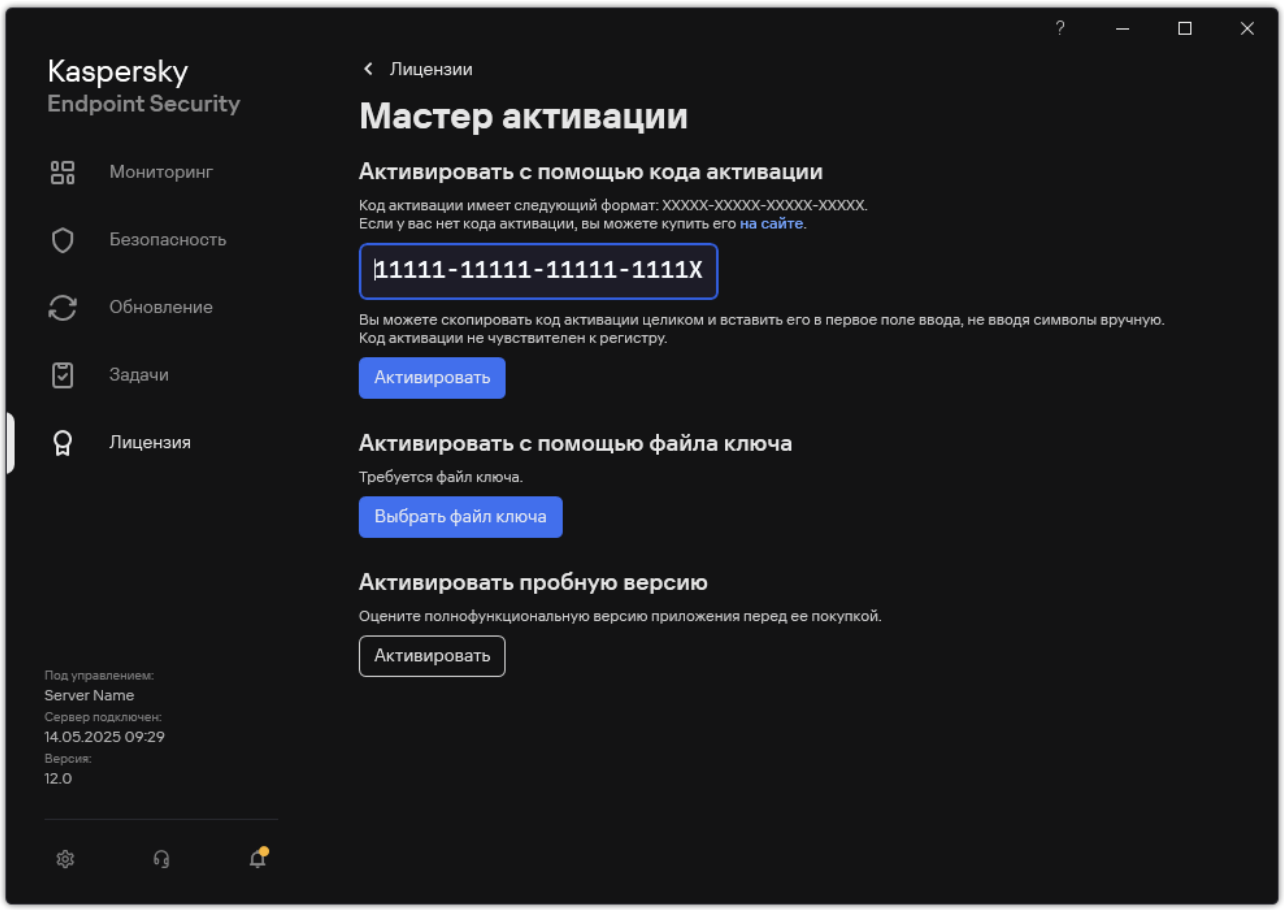


Рисунок 4. Активация приложения

В сертифицированной версии программы Kaspersky Endpoint Security допускается только активация файлом ключа. Иные способы активации ведут к выходу из безопасного состояния программы.

3. В блоке **Активировать с помощью файла ключа** нажмите на кнопку **Выбрать файл ключа**.

   Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу. Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

4. В открывшемся окне выберите файл ключа.

   Kaspersky Endpoint Security покажет информацию о лицензии: тип лицензии, срок действия лицензии и другая информация.

5. Нажмите на кнопку **Активировать**.

В результате на компьютер будет добавлен лицензионный ключ (см. рис. ниже).

Удаление приложения

► *Чтобы удалить Kaspersky Endpoint Security с помощью мастера установки приложения, выполните следующие действия:*

1. Откройте системное приложение Windows *Панель управления*.
2. В окне **Панель управления** выберите пункт **Программы и компоненты**.
3. В списке установленных приложений выберите элемент **Kaspersky Endpoint Security для Windows**.
4. Нажмите на кнопку **Удалить/Изменить**.

   Запустится мастер установки приложений.
5. В окне мастера установки приложения **Изменение, восстановление или удаление программы** нажмите на кнопку **Удаление**.
6. Следуйте указаниям мастера установки приложения.

kaspersky

Процедура приемки

Перед вводом приложения в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние 28

Проверка работоспособности. Тестовый файл EICAR 28

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение 1. Значения параметров программы в сертифицированной конфигурации" на стр. 465).

Проверка работоспособности. Тестовый файл EICAR

Чтобы проверить работоспособность программы, вы можете использовать тестовый файл EICAR.

Тестовый файл EICAR предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый файл EICAR не является вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR.

Проверка работоспособности Защиты от веб-угроз

Проверку работоспособности Защиты от веб-угроз не рекомендуется выполнять в браузере Edge. У браузера Edge есть встроенная система безопасности. Браузер Edge блокирует тестовый вредоносный веб-сайт раньше Kaspersky Endpoint Security. Для проверки работоспособности Защиты от веб-угроз используйте браузер Explorer.

► *Чтобы проверить работоспособность Защиты от веб-угроз, выполните следующие действия:*

1. Включите защиту виртуальной машины от веб-угроз.
   a. В главном окне программы нажмите на кнопку ⚙.
   b. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.
   c. В правой части окна настройки программы убедитесь, что переключатель **Защита от веб-угроз** включен.
   d. Сохраните внесенные изменения.
2. В окне браузера перейдите по ссылке на тестовый вредоносный веб-сайт.

   Kaspersky Endpoint Security сообщает о запрете доступа, отобразив уведомление в окне браузера (см. рис. ниже).

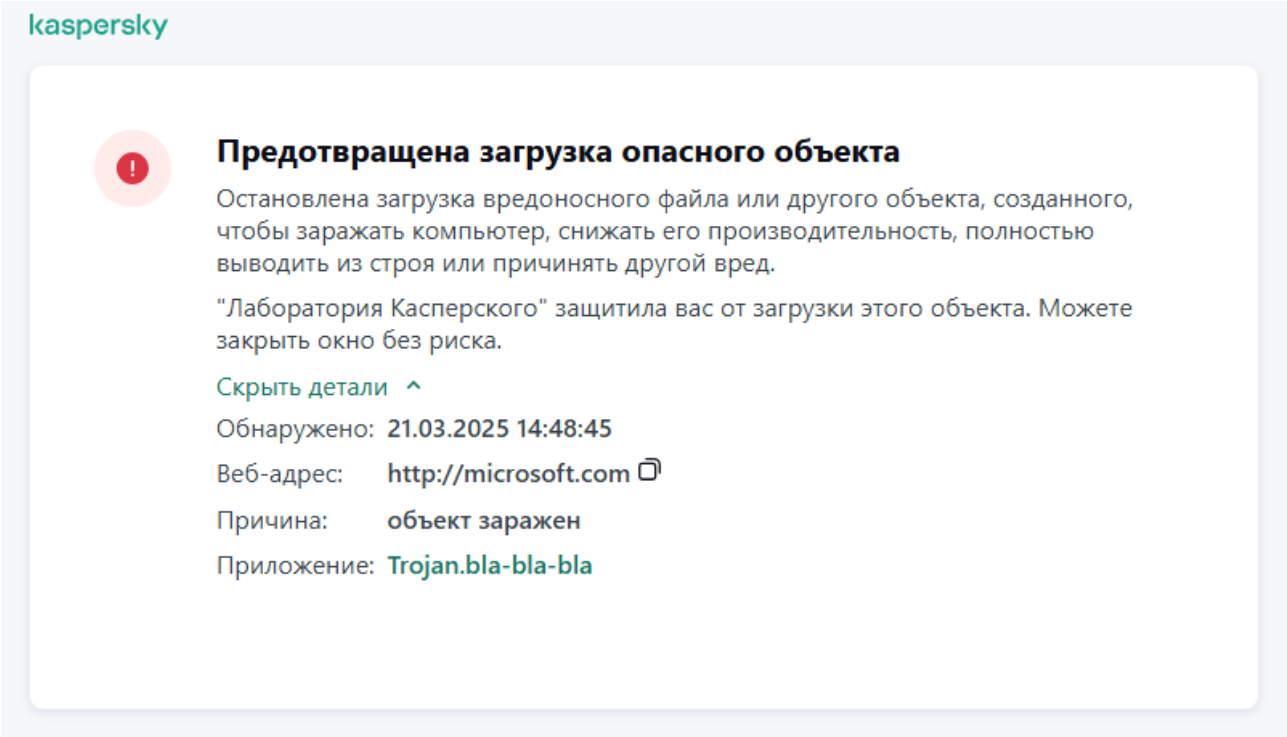


Рисунок 5. Сообщение о запрете доступа к веб-сайту

3. Проверьте информацию в отчете об обнаруженных вирусах:
   a. В главном окне программы в разделе **Мониторинг** нажмите на плитку **Отчеты**.
   b. В открывшемся окне перейдите в раздел **Защита от веб-угроз**.
   c. Убедитесь, что в отчете присутствует сообщение об обнаружении вируса и информация об этом событии верна (см. рис. ниже).

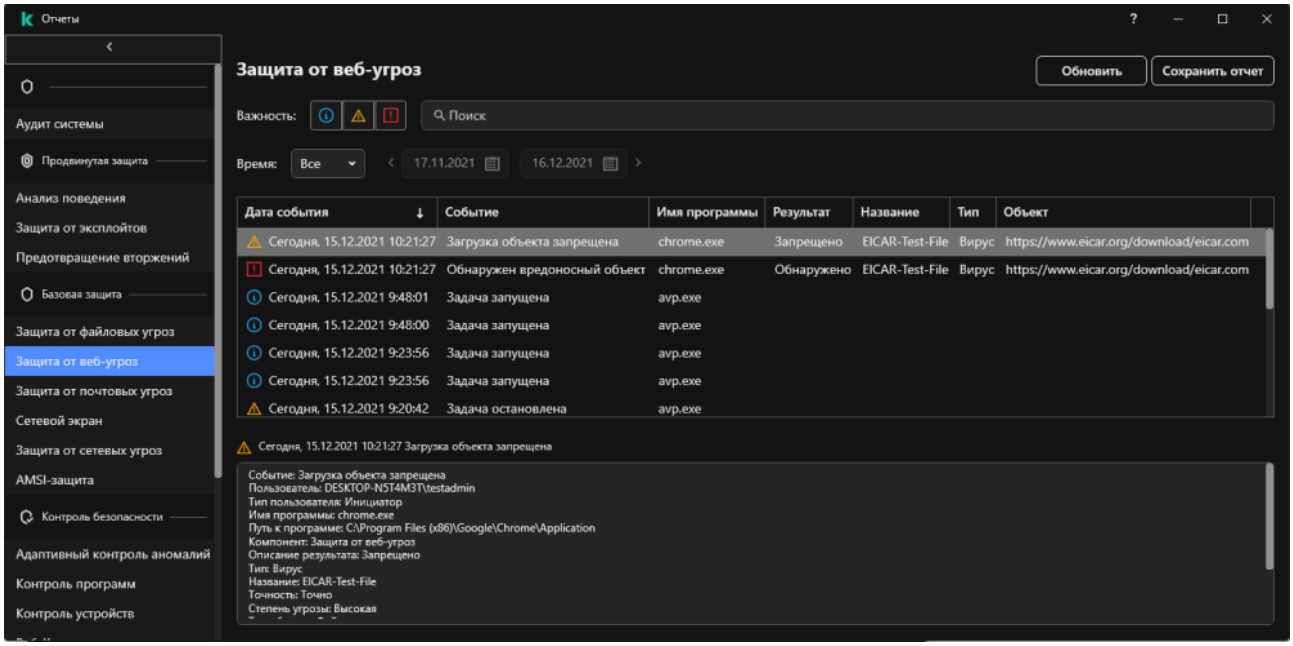


Рисунок 6. Отчет Защиты от веб-угроз

Проверка работоспособности Защиты от файловых угроз

► *Чтобы проверить работоспособность Защиты от файловых угроз, выполните следующие действия:*

1. Отключите защиту виртуальной машины от веб-угроз:

   Этот шаг необходим для успешного размещения на виртуальной машине тестового файла, иначе он будет мгновенно удален программой.

   a. В главном окне программы нажмите на кнопку ⚙.

   b. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.

   c. В правой части окна настройки программы выключите переключатель **Защита от веб-угроз**.

   d. Сохраните внесенные изменения.

2. Загрузите тестовый файл EICAR (http://eicar.org/download/eicar.com.txt) и разместите его в новую папку на системном диске виртуальной машины.

3. Перейдите в папку с тестовым файлом, загруженным на шаге, и запустите его.

   Kaspersky Endpoint Security удаляет тестовый файл с виртуальной машины.

4. Проверьте информацию в отчете об обнаруженных вирусах:

   a. В главном окне программы в разделе **Мониторинг** нажмите на плитку **Отчеты**.

   b. В открывшемся окне перейдите в раздел **Защита от файловых угроз**.

   c. Убедитесь, что в отчете отображается верная информация об обнаружении зараженного файла (время события, путь к файлу).

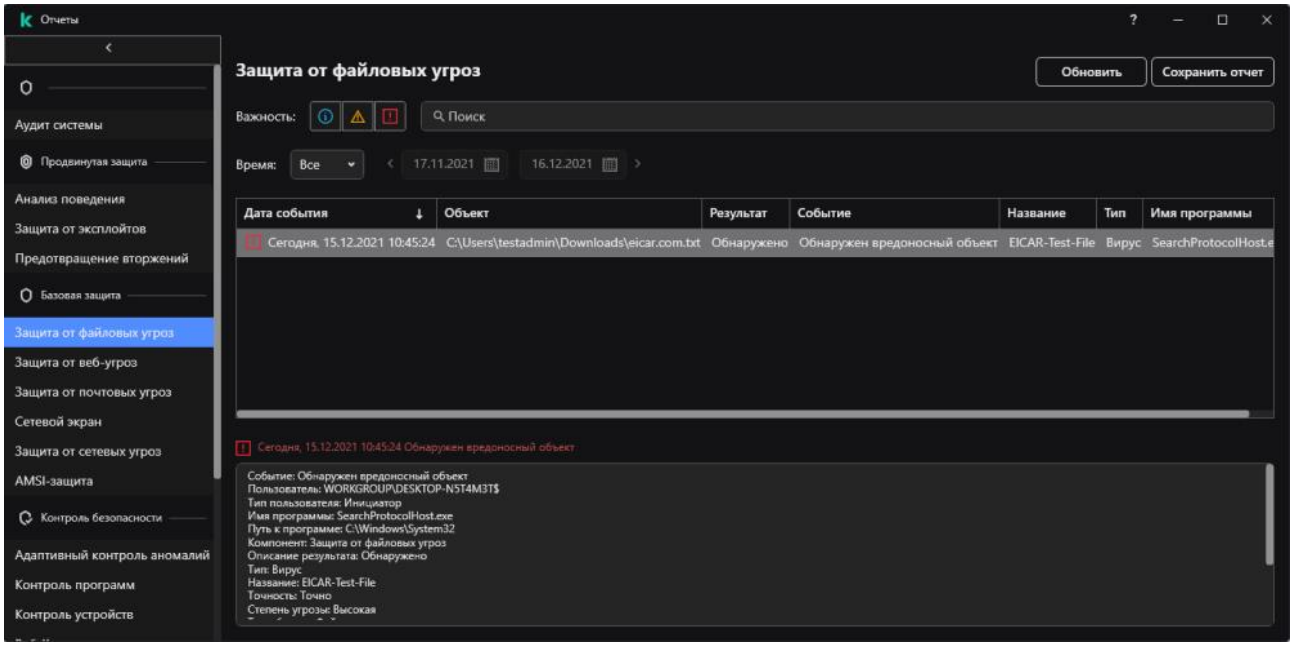


Рисунок 7. Отчет Защиты от файловых угроз

Проверка работоспособности антивирусной проверки

► *Что проверить работоспособность функции антивирусной проверки, выполните следующие действия:*

1. Отключите защиту виртуальной машины:

   Этот шаг необходим для успешного размещения на виртуальной машине тестового файла, иначе он будет мгновенно удален программой.

   a. В главном окне программы нажмите на кнопку ⚙.

   b. В окне параметров программы выберите раздел **Базовая защита** → **Защита от веб-угроз**.

   c. В правой части окна настройки программы выключите переключатель **Защита от веб-угроз**.

   d. Сохраните внесенные изменения.

2. Загрузите тестовый файл EICAR (http://eicar.org/download/eicar.com.txt) и разместите его в новую папку на системном диске виртуальной машины.

3. Добавьте в область проверки папку с тестовым файлом EICAR:

   a. В главном окне программы перейдите в раздел **Задачи**.

   b. В открывшемся окне выберите виджет задачи **Выборочная проверка**.

   c. Нажмите на кнопку **Выбрать** и добавьте в область проверки папку с тестовым файлом EICAR.

      В виджете задачи будет добавлена информация о количестве выбранных объектов для проверки.

4. В виджете задачи выборочной проверки нажмите на кнопку **Запустить проверку**.

5. По окончании выполнения задачи проверки проверьте информацию в отчете об обнаруженных вирусах:
   a. В главном окне программы в разделе **Мониторинг** нажмите на плитку **Отчеты**.
   b. В открывшемся окне перейдите в раздел **Проверка**.
   c. Убедитесь, что в отчете отображается верная информация об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности функции контроля запуска программ

Перед проверкой работоспособности функции контроля запуска программ установите программу для тестирования, например, Notepad++. Контроль программ по умолчанию разрешает запуск программ для правила *Операционная система и ее компоненты*. Это правило включает в себя программы, такие как Блокнот, Explorer, WordPad и другие. Специалисты "Лаборатории Касперского" не рекомендует выключать правило *Операционная система и ее компоненты*, так как возможна некорректная работа операционной системы и пользовательских программ.

► *Чтобы проверить работоспособность функции контроля запуска программ, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** → **Контроль программ**.
3. Включите переключатель **Контроль программ**.
4. В блоке **Действие при запуске запрещенных программ** выберите **Блокировать запуск программ, запрещенных правилами**.
5. В блоке **Режим контроля запуска программ** выберите значение **Список запрещенных**.

   Если выбран этот вариант, Контроль программ разрешает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля программ.
6. Нажмите на кнопку **Запрещенные программы**.

   Откроется список правил Контроля программ.
7. Нажмите на кнопку **Добавить**.

   Откроется окно для добавления условий контроля программы.
8. На закладке **Общие настройки** задайте основные параметры правила:
   a. В поле **Название правила** укажите произвольное имя.
   b. В поле **Описание** введите описание правила.
   c. Убедитесь, что в таблице **Субъекты и их права** для пользователей из группы **Все** установлено значение **Запрещено**.
9. На закладке **Условия** добавьте условие срабатывания правила.
   a. Нажмите на кнопку **Добавить**.

      Запустится мастер добавления условия для работы правила.

b. Выберите вариант **Условие вручную** и перейдите на следующий шаг.

c. Выберите вариант **Метаданные**, установите флажок **Название файла,** в поле ввода введите `Notepad++.exe`.

d. Сохраните внесенные изменения.

10. Запустите программу Notepad++.
11. Убедитесь, что запуск программы запрещен (см. рис. ниже).

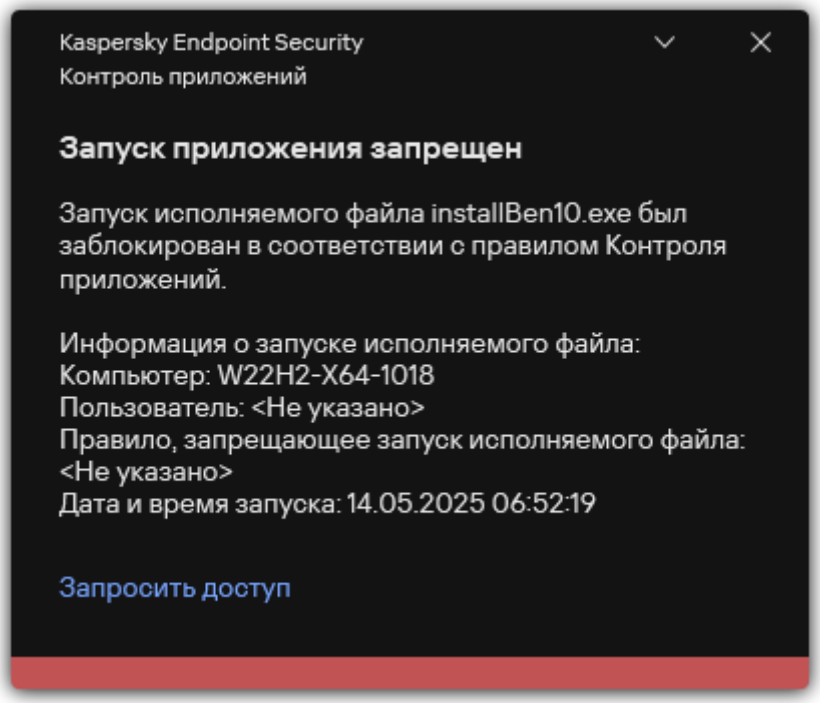


Рисунок 8. Уведомление Контроля программ

12. Проверьте информацию в отчете:

a. В главном окне программы в разделе **Мониторинг** нажмите на плитку **Отчеты**.

b. В открывшемся окне перейдите в раздел **Контроль программ**.

c. Убедитесь, что в отчете присутствует сообщение о запрете запуска программы Notepad++ и информация об этом событии верна.

Проверка работоспособности функции контроля подключения устройств

Перед проверкой работоспособности функции контроля подключения устройств подготовьте устройство для тестирования, например, съемный диск. Контроль устройств по умолчанию разрешает подключение всех устройств.

► *Чтобы проверить работоспособность функции контроля подключения устройств, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** → **Контроль устройств**.
3. Включите переключатель **Контроль устройств**.
4. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

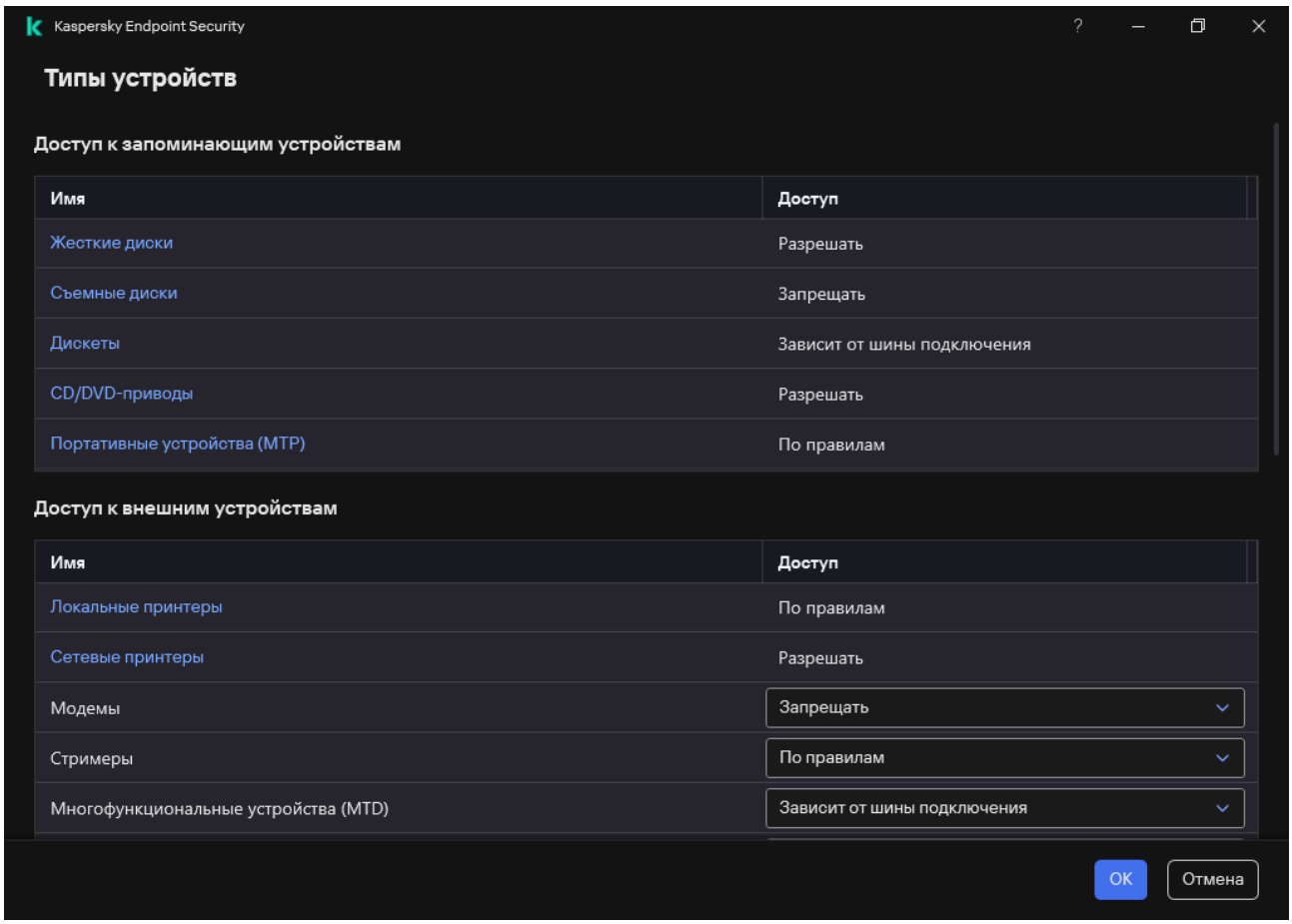


Рисунок 9. Типы устройств Контроля устройств

5. В блоке **Доступ к запоминающим устройствам** выберите правило доступа **Съемные диски**.

   Откроются свойства правила доступа к съемным дискам.
6. В графе **Доступ** выберите значение **Запрещать**.

   Контроль устройств работает в режиме Списка разрешенных устройств. В этом режиме Контроль устройств запрещает пользователям подключение любых съемных дисков, кроме доверенных устройств (см. раздел "Добавление устройства в список доверенных из интерфейса приложения" на стр. 232).
7. Сохраните внесенные изменения.
8. Подключите съемный диск к компьютеру.

9. Убедитесь, что доступ к устройству запрещен (см. рис. ниже).

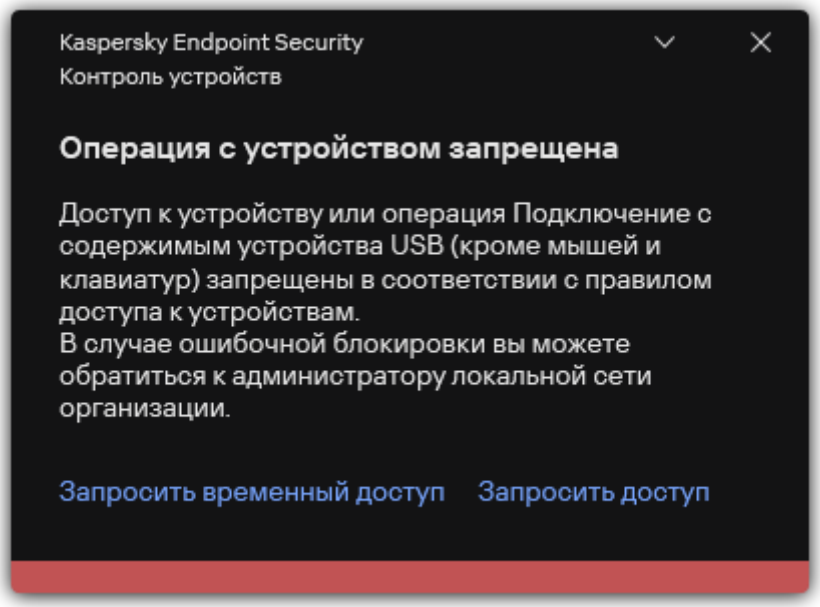


Рисунок 10. Уведомление Контроля устройств

10. Проверьте информацию в отчете:
    a. В главном окне программы в разделе **Мониторинг** нажмите на плитку **Отчеты**.
    b. В открывшемся окне перейдите в раздел **Контроль устройств**.
    c. Убедитесь, что в отчете присутствует сообщение о запрете доступа к съемному диску и информация об этом событии верна.

kaspersky

Разделение доступа к функциям программы по пользовательским ролям

По умолчанию пользователи с ролью "Администратор Kaspersky Endpoint Security" в системе администрирования Kaspersky Security Center, имеют доступ ко всем функциям Kaspersky Endpoint Security.

Пользователи, которые имеют право **Изменение** в Kaspersky Endpoint Security, могут предоставлять доступ к функциям Kaspersky Endpoint Security другим пользователям, добавленным в Kaspersky Security Center или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Endpoint Security один из следующих предустановленных уровней доступа к функциям Kaspersky Endpoint Security:

- **Чтение** – возможность просматривать общие параметры работы Kaspersky Endpoint Security, параметры работы компонентов Kaspersky Endpoint Security, статистику работы Kaspersky Endpoint Security и права пользователей Kaspersky Endpoint Security.
- **Изменение** – доступ ко всем функциям приложения, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Endpoint Security, параметры работы компонентов Kaspersky Endpoint Security, а также просматривать статистику работы Kaspersky Endpoint Security и права пользователей Kaspersky Endpoint Security.
- **Выполнение** – возможность запускать и останавливать задачи Kaspersky Endpoint Security.
- **Выполнение операций с выборкой устройств** – возможность запускать и останавливать задачи Kaspersky Endpoint Security для выборки устройств.

Также вы можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к отдельным функциям Kaspersky Endpoint Security.

Таблица 1. Права доступа к функциям Kaspersky Endpoint Security

Функциональная область	Компонент Kaspersky Endpoint Security
Адаптивный контроль аномалий	Адаптивный контроль аномалий.
Антивирусная функциональность	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз Защита от сетевых угроз Сетевой экран AMSI-защита Защита от эксплойтов Анализ поведения Откат вредоносных действий
Контроль программ	Контроль приложений

Функциональная область	Компонент Kaspersky Endpoint Security
Базовая функциональность	Поиск вредоносного ПО Обновление баз / Откат обновления баз Проверка целостности Удаление данных Добавление ключа Установка Изменение состава компонентов Управление учетными записями Агента аутентификации
Обнаружение и реагирование	Endpoint Detection and Response (KATA) Network Detection and Response (KATA) Endpoint Detection and Response Optimum Endpoint Detection and Response Expert Kaspersky Sandbox Managed Detection and Response
Контроль устройств	Контроль устройств
Шифрование	Шифрование диска Kaspersky Шифрование диска BitLocker Шифрование файлов Шифрование съемных дисков
Предотвращение вторжений	Предотвращение вторжений
Исключения	Угрозы и исключения
Веб-Контроль	Веб-Контроль

kaspersky

Управление приложением через Консоль администрирования Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Security, настраивать параметры работы приложения, изменять состав компонентов приложения, добавлять ключи, запускать и останавливать задачи обновления и проверки.

Управление приложением через Kaspersky Security Center осуществляется с помощью плагина управления Kaspersky Endpoint Security.

Подробнее об управлении приложением через Kaspersky Security Center см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm.

В этом разделе

О плагине управления Kaspersky Endpoint Security для Windows 38

Особенности использования защищенных протоколов для взаимодействия с внешними службами 39

Настройка локальных параметров приложения 40

Управление задачами 41

Управление политиками 44

О плагине управления Kaspersky Endpoint Security для Windows

Плагин управления Kaspersky Endpoint Security для Windows обеспечивает взаимодействие Kaspersky Endpoint Security с Kaspersky Security Center. Плагин управления позволяет управлять Kaspersky Endpoint Security с помощью следующих инструментов: политики (см. раздел "Управление политиками" на стр. 44), задачи (см. раздел "Управление задачами" на стр. 41), а также локальные параметры приложения (см. раздел "Настройка локальных параметров приложения" на стр. 40). Для взаимодействия с Kaspersky Security Center Web Console предназначен веб-плагин.

Версия плагина управления может отличаться от версии приложения Kaspersky Endpoint Security, установленной на клиентском компьютере. Если в установленной версии плагина управления предусмотрено меньше функций, чем в установленной версии Kaspersky Endpoint Security, то параметры недостающих функций не регулируются плагином управления. Такие параметры могут быть изменены пользователем в локальном интерфейсе Kaspersky Endpoint Security.

Веб-плагин по умолчанию не установлен в Kaspersky Security Center Web Console. Веб-плагин требуется установить на компьютер с установленным приложением Kaspersky Security Center Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Web Console в браузере. Вы можете просмотреть список установленных веб-плагинов в интерфейсе Web Console

(**Параметры консоли** → **Веб-плагины**). Подробнее о совместимости версий веб-плагинов и Web Console см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm.

Если вы используете Kaspersky Endpoint Security в составе решения Kaspersky Endpoint Detection and Response Optimum, вам нужно установить плагин управления Kaspersky Endpoint Detection and Response. Плагин управления нужен для отображения деталей алерта. *Детали алерта* – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Таким образом, для создания задач реагирования на угрозы вам нужен плагин управления Kaspersky Endpoint Security, а для просмотра деталей алерта вам нужен плагин управления EDR.

Установка веб-плагина

Вы можете установить веб-плагин следующими способами:

- Установить веб-плагин с помощью мастера первоначальной настройки Kaspersky Security Center Web Console.

  Web Console автоматически предлагает запустить мастер первоначальной настройки при первом подключении Web Console к Серверу администрирования. Также вы можете запустить мастер первоначальной настройки в интерфейсе Web Console (**Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер первоначальной настройки**). Мастер первоначальной настройки также может проверить актуальность установленных веб-плагинов и загрузит необходимые обновления для них. Подробнее о мастере первоначальной настройки Kaspersky Security Center Web Console см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm.

- Установить веб-плагин из списка доступных дистрибутивов в Web Console.

  Для установки веб-плагина требуется выбрать дистрибутив веб-плагина Kaspersky Endpoint Security в интерфейсе Web Console (**Параметры консоли** → **Веб-плагины**). Список доступных дистрибутивов обновляется автоматически после выпуска новых версий приложений "Лаборатории Касперского".

- Загрузить дистрибутив в Web Console из стороннего источника.

  Для установки веб-плагина требуется добавить ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Security в интерфейсе Web Console (**Параметры консоли** → **Веб-плагины**). Дистрибутив веб-плагина вы можете загрузить, например, на веб-сайте "Лаборатории Касперского".

Особенности использования защищенных протоколов для взаимодействия с внешними службами

Kaspersky Endpoint Security и Kaspersky Security Center используют защищенный канал связи с TLS (Transport Layer Security) для работы с внешними службами "Лаборатории Касперского". Kaspersky Endpoint Security использует внешние службы для работы следующих функций:

- обновление баз и модулей приложения;
- активация приложения с помощью кода активации (тип активации 2.0);
- использование Kaspersky Security Network.

Использование TLS обеспечивает безопасность работы приложения за счет следующих свойств:

- Шифрование. Содержание сообщений конфиденциально и не раскрывается посторонним пользователям.
- Целостность. Получатель сообщения уверен в неизменности содержания с момента отсылки отправителем.
- Аутентификация. Получатель уверен, что связь устанавливается только с доверенным сервером "Лаборатории Касперского".

Для аутентификации серверов Kaspersky Endpoint Security использует сертификаты открытых ключей. Для работы с сертификатами требуется инфраструктура открытых ключей (англ. Public Key Infrastructure, PKI). Удостоверяющий центр является частью PKI. Так как службы "Лаборатории Касперского" не являются публичными и носят технический характер, "Лаборатория Касперского" использует собственный Удостоверяющий центр. В этом случае при отзыве корневых сертификатов Thawte, VeriSign, GlobalTrust и других, работоспособность PKI "Лаборатории Касперского" не будет нарушена.

Окружения, имеющие MITM (программные и аппаратные средства, поддерживающие разбор протокола HTTPS), Kaspersky Endpoint Security считает небезопасными. При работе со службами "Лаборатории Касперского" могут возникать ошибки, например, ошибки об использовании самозаверяющих сертификатов (англ. Self-Signed Certificate). Эти ошибки могут возникать из-за того, что средство HTTPS Inspection из вашего окружения не распознает PKI "Лаборатории Касперского". Для устранения проблем необходимо настроить исключения для взаимодействия с внешними службами (см. раздел "Приложение 5. Сетевые параметры для взаимодействия с внешними службами" на стр. 476).

Настройка локальных параметров приложения

В Kaspersky Security Center вы можете настроить параметры Kaspersky Endpoint Security на конкретном компьютере – *локальные параметры приложения*. Некоторые параметры могут быть недоступны для изменения. Эти параметры заблокированы атрибутом в свойствах политики (см. раздел "Управление политиками" на стр. 44).

► *Как настроить локальные параметры приложения в Консоли администрирования (MMC)*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Приложения**.
6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (12.12)** и откройте свойства приложения двойным щелчком мыши.
7. В разделе **Общие настройки** настройте параметры работы Kaspersky Endpoint Security, а также параметры отчетов и хранилищ.

   Остальные разделы окна свойств приложения стандартны для Kaspersky Security Center. Описание этих разделов вы можете прочитать в справке для Kaspersky Security Center.

> Если для приложения создана политика, в которой запрещено изменение некоторых параметров, то во время настройки параметров приложения в разделе **Общие настройки** их изменение недоступно.

8. Сохраните внесенные изменения.

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите закладку **Приложения**.
4. Нажмите на **Kaspersky Endpoint Security для Windows**.

   Откроются локальные параметры приложения.
5. Выберите закладку **Параметры приложения**.
6. Настройте локальные параметры приложения.
7. Сохраните внесенные изменения.

Локальные параметры приложения повторяют параметры политики, кроме параметров шифрования.

Управление задачами

Для работы с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного клиентского компьютера;
- групповые задачи, определенные для клиентских компьютеров, входящих в группы администрирования;
- задачи для выборки компьютеров.

Вы можете создавать любое количество групповых задач, задач для выборки компьютеров и локальных задач. Подробнее о работе с группами администрирования и выборками компьютеров см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm.

Kaspersky Endpoint Security поддерживает выполнение следующих задач:

- **Поиск вредоносного ПО** (см. раздел "**Поиск вредоносного ПО**" на стр. 62). Kaspersky Endpoint Security проверяет на вирусы и другие приложения, представляющие угрозу, области компьютера, указанные в параметрах задачи. Задача *Поиск вредоносного ПО* является обязательной для работы Kaspersky Endpoint Security и создается во время работы мастера первоначальной настройки. Рекомендуется настроить расписание выполнения задачи (см. раздел "Запуск проверки по расписанию" на стр. 80) минимум раз в неделю.
- **Добавление ключа**. Kaspersky Endpoint Security добавляет ключ для активации приложения, в том числе дополнительный. Перед выполнением задачи убедитесь, что количество компьютеров, на которых будет выполняться задача, не превышает количество компьютеров, на которые рассчитана лицензия.
- **Изменение состава компонентов приложения**. Kaspersky Endpoint Security устанавливает или удаляет на клиентских компьютерах компоненты согласно списку компонентов, указанному в параметрах задачи. Компонент Защита от файловых угроз удалить невозможно. Оптимальный состав компонентов Kaspersky Endpoint Security позволяет экономить ресурсы компьютера.

- **Инвентаризация**. Kaspersky Endpoint Security получает информацию обо всех исполняемых файлах приложений, хранящихся на компьютерах. Задачу *Инвентаризация* выполняет компонент Контроль приложений. Если компонент Контроль приложений не установлен, задача завершит работу с ошибкой.
- **Обновление баз и модулей приложения**. Kaspersky Endpoint Security обновляет базы и модули приложения. Задача *Обновление баз и модулей приложения* является обязательной для работы Kaspersky Endpoint Security и создается во время работы мастера первоначальной настройки. Рекомендуется настроить расписание выполнения задачи минимум раз в день.
- **Удаление данных**. Kaspersky Endpoint Security удаляет файлы и папки с компьютеров пользователей немедленно или при длительном отсутствии связи с Kaspersky Security Center.
- **Откат обновления** (см. раздел "**Откат последнего обновления**" на стр. 99). Kaspersky Endpoint Security откатывает последнее обновление баз и модулей приложения. Это может понадобиться, например, если новые базы содержат некорректные данные, из-за которых Kaspersky Endpoint Security может блокировать безопасное приложение.
- **Проверка целостности приложения** (см. раздел "**Проверка целостности приложения**" на стр. 77). Kaspersky Endpoint Security анализирует файлы приложения, проверяет файлы на наличие повреждений или изменений и проверяет цифровые подписи файлов приложения.
- **Управление учетными записями Агента аутентификации**. Kaspersky Endpoint Security настраивает параметры учетных записей Агента аутентификации. Агент аутентификации нужен для работы с зашифрованными дисками. Перед загрузкой операционной системы пользователю нужно пройти аутентификацию с помощью агента.

Если приложение работает в составе решения Endpoint Detection and Response от "Лаборатории Касперского", вы можете запускать дополнительные задачи в качестве действий по реагированию на обнаружение (responses). Например, вы можете удаленно завершать процессы с помощью задачи *Завершение процесса*.

Запуск задач на компьютере выполняется только в том случае, если запущено приложение Kaspersky Endpoint Security (см. раздел "Запуск и остановка Kaspersky Endpoint Security" на стр. 57).

Создание задачи

► *Как создать задачу в Консоли администрирования (MMC)*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** дерева Консоли администрирования.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.

В списке задач отобразится новая задача. Задача будет иметь параметры по умолчанию. Для настройки параметров задачи вам нужно перейти в свойства задачи. Для выполнения задачи вам нужно установить флажок напротив задачи и нажать на кнопку **Запустить**. После запуска задачи вы можете остановить задачу и возобновить выполнение задачи позже.

В списке задач вы можете контролировать результат выполнения задачи: статус задачи и статистику выполнения задачи на компьютерах. Также вы можете создать выборку событий для контроля за выполнением задач (**Мониторинг и отчеты** → **Выборки событий**). Подробнее о выборке событий см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm. Также

результаты выполнения задач сохраняются локально на компьютере в журнале событий Windows и в отчетах Kaspersky Endpoint Security (см. раздел "Работа с отчетами" на стр. 342).

Управление доступом к задачам

Права на доступ к задачам Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки доступа к функциональным областям Kaspersky Endpoint Security перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center. Подробнее о концепции управления задачами через Kaspersky Security Center см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm.

Вы можете настроить права доступа к задачам для пользователей компьютеров с помощью политики (*режим работы с задачами*). Например, вы можете скрыть групповые задачи в интерфейсе Kaspersky Endpoint Security.

► *Как настроить режим работы с задачами в интерфейсе Kaspersky Endpoint Security через Консоль администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Локальные задачи** → **Управление задачами**.
4. Настройте режим работы с задачами (см. таблицу ниже).
5. Сохраните внесенные изменения.

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Взаимодействие с пользователем**.
5. В блоке **Разрешенные действия** настройте режим работы с задачами (см. таблицу ниже).
6. Сохраните внесенные изменения.

Таблица 2. Параметры управления задачами

Параметр	Описание
Доступ к локальным задачам	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь, при отсутствии дополнительных ограничений политики, может настраивать и запускать задачи. При этом параметры расписания запуска задачи остаются недоступными для пользователя. Пользователь может запускать задачи только вручную. Если флажок снят, то использование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в локальном интерфейсе Kaspersky Endpoint Security, а также при работе с командной строкой. Пользователь по-прежнему может запустить проверку файла или папки, выбрав пункт **Проверить на вирусы** в контекстном меню файла или папки. При этом задача проверки запустится со значениями параметров, установленными по умолчанию для задачи выборочной проверки.
Просмотр групповых задач	Если флажок установлен, то групповые задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь может просмотреть полный список задач в интерфейсе приложения. Если флажок снят, Kaspersky Endpoint Security показывает пустой список задач.
Управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в консоли Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе приложения или в упрощенном интерфейсе приложения. Если флажок снят, Kaspersky Endpoint Security запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в консоли Kaspersky Security Center.

Управление политиками

Политика – это набор параметров работы приложения, определенный для группы администрирования. Для одного приложения можно настроить несколько политик с различными значениями. Для разных групп администрирования параметры работы приложения могут быть различными. В каждой группе администрирования может быть создана собственная политика для приложения.

Параметры политики передаются на клиентские компьютеры с помощью Агента администрирования при *синхронизации*. По умолчанию Сервер администрирования выполняет синхронизацию сразу после изменения параметров политики. Синхронизация выполняется через UDP-порт 15000 на клиентском компьютере. Сервер администрирования по умолчанию выполняет синхронизацию каждые 15 минут. Если синхронизация после изменения параметров политики не удалась, следующая попытка синхронизации будет выполнена по настроенному расписанию.

Наследование параметров

Политики, как и группы администрирования, имеют иерархию. По умолчанию дочерняя политика наследует параметры родительской политики. *Дочерняя политика* – политика вложенного уровня иерархии, т.е. политика для вложенных групп администрирования и подчиненных Серверов администрирования. Вы можете выключить наследование параметров из родительской политики.

Каждый параметр, представленный в политике, имеет атрибут , который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локальных параметрах приложения (см. раздел "Настройка локальных параметров приложения" на стр. 40). Атрибут работает только, если в дочерней политике включено наследование параметров из родительской политики. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

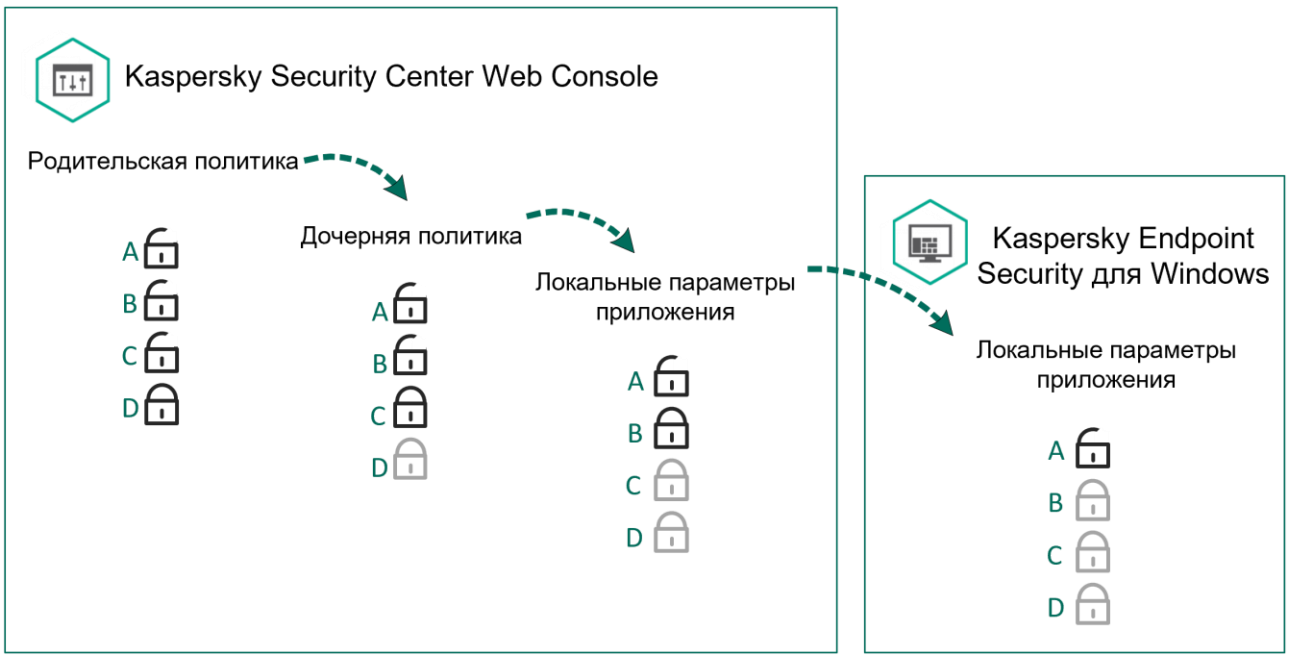


Рисунок 11. Наследование параметров

Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security. Для настройки прав доступа к параметрам политики перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center (по умолчанию этот раздел скрыт в интерфейсе консоли).

Создание политики

При создании политики мастер предлагает настроить параметры, которые важны для выбранного режима использования. Например, для работы приложения в режиме Легкого агента необходимо обязательно добавить Сервер защиты (SVM). При использовании приложения для защиты SQL-сервера необходимо добавить предустановленные исключения из проверки для стабильной работы сервера. Мастер предлагает настроить соответствующие параметры политики после выбора режима использования приложения. Далее вы можете изменить эти параметры в свойствах политики.

► *Как создать политику в Консоли администрирования (MMC)*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят интересующие вас клиентские компьютеры.

3. В рабочей области выберите закладку **Политики**.
4. Нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики.
5. Следуйте указаниям мастера создания политики.

Шаг 1. Выбор приложения для создания групповой политики

Выберите приложение **Kaspersky Endpoint Security для Windows (12.12)**.

Шаг 2. Определение названия для групповой политики

Введите имя групповой политики, например, *Политика для офиса*.

Вы также можете создавать новые политики на основе имеющихся с помощью мастера создания политики. Для этого на шаге ввода названия групповой политики требуется установить флажок **Использовать параметры политики для предыдущей версии приложения**. Мастер также позволяет создать политику Kaspersky Endpoint Security (KES) на основании политики других решений, например, Kaspersky Security для Windows Server (KSWS) или Kaspersky Security для виртуальных сред Легкий агент для Windows

Шаг 3. Участие в Kaspersky Security Network

Прочитайте и примите условия Положения о Kaspersky Security Network (KSN).

Шаг 4. Выбор режима использования приложения на компьютерах

В зависимости от назначения Kaspersky Endpoint Security вы можете развернуть приложение Kaspersky Endpoint Security в разных режимах:

- Стандартный режим.

  Если вы выбрали этот режим, вы можете настроить основные параметры политики во время работы мастера. Также вам доступен импорт основных параметров политики из конфигурационного файла.
- Агент Endpoint Detection and Response.

  Если вы выбрали этот режим, вы можете создать политику только с параметрами по умолчанию. Для настройки параметров EDR-агента вам нужно перейти в свойства политики после завершения работы мастера.
- Легкий агент для защиты виртуальных сред.

  Если вы выбрали этот режим, на следующем шаге вам нужно настроить параметры подключения к Серверу защиты (SVM). Эти параметры являются обязательными для работы приложения в режиме Легкого агента.

В сертифицированной версии приложения интеграция с Kaspersky Managed Detection and Response не поддерживается. Включение интеграции с Kaspersky Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.

Kaspersky Endpoint Security предоставляет единую политику для всех режимов использования приложения и типов ОС. То есть политика содержит полный набор параметров. При этом некоторые параметры политики приложение может игнорировать, так как Kaspersky Endpoint Security развернуто в режиме, в котором недоступны некоторые функции. Например, при использовании приложения в режиме Агента Endpoint Detection and Response доступны только параметры интеграции с решениями Detection and Response от "Лаборатории Касперского" и параметры интеграции с KUMA.

Рекомендуется использовать разные политики для разных режимов использования и разных типов операционных систем.

Шаг 5. Настройка доверенной зоны

Настройте доверенную зону. Вы можете добавить предустановленные исключения из проверки (см. раздел "Создание исключения из проверки" на стр. 320) и доверенные приложения (см. раздел "Формирование списка доверенных приложений" на стр. 326). Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Также предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в режиме Легкого агента в виртуальных средах Citrix и VMware.

Шаг 6. Выбор состояния политики

- **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.

  Параметры активной политики во время синхронизации сохраняются на клиентских компьютерах. К одному компьютеру нельзя одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.

- **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.

  Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры приложения на компьютерах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например, в случае вирусной атаки. В случае атаки через флеш-накопители вы можете активировать политику, блокирующую доступ к флеш-накопителям. При этом активная политика автоматически становится неактивной.

- **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.

Завершите работу мастера.

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
3. Выберите приложение Kaspersky Endpoint Security и нажмите **Далее**.
4. Прочитайте и примите условия Положения о Kaspersky Security Network (KSN) и нажмите **Далее**.
5. Выберите режим использования приложения:
   - Стандартный режим для защиты рабочих станций и серверов.
   - Агент Endpoint Detection and Response для защиты от сложных угроз и целевых атак.

     Если вы выбрали этот режим, вы можете создать политику для интеграции компьютера с решениями Detection and Response от "Лаборатории Касперского". Мастер последовательно предложит настроить параметры интеграции для решений Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform (EDR).

В сертифицированной версии приложения интеграция с Kaspersky Managed Detection and Response не поддерживается. Включение интеграции с Kaspersky Managed Detection and Response приводит к выходу приложения из сертифицированного состояния.

- Легкий агент для защиты виртуальных сред.

  Если вы выбрали этот режим, на следующем шаге вам нужно настроить параметры подключения к Серверу защиты (SVM). Эти параметры являются обязательными для работы приложения в режиме Легкого агента.

Kaspersky Endpoint Security предоставляет единую политику для всех режимов использования приложения и типов ОС. То есть политика содержит полный набор параметров. При этом некоторые параметры политики приложение может игнорировать, так как Kaspersky Endpoint Security развернуто в режиме, в котором недоступны некоторые функции. Например, при использовании приложения в режиме Агента Endpoint Detection and Response доступны только параметры интеграции с решениями Detection and Response от "Лаборатории Касперского" и параметры интеграции с KUMA.

Рекомендуется использовать разные политики для разных режимов использования и разных типов операционных систем.

6. Настройте доверенную зону. Вы можете добавить предустановленные исключения из проверки (см. раздел "Создание исключения из проверки" на стр. 320) и доверенные приложения (см. раздел "Формирование списка доверенных приложений" на стр. 326). Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Также предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в режиме Легкого агента в виртуальных средах Citrix и VMware.
7. На закладке **Общие** вы можете выполнить следующие действия:
   - Изменить имя политики.
   - Выбрать состояние политики:
     - **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.

       Параметры активной политики во время синхронизации сохраняются на клиентских компьютерах. К одному компьютеру нельзя одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.
     - **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.

       Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры приложения на компьютерах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например, в случае вирусной атаки. В случае атаки через флеш-накопители, вы можете активировать политику, блокирующую доступ к флеш-накопителям. При этом активная политика автоматически становится неактивной.
     - **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.

- Настроить наследование параметров:
  - **Наследовать параметры родительской политики**. Если переключатель включен, значения параметров политики наследуются из политики верхнего уровня иерархии. Параметры политики недоступны для изменения, если в родительской политике установлен .
  - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики будут распространены на дочерние политики. В свойствах дочерней политики будет автоматически включен и недоступен для выключения переключатель **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из родительской политики, кроме параметров с . Параметры дочерних политик недоступны для изменения, если в родительской политике установлен .

8. На закладке **Параметры приложения** вы можете настроить параметры политики Kaspersky Endpoint Security.
9. Завершите работу мастера.

В результате параметры Kaspersky Endpoint Security будут настроены на клиентских компьютерах при следующей синхронизации. Вы можете просмотреть информацию о политике, которая применена к компьютеру, в интерфейсе Kaspersky Endpoint Security по кнопке на главном экране (например, имя политики). Для этого в параметрах политики Агента администрирования нужно включить получение расширенных данных политики. Подробнее о политике Агента администрирования см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm.

Индикатор уровня защиты

В верхней части окна свойств политики отображается индикатор уровня защиты. Индикатор может принимать одно из следующих значений:

- **Уровень защиты высокий**. Индикатор принимает это значение и цвет индикатора изменяется на зеленый, если включены все компоненты, относящиеся к следующим категориям:
  - **Критические**. Категория включает следующие компоненты:
    - Защита от файловых угроз (см. раздел "Включение и выключение Защиты от файловых угроз" на стр. 139).
    - Анализ поведения (см. раздел "Анализ поведения" на стр. 115).
    - Защита от эксплойтов (см. раздел "Включение и выключение Защиты от эксплойтов" на стр. 124).
    - Откат вредоносных действий (см. раздел "Откат вредоносных действий" на стр. 122).
    - Защита служб приложения от внешнего управления (см. раздел "Защита служб приложения от внешнего управления" на стр. 351).
  - **Важные**. Категория включает следующие компоненты:
    - Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110).
    - Защита от веб-угроз (см. раздел "Включение и выключение Защиты от веб-угроз" на стр. 152).

  - Защита от почтовых угроз (см. раздел "Включение и выключение Защиты от почтовых угроз" на стр. 159).
  - Предотвращение вторжений (см. раздел "Включение и выключение Предотвращения вторжений" на стр. 128).
  - Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355).
- **Уровень защиты средний**. Индикатор принимает это значение и цвет индикатора изменяется на желтый, если отключен один важный компонент.
- **Уровень защиты низкий**. Индикатор принимает это значение и цвет индикатора изменяется на красный в одном из следующих случаев:
  - отключены один или несколько критических компонентов;
  - отключены два или более важных компонента.

Если отображается индикатор со значением **Уровень защиты средний** или **Уровень защиты низкий**, то справа от индикатора доступна ссылка, по которой открывается окно **Рекомендуемые компоненты защиты**. В этом окне вы можете включить любой из рекомендованных компонентов защиты.

После обновления версии приложения индикатор уровня защиты может показать более низкий уровень защиты, чем до обновления. Это связано с тем, что в новой версии приложения добавлены новые компоненты или функции, важные для безопасности компьютера. После обновления версии приложения настройте новые параметры в соответствии с высоким уровнем защиты.

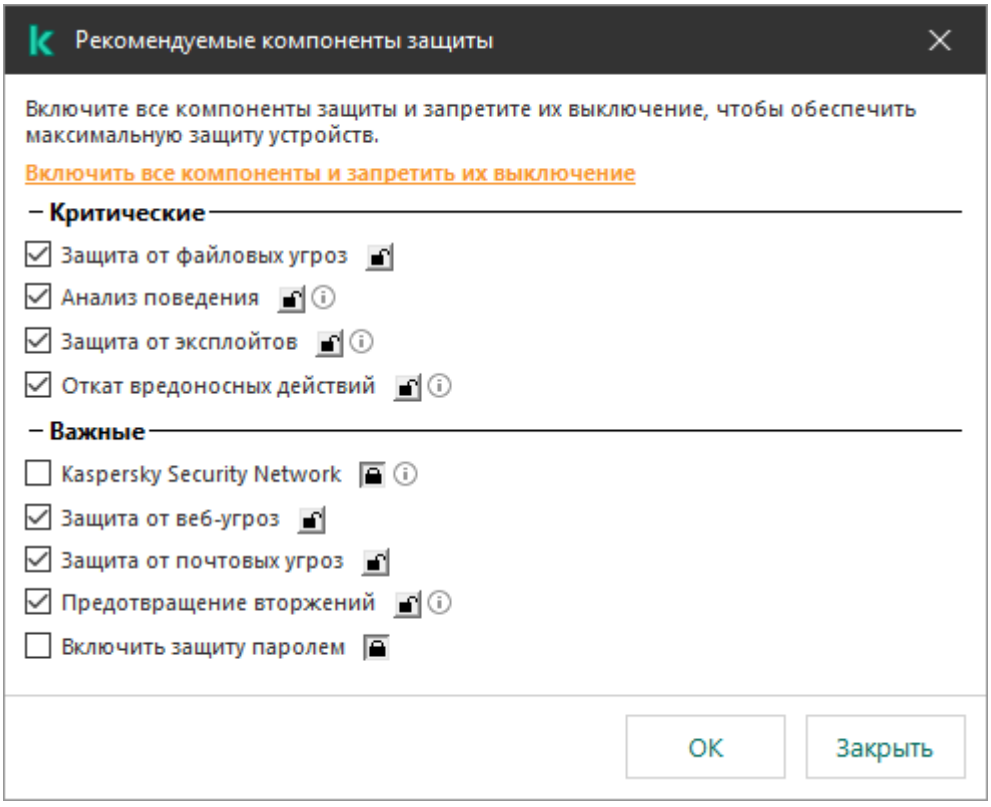


Рисунок 12. Индикатор уровня защиты политики.

Интерфейс приложения

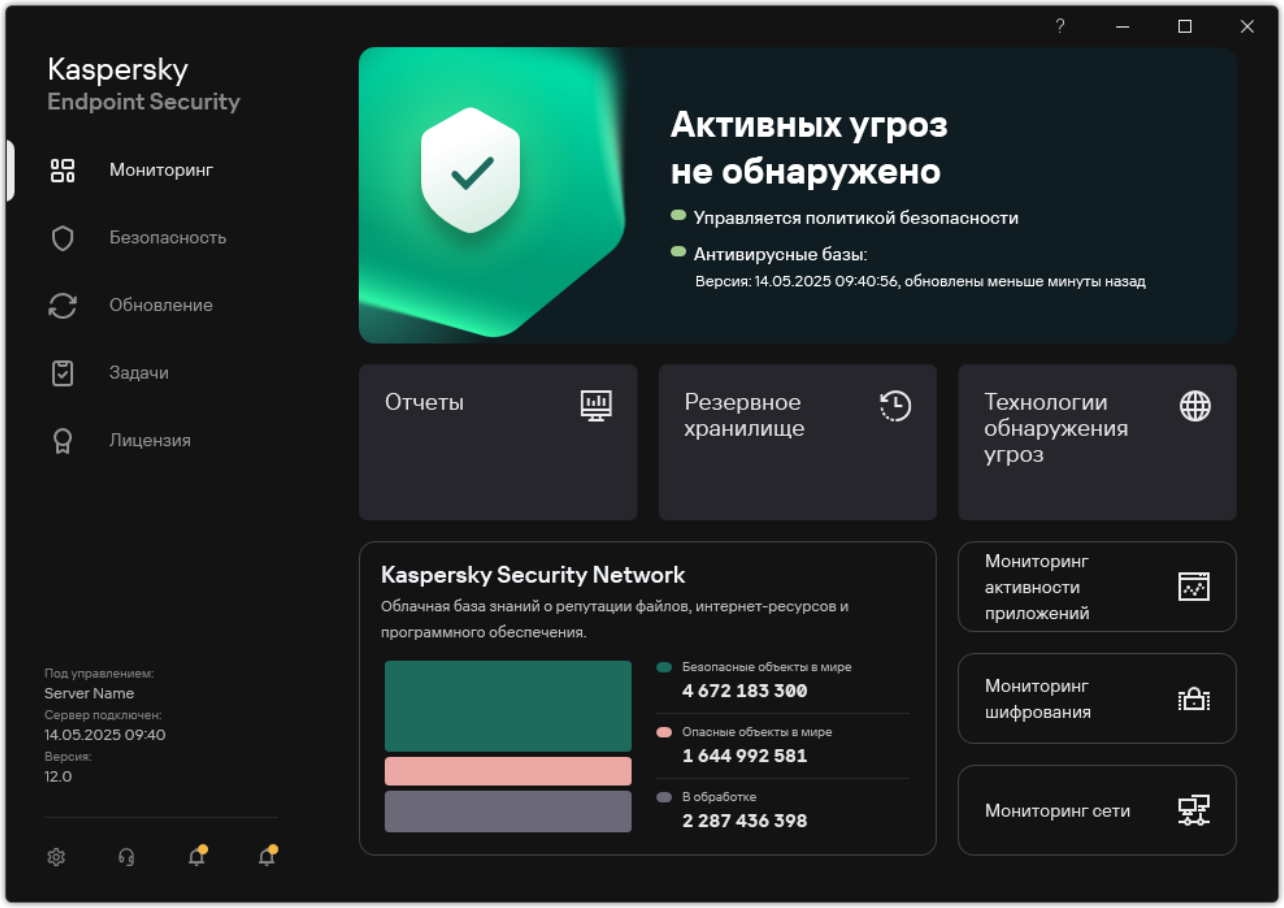


Рисунок 13. Главное окно программы

Мониторинг	• **Отчеты**. Просмотр событий, произошедших во время работы приложения, отдельных компонентов и задач. • **Резервное хранилище**. Просмотр списка копий зараженных файлов, которые были удалены в ходе работы приложения. • **Технологии обнаружения угроз**. Просмотр информации о технологиях обнаружения угроз и количестве угроз, обнаруженных с помощью этих технологий. • **Kaspersky Security Network**. Статус подключения Kaspersky Endpoint Security к Kaspersky Security Network и глобальная статистика KSN. *Kaspersky Security Network (KSN)* – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых веб-адресов. • **Мониторинг активности приложений**. Просмотр информации о работе установленных приложениях. Мониторинг активности приложений отслеживает файловые, реестровые и системные события в операционной системе, связанные с приложением. • **Мониторинг сети**. Просмотр информации о сетевой активности компьютера в режиме реального времени. • **Мониторинг шифрования**. Контроль процесса шифрования или расшифровки дисков в режиме реального времени. Мониторинг шифрования доступен, если установлены компоненты Шифрование диска Kaspersky или Шифрование диска BitLocker.
Безопасность	Статус работы установленных компонентов. Также вы можете перейти к настройке компонентов или просмотреть отчеты.
Обновление	Управление задачами обновления Kaspersky Endpoint Security. Вы можете выполнять обновление антивирусных баз и модулей приложения и откат последнего обновления (на стр. 99). Администратор может скрыть раздел от пользователя (см. раздел "Управление задачами" на стр. 41) или ограничить управление задачами (см. раздел "Управление задачами" на стр. 41).
Задачи	Управление задачами проверки Kaspersky Endpoint Security. Вы можете выполнять поиск вредоносного ПО (на стр. 62) и проверку целостности приложения (см. раздел "Проверка целостности приложения" на стр. 77). Администратор может скрыть задачи от пользователя (см. раздел "Управление задачами" на стр. 41) или ограничить управление задачами (см. раздел "Управление задачами" на стр. 41).
Лицензия	Лицензирование приложения. Вы можете приобрести лицензию, активировать приложение или продлить подписку. Так же вы можете просмотреть информацию о действующей лицензии.
⚙	Настройка параметров приложения. Администратор может запретить изменение параметров в Kaspersky Security Center (см. раздел "Управление политиками" на стр. 44).



Информация о приложении: текущая версия Kaspersky Endpoint Security, дата выпуска баз, ключ и другая информация. Также вы можете перейти на информационные ресурсы "Лаборатории Касперского", чтобы получить полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.



Сообщения с информацией о доступных обновлениях, а также запросы доступа к зашифрованным файлам и устройствам.

В этом разделе

Значок приложения в области уведомлений 53
Упрощенный интерфейс приложения 54
Настройка отображения интерфейса приложения 55

Значок приложения в области уведомлений

Сразу после установки Kaspersky Endpoint Security значок приложения появляется в области уведомлений панели задач Microsoft Windows.

Если значок приложения в области уведомлений скрыт, администратор выключил отображение интерфейса приложения в политике (см. раздел "Настройка отображения интерфейса приложения" на стр. 55).

Значок приложения выполняет следующие функции:

- служит индикатором работы приложения;
- обеспечивает доступ к контекстному меню значка приложения и главному окну приложения.

Для отображения информации о работе приложения предназначены следующие статусы значка приложения:

- Значок  означает, что работа критически важных компонентов защиты приложения включена. Kaspersky Endpoint Security покажет предупреждение  , если от пользователя требуется выполнить действие, например, перезагрузить компьютер после обновления приложения.
- Значок  означает, что работа критически важных компонентов защиты приложения выключена или нарушена. Работа компонентов защиты может быть нарушена, например, если срок действия лицензии истек или произошел сбой в работе приложения. Kaspersky Endpoint Security покажет предупреждение  с описанием проблемы в защите компьютера.

Контекстное меню значка приложения содержит следующие пункты:

- **Kaspersky Endpoint Security для Windows**. Открывает главное окно приложения. В этом окне вы можете регулировать работу компонентов и задач приложения, просматривать статистику об обработанных файлах и обнаруженных угрозах.

- **Приостановить защиту** / **Возобновить защиту**. Приостановка работы всех компонентов защиты и контроля, не отмеченных в политике замком ( ). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.

  Перед приостановкой работы компонентов защиты и контроля приложение запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. 352) (пароль учетной записи или временный пароль). Далее вы можете выбрать период приостановки: на указанное время, до перезагрузки или по требованию пользователя.

  Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Для возобновления работы компонентов защиты и контроля выберите пункт **Возобновить защиту** в контекстном меню приложения.

  > Приостановка работы компонентов защиты и контроля не влияет на выполнение задач обновления и поиска вредоносного ПО. Также приложение продолжает использование Kaspersky Security Network.

- **Выключить политику** / **Включить политику**. Выключение политики Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком ( ). При выключении политики приложение запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. 352) (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Для включения политики выберите пункт **Включить политику** в контекстном меню приложения.
- **Настройка**. Открывает окно настройки параметров приложения.
- **Поддержка**. Открывает окно, содержащее информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- **О приложении**. Открывает информационное окно со сведениями о приложении.
- **Выход**. Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, приложение выгружается из оперативной памяти компьютера.

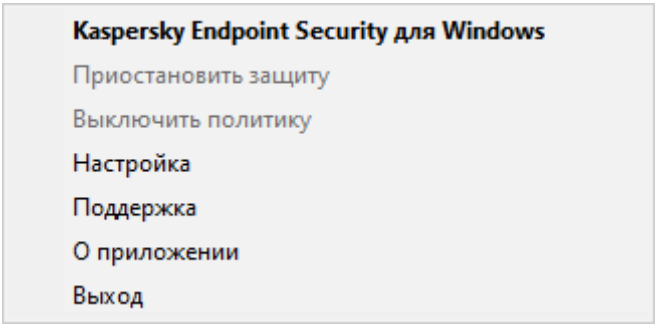


Рисунок 14. Контекстное меню значка программы

kaspersky

Упрощенный интерфейс приложения

Если к клиентскому компьютеру, на котором установлено приложение Kaspersky Endpoint Security, применена политика Kaspersky Security Center, в которой настроено отображение упрощенного интерфейса приложения (см. раздел "Настройка отображения интерфейса приложения" на стр. 55), то на этом клиентском компьютере недоступно главное окно приложения. По правой клавише мыши пользователь может открыть контекстное меню значка Kaspersky Endpoint Security (см. рис. ниже), содержащее следующие пункты:

- **Выключить политику** / **Включить политику**. Выключение политики Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком ( ). При выключении политики приложение запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. 352) (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Для включения политики выберите пункт **Включить политику** в контекстном меню приложения.
- **Задачи**. Раскрывающийся список, содержащий следующие элементы:
  - **Проверка целостности приложения**.
  - **Откат к предыдущей версии баз**.
  - **Полная проверка**.
  - **Выборочная проверка**.
  - **Проверка важных областей**.
  - **Обновление**.
- **Поддержка**. Открывает окно, содержащее информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- **Выход**. Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, приложение выгружается из оперативной памяти компьютера.

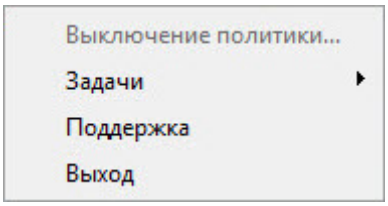


Рисунок 15. Контекстное меню значка программы при отображении упрощенного интерфейса программы

Настройка отображения интерфейса приложения

Вы можете настроить отображение интерфейса приложения для пользователя компьютера. Пользователь может взаимодействовать с приложением следующими способами:

- **Отображать упрощенный интерфейс**. На клиентском компьютере недоступно главное окно приложения, а доступен только значок в области уведомлений Windows (см. раздел "Значок приложения в области уведомлений" на стр. 53). В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security (см. раздел "Упрощенный интерфейс приложения" на стр. 54). Также Kaspersky Endpoint Security показывает уведомления над значком приложения.

- **Отображать пользовательский интерфейс**. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows (см. раздел "Значок приложения в области уведомлений" на стр. 53). В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком приложения.
- **Не отображать пользовательский интерфейс**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows (см. раздел "Значок приложения в области уведомлений" на стр. 53) и уведомления.

► *Как настроить отображение интерфейса приложения в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Интерфейс**.
4. В блоке **Взаимодействие с пользователем** выполните одно из следующих действий:
   - Установите флажок **Отображать пользовательский интерфейс**, если вы хотите, чтобы на клиентском компьютере отображались следующие элементы интерфейса:
     - папка с названием приложения в меню **Пуск**;
     - значок Kaspersky Endpoint Security (см. раздел "Значок приложения в области уведомлений" на стр. 53) в области уведомлений панели задач Microsoft Windows;
     - всплывающие уведомления.

     Если установлен этот флажок, пользователь может просматривать и, при наличии прав, изменять параметры приложения из интерфейса приложения.
   - Снимите флажок **Отображать пользовательский интерфейс**, если вы хотите скрыть все признаки работы Kaspersky Endpoint Security на клиентском компьютере.
5. В блоке **Взаимодействие с пользователем** установите флажок **Отображать упрощенный интерфейс**, если вы хотите, чтобы на клиентском компьютере с установленным приложением Kaspersky Endpoint Security отображался упрощенный интерфейс приложения (на стр. 54).

kaspersky

Запуск и остановка Kaspersky Endpoint Security

После установки Kaspersky Endpoint Security на компьютер пользователя запуск приложения выполняется автоматически. Далее по умолчанию запуск Kaspersky Endpoint Security выполняется сразу после операционной системы. Настроить автоматический запуск приложения в параметрах операционной системы невозможно.

Загрузка антивирусных баз Kaspersky Endpoint Security после загрузки операционной системы занимает до двух минут, в зависимости от производительности (технических возможностей) компьютера. В течение этого времени уровень защиты компьютера снижен. Загрузка антивирусных баз при запуске приложения Kaspersky Endpoint Security в уже запущенной операционной системе не вызывает снижения уровня защиты компьютера.

► *Как настроить запуск Kaspersky Endpoint Security в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

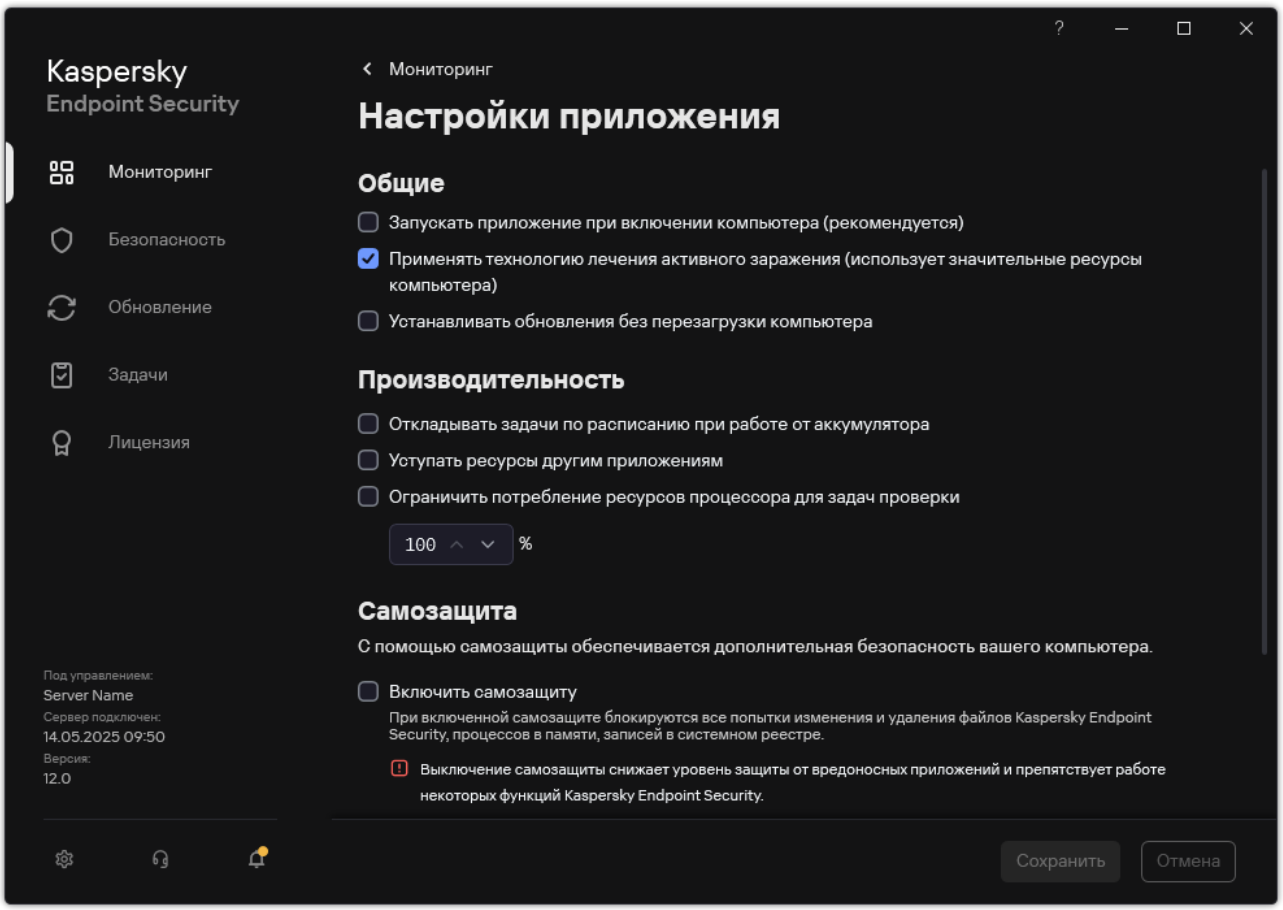


Рисунок 16. Параметры приложения Kaspersky Endpoint Security для Windows

3. С помощью флажка **Запускать приложение при включении компьютера (рекомендуется)** настройте запуск приложения.
4. Сохраните внесенные изменения.

Специалисты "Лаборатории Касперского" рекомендуют не завершать работу Kaspersky Endpoint Security, поскольку в этом случае защита компьютера и ваших данных окажется под угрозой. Если требуется, вы можете приостановить защиту компьютера (см. раздел "Приостановка и возобновление защиты и контроля компьютера" на стр. 60) на необходимый срок, не завершая работу приложения.

Вы можете контролировать статус работы приложения с помощью виджета **Состояние защиты**.

► *Как запустить или остановить Kaspersky Endpoint Security в Консоли администрирования (MMC)*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Приложения**.
6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (12.12)** и откройте свойства приложения двойным щелчком мыши.
7. Выполните одно из следующих действий:
   - Если вы хотите запустить приложение, справа от списка приложений "Лаборатории Касперского" нажмите на кнопку  .
   - Если вы хотите остановить работу приложения, справа от списка приложений "Лаборатории Касперского" нажмите на кнопку  .

Приостановка и возобновление защиты и контроля компьютера

Приостановка защиты и контроля компьютера означает выключение на некоторое время всех компонентов защиты и всех компонентов контроля Kaspersky Endpoint Security.

Состояние приложения отображается с помощью значка приложения в области уведомлений панели задач (см. раздел «Значок приложения в области уведомлений» на стр. 53):

- значок свидетельствует о приостановке защиты и контроля компьютера;
- значок свидетельствует о том, что защита и контроль компьютера включены.

Приостановка и возобновление защиты и контроля компьютера не оказывает влияния на выполнение задач проверки и задачи обновления.

Если в момент приостановки и возобновления защиты и контроля компьютера были установлены сетевые соединения, на экран выводится уведомление о разрыве этих сетевых соединений.

► *Чтобы приостановить защиту и контроль компьютера, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка приложения, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Приостановить защиту** (см. рисунок ниже).

   Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355).
3. Выберите один из следующих вариантов:
   - **Приостановить на <период времени>** – защита и контроль компьютера включатся через интервал времени, указанный в раскрывающемся списке ниже.
   - **Приостановить до перезапуска приложения** – защита и контроль компьютера включатся после перезапуска приложения или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск приложения.
   - **Приостановить** – защита и контроль компьютера включатся тогда, когда вы решите возобновить их.
4. Нажмите на кнопку **Приостановить защиту**.

Kaspersky Endpoint Security приостановит работу всех компонентов защиты и контроля, не отмеченных в политике замком ( ). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.

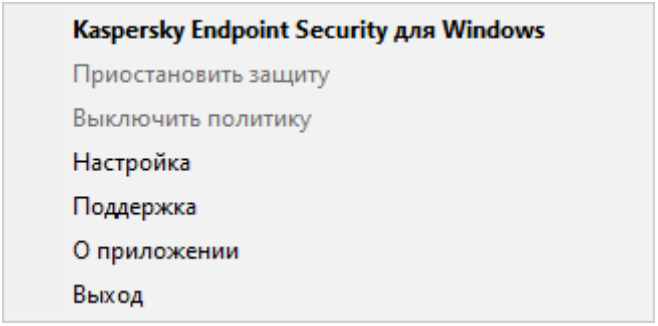


Рисунок 17. Контекстное меню значка программы

► *Чтобы возобновить защиту и контроль компьютера, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка приложения, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Возобновить защиту**.

Вы можете возобновить защиту и контроль компьютера в любой момент, независимо от того, какой вариант приостановки защиты и контроля компьютера вы выбрали ранее.

kaspersky

Поиск вредоносного ПО

Проверка на наличие вредоносного ПО является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять поиск вредоносного ПО, чтобы исключить возможность распространения вредоносных приложений, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive, и создает в журнале записи о том, что эти файлы не были проверены.

Полная проверка

Тщательная проверка всей системы. Kaspersky Endpoint Security проверяет следующие объекты:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- загрузочные секторы;
- резервное хранилище операционной системы;
- все жесткие и съемные диски.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи *Полная проверка*.
Для экономии ресурсов компьютера рекомендуется вместо задачи полной проверки использовать задачу фоновой проверки (см. раздел "Фоновая проверка" на стр. 72). Уровень защиты компьютера при этом не изменится.

Проверка важных областей

По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи *Проверка важных областей*.

Выборочная проверка

Kaspersky Endpoint Security проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:

- системная память;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- резервное хранилище операционной системы;
- жесткие, съемные и сетевые диски;
- любой выбранный файл.

kaspersky

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, загрузочного сектора, системной памяти и системного раздела.

Проверка целостности приложения

Kaspersky Endpoint Security проверяет модули приложения на наличие повреждений или изменений.

В этом разделе

Проверка компьютера ... 63
Проверка съемных дисков при подключении к компьютеру ... 70
Фоновая проверка ... 72
Проверка из контекстного меню ... 73
Проверка целостности приложения ... 77
Формирование области проверки ... 78
Запуск проверки по расписанию ... 80
Запуск проверки с правами другого пользователя ... 82
Оптимизация проверки ... 83

Проверка компьютера

Проверка является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять поиск вредоносного ПО, чтобы исключить возможность распространения вредоносных приложений, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110) и эвристического анализа.

В Kaspersky Endpoint Security предустановлены стандартные задачи *Полная проверка*, *Проверка важных областей*, *Выборочная проверка*. Если в вашей организации развернута система администрирования Kaspersky Security Center, вы можете создать задачу *Поиск вредоносного ПО* и настроить параметры проверки. Также в Kaspersky Security Center доступна задача *Фоновая проверка* (см. раздел "*Фоновая проверка*" на стр. 72). Настроить параметры фоновой проверки невозможно.

► *Как запустить проверку в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. Настройте параметры задачи проверки (см. таблицу ниже).

   Если требуется, настройте расписание запуска задачи проверки (см. раздел "Запуск проверки по расписанию" на стр. 80).

4. Сохраните внесенные изменения.
5. Запустите задачу проверки.

   Kaspersky Endpoint Security запустит проверку компьютера. Приложение покажет процесс проверки, количество проверенных файлов и оставшиеся время. Вы можете остановить выполнение задачи в любое время по кнопке **Стоп**. Если задача проверки не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

В результате Kaspersky Endpoint Security проверит компьютер и при обнаружении угроз выполнит действие, заданное в параметрах приложения. Обычно приложение пытается вылечить зараженные файлы. При этом зараженные файлы могут получать следующие статусы:

- **Отложено**. Вылечить зараженный файл не удалось. Приложение удалит зараженный файл после перезагрузки компьютера.
- **Записано в отчет**. Вылечить зараженный файл не удалось. Приложение добавит информацию об обнаруженных зараженных файлах в список активных угроз.
- **Запись не поддерживается** или **Ошибка записи**. Вылечить зараженный файл не удалось. У приложения нет прав на запись.
- **Обработка уже выполнена**. Приложение обнаружило зараженный файл ранее. Приложение вылечит или удалит зараженный файл после перезагрузки компьютера.

Таблица 3. Параметры проверки

Параметр	Описание
Уровень безопасности	Для проверки Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*: • **Высокий**. Приложение Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Глубокий**. • **Рекомендуемый**. Приложение Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Средний**. • **Низкий**. Приложение Kaspersky Endpoint Security проверяет только файлы определенных форматов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Поверхностный**. Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

Параметр	Описание
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. **Лечить. Информировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз. **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз. Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить (см. раздел "Восстановление файлов из резервного хранилища" на стр. 334). При обнаружении зараженных файлов, являющихся частью приложения Windows Store, Kaspersky Endpoint Security пытается удалить файл.
Выполнять лечение активного заражения немедленно *(доступен только в консоли Kaspersky Security Center)*	Лечение активного заражения в ходе выполнения задачи поиска вирусов на компьютере осуществляется только в том случае, если в свойствах примененной к этому компьютеру политики включена функция лечения активного заражения (см. раздел "Технология лечения активного заражения" на стр. 102). Если флажок установлен, Kaspersky Endpoint Security лечит активное заражение сразу после его обнаружения в ходе выполнения задачи поиска вирусов. После лечения активного заражения Kaspersky Endpoint Security перезагружает компьютер, не запрашивая подтверждение у пользователя. Если флажок снят, Kaspersky Endpoint Security не лечит активное заражение сразу после его обнаружения в ходе выполнения задачи поиска вирусов. Приложение формирует события об активном заражении в локальных отчетах приложения и на стороне Kaspersky Security Center. Лечение активного заражения возможно при повторном запуске задачи поиска вирусов с включенной функцией лечения активного заражения. Таким образом, системный администратор имеет возможность выбрать подходящее время для лечения активного заражения компьютеров и их последующей автоматической перезагрузки.

Параметр	Описание
Область проверки	Список объектов, которые Kaspersky Endpoint Security проверяет во время выполнения задачи проверки. Объектом проверки может быть память ядра, запущенные процессы, загрузочные секторы, системное резервное хранилище, жесткий, съемный или сетевой диск, папка или файл. В Kaspersky Endpoint Security для Windows версии 12.12 почта исключена из области проверки приложения. Проверку входящих и исходящих сообщений выполняет компонент Защита от почтовых угроз (см. раздел "Формирование области защиты компонента Защита от почтовых угроз" на стр. 163). Если вы используете плагин управления более ранней версии, то приложение исключает почту из области проверки, даже если эта область включена в политике.
Расписание проверки	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Отложить запуск после старта приложения на N минут	Отложенный запуск задачи проверки после старта приложения. После старта операционной системы запускается множество процессов, поэтому удобно запускать задачу проверки не сразу после запуска Kaspersky Endpoint Security, а через некоторое время.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.
Выполнять только во время простоя компьютера	Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.
Запускать проверку с правами	По умолчанию задача проверки запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Область защиты может включать сетевые диски или другие объекты, для доступа к которым нужны специальные права. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения, и запускать задачу проверки от имени этого пользователя.

Параметр	Описание
Типы файлов	Файлы без расширения приложение Kaspersky Endpoint Security считает исполняемыми. Приложение проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки. **Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Формат файла определяется на основании его расширения. По умолчанию Kaspersky Endpoint Security проверяет файлы по формату. Проверять файлы по расширению менее безопасно, так как вредоносный файл может иметь расширение, которое не входит в список потенциально заражаемых (например, `.123`).
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Пропускать файл, если его проверка длится более N секунд	Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Endpoint Security останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Endpoint Security выполнит сначала и по расписанию.

Параметр	Описание
Не запускать несколько задач проверки одновременно	Отложенный запуск задач проверки, если проверка уже выполняется. Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, приложение запустило задачу полной проверки по расписанию. Если пользователь пытается запустить быструю проверку в интерфейсе приложения, Kaspersky Endpoint Security поставит задачу быстрой проверки в очередь и автоматически запустит задачу после завершения полной проверки. Kaspersky Endpoint Security запускает задачу проверки немедленно, даже если запущена другая задача проверки, в следующих случаях: • Проверка съемного диска при подключении (см. раздел "Проверка съемных дисков при подключении к компьютеру" на стр. 70). • Проверка из контекстного меню (на стр. 73). • Проверка важных областей, запущенная в результате обнаружения индикатора компрометации (IOC) (см. раздел "Поиск индикаторов компрометации (стандартная задача)" на стр. 298). Если флажок снят, Kaspersky Endpoint Security позволяет запускать несколько задач проверки одновременно. Запуск нескольких задач проверки требует больше ресурсов компьютера.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Проверка дистрибутивов сторонних приложений.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.

Параметр	Описание
Проверять файлы почтовых форматов	Проверка файлов почтовых форматов, а также почтовой базы данных. Приложение проверяет PST- и OST-файлы, которые используют почтовые клиенты MS Outlook / Windows Mail, и EML-файлы. Kaspersky Endpoint Security не поддерживает работу с 64-битной версией почтового клиента MS Outlook. То есть, Kaspersky Endpoint Security не проверяет файлы, связанные с работой 64-битной версии почтового клиента MS Outlook (PST- и OST-файлы), даже если почта включена в область проверки (см. раздел "Формирование области проверки" на стр. 78). Если флажок установлен, Kaspersky Endpoint Security разбирает файл почтового формата на составляющие части (заголовок, тело, вложения) и анализирует их на наличие угроз. Если флажок снят, Kaspersky Endpoint Security проверяет файл почтового формата как единый файл. При обнаружении вредоносного объекта в PST- и OST-файлах Kaspersky Endpoint Security обезвреживает его в соответствии с выбранным действием (например, лечение или удаление файла). При обнаружении вредоносного объекта в файлах других почтовых клиентов (например, Mozilla Thunderbird), Kaspersky Endpoint Security только отмечает зараженное письмо. Вам необходимо удалить письмо с вредоносным файлом во вложении вручную.
Проверять архивы, защищенные паролем	Если флажок установлен, приложение проверяет архивы, защищенные паролем. Перед проверкой файлов, содержащихся в архиве, на экран выводится запрос пароля. Если флажок не установлен, приложение пропускает проверку защищенных паролем архивов.
Не распаковывать составные файлы большого размера	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Машинное обучение и сигнатурный анализ	При методе проверки Машинное обучение и сигнатурный анализ используются базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защиту с использованием этого метода проверки обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Параметр	Описание
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Технология iSwift *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
Технология iChecker *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Проверка съемных дисков при подключении к компьютеру

Kaspersky Endpoint Security проверяет все файлы, которые вы запускаете или копируете, даже если файл расположен на съемном диске (компонент Защита от файловых угроз). Для предотвращения распространения вирусов и других приложений, представляющих угрозу, вы можете настроить автоматическую проверку съемных дисков при подключении к компьютеру. При обнаружении угрозы Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет. Компонент обеспечивают защиту компьютера с помощью следующих методов проверки: машинное обучение, эвристический анализ (высокий уровень) и сигнатурный анализ. Также Kaspersky Endpoint Security использует технологии оптимизации проверки iSwift и iChecker. Технологии включены постоянно и выключить их невозможно.

► *Как настроить запуск проверки съемных дисков в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. Используйте переключатель **Проверка съемных дисков**, чтобы включить или выключить проверку съемных дисков при подключении к компьютеру.
4. Настройте дополнительные параметры проверки съемных дисков (см. таблицу ниже).
5. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет запускать проверку съемных дисков, размер которых не превышает указанный максимальный размер. Если задача *Проверка съемных дисков* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

Таблица 4. Параметры задачи Проверка съемных дисков

Параметр	Описание
Тип проверки	**Подробная проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security проверяет все файлы, расположенные на съемном диске, в том числе вложенные файлы внутри составных объектов, архивы, дистрибутивы, файлы офисных форматов. Kaspersky Endpoint Security не проверяет файлы почтовых форматов и защищенные паролем архивы. **Быстрая проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security проверяет только файлы определенных форматов (см. раздел "Приложение 3. Расширения файлов для быстрой проверки съемных дисков" на стр. 470), наиболее подверженные заражению, а также не распаковывает составные объекты.
Максимальный размер диска (МБ)	Если флажок установлен, то Kaspersky Endpoint Security выполняет выбранное действие над съемными дисками, размер которых не превышает указанный максимальный размер. Если размер съемного диска превышает указанное значение, Kaspersky Endpoint Security пропускает проверку. Если флажок снят, то Kaspersky Endpoint Security выполняет выбранное действие над съемными дисками любого размера.
Скрыть индикатор выполнения задачи проверки	Если флажок установлен, то Kaspersky Endpoint Security отображает ход проверки съемных дисков в отдельном окне, а также в разделе **Задачи**. Если флажок снят, то Kaspersky Endpoint Security выполняет проверку съемных дисков в фоновом режиме.
Запретить пользователям останавливать задачу проверки	Если флажок установлен, то в локальном интерфейсе Kaspersky Endpoint Security для задачи проверки съемных дисков недоступны кнопка **Стоп** в разделе **Задачи** и кнопка **Стоп** в окне проверки съемного диска.

kaspersky

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, загрузочного сектора, системной памяти и системного раздела.

Для экономии ресурсов компьютера рекомендуется вместо задачи полной проверки (см. раздел "Проверка компьютера" на стр. 63) использовать задачу фоновой проверки. Уровень защиты компьютера при этом не изменится. Область проверки для этих задач одинаковая. Для оптимизации нагрузки на компьютер приложение не запускает задачи полной проверки и фоновой проверки одновременно. Если вы запустили задачу полной проверки, Kaspersky Endpoint Security не будет запускать задачу фоновой проверки в течение семи дней после выполнения полной проверки.

Фоновая проверка запускается в следующих случаях:

- после обновления антивирусных баз;
- через 30 минут после запуска Kaspersky Endpoint Security;
- каждые шесть часов;
- при простое компьютера в течение пяти и более минут (компьютер заблокирован или включена экранная заставка).

Фоновая проверка при простое компьютера прерывается при выполнении любого из следующих условий:

- Компьютер перешел в активный режим.

  Если фоновая проверка не выполнялась более десяти дней, проверка не прерывается.

- Компьютер (ноутбук) перешел в режим питания от батареи.

При выполнении фоновой проверки Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

► *Как включить фоновую проверку в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. Используйте переключатель **Фоновая проверка**, чтобы включить или выключить фоновую проверку.
4. Сохраните внесенные изменения.

Если задача *Фоновая проверка* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

Проверка из контекстного меню

Kaspersky Endpoint Security позволяет проверять отдельные файлы на вирусы и другие приложения, представляющие угрозу, из контекстного меню (см. рис. ниже).

При выполнении проверки из контекстного меню Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

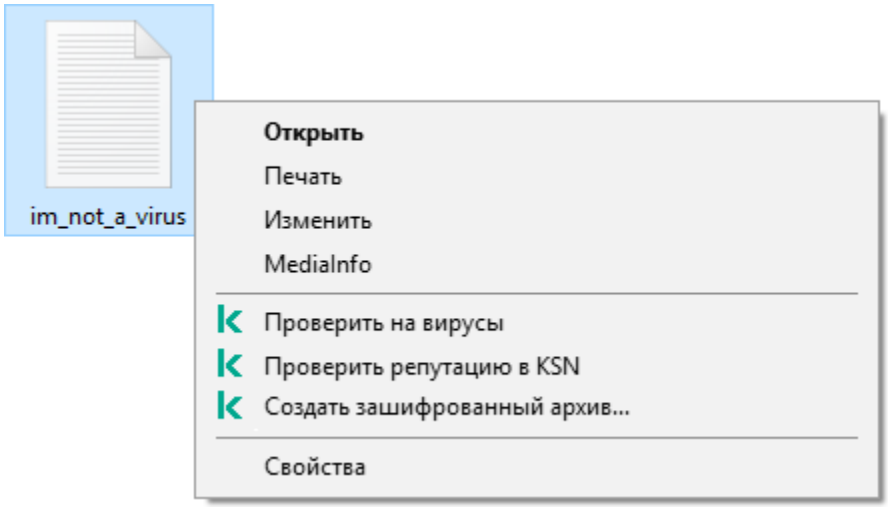


Рисунок 18. Контекстное меню файла

► *Как настроить параметры проверки из контекстного меню в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. Настройте параметры проверки из контекстного меню (см. таблицу ниже).
4. Сохраните внесенные изменения.

Если задача *Проверка из контекстного меню* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

Таблица 5. Параметры задачи Проверка из контекстного меню

Параметр	Описание
Уровень безопасности	Для проверки Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*: • **Высокий**. Приложение Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Глубокий**. • **Рекомендуемый**. Приложение Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Средний**. • **Низкий**. Приложение Kaspersky Endpoint Security проверяет только файлы определенных форматов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Поверхностный**.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. **Лечить. Информировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз. **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.

Параметр	Описание
Типы файлов	Файлы без расширения приложение Kaspersky Endpoint Security считает исполняемыми. Приложение проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки. **Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Формат файла определяется на основании его расширения. По умолчанию Kaspersky Endpoint Security проверяет файлы по формату. Проверять файлы по расширению менее безопасно, так как вредоносный файл может иметь расширение, которое не входит в список потенциально заражаемых (например, `.123`).
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Пропускать файл, если его проверка длится более N секунд	Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Endpoint Security останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Endpoint Security выполнит сначала и по расписанию.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.

Параметр	Описание
Проверять файлы почтовых форматов	Проверка файлов почтовых форматов, а также почтовой базы данных. Приложение проверяет PST- и OST-файлы, которые используют почтовые клиенты MS Outlook / Windows Mail, и EML-файлы. Kaspersky Endpoint Security не поддерживает работу с 64-битной версией почтового клиента MS Outlook. То есть, Kaspersky Endpoint Security не проверяет файлы, связанные с работой 64-битной версии почтового клиента MS Outlook (PST- и OST-файлы), даже если почта включена в область проверки (см. раздел "Формирование области проверки" на стр. 78). Если флажок установлен, Kaspersky Endpoint Security разбирает файл почтового формата на составляющие части (заголовок, тело, вложения) и анализирует их на наличие угроз. Если флажок снят, Kaspersky Endpoint Security проверяет файл почтового формата как единый файл. При обнаружении вредоносного объекта в PST- и OST-файлах Kaspersky Endpoint Security обезвреживает его в соответствии с выбранным действием (например, лечение или удаление файла). При обнаружении вредоносного объекта в файлах других почтовых клиентов (например, Mozilla Thunderbird), Kaspersky Endpoint Security только отмечает зараженное письмо. Вам необходимо удалить письмо с вредоносным файлом во вложении вручную.
Проверять архивы, защищенные паролем	Если флажок установлен, приложение проверяет архивы, защищенные паролем. Перед проверкой файлов, содержащихся в архиве, на экран выводится запрос пароля. Если флажок не установлен, приложение пропускает проверку защищенных паролем архивов.
Не распаковывать составные файлы большого размера	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Машинное обучение и сигнатурный анализ	При методе проверки Машинное обучение и сигнатурный анализ используются базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защиту с использованием этого метода проверки обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Параметр	Описание
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Технология iSwift	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
Технология iChecker	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Проверка целостности приложения

Kaspersky Endpoint Security проверяет модули приложения на наличие повреждений или изменений. Например, если библиотека приложения имеет некорректную цифровую подпись, то такая библиотека считается поврежденной. Для проверки файлов приложения предназначена задача *Проверка целостности приложения*. Запускайте задачу *Проверка целостности приложения*, если приложение Kaspersky Endpoint Security обнаружило вредоносный объект и не обезвредило его.

Вы можете создать задачу *Проверка целостности приложения* в Kaspersky Security Center Web Console и Консоли администрирования. Создать задачу в приложении Kaspersky Security Center Cloud Console невозможно.

Нарушения целостности приложения могут, например, возникать в следующих случаях:

- Вредоносный объект внес изменения в файлы Kaspersky Endpoint Security. В этом случае выполните процедуру восстановления Kaspersky Endpoint Security средствами операционной системы. После восстановления запустите полную проверку компьютера и повторите проверку целостности.
- Истек срок действия цифровой подписи. В этом случае обновите Kaspersky Endpoint Security.

► *Как выполнить проверку целостности в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу *Проверка целостности приложения* и нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security выполнит проверку целостности приложения. Вы также можете настроить расписание проверки целостности приложения в свойствах задачи (см. таблицу ниже). Если задача *Проверка целостности приложения* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

Таблица 6. Параметры задачи Проверка целостности

Параметр	Описание
Расписание проверки	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.
Выполнять только во время простоя компьютера	Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

Формирование области проверки

Область проверки – список путей к папкам и файлам, которые Kaspersky Endpoint Security проверяет во время выполнения задачи. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

kaspersky

Для формирования области проверки рекомендуется использовать задачу *Выборочная проверка*. Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задач *Полная проверка* и *Проверка важных областей*.

В Kaspersky Endpoint Security предустановлены следующие объекты для формирования области проверки:

- **Системная память**.
- **Объекты автозапуска**.

  Память, занятая процессами, и исполняемые файлы приложения, которые запускаются при старте операционной системы.
- **Загрузочные секторы**.

  Загрузочные секторы жестких и съемных дисков.
- **Системное резервное хранилище**.

  Содержимое папки System Volume Information.
- **Все внешние устройства**.
- **Все жесткие диски**.
- **Все сетевые диски**.

  В Kaspersky Endpoint Security для Windows версии 12.12 почта исключена из области проверки приложения. Проверку входящих и исходящих сообщений выполняет компонент Защита от почтовых угроз (см. раздел "Формирование области защиты компонента Защита от почтовых угроз" на стр. 163). Если вы используете плагин управления более ранней версии, то приложение исключает почту из области проверки, даже если эта область включена в политике.
  Для проверки сетевых дисков или сетевых папок рекомендуется создавать отдельную задачу проверки. В параметрах задачи *Поиск вредоносного ПО* укажите пользователя, у которого есть права на запись на этом диске, для устранения обнаруженных угроз. Если на сервере, на котором расположен сетевой диск, установлены собственные инструменты защиты, запускать задачу проверки на этом диске не требуется. Это позволит не проверять объекты дважды и повысит производительность сервера.

Для исключения папок или файлов из области проверки вам нужно добавить папку или файл в доверенную зону. (см. раздел "Создание исключения из проверки" на стр. 320)

► *Как сформировать область проверки в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу *Выборочная проверка* и нажмите на кнопку **Выбрать**.

   Вы также можете изменить область проверки для других задач. Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задач *Полная проверка* и *Проверка важных областей*.
3. В открывшемся окне выберите объекты, которые вы хотите добавить в область проверки.
4. Сохраните внесенные изменения.

Если задача проверки не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

kaspersky

Запуск проверки по расписанию

Проверка компьютера занимает некоторое время и требует затрат ресурсов компьютера. Выберите оптимальное время для запуска проверки компьютера, чтобы производительность других приложений не снижалась. Kaspersky Endpoint Security позволяет настроить обычное расписание проверки компьютера. Этот способ удобен, если сотрудники вашей организации работают по графику. Вы можете настроить запуск проверки компьютера ночью или в выходные дни. Если по каким-либо причинам запуск задачи проверки невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи проверки, как только это станет возможным.

Если настроить оптимальное расписание проверки компьютера не удалось, Kaspersky Endpoint Security позволяет запускать проверку компьютера при выполнении следующих специальных условий:

- После обновления баз.

  Kaspersky Endpoint Security запускает проверку компьютера с новыми базами сигнатур.

- При запуске приложения.

  Kaspersky Endpoint Security запускает проверку компьютера по истечении заданного времени после старта приложения. После старта операционной системы запускается множество процессов, поэтому удобно запускать задачу проверки не сразу после запуска Kaspersky Endpoint Security, а через некоторое время.

- Функция Wake-on-LAN.

  Kaspersky Endpoint Security запускает проверку компьютера по расписанию даже если компьютер выключен. Для этого приложение использует функцию операционной системы Wake-on-LAN. Функция Wake-on-LAN позволяет удаленно включать компьютер с помощью отправки специального сигнала через локальную сеть. Для использования этой функции необходимо включить Wake-on-LAN в параметрах BIOS компьютера.

  Вы можете настроить запуск проверки компьютера с функцией Wake-on-LAN только для задачи *Поиск вредоносного ПО* в Kaspersky Security Center. Включить функцию Wake-on-LAN для проверки компьютера в интерфейсе приложения невозможно.

- При простое компьютера.

  Kaspersky Endpoint Security запускает проверку компьютера по расписанию, если включена экранная заставка или компьютер заблокирован. Если пользователь разблокировал компьютер, Kaspersky Endpoint Security приостанавливает проверку компьютера. Таким образом, приложение может выполнять полную проверку компьютера несколько дней.

► *Как настроить расписание проверки компьютера в интерфейсе приложения*

Вы можете настроить расписание проверки, только если к компьютеру не применена политика. Для компьютеров под политикой вы можете настроить расписание запуска задачи *Поиск вредоносного ПО* в Kaspersky Security Center.

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.

   Вы можете настроить расписание для запуска полной проверки, проверки важных областей и проверки целостности. Выборочную проверку вы можете запускать только вручную.

3. Нажмите на кнопку **Расписание проверки**.
4. В открывшемся окне настройте расписание запуска задачи проверки.
5. В зависимости от выбранной периодичности настройте дополнительные параметры, которые уточняют расписание запуска задачи (см. таблицу ниже).
6. Сохраните внесенные изменения.

Таблица 7. Параметры расписания проверки

Параметр	Описание
Расписание проверки	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Отложить запуск после старта приложения на N минут	Отложенный запуск задачи проверки после старта приложения. После старта операционной системы запускается множество процессов, поэтому удобно запускать задачу проверки не сразу после запуска Kaspersky Endpoint Security, а через некоторое время.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.
Выполнять только во время простоя компьютера	Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

Параметр	Описание
Использовать автоматическое определение случайного интервала между запусками задачи *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, задача запускается на компьютерах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит распределенный запуск задачи. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества компьютеров, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако, когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Использовать случайную задержку запуска задачи в интервале (мин)	Если флажок установлен, задача запускается на компьютерах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Остановить, если задача выполняется дольше (мин) *(доступен только в консоли Kaspersky Security Center)*	Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Endpoint Security останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Endpoint Security выполнит сначала и по расписанию. Чтобы уменьшить время выполнения задачи, вы можете, например, настроить область проверки (см. раздел "Формирование области проверки" на стр. 78) или оптимизировать проверку (см. раздел "Оптимизация проверки" на стр. 83).
Активировать устройства перед запуском задачи функцией Wake-on-LAN за (мин) *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, операционная система на компьютере будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут. Установите флажок, если вы хотите запустить выполнение задачи на всех компьютерах, включая компьютеры, которые выключены.
Выключать устройства после выполнения задачи *(доступен только в консоли Kaspersky Security Center)*	Например, вы можете включить эту функцию для проверки компьютера в пятницу после рабочего дня. После завершения работы задачи приложение выключает компьютер на выходные.

Запуск проверки с правами другого пользователя

По умолчанию задача проверки запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Область защиты может включать сетевые диски или другие объекты, для доступа к которым нужны специальные права. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения, и запускать задачу проверки от имени этого пользователя.

Вы можете запускать проверку с правами другого пользователя для следующих типов проверки:

- Проверка важных областей.
- Полная проверка.
- Выборочная проверка.
- Проверка из контекстного меню (на стр. 73).

Настроить права пользователя для запуска проверки съемных дисков (см. раздел "Проверка съемных дисков при подключении к компьютеру" на стр. 70), фоновой проверки (см. раздел "Фоновая проверка" на стр. 72) и проверки целостности (см. раздел "Проверка целостности приложения" на стр. 77) невозможно.

► *Как запустить проверку с правами другого пользователя в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. В свойствах задачи выберите **Расширенная настройка → Запускать проверку с правами**.
4. В открывшемся окне введите учетные данные пользователя, права которого требуется использовать для запуска задачи проверки.
5. Сохраните внесенные изменения.

Если задача проверки не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

Оптимизация проверки

Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы. Вы можете также ограничить длительность проверки одного файла. По истечении заданного времени Kaspersky Endpoint Security исключает файл из текущей проверки (кроме архивов и объектов, в состав которых входит несколько файлов).

Распространенной практикой сокрытия вирусов и других приложений, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие приложения, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки.

Вы также можете включить использование технологий iChecker и iSwift. Технологии iChecker и iSwift позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Как оптимизировать проверку в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Оптимизация** настройте параметры проверки:
   - **Проверять только новые и измененные файлы**. Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.

     Вы также можете настроить проверку новых файлов по типам. Например, вы можете запускать проверку всех дистрибутивов и проверку только новых архивов и файлов офисных форматов.
   - **Пропускать файл, если его проверка длится более N секунд**. Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Endpoint Security останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Endpoint Security выполнит сначала и по расписанию.
   - **Не запускать несколько задач проверки одновременно**. Отложенный запуск задач проверки, если проверка уже выполняется. Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, приложение запустило задачу полной проверки по расписанию. Если пользователь пытается запустить быструю проверку в интерфейсе приложения, Kaspersky Endpoint Security поставит задачу быстрой проверки в очередь и автоматически запустит задачу после завершения полной проверки.
5. В блоке **Ограничение по размеру** установите флажок **Не распаковывать составные файлы большого размера**. Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Endpoint Security останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Endpoint Security выполнит сначала и по расписанию.

   Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
6. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать во время проверки:
   - **Технология iSwift**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
   - **Технология iChecker**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

7. Сохраните внесенные изменения.

Если задача проверки не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

Контроль потребления ресурсов процессора при проверке компьютера

Вы можете ограничить потребление ресурсов процессора при выполнении задачи *Поиск вредоносного ПО*. При этом время проверки компьютера может увеличиться.

► *Как ограничить потребление ресурсов процессора при проверке компьютера в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

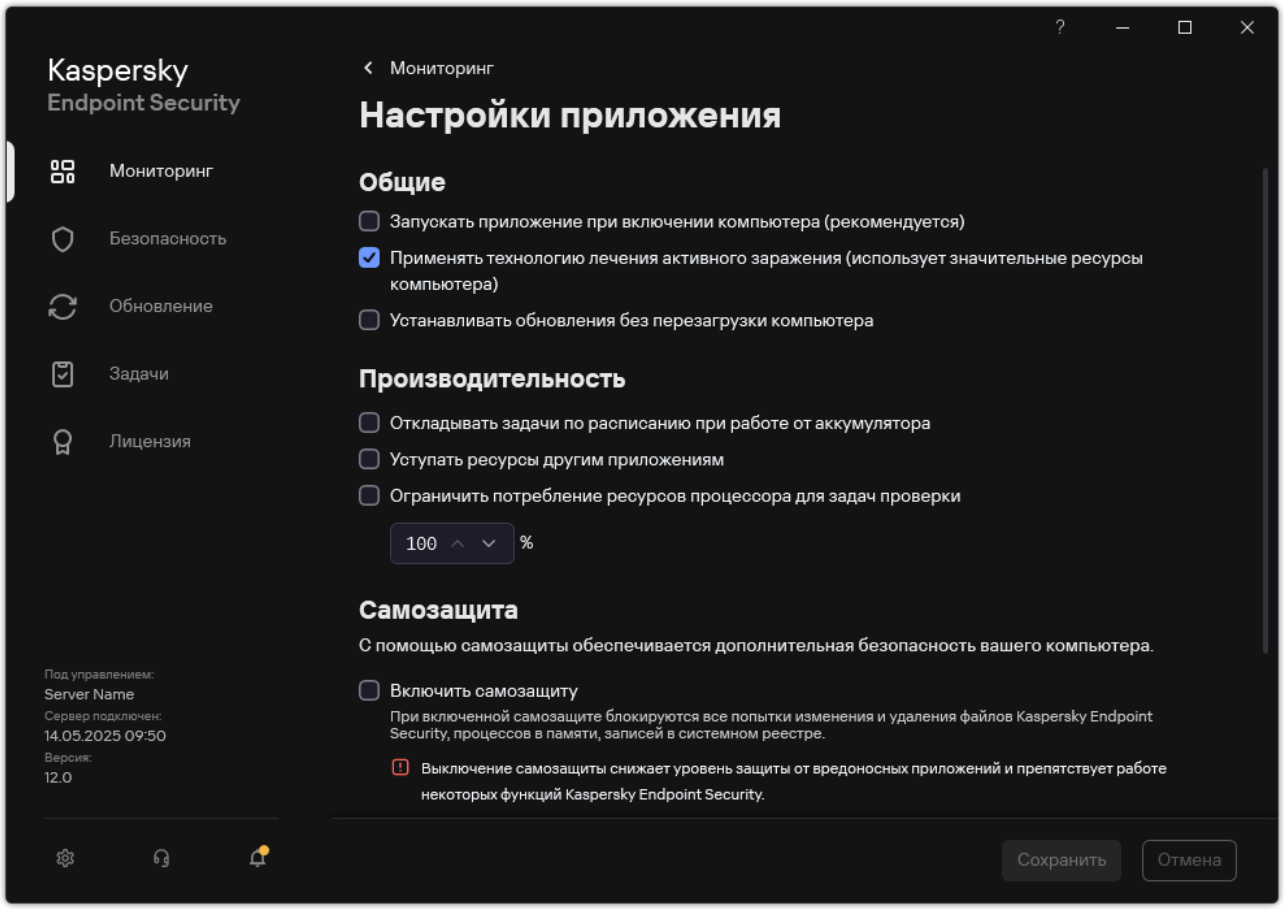


Рисунок 19. Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Производительность** установите флажок **Ограничить потребление ресурсов процессора для задач проверки** и введите среднее значение потребления ресурсов процессора в процентах.
4. Сохраните внесенные изменения.

kaspersky

Обновление баз и модулей программы

В сертифицированной конфигурации не допускается загружать и устанавливать обновления модулей программы. Изменение модулей программы может привести к выходу из безопасного состояния.

Обновление баз и модулей приложения Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие приложения, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули приложения.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в приложении на территории США.

Для регулярного обновления требуется действующая лицензия на использование приложения. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера.

Загрузка обновлений осуществляется по протоколу HTTPS. Загрузка по протоколу HTTP может осуществляться в случае, когда загрузка обновлений по протоколу HTTPS невозможна.

В процессе обновления на ваш компьютер загружаются и устанавливаются следующие объекты:

- Базы Kaspersky Endpoint Security. Защита компьютера обеспечивается на основании баз данных, содержащих сигнатуры вирусов и других приложений, представляющих угрозу, и информацию о способах борьбы с ними. Компоненты защиты используют эту информацию при поиске и обезвреживании зараженных файлов на компьютере. Базы регулярно пополняются записями о появляющихся угрозах и способах борьбы с ними. Поэтому рекомендуется регулярно обновлять базы.

  Наряду с базами Kaspersky Endpoint Security обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

- Модули приложения. Помимо баз Kaspersky Endpoint Security, можно обновлять и модули приложения. Обновления модулей приложения устраняют уязвимости Kaspersky Endpoint Security, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули приложения на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули приложения отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Информация о текущем состоянии баз Kaspersky Endpoint Security отображается в главном окне приложения или в подсказке при наведении курсора на значок приложения в области уведомлений.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Endpoint Security (см. раздел "Работа с отчетами" на стр. 342).

Если приложение работает в режиме Легкого агента, обновление баз и модулей приложения имеет особенности.

В этом разделе

Схема обновления с серверного хранилища 87
Запуск и остановка задачи обновления 90
Запуск задачи обновления с правами другого пользователя 91
Выбор режима запуска для задачи обновления 91
Добавление источника обновлений 92
Обновление модулей приложения 95
Использование прокси-сервера при обновлении 96
Откат последнего обновления 99
Обновление антивирусных баз в ручном режиме 100
Устранение уязвимостей и установка критических обновлений в приложении 101

Схема обновления с серверного хранилища

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на компьютерах локальной сети организации с серверного хранилища. Для этого Kaspersky Security Center должен загружать пакет обновлений в хранилище (FTP-сервер, сетевая или локальная папка) с серверов обновлений "Лаборатории Касперского". В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений с серверного хранилища.

В сертифицированной конфигурации приложения для загрузки обновлений с серверов "Лаборатории Касперского" используйте протокол HTTPS.

Настройка обновления баз и модулей приложения с серверного хранилища состоит из следующих этапов:

1. Настройка перемещения пакета обновлений в хранилище на Сервере администрирования (задача *Загрузка обновлений в хранилище Сервера администрирования*).

Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически мастером первоначальной настройки Сервера администрирования и может существовать только в единственном экземпляре. По умолчанию Kaspersky Security Center копирует пакет обновлений в папку `\\<server name>\KLSHARE\Updates`. Подробнее о загрузке обновлений в хранилище Сервера администрирования см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/180697.htm.

2. Настройка обновления баз и модулей приложения из указанного серверного хранилища на остальных компьютерах локальной сети организации (задача *Обновление баз и модулей приложения*).

Как настроить обновление Kaspersky Endpoint Security из указанного серверного хранилища в интерфейсе приложения

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

1. В главном окне приложения перейдите в раздел **Обновление**.

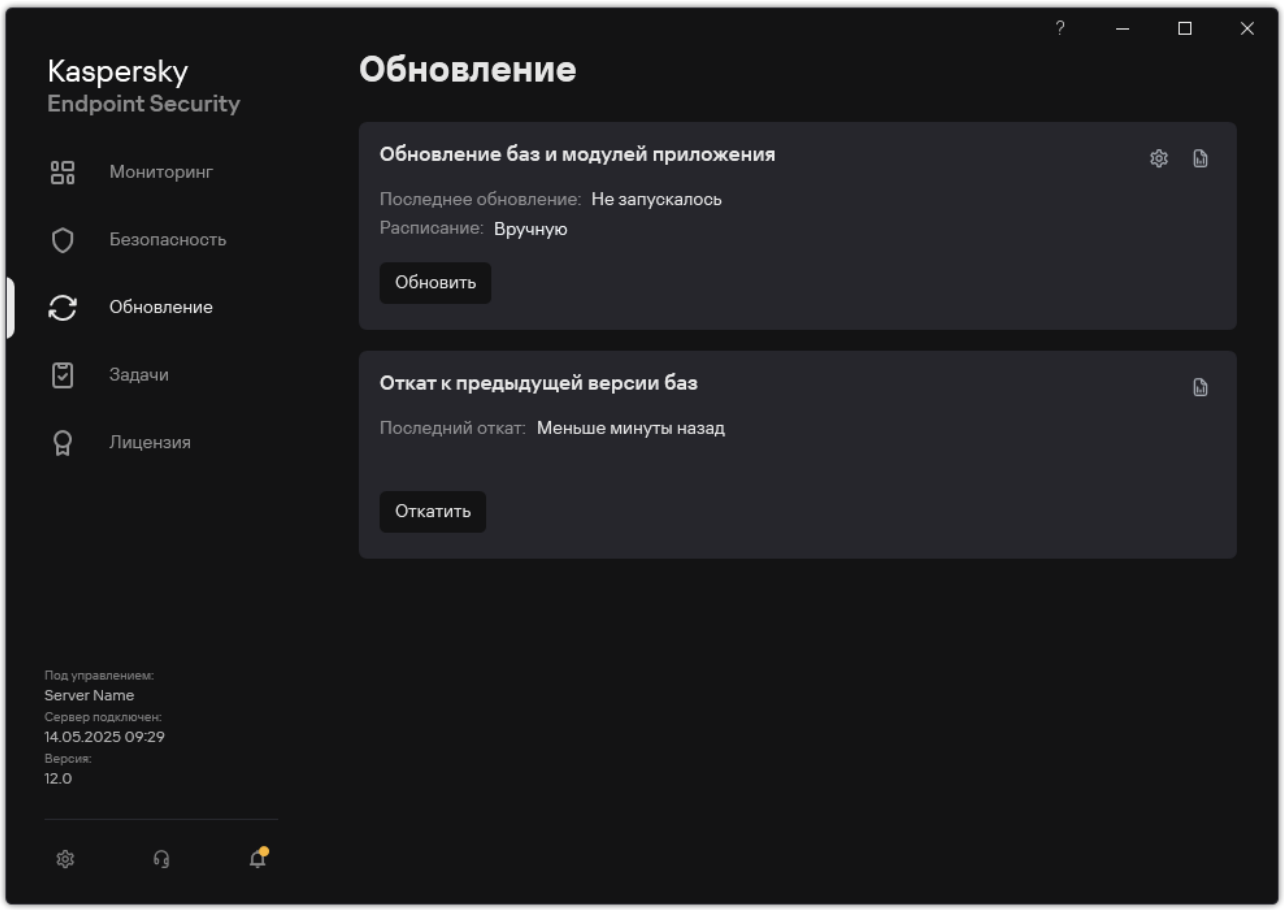


Рисунок 20. Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку .

   Откроется окно свойств задачи.

3. В окне свойств задачи нажмите **Настроить источники обновлений**.
4. В списке источников обновлений убедитесь, что обновление из источника **Kaspersky Security Center** включено. Также у источника **Kaspersky Security Center** должен быть наивысший приоритет.
5. Если требуется, добавьте источники обновлений:
   a. В списке источников обновлений нажмите на кнопку **Добавить**.

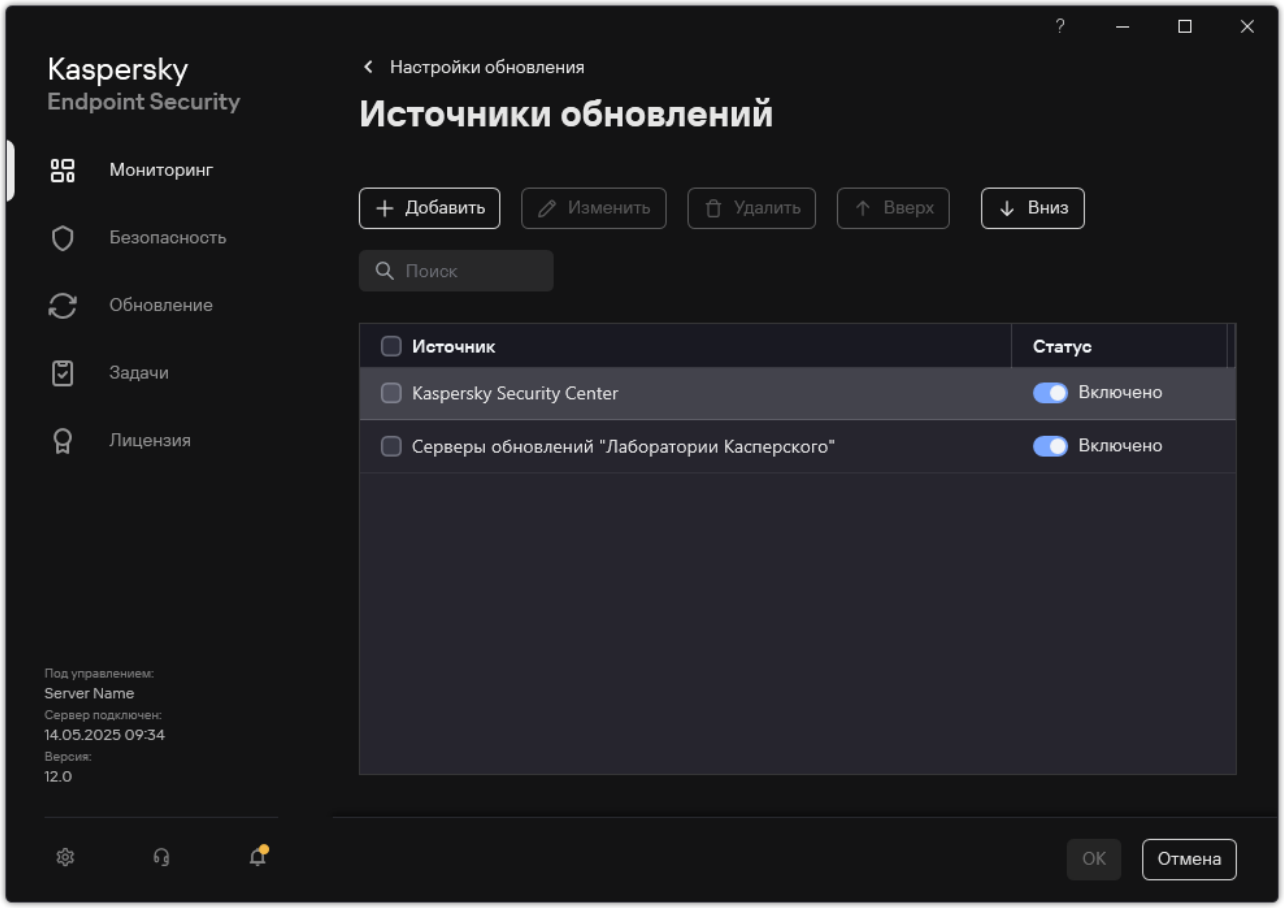


Рисунок 21. Источники обновлений

   b. Укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

   > Адрес источника должен совпадать с адресом, указанным в поле **Папка для хранения обновлений** при настройке загрузки обновлений в серверное хранилище (задача *Загрузка обновлений в хранилище Сервера администрирования*).

   c. Нажмите на кнопку **Выбрать**.

Вы можете исключить источник обновлений, не удаляя его из списка источников. Для этого выключите переключатель рядом с ним.

6. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

   > Если компьютер находится под управлением Kaspersky Security Center, настроить режим запуска задачи *Обновление баз и модулей приложения* невозможно. Вы можете запустить задачу только вручную.

7. Сохраните внесенные изменения.

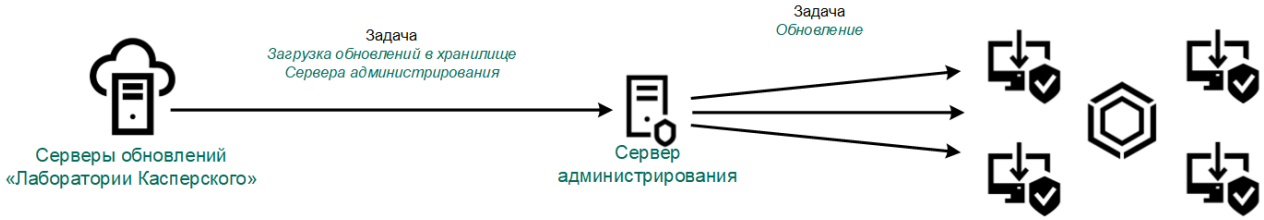


Рисунок 22. Обновление с серверного хранилища

Запуск и остановка задачи обновления

Независимо от выбранного режима запуска задачи обновления вы можете запустить или остановить задачу обновления Kaspersky Endpoint Security в любой момент.

► *Чтобы запустить или остановить задачу обновления, выполните следующие действия:*

1. В главном окне приложения перейдите в раздел **Обновление**.
2. В плитке **Обновление баз и модулей приложения** нажмите на кнопку **Обновить**, если вы хотите запустить задачу обновления.

Kaspersky Endpoint Security запустит обновление баз и модулей приложения. Приложение покажет процесс проверки, размер загруженных файлов и источник обновления. Вы можете остановить выполнение задачи в любое время кнопкой **Остановить обновление**.

► *Чтобы запустить или остановить задачу обновления при отображении упрощенного интерфейса приложения, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка приложения, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
   - выберите незапущенную задачу обновления, чтобы запустить ее;
   - выберите запущенную задачу обновления, чтобы остановить ее;
   - выберите остановленную задачу обновления, чтобы возобновить ее или запустить ее заново.

kaspersky

Запуск задачи обновления с правами другого пользователя

По умолчанию задача обновления приложения Kaspersky Endpoint Security запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление приложения Kaspersky Endpoint Security может производиться из источника обновления, к которому у пользователя нет прав доступа (например, из папки общего доступа, содержащей пакет обновлений) или для которого не настроено использование аутентификации на прокси-сервере. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения и запускать задачу обновления приложения Kaspersky Endpoint Security от имени этого пользователя.

► *Чтобы запускать задачу обновления с правами другого пользователя, выполните следующие действия:*

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

1. В главном окне приложения перейдите в раздел **Обновление**.
2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.
3. Нажмите на кнопку **Запускать обновление баз с правами пользователя**.
4. В открывшемся окне выберите вариант **Другого пользователя**.
5. Введите учетные данные пользователя, права которого требуется использовать для доступа к источнику обновлений.
6. Сохраните внесенные изменения.

Выбор режима запуска для задачи обновления

Если по каким-либо причинам запуск задачи обновления невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи обновления, как только это станет возможным.

Вы можете отложить запуск задачи обновления после старта приложения для случаев, если вы выбрали режим запуска задачи обновления **По расписанию** и время запуска Kaspersky Endpoint Security совпадает с расписанием запуска задачи обновления. Задача обновления запускается только по истечении указанного времени после старта Kaspersky Endpoint Security.

► *Чтобы выбрать режим запуска для задачи обновления, выполните следующие действия:*

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

1. В главном окне приложения перейдите в раздел **Обновление**.
2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку .

   Откроется окно свойств задачи.
3. Нажмите на кнопку **Режим запуска**.
4. В открывшемся окне выберите режим запуска задачи обновления:
   - Выберите вариант **Автоматически**, если вы хотите, чтобы Kaspersky Endpoint Security запускал задачу обновления в зависимости от наличия пакета обновлений в источнике обновления. Частота проверки Kaspersky Endpoint Security наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии.
   - Выберите вариант **Вручную**, если вы хотите запускать задачу обновления вручную.
   - Выберите другие варианты, если вы хотите настроить расписание запуска задачи обновления. Настройте дополнительные параметры запуска задачи обновления:
     - В поле **Отложить запуск после старта приложения на N минут** укажите время, на которое следует отложить запуск задачи обновления после старта Kaspersky Endpoint Security.
     - Установите флажок **Запускать проверку по расписанию на следующий день, если компьютер был выключен**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенные вовремя задачи обновления. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени.
5. Сохраните внесенные изменения.

Добавление источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Endpoint Security.

Источником обновлений могут быть сервер Kaspersky Security Center, серверы обновлений "Лаборатории Касперского", сетевая или локальная папка.

По умолчанию список источников обновлений содержит сервер Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указывать HTTP- или FTP-серверы, папки общего доступа.

Kaspersky Endpoint Security не поддерживает загрузку обновлений с HTTPS-серверов, если это не серверы обновлений "Лаборатории Касперского".

Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления Kaspersky Endpoint Security обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений.

По умолчанию Kaspersky Endpoint Security использует сервер Kaspersky Security Center в качестве первого источника обновлений. Это позволяет сократить расход трафика при обновлении. Если к компьютеру не применена политика, в параметрах локальной задачи *Обновление баз и модулей приложения* выбраны серверы "Лаборатории Касперского" в качестве первого источника обновления, так как у приложения может отсутствовать доступ к серверу Kaspersky Security Center.

Если приложение работает в режиме Легкого агента, в качестве источника обновлений выбрана папка на SVM.

► *Как добавить источник обновлений в интерфейсе приложения*

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

1. В главном окне приложения перейдите в раздел **Обновление**.
2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.
3. Нажмите на кнопку **Настроить источники обновлений**.
4. В открывшемся окне нажмите на кнопку **Добавить**.

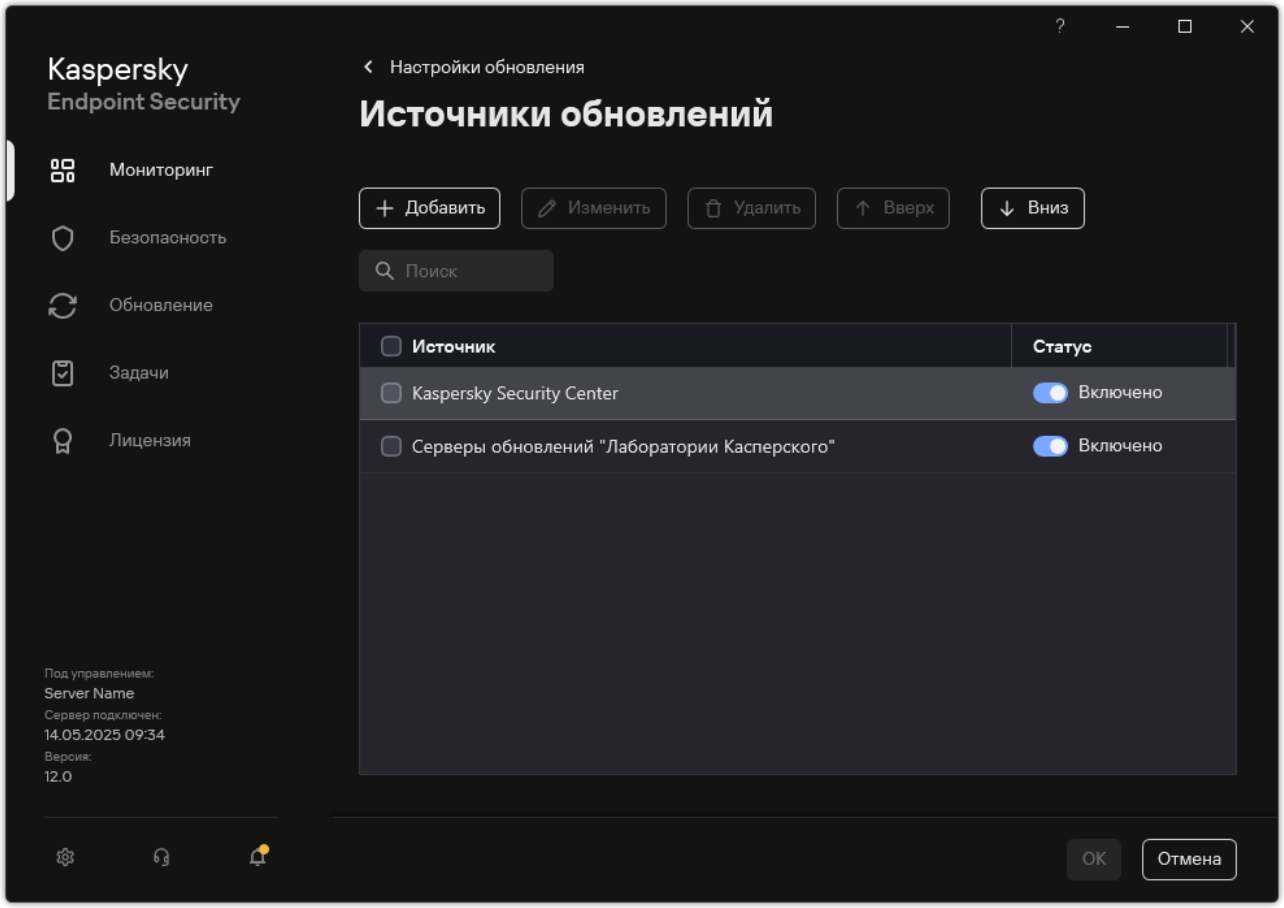


Рисунок 23. Источники обновлений

5. В открывшемся окне укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, которая содержит пакет обновлений.

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` или `93.191.13.103`.

     Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<user name>:<password>@<node>:<port>`.

   - Для сетевой папки введите UNC-путь.

     Например, `\\Server\Share\Update distribution`.

   - Для локальной папки введите полный путь к папке.

     Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Нажмите на кнопку **Выбрать**.
7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.
8. Сохраните внесенные изменения.

kaspersky

Обновление модулей приложения

Обновления модулей приложения исправляют ошибки, улучшают производительность, а также добавляют новые функции. При появлении нового обновления модулей приложения вам необходимо подтвердить установку обновления. Вы можете подтвердить установку обновления модулей приложения в интерфейсе приложения или в Kaspersky Security Center. При появлении обновления приложение покажет уведомление в главном окне Kaspersky Endpoint Security –  . Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения, то приложение устанавливает обновление после согласия с положениями Лицензионного соглашения.

Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

После установки обновления приложения может потребоваться перезагрузка компьютера.

Как настроить обновление модулей приложения в интерфейсе приложения

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

1. В главном окне приложения перейдите в раздел **Обновление**.
2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку  .

   Откроется окно свойств задачи.
3. В блоке **Загрузка и установка обновлений модулей приложения** установите флажок **Загружать обновления модулей приложения**.
4. Выберите обновления модулей приложения, которые вы хотите устанавливать:
   - **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает критические обновления автоматически, а остальные обновления модулей приложения – после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center.
   - **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию.
5. Сохраните внесенные изменения.

Использование прокси-сервера при обновлении

Для загрузки обновлений баз и модулей приложения из источника обновлений может потребоваться указать параметры прокси-сервера. Если источников обновлений несколько, параметры прокси-сервера применяются для всех источников. Если для некоторых источников обновлений прокси-сервер не нужен, вы можете выключить использование прокси-сервера в свойствах политики. Kaspersky Endpoint Security также будет использовать прокси-сервер для доступа к Kaspersky Security Network и серверам активации.

► *Чтобы настроить подключение к источникам обновлений через прокси-сервер, выполните следующие действия:*

1. В главном окне Web Console нажмите .

   Откроется окно свойств Сервера администрирования.
2. Перейдите в раздел **Параметры доступа к сети интернет**.
3. Установите флажок **Использовать прокси-сервер**.
4. Настройте параметры подключения к прокси-серверу: адрес прокси-сервера, порт и параметры аутентификации (имя пользователя и пароль).
5. Сохраните внесенные изменения.

► *Чтобы выключить использование прокси-сервера для определенной группы администрирования, выполните следующие действия:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки сети**.
5. В блоке **Прокси-сервер** нажмите на кнопку **Настройки**.
6. В открывшемся окне установите флажок **Не использовать прокси-сервер для локальных адресов**.
7. Сохраните внесенные изменения.

► *Чтобы настроить параметры прокси-сервера в интерфейсе приложения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

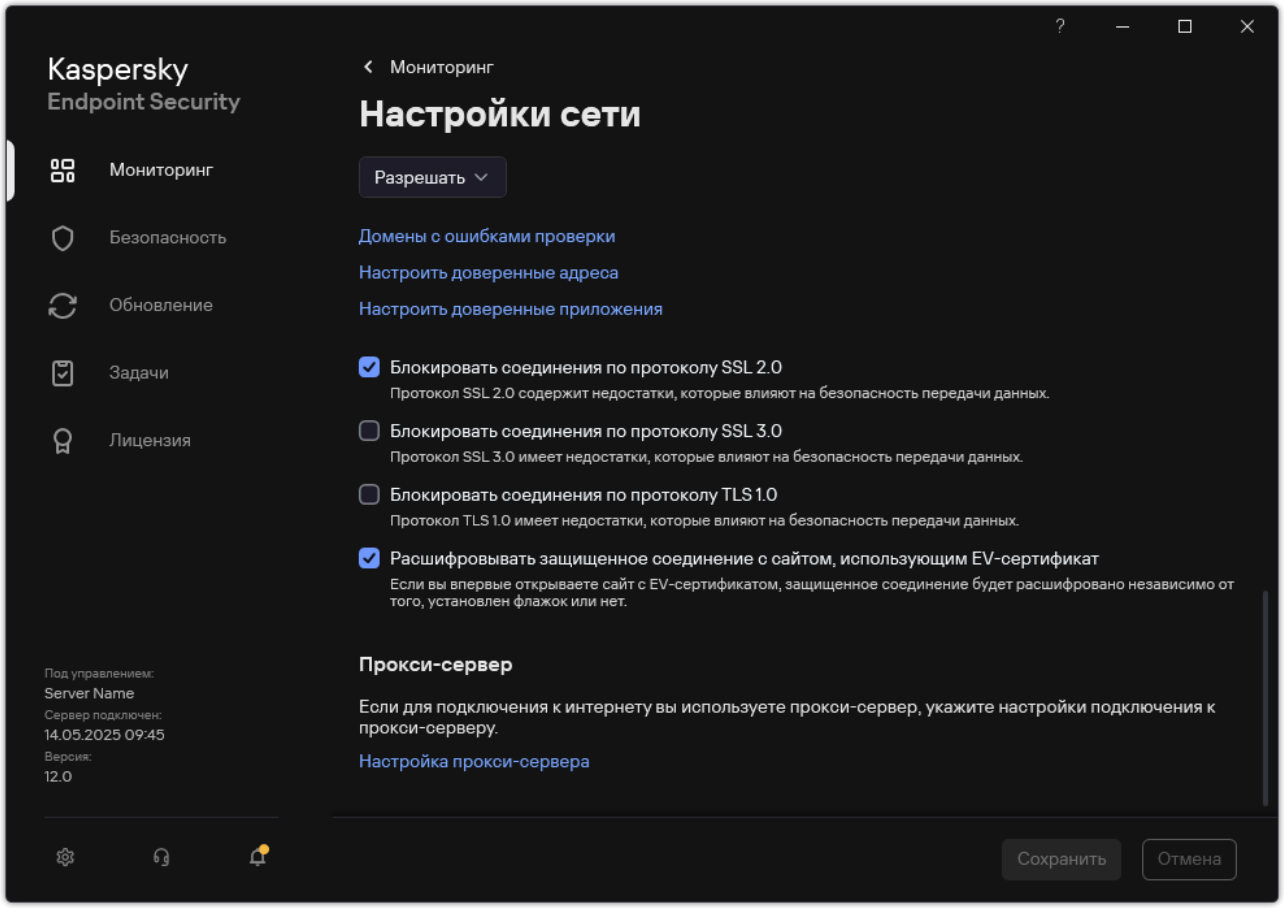


Рисунок 24. Параметры сети приложения

3. В блоке **Прокси-сервер** перейдите по ссылке **Настройка прокси-сервера**.

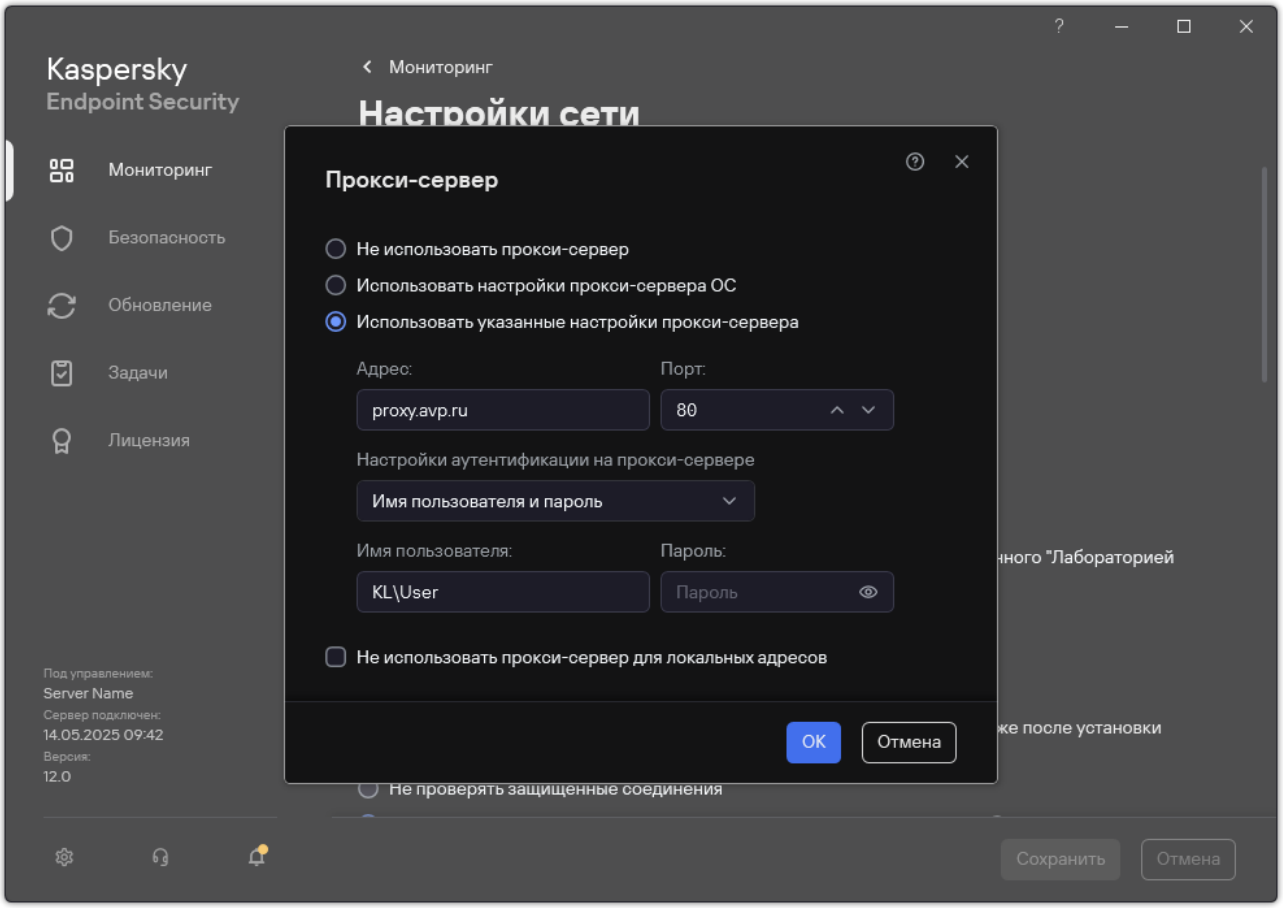


Рисунок 25. Параметры подключения к прокси-серверу

4. В открывшемся окне выберите один из следующих вариантов определения адреса прокси-сервера:
   - **Использовать настройки прокси-сервера ОС**.

     Этот вариант выбран по умолчанию. Kaspersky Endpoint Security использует параметры прокси-сервера, заданные в параметрах операционной системы.
   - **Использовать указанные настройки прокси-сервера**.

     Если вы выбрали этот вариант, настройте параметры подключения к прокси-серверу: адрес прокси-сервера и порт.
5. Выберите способ аутентификации приложения на прокси-сервере. По умолчанию приложение использует доменную NTLM-аутентификацию текущего пользователя.
6. Если вы хотите выключить использование прокси-сервера при обновлении баз и модулей приложения из папки общего доступа, установите флажок **Не использовать прокси-сервер для локальных адресов**.
7. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет использовать прокси-сервер для загрузки обновлений баз и модулей приложения. Также Kaspersky Endpoint Security использует прокси-сервер для доступа к серверам KSN и серверам активации "Лаборатории Касперского". Если требуется аутентификация на прокси-сервере, а учетные данные пользователя не указаны или указаны неверно, Kaspersky Endpoint Security запросит имя пользователя и пароль.

Откат последнего обновления

После первого обновления баз и модулей приложения становится доступна функция отката к предыдущим базам и модулям приложения.

Каждый раз, когда пользователь запускает обновление, Kaspersky Endpoint Security создает резервную копию используемых баз и модулей приложения и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущих баз и модулей приложения при необходимости. Возможность отката последнего обновления полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасное приложение.

Kaspersky Endpoint Security в режиме Легкого агента не поддерживает задачу *Откат обновления*.

► *Как откатить последнее обновление в интерфейсе приложения*

1. В главном окне приложения перейдите в раздел **Обновление**.
2. В плитке **Откат к предыдущей версии баз** нажмите на кнопку **Откатить**.

Kaspersky Endpoint Security запустит откат последнего обновления баз. Приложение покажет процесс отката, размер загруженных файлов и источник обновления. Вы можете остановить выполнение задачи в любое время кнопкой **Остановить обновление**.

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В приложении Kaspersky Security Center, находящемся в открытом сегменте сети, настроить задачу загрузки обновлений в хранилище.
2. Убедиться в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые машины с установленными приложениями, базы для которых необходимо обновить.
3. Запустить задачу. В процессе загрузки обновлений с открытых серверов «Лаборатории Касперского» Kaspersky Security Center проведет проверку контроля целостности обновлений, прежде чем добавит их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.

Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления с указанием перенесенного хранилища как источника обновлений. При загрузке обновлений из хранилища, приложения еще раз проведут контроль целостности загружаемых обновлений.

kaspersky

Устранение уязвимостей и установка критических обновлений в приложении

"Лаборатория Касперского" может выпускать обновления приложения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе приложения, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Допускается устанавливать только обновления модулей приложения, прошедшие процедуру сертификации, и критические обновления. Включение автоматического обновления модулей приводит к выходу приложения из сертифицированного состояния.

Лицо, ответственное за эксплуатацию приложения, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в приложении, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях приложения следующими способами:

- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

kaspersky

Технология лечения активного заражения

Для работы с активными угрозами Kaspersky Endpoint Security использует технологию лечения активного заражения. Лечение активного заражения для рабочих станций и серверов отличается. Вы можете настроить лечение активного заражения в свойствах задачи *Поиск вредоносного ПО* (см. раздел "*Проверка компьютера*" на стр. 63) и в параметрах приложения.

Если Kaspersky Endpoint Security не может остановить выполнение вредоносного приложения, вы можете использовать технологию лечения активного заражения. Для компьютеров под политикой технология лечения активного заражения по умолчанию выключена, так как технология использует значительные ресурсы компьютера. Для компьютеров не под политикой технология лечения активного заражения по умолчанию включена.

Работа технологии лечения активного заражения для рабочих станций и серверов отличается. Для работы технологии на серверах вам нужно включить немедленное лечение активного заражения (см. раздел "Проверка компьютера" на стр. 63) в свойствах задачи *Поиск вредоносного ПО*. Для работы технологии на рабочих станциях это условие не является обязательным.

Как включить или выключить технологию лечения активного заражения в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

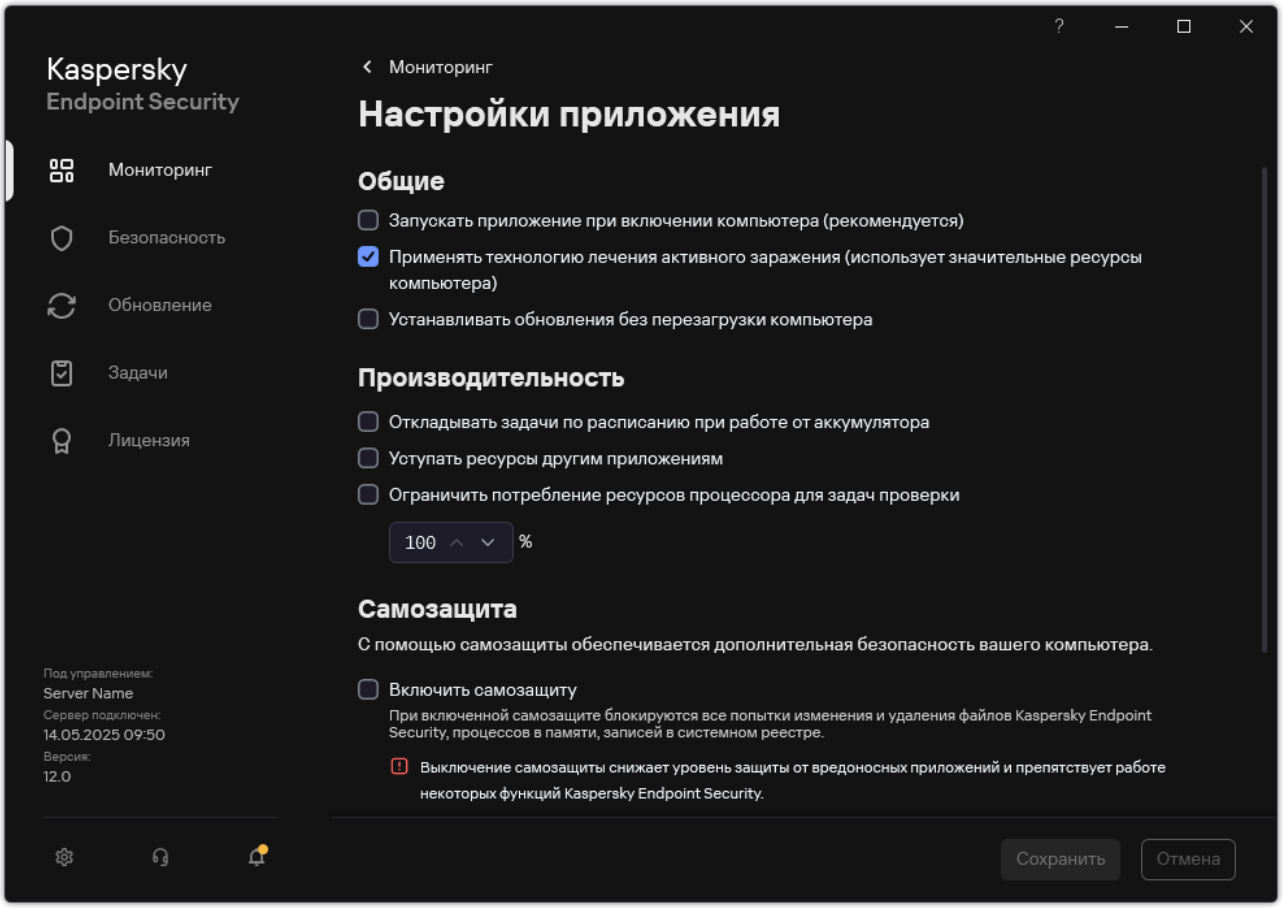


Рисунок 26. Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Общие** используйте флажок **Применять технологию лечения активного заражения (использует значительные ресурсы компьютера)**, чтобы включить или выключить технологию лечения активного заражения.
4. Сохраните внесенные изменения.

В результате при лечении активного заражения пользователю не будут доступны большинство функций операционной системы. После завершения лечения компьютер будет перезагружен.

В этом разделе

Лечение активных угроз на рабочих станциях 103
Лечение активных угроз на серверах 105

Лечение активных угроз на рабочих станциях

Для работы с активными угрозами на рабочих станциях вам нужно включить технологию лечения активного заражения (см. раздел "Технология лечения активного заражения" на стр. 102) в параметрах приложения. Далее вам нужно настроить взаимодействие приложения с пользователем в свойствах задачи *Поиск вредоносного ПО* (см. раздел "*Проверка компьютера*" на стр. 63). В свойствах задачи есть флажок **Выполнять лечение активного заражения немедленно**. Если флажок установлен, Kaspersky Endpoint Security выполнит лечение без уведомления пользователя. После лечения угроз компьютер будет перезагружен. Если флажок снят, Kaspersky Endpoint Security показывает уведомление об обнаружении активных угроз (см. рис. ниже). Закрыть уведомление, не обработав файл, невозможно.

Лечение активного заражения в ходе выполнения задачи поиска вирусов на компьютере осуществляется только в том случае, если в свойствах примененной к этому компьютеру политики включена функция лечения активного заражения (см. раздел "Технология лечения активного заражения" на стр. 102).

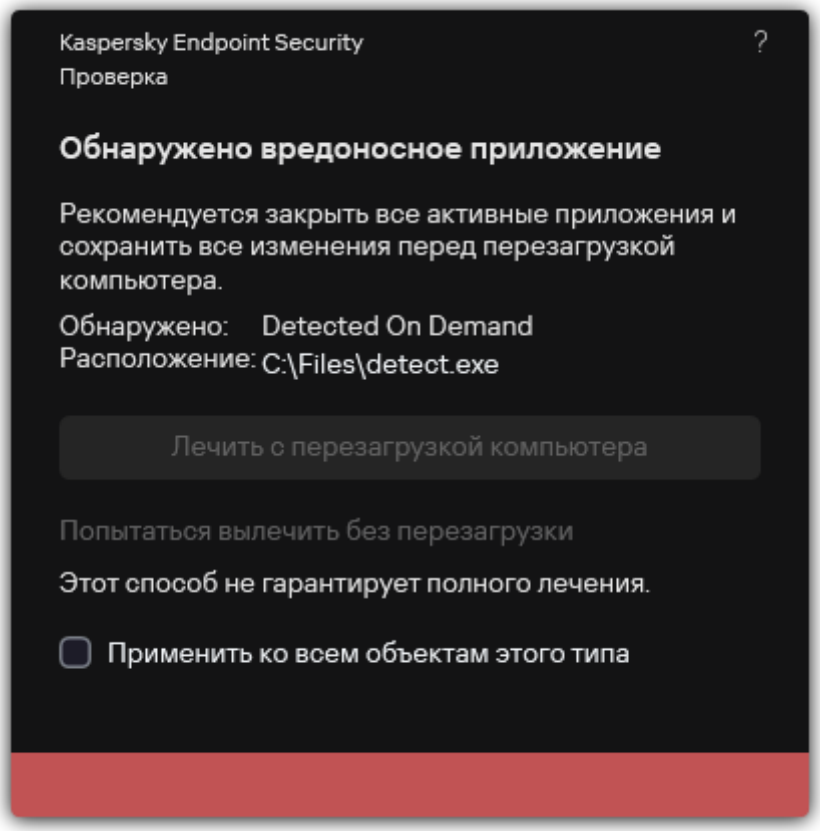


Рисунок 27. Уведомление об активной угрозе

kaspersky

Лечение активных угроз на серверах

Для работы с активными угрозами на серверах вам нужно выполнить следующие действия:

- включите технологию лечения активного заражения (см. раздел "Технология лечения активного заражения" на стр. 102) в параметрах приложения;
- включите немедленное лечение активного заражения (см. раздел "Проверка компьютера" на стр. 63) в свойствах задачи *Поиск вредоносного ПО*.

Если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов, Kaspersky Endpoint Security не показывает уведомление. Таким образом, пользователь не может выбрать действие для лечения активного заражения. Для устранения угрозы вам необходимо включить технологию лечения активного заражения (см. раздел "Технология лечения активного заражения" на стр. 102) в параметрах приложения и включить немедленное лечение активного заражения (см. раздел "Проверка компьютера" на стр. 63) в свойствах задачи *Поиск вредоносного ПО*. Далее вам нужно запустить задачу *Поиск вредоносного ПО*.

Устранение необработанных угроз

Kaspersky Endpoint Security фиксирует информацию о файлах, которые она по каким-либо причинам не обработала. Эта информация записывается в виде событий в список активных угроз (см. рис. ниже).

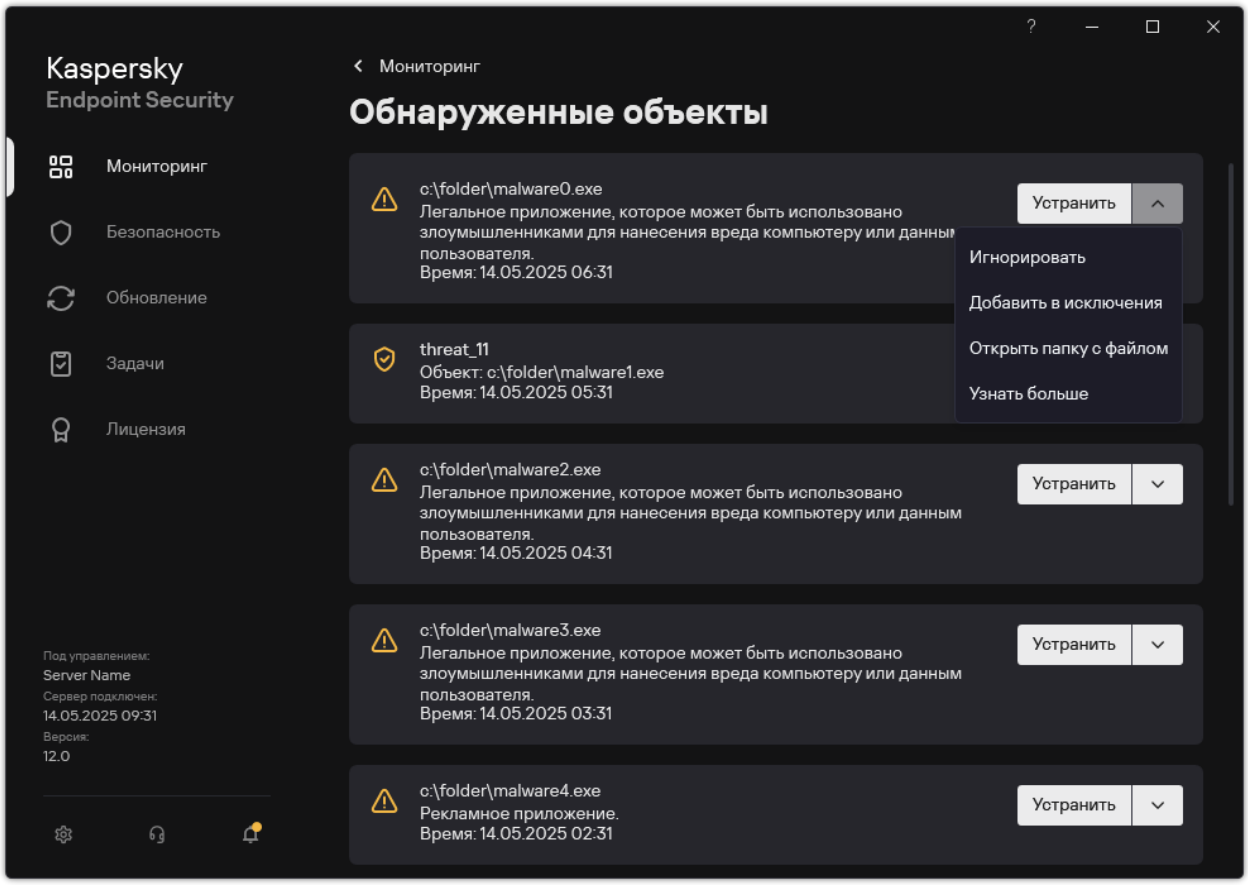


Рисунок 28. Список активных угроз

Зараженный файл считается *обработанным*, если Kaspersky Endpoint Security в процессе проверки компьютера на вирусы и другие приложения, представляющие угрозу, вылечил или удалил угрозу.

Kaspersky Endpoint Security помещает файл в список активных угроз, если в процессе проверки компьютера на вирусы и другие приложения, представляющие угрозу, Kaspersky Endpoint Security по каким-либо причинам не совершил действие с этим файлом согласно заданным настройкам приложения.

Такая ситуация возможна в следующих случаях:

- Проверяемый файл недоступен (например, находится на сетевом диске или внешнем диске без прав на запись данных).
- В настройках задачи *Поиск вредоносного ПО* (см. раздел "*Проверка компьютера*" на стр. 63) при обнаружении угрозы выбрано действие **Информировать**. Далее, когда на экране отобразилось уведомление о зараженном файле, пользователь выбрал вариант **Пропустить**.

При наличии необработанных угроз Kaspersky Endpoint Security изменит значок на . В главном окне приложения появится сообщение об угрозе (см. рис ниже). В консоли Kaspersky Security Center статус компьютера будет изменен на *Критический* – .

► *Как обработать угрозу в интерфейсе приложения*

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Безопасность под угрозой**.

   Откроется список активных угроз.

2. Выберите объект, который вы хотите обработать.
3. Выберите способ обработки угрозы:

   - **Устранить**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.
   - **Добавить в исключения**. Если выбран этот вариант действия, то Kaspersky Endpoint Security предложит добавить файл в список исключений из проверки (см. раздел "Создание исключения из проверки" на стр. 320). Приложение автоматически настроит параметры исключения. Если добавление исключения недоступно, администратор запретил добавление исключений в параметрах политики.
   - **Игнорировать**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удалит запись из списка активных угроз. Если в списке не осталось активных угроз, статус компьютера будет изменен на *ОК*. При повторном обнаружении объекта Kaspersky Endpoint Security снова добавит запись в список активных угроз.
   - **Открыть папку с файлом**. Если выбран этот вариант действия, то Kaspersky Endpoint Security откроет папку с объектом в файловом менеджере. Далее вы можете вручную удалить объект или переместить объект в папку, которая не входит в область защиты.
   - **Узнать больше**. Если выбран этот вариант действия, то Kaspersky Endpoint Security откроет сайт с базой угроз и уязвимостей от "Лаборатории Касперского" https://threats.kaspersky.com/.

Для обработки активных угроз в консоли Kaspersky Security Center необходимо включить передачу данных о необработанных файлах на Сервер администрирования. По умолчанию передача данных включена.

► *Как включить передачу данных о необработанных угрозах в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Отчеты и хранилище**.
4. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Настройка**.
5. Установите флажок **Необработанные файлы**.

6. Сохраните внесенные изменения.

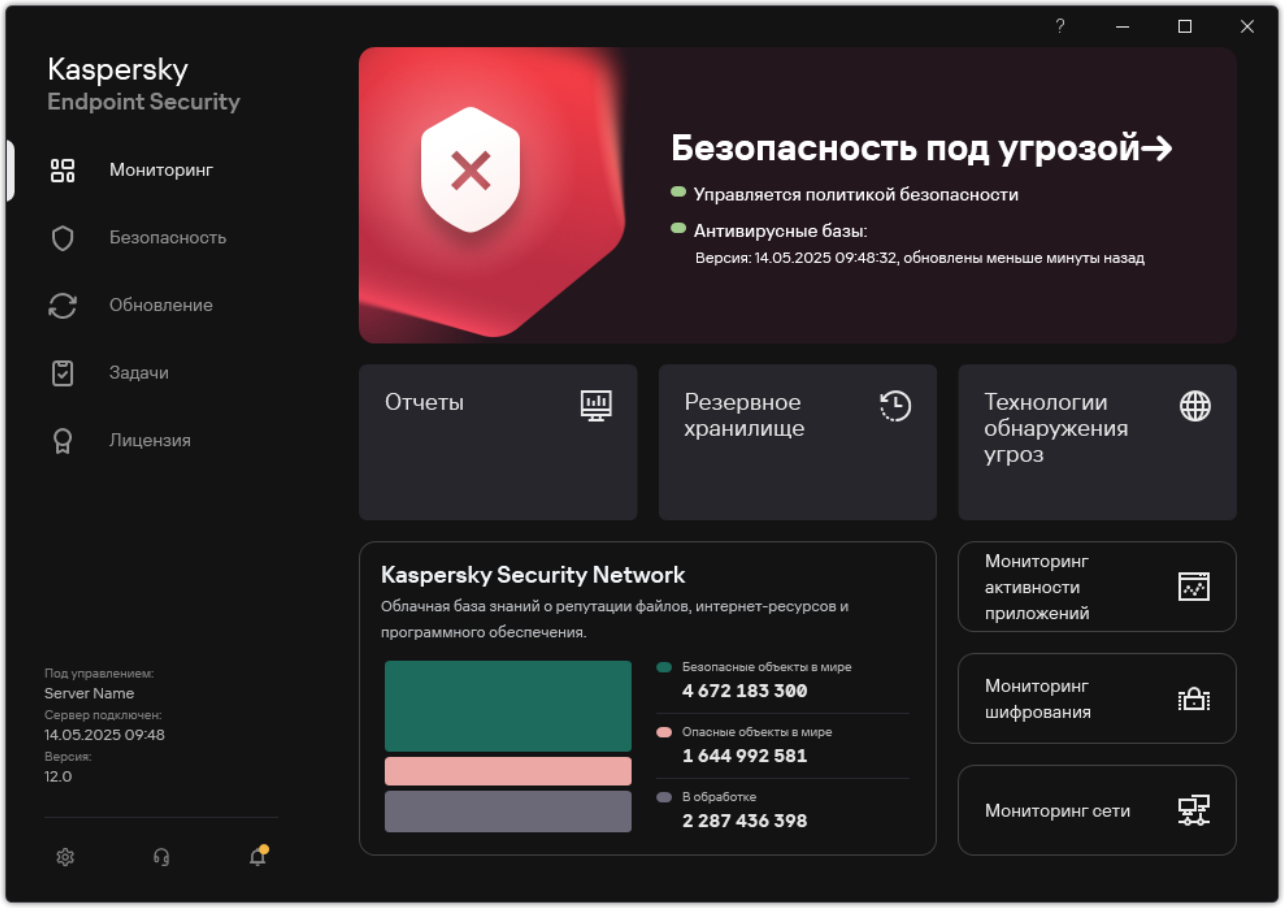


Рисунок 29. Главное окно приложения при обнаружении угрозы

kaspersky

Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры различают Глобальный KSN (инфраструктура расположена на серверах "Лаборатории Касперского") и Локальный KSN.

В сертифицированной версии программы Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается.

Участие пользователей в KSN позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках угроз, разрабатывать способы нейтрализации угроз, уменьшать количество ложных срабатываний компонентов программы.

При использовании расширенного режима KSN программа автоматически отправляет в KSN статистическую информацию, полученную в результате своей работы. Также программа может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые злоумышленники могут использовать для нанесения вреда компьютеру или данным.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского" (https://www.kaspersky.ru/products-and-services-privacy-policy). Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.
Для снижения нагрузки на серверы KSN специалисты "Лаборатории Касперского" могут выпускать антивирусные базы программы, которые временно выключают или частично ограничивают обращения в Kaspersky Security Network. В этом случае статус подключения к KSN – *Включено с ограничениями*.

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение компьютером пользователя запрошенной информации.

Подробнее о службе KSN Proxy вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Настройка параметров использования службы KSN Proxy доступна в свойствах политики *Kaspersky Security Center*.

Использование Kaspersky Security Network является добровольным. Программа предлагает использовать KSN во время первоначальной настройки программы. Начать или прекратить использование KSN можно в любой момент.

В этом разделе

Включение и выключение использования Kaspersky Security Network 110

Ограничения работы с Локальным KSN 110

Включение и выключение облачного режима для компонентов защиты 111

Проверка репутации файла в Kaspersky Security Network 112

Включение и выключение использования Kaspersky Security Network

По умолчанию Kaspersky Endpoint Security использует расширенный режим KSN. *Расширенный режим KSN* – режим работы приложения, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные.

► *Как включить или выключить использование KSN в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Kaspersky Security Network**.
3. Используйте переключатель **Kaspersky Security Network**, чтобы включить или выключить компонент.

   Если вы включили использование KSN, Kaspersky Endpoint Security покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования KSN.
4. Если требуется, выключите переключатель **Включить расширенный режим KSN**.
5. Сохраните внесенные изменения.

В результате, если использование KSN включено, Kaspersky Endpoint Security использует информацию о репутации файлов, веб-ресурсов и приложений, полученную из Kaspersky Security Network.

Ограничения работы с Локальным KSN

В сертифицированной версии приложения Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается.

Kaspersky Private Security Network (KPSN) – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. Kaspersky Private Security Network позволяет использовать собственную базу данных репутаций объектов (файлов или веб-адресов) с помощью локальной репутационной базы. Репутация объекта, добавленного в локальную репутационную базу, имеет приоритет выше, чем в KSN / KPSN. То есть, если Kaspersky Endpoint Security при проверке компьютера запросит репутацию файла в KSN / KPSN, и в локальной репутационной базе файл имеет репутацию *Недоверенные*, а в KSN / KPSN объект имеет репутацию *Доверенные*, то Kaspersky Endpoint Security обнаружит файл как *Недоверенные* и выполнит действие, заданное для обнаруженных угроз.

Однако в некоторых случаях Kaspersky Endpoint Security может не запрашивать репутацию объекта в KSN / KPSN. В результате Kaspersky Endpoint Security не получит данные из локальной репутационной базы KPSN. Kaspersky Endpoint Security может не запрашивать репутацию объекта в KSN / KPSN, например, по следующим причинам:

- Приложения "Лаборатории Касперского" используют офлайн репутационные базы. Офлайн репутационные базы предназначены для оптимизации ресурсов при работе приложений "Лаборатории Касперского" и защите критически важных объектов компьютера. Офлайн репутационные базы формируют специалисты "Лаборатории Касперского" на основании данных Kaspersky Security Network. приложения "Лаборатории Касперского" обновляют офлайн репутационные базы с антивирусными базами приложения. Если информация о проверяемом объекте содержится в офлайн репутационных базах, приложение не запрашивает репутацию этого объекта в KSN / KPSN.
- В параметрах приложения настроены исключения из проверки (доверенная зона (на стр. 320)). В этом случае приложение не учитывает репутацию объекта в локальной репутационной базе.
- Приложение использует технологии оптимизации проверки, например, технологии iSwift, iChecker или кеширование запросов репутации в KSN / KPSN. В этом случае приложение может не запрашивать репутацию ранее проверенных объектов.
- Для оптимизации нагрузки приложение проверяет файлы определенного формата и размера. Список форматов и ограничения по размеру определяют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения. Также вы можете настроить параметры оптимизации проверки в интерфейсе приложения, например, для компонента Защита от файловых угроз (см. раздел "Оптимизация проверки файлов" на стр. 147).
- Kaspersky Endpoint Security в режиме Легкого агента взаимодействует с серверами KSN с помощью прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается.

Включение и выключение облачного режима для компонентов защиты

Облачный режим – режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз. Работу приложения с облегченными антивирусными базами обеспечивает Kaspersky Security Network. Облегченная версия антивирусных баз позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию антивирусных баз с серверов "Лаборатории Касперского".

Включение облачного режима приводит к выходу приложения из сертифицированного состояния.

При использовании Kaspersky Private Security Network функциональность облачного режима доступна начиная с версии Kaspersky Private Security Network 3.0.
Если приложение работает в режиме Легкого агента, облачный режим недоступен.

► *Чтобы включить или выключить облачный режим для компонентов защиты, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Kaspersky Security Network**.
3. Используйте переключатель **Включить облачный режим**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security загружает облегченную или полную версию антивирусных баз в ходе ближайшего обновления.

Если облегченная версия антивирусных баз недоступна для использования, Kaspersky Endpoint Security автоматически переключается на использование полной версии антивирусных баз.

Проверка репутации файла в Kaspersky Security Network

Если вы сомневаетесь в безопасности файла, вы можете проверить его репутацию в Kaspersky Security Network.

Проверка репутации файла доступна, если вы приняли условия Положения о Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110).

► *Чтобы проверить репутацию файла в Kaspersky Security Network,*

откройте контекстное меню файла и выберите пункт **Проверить репутацию в KSN** (см. рис. ниже).

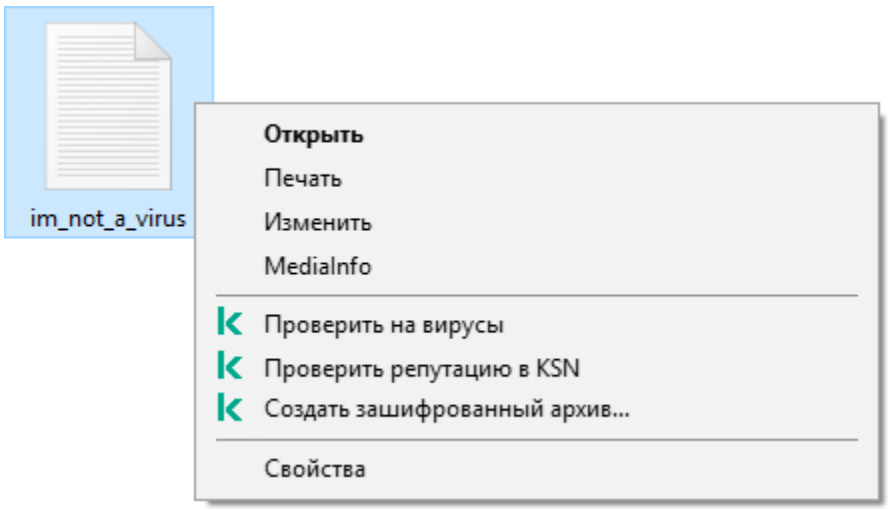


Рисунок 30. Контекстное меню файла

Kaspersky Endpoint Security отображает репутацию файла:

Доверенная (Kaspersky Security Network). Приложение считает файл доверенным при выполнении одного или более следующих условий:

- файл обладает цифровой подписью доверенного производителя;
- файл имеет репутацию доверенного в Kaspersky Security Network;
- пользователь поместил файл в группу "Доверенные" (см. раздел "Изменение группы доверия для приложения" на стр. 129).

Легальное приложение, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие приложения сами по себе не имеют вредоносных функций, но эти приложения могут быть использованы злоумышленниками. Подробную информацию о легальных приложениях, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского" https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/. Вы можете добавить эти приложения в список доверенных (см. раздел "Формирование списка доверенных приложений" на стр. 326).

Недоверенная (Kaspersky Security Network). Вирус или другое приложение, представляющее угрозу (см. раздел "Устранение необработанных угроз" на стр. 106).

Неизвестен (Kaspersky Security Network). В Kaspersky Security Network отсутствует информация о файле. Вы можете проверить файл с помощью антивирусных баз (пункт контекстного меню **Проверить на вирусы**).

Kaspersky Endpoint Security отображает решение KSN, которое было использовано для определения репутации файла: *Kaspersky Security Network* или *Kaspersky Private Security Network*.

Также Kaspersky Endpoint Security отображает дополнительную информацию о файле (см. рис. ниже).

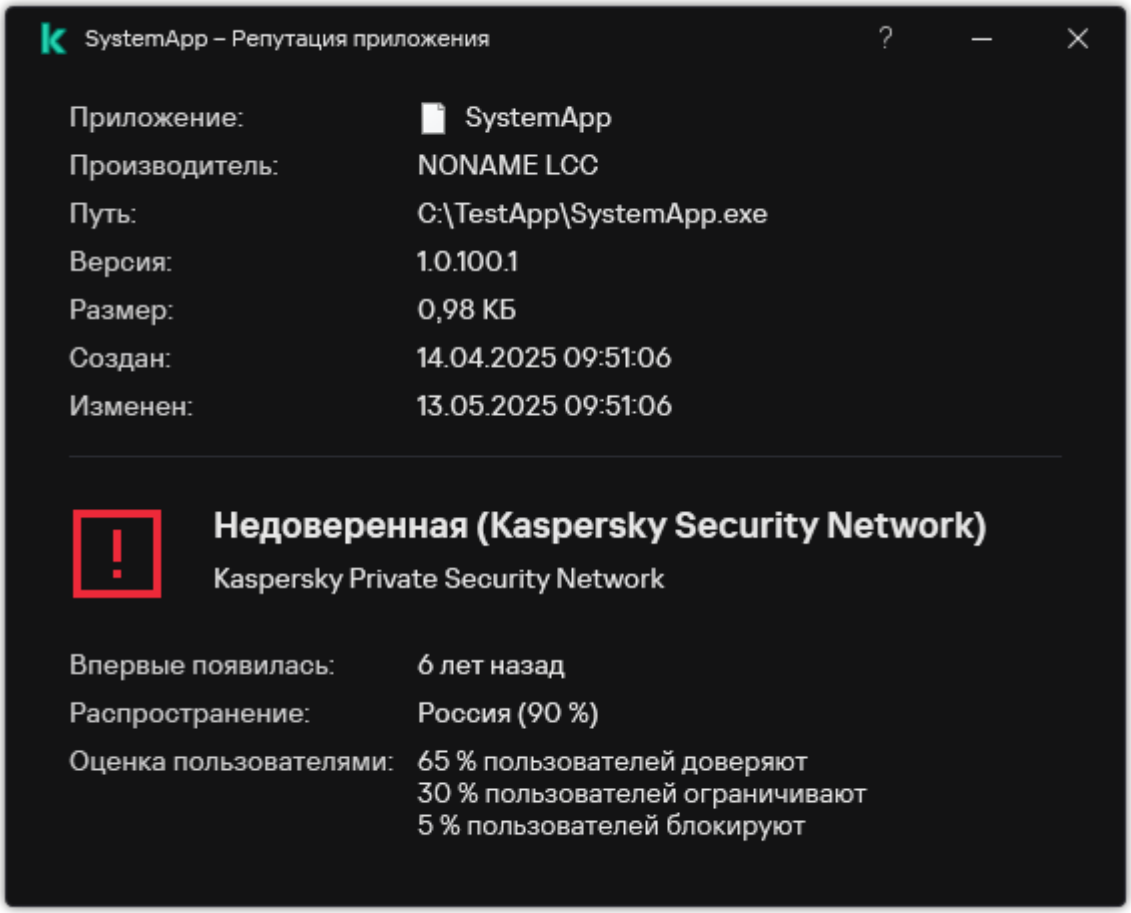


Рисунок 31. Репутация файла в Kaspersky Security Network

Анализ поведения

Компонент Анализ поведения получает данные о действиях приложений на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы. Компонент Анализ поведения использует шаблоны опасного поведения приложений. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

Компонент Анализ поведения дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

По умолчанию Анализ поведения включен и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". При обнаружении вредоносной активности Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения.

Не рекомендуется выключать Анализ поведения без необходимости, так как это снижает эффективность работы компонентов защиты. Компоненты защиты могут запрашивать данные, полученные компонентом Анализ поведения, для обнаружения угроз.

► *Как включить или выключить Анализ поведения в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Анализ поведения**.

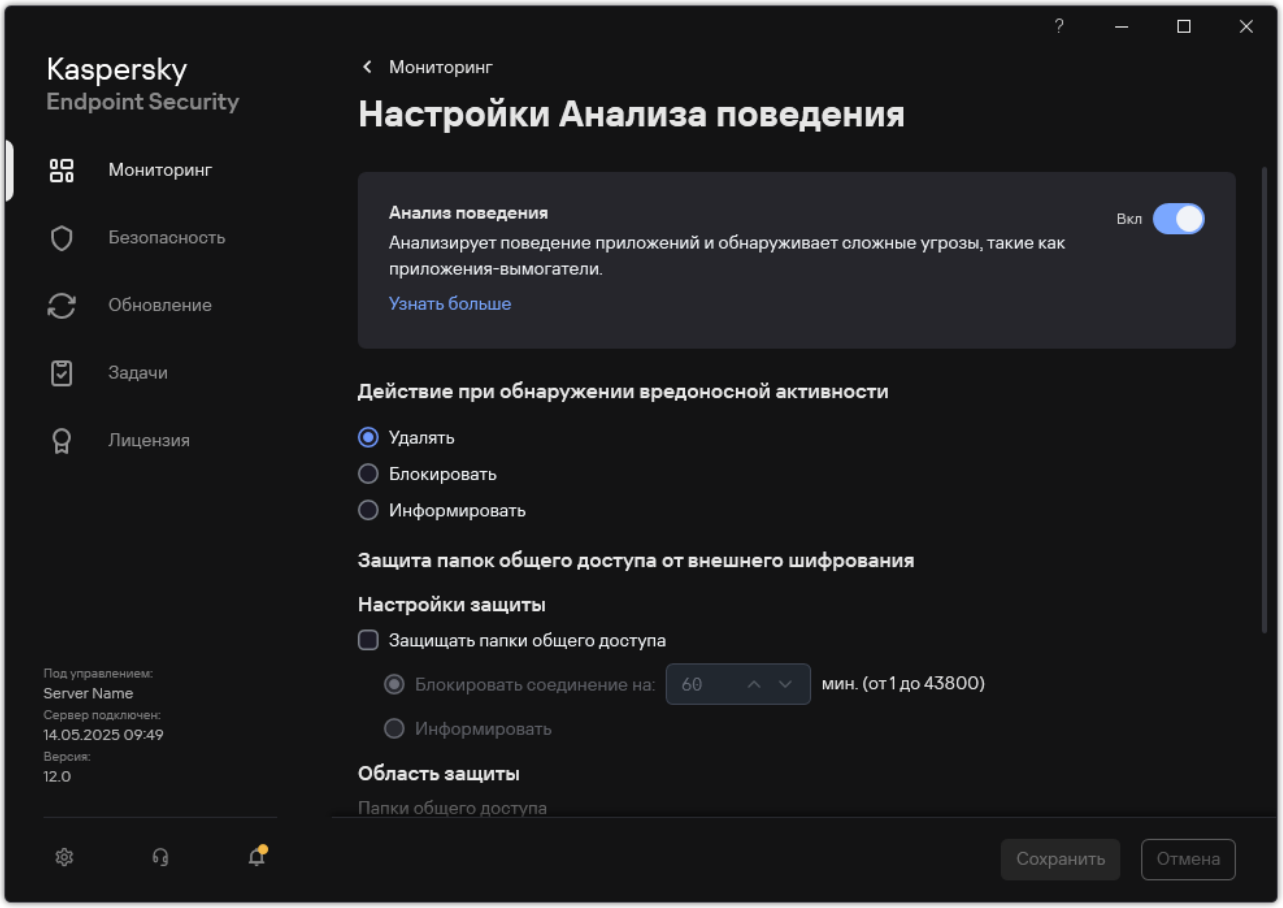


Рисунок 32. Параметры Анализа поведения

3. Используйте переключатель **Анализ поведения**, чтобы включить или выключить компонент.
4. В блоке **Действие при обнаружении вредоносной активности** выберите нужное действие:
   - **Удалять**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в резервном хранилище.
   - **Блокировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security завершает работу этого приложения.
   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security добавляет информацию о вредоносной активности этого приложения в список активных угроз.
5. Сохраните внесенные изменения.

В результате, если Анализ поведения включен, Kaspersky Endpoint Security будет анализировать активность приложений в операционной системе, используя шаблоны опасного поведения.

kaspersky

Защита от шифрования

Начиная с версии Kaspersky Endpoint Security для Windows 12.12 функция защиты папок общего доступа от внешнего шифрования, которая входила в состав компонента Анализ поведения (см. раздел "Анализ поведения" на стр. 115), выделена в отдельный компонент Защита от шифрования.

Компонент обеспечивает отслеживание операций только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы системой EFS.

Компонент Защита от шифрования обеспечивает анализ активности в папках общего доступа. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security выполняет выбранное действие.

Для работы компонента Защита от шифрования необходимо включить компонент Анализ поведения (см. раздел "Анализ поведения" на стр. 115).

При обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security выполняет следующие действия:

- блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность (файл доступен только на чтение);
- создает резервные копии подверженных изменению файлов;
- добавляет запись в отчеты локального интерфейса приложения (см. раздел "Работа с отчетами" на стр. 342) и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности;
- если при этом включен компонент Откат вредоносных действий (см. раздел "Откат вредоносных действий" на стр. 122), то выполняется восстановление измененных файлов из резервных копий.

В этом разделе

Включение и выключение защиты папок общего доступа от внешнего шифрования 117

Настройка периода блокировки недоверенного компьютера 119

Формирование области защиты 119

Добавление доверенных компьютеров для внешнего шифрования данных 120

kaspersky

Включение и выключение защиты папок общего доступа от внешнего шифрования

По умолчанию функция защиты папок общего доступа от внешнего шифрования включена и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для настройки функции вы можете сформировать область защиты, а также задать исключения, если требуется. По умолчанию приложение автоматически определяет папки общего доступа и отслеживает файловую активность во всех папках. При обнаружении попытки внешнего шифрования файлов в папках общего доступа Kaspersky Endpoint Security блокирует сессию удаленного пользователя на один час (по умолчанию).

После установки Kaspersky Endpoint Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

► *Как включить или выключить защиту папок общего доступа от внешнего шифрования в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от шифрования**.
3. Используйте флажок **Защита папок общего доступа от внешнего шифрования**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.
4. Используйте флажок **Защита папок общего доступа от внешнего шифрования**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.
5. Выберите нужное действие приложения при обнаружении попытки изменения файлов в папках общего доступа:
   - **Блокировать соединение на (мин) N мин**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов.

     Если включен компонент Откат вредоносных действий (см. раздел "Откат вредоносных действий" на стр. 122) и выбран вариант **Блокировать соединение на (мин) N мин**, то выполняется восстановление измененных файлов из резервных копий.

   - **Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчеты локального интерфейса приложения (см. раздел "Работа с отчетами" на стр. 342) и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.
6. Если требуется сформируйте область защиты и задайте исключения (см. раздел "Формирование области защиты" на стр. 119).
7. Сохраните внесенные изменения.

kaspersky

Настройка периода блокировки недоверенного компьютера

Недоверенный компьютер – удаленный компьютер, с которого ведется вредоносная активность или шифрование данных. По умолчанию Kaspersky Endpoint Security блокирует сессию удаленного пользователя на один час. По истечении периода блокировки Kaspersky Endpoint Security удаляет компьютер из списка заблокированных и восстанавливает доступ к папке общего доступа.

► *Как настроить период блокировки недоверенного компьютера в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от шифрования**.
3. В блоке **Действие при обнаружении угрозы** выберите вариант **Блокировать соединение на (мин)**.
4. Настройте период блокировки удаленного компьютера, с которого ведется вредоносная активность или шифрование данных.
5. Сохраните внесенные изменения.

В результате удаленный компьютер будет заблокирован. Для разблокировки удаленного компьютера вы можете перезапустить Kaspersky Endpoint Security.

Формирование области защиты

Область защиты – список путей к папкам общего доступа, в которых Kaspersky Endpoint Security отслеживает файловую активность. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски. По умолчанию приложение автоматически определяет папки общего доступа и отслеживает файловую активность во всех папках.

Исключение папки из области защиты позволит сократить количество ложных срабатываний, если в вашей организации используется шифрование данных при обмене файлами с помощью папок общего доступа. Например, Анализ поведения может создавать ложные срабатывания при работе пользователя с файлами с расширением ENC в папке общего доступа. Такая активность совпадает с шаблоном поведения, характерного для внешнего шифрования. Если вы зашифровали файлы в папке общего доступа для защиты данных, добавьте эту папку в исключения.

Вы также можете исключить компьютеры, попытки внешнего шифрования с которого, не должны обрабатываться (см. раздел "Добавление доверенных компьютеров для внешнего шифрования данных" на стр. 120).

► *Как сформировать область защиты в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от шифрования**.

3. В блоке **Область защиты** выберите вариант **Только указанные общие папки**.
4. В списке папок нажмите на кнопку **Добавить**.
5. В открывшемся окне введите путь к папке общего доступа, которую вы хотите включить область защиты (например, `C:\Share`).

   Для добавления папки общего доступа в область защиты используйте локальный путь.

6. Нажмите на кнопку **OK**.
7. Если требуется, задайте исключения из области защиты:
   a. В верхней части окна перейдите по ссылке **Исключения по маске**.
   b. В открывшемся окне нажмите на кнопку **Добавить**.
   c. В открывшемся окне укажите расширение файла в формате `*.<file extension>` или путь к папке. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

      Приложение не поддерживает некоторые расширения файлов для исключений. Таким образом, вы можете указать исключение в следующем виде `*.docx` или `**\Folder\**`.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области защиты. Для этого снимите флажок рядом с ним.
8. Сохраните внесенные изменения.

Добавление доверенных компьютеров для внешнего шифрования данных

Если в вашей организации используется внешнее шифрование данных при обмене файлами, вам нужно сформировать список доверенных компьютеров. Kaspersky Endpoint Security не отслеживает шифрование данных с доверенных компьютеров.

Для работы функциональности исключений адресов из защиты папок общего доступа от внешнего шифрования необходимо включить службу Аудит входа в систему. По умолчанию служба Аудит входа в систему выключена (подробную информацию о включении службы Аудит входа в систему см. на сайте корпорации Microsoft).
Функциональность исключений адресов из защиты папок общего доступа не работает на удаленном компьютере, если этот удаленный компьютер был включен до запуска Kaspersky Endpoint Security. Вы можете перезагрузить этот удаленный компьютер после запуска Kaspersky Endpoint Security, чтобы обеспечить работу функциональности исключений адресов из защиты папок общего доступа на этом удаленном компьютере.

► *Как добавить доверенный компьютер для внешнего шифрования данных в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от шифрования**.

3. В верхней части окна перейдите по ссылке **Исключения по имени или IP-адресу**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Введите IP-адреса компьютеров, диапазон IP-адресов или имена компьютеров, попытки внешнего шифрования с которых не должны обрабатываться.

   Примеры:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
6. Сохраните внесенные изменения.

kaspersky

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security отменять действия, произведенные вредоносными приложениями в операционной системе.

Во время отката действий вредоносного приложения в операционной системе Kaspersky Endpoint Security обрабатывает следующие типы активности вредоносного приложения:

- **Файловая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет исполняемые файлы, созданные вредоносным приложением (на всех носителях, кроме сетевых дисков);
  - удаляет исполняемые файлы, созданные приложениями, в которые внедрилось вредоносное приложение;
  - восстанавливает измененные или удаленные вредоносным приложением файлы.

  Функциональность восстановления файлов имеет ряд ограничений.

- **Реестровая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет разделы и ключи реестра, созданные вредоносным приложением;
  - не восстанавливает измененные или удаленные вредоносным приложением разделы и ключи реестра.

- **Системная активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - завершает процессы, которые запускало вредоносное приложение;
  - завершает процессы, в которые внедрялось вредоносное приложение;
  - не возобновляет процессы, которые остановило вредоносное приложение.

- **Сетевая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - запрещает сетевую активность вредоносного приложения;
  - запрещает сетевую активность тех процессов, в которые внедрялось вредоносное приложение.

Откат действий вредоносного приложения может быть запущен компонентом Защита от файловых угроз (см. стр. 139), Анализ поведения (на стр. 115) или при поиске вредоносного ПО (см. раздел "Поиск вредоносного ПО" на стр. 62).

Откат действий вредоносного приложения затрагивает строго ограниченный набор данных. Откат не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

► *Как включить или выключить компонент Откат вредоносных действий в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Откат вредоносных действий**.
3. Используйте переключатель **Откат вредоносных действий**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Откат вредоносных действий включен, Kaspersky Endpoint Security будет откатывать действия, которые вредоносные приложения совершили в операционной системе.

kaspersky

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимое приложение. При обработке этих данных уязвимое приложение выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО. Если попытка запустить исполняемый файл из уязвимого приложения не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

Компонент Защита от эксплойтов дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

В этом разделе

Включение и выключение Защиты от эксплойтов 124

Защита памяти системных процессов 125

Включение и выключение Защиты от эксплойтов

По умолчанию компонент Защита от эксплойтов включен и работает в оптимальном режиме. Kaspersky Endpoint Security будет отслеживать исполняемые файлы, запускаемые уязвимыми приложениями. Если Kaspersky Endpoint Security обнаруживает, что исполняемый файл из уязвимого приложения был запущен не пользователем, то Kaspersky Endpoint Security выполняет выбранное действие (например, блокирует операцию).

► *Как включить или выключить Защиту от эксплойтов в интерфейсе приложении*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от эксплойтов**.

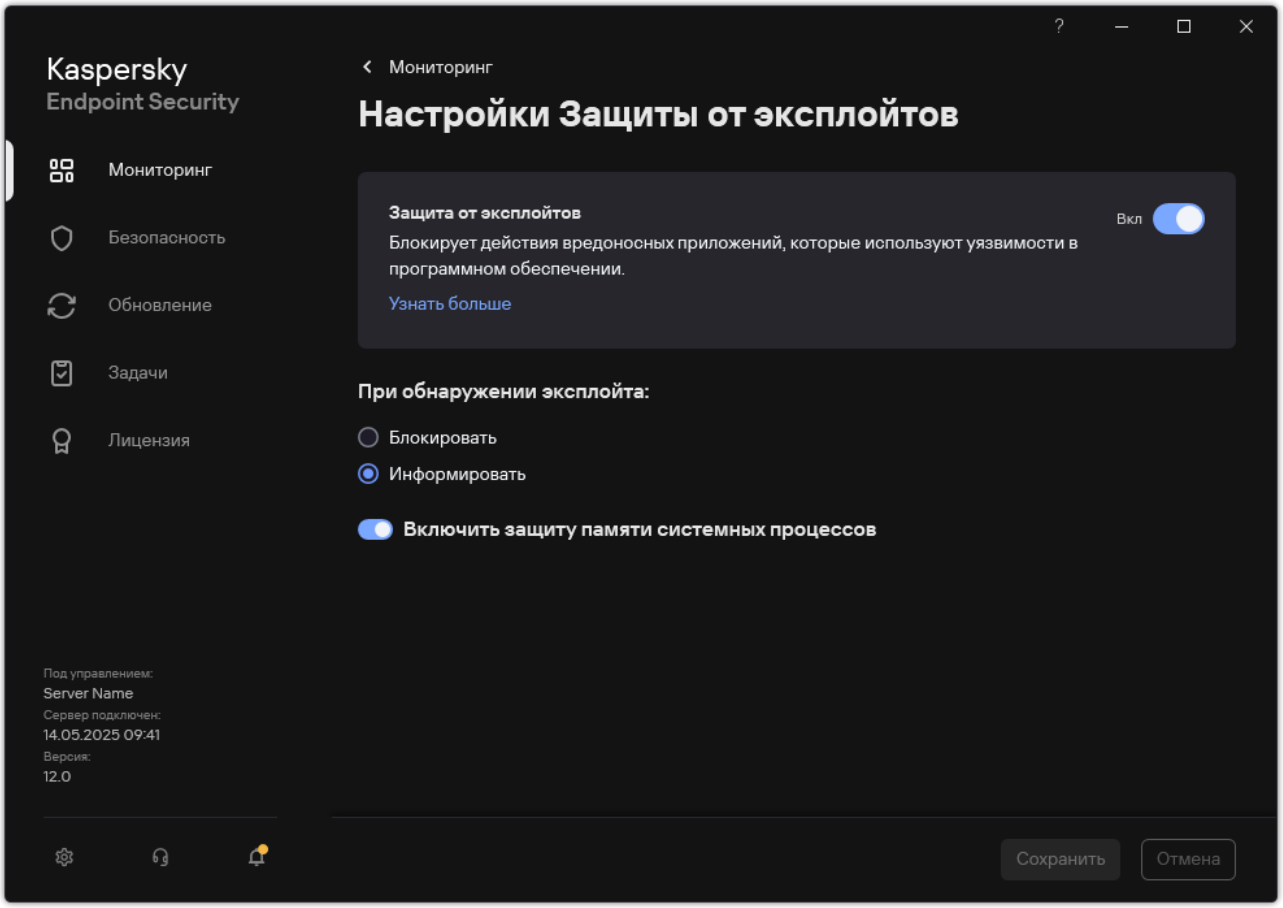


Рисунок 33. Параметры Защиты от эксплойтов

3. Используйте переключатель **Защита от эксплойтов**, чтобы включить или выключить компонент.
4. В блоке **При обнаружении эксплойта** выберите нужное действие:
   - **Блокировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте.
   - **Информировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз (см. раздел "Устранение необработанных угроз" на стр. 106).
5. Сохраните внесенные изменения.

kaspersky

Защита памяти системных процессов

По умолчанию защита памяти системных процессов включена. Kaspersky Endpoint Security блокирует сторонние процессы, которые осуществляют попытки доступа к системным процессам.

► *Как включить ли выключить защиту памяти системных процессов в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от эксплойтов**.
3. Используйте переключатель **Включить защиту памяти системных процессов**, чтобы включить или выключить функцию.
4. Сохраните внесенные изменения.

kaspersky

Предотвращение вторжений

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Компонент Предотвращение вторжений (англ. Host Intrusion Prevention System, HIPS) предотвращает выполнение приложениями опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным. Компонент обеспечивает защиту компьютера с помощью антивирусных баз и облачной службы Kaspersky Security Network.

Компонент контролирует работу приложений с помощью *прав приложений*. Права приложений включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, приложениям).

Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.

Во время первого запуска приложения компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность приложения с помощью загруженных антивирусных баз.
2. Проверяет безопасность приложения в Kaspersky Security Network.

   Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110).

3. Помещает приложение в одну из групп доверия: *Доверенные*, *Слабые ограничения*, *Сильные ограничения*, *Недоверенные*.

   Группа доверия определяет права (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469), которые Kaspersky Endpoint Security использует для контроля активности приложений. Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера.

   Kaspersky Endpoint Security помещает приложение в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

> Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от параметров компонента Предотвращение вторжений (см. раздел "Выбор группы доверия для неизвестных приложений" на стр. 131). После получения данных о репутации приложения от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия приложения в зависимости от группы доверия. Например, приложениям из группы доверия *Сильные ограничения* запрещен доступ к модулям операционной системы.

При следующем запуске приложения Kaspersky Endpoint Security проверяет целостность приложения. Если приложение не было изменено, компонент применяет к ней текущие права приложения. Если приложение было изменено, Kaspersky Endpoint Security исследует приложение как при первом запуске.

В этом разделе

Включение и выключение Предотвращения вторжений 128
Работа с группами доверия приложений 129
Работа с правами приложений 132
Защита ресурсов ОС и персональных данных 135
Удаление информации о неиспользуемых приложениях 136
Мониторинг работы Предотвращения вторжений 137
Защита доступа к аудио и видео 137

Включение и выключение Предотвращения вторжений

По умолчанию компонент Предотвращение вторжений включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме.

► *Как включить или выключить компонент Предотвращение вторжений в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. Используйте переключатель **Предотвращение вторжений**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если компонент Предотвращение вторжений включен, Kaspersky Endpoint Security помещает приложение в группу доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469) в зависимости от уровня опасности, которую это приложение может представлять для компьютера. Далее Kaspersky Endpoint Security будет блокировать действия приложения в зависимости от группы доверия.

kaspersky

Работа с группами доверия приложений

Во время первого запуска каждого приложения компонент Предотвращение вторжений проверяет безопасность приложения и помещает приложение в одну из групп доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469).

На первом этапе проверки приложения Kaspersky Endpoint Security ищет запись о приложении во внутренней базе известных приложений и одновременно отправляет запрос в базу Kaspersky Security Network (при наличии подключения к интернету). По результатам проверки по внутренней базе и по базе Kaspersky Security Network приложение помещается в группу доверия. При каждом повторном запуске приложения Kaspersky Endpoint Security отправляет новый запрос в базу KSN и перемещает приложение в другую группу доверия, если репутация приложения в базе KSN изменилась.

Вы можете выбрать группу доверия, в которую Kaspersky Endpoint Security должен автоматически помещать все неизвестные приложения (см. раздел "Выбор группы доверия для неизвестных приложений" на стр. 131). Приложения, которые были запущены до Kaspersky Endpoint Security, автоматически помещаются в группу доверия, установленную в параметрах компонента Предотвращение вторжений (см. раздел "Выбор группы доверия для приложений, запускаемых до Kaspersky Endpoint Security" на стр. 131).

Для приложений, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана.

В этом разделе

Изменение группы доверия для приложения 129

Настройка прав группы доверия 130

Выбор группы доверия для приложений, запускаемых до Kaspersky Endpoint Security 131

Выбор группы доверия для неизвестных приложений 131

Выбор группы доверия для приложений с цифровой подписью 132

Изменение группы доверия для приложения

Во время первого запуска каждого приложения компонент Предотвращение вторжений проверяет безопасность приложения и помещает приложение в одну из групп доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469).

Специалисты "Лаборатории Касперского" не рекомендуют перемещать приложения из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого при необходимости измените права отдельного приложения (см. раздел "Работа с правами приложений" на стр. 132).

► *Как изменить группу доверия для приложения в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление приложениями**.

   Откроется список установленных приложений.
4. Выберите нужное приложение.
5. В контекстном меню приложения выберите пункт **Ограничения → <группа доверия>**.
6. Сохраните внесенные изменения.

В результате приложение будет перемещено в другую группу доверия. Далее Kaspersky Endpoint Security будет блокировать действия приложения в зависимости от группы доверия. Приложению будет присвоен статус *(задано пользователем)*. При изменении репутации приложения в Kaspersky Security Network компонент Предотвращение вторжений оставит группу доверия для этого приложения без изменений.

Настройка прав группы доверия

По умолчанию для разных групп доверия созданы оптимальные права приложений (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469). Параметры прав групп приложений, входящих в группу доверия, наследуют значения параметров прав групп доверия.

► *Как изменить права группы доверия в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление приложениями**.

   Откроется список установленных приложений.
4. Выберите нужную группу доверия.
5. В контекстном меню группы доверия выберите пункт **Подробности и правила**.

   Откроются свойства группы доверия.
6. Выполните одно из следующих действий:
   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами приложений.
   - Выберите закладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

   Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешить** (✓), **Запретить** (!).

8. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** ( ).

   Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.

9. Сохраните внесенные изменения.

В результате права группы доверия будут изменены. Далее Kaspersky Endpoint Security будет блокировать действия приложения в зависимости от группы доверия. Группе доверия будет присвоен статус (*Настройки пользователя*).

Выбор группы доверия для приложений, запускаемых до Kaspersky Endpoint Security

Для приложений, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана. Чтобы указать, какими сетевыми правилами должен регулироваться контроль сетевой активности таких приложений, необходимо выбрать группу доверия.

► *Как выбрать группу доверия для приложений, запускаемых до Kaspersky Endpoint Security, в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. В блоке **Группа доверия для приложений, запущенных до <PRODUCT>** выберите нужную группу доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469).
4. Сохраните внесенные изменения.

В результате приложение, запускаемое до Kaspersky Endpoint Security, будет помещено в другую группу доверия. Далее Kaspersky Endpoint Security будет блокировать действия приложения в зависимости от группы доверия.

Выбор группы доверия для неизвестных приложений

Во время первого запуска приложения компонент Предотвращение вторжений определяет группу доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469) для приложения. Если у вас отсутствует доступ в интернет или в Kaspersky Security Network нет информации об этом приложении, то Kaspersky Endpoint Security по умолчанию помещает приложение в группу *Слабые ограничения*. При обнаружении в KSN информации о ранее неизвестном приложении Kaspersky Endpoint Security обновит права приложения. После этого вы можете изменить права приложения вручную (см. раздел "Работа с правами приложений" на стр. 132).

► *Как выбрать группу доверия для неизвестных приложений в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. В блоке **Правила обработки приложений** выберите нужную группу доверия.

   Если участие в Kaspersky Security Network включено (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110), Kaspersky Endpoint Security отправляет запрос о репутации приложения в KSN при каждом запуске приложения. На основе полученного ответа приложение может быть перемещено в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.
4. Используйте флажок **Обновлять правила для ранее неизвестных приложений из KSN**, чтобы настроить автоматическое обновление прав неизвестных приложений.
5. Сохраните внесенные изменения.

Выбор группы доверия для приложений с цифровой подписью

Kaspersky Endpoint Security всегда помещает приложения, подписанные сертификатами Microsoft или сертификатами "Лаборатории Касперского", в группу доверия *Доверенные*.

► *Как выбрать группу доверия для приложений с цифровой подписью в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. В блоке **Правила обработки приложений** используйте флажок **Доверять приложениям, имеющим цифровую подпись**, чтобы включить или выключить автоматическое перемещение приложений с цифровой подписью доверенных производителей в группу доверия *Доверенные*.

   Доверенные производители – производители, которые включены в список доверенных "Лабораторией Касперского". Также вы можете добавить сертификат производителя в доверенное системное хранилище сертификатов вручную (см. раздел "Работа с приложениями, подписанными доверенной цифровой подписью" на стр. 331).

   Если флажок снят, компонент Предотвращение вторжений не считает приложения с цифровой подписью доверенными и распределяет их по группам доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469) на основании других параметров.
4. Сохраните внесенные изменения.

Работа с правами приложений

По умолчанию для контроля работы приложения применяются права приложений, определенные для той группы доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469), в которую Kaspersky Endpoint Security поместил приложение при первом ее запуске. При необходимости вы можете изменить права приложений для всей группы доверия (см. раздел "Настройка прав группы доверия" на стр. 130), для отдельного приложения или группы приложений внутри группы доверия.

Права приложений, заданные вручную, имеют более высокий приоритет, чем права приложений, определенные для группы доверия. То есть, если права приложения, заданные вручную, отличаются от прав приложений, определенных для группы доверия, компонент Предотвращение вторжения контролирует работу приложения в соответствии с правами приложений, заданными вручную.

Правила, которые вы создаете для приложений, наследуются дочерними приложениями. Например, если вы запретили любую сетевую активность приложению cmd.exe, этот запрет будет распространятся на приложение notepad.exe, если она была запущена с помощью cmd.exe. При опосредованном запуске приложения (если приложение не является дочерним по отношению к приложению, из которого оно запускается), правила унаследованы не будут.

► *Как изменить права приложения в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление приложениями**.

   Откроется список установленных приложений.
4. Выберите нужное приложение.
5. В контекстном меню приложения выберите пункт **Подробности и правила**.

   Откроются свойства приложения.
6. Выполните одно из следующих действий:
   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами приложений.
   - Выберите закладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешить** (), **Запретить** ().
8. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** ().

   Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.
9. Выберите закладку **Исключения** и настройте дополнительные параметры приложения (см. таблицу ниже).
10. Сохраните внесенные изменения.

Таблица 8. Дополнительные параметры приложения

Параметр	Описание
Не проверять открываемые файлы	Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью приложения. Например, если вы используете приложения резервного копирования файлов, функция позволит снизить потребление ресурсов компьютера Kaspersky Endpoint Security.
Не контролировать активность приложения	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложения в операционной системе. Вы можете настроить контроль активности приложения для разных компонентов Kaspersky Endpoint Security: • **Не контролировать для компонентов защиты и контроля**. Контроль за активностью приложения выполняют следующие компоненты: Анализ поведения (на стр. 115), Защита от эксплойтов (на стр. 124), Предотвращение вторжений (на стр. 127), Откат вредоносных действий (на стр. 122) и Сетевой экран. • **Не контролировать для Managed Detection and Response и Endpoint Detection and Response**. Контроль за активностью приложения выполняют встроенный агент MDR и встроенный агент EDR (KATA). • **Не перехватывать консольный ввод для Endpoint Detection and Response**. Kaspersky Endpoint Security не отправляет данные телеметрии об управлении приложением через консоль. Данные телеметрии использует Kaspersky Anti Targeted Attack Platform (EDR).
Не наследовать ограничения родительского процесса (приложения)	Kaspersky Endpoint Security не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает приложение, для которой настроены права приложения (см. раздел "Работа с правами приложений" на стр. 132) (Предотвращение вторжений) и сетевые правила приложения (Сетевой экран).
Не контролировать активность дочерних приложений	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложений, которые запускает приложение. Вы можете применить исключение рекурсивно. То есть приложение не контролирует активность всей цепочки дочерних приложений.
Разрешить взаимодействие с интерфейсом <PRODUCT>	Самозащита Kaspersky Endpoint Security (на стр. 347) блокирует все попытки управления службами приложения с удаленного компьютера. Если флажок установлен, то приложению удаленного доступа к компьютеру разрешено управлять параметрами Kaspersky Endpoint Security через интерфейс Kaspersky Endpoint Security.

Параметр	Описание
Не проверять зашифрованный трафик / Не проверять весь трафик	Kaspersky Endpoint Security исключает из проверки сетевой трафик, инициируемый приложением. Вы можете исключить из проверки весь трафик или только зашифрованный трафик. Также вы можете исключить из проверки отдельные IP-адреса или номера портов.

Защита ресурсов ОС и персональных данных

Компонент Предотвращение вторжений управляет правами приложений на операции над различными категориями ресурсов операционной системы и персональных данных. Специалисты "Лаборатории Касперского" выделили предустановленные категории защищаемых ресурсов. Например, в категории *Операционная система* есть подкатегория *Настройки автозапуска*, где перечислены все ключи реестра, относящиеся к автозапуску приложений. Вы не можете изменять или удалять предустановленные категории защищаемых ресурсов и относящиеся к ним защищаемые ресурсы.

► *Как добавить защищаемый ресурс в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление ресурсами**.

   Откроется список защищаемых ресурсов.
4. Выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

   Если вы хотите добавить вложенную категорию, нажмите на кнопку **Добавить** → **Категорию**.
5. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить: **Файл или папку** или **Ключ реестра**.
6. В открывшемся окне выберите файл, папку или ключ реестра.

   Вы можете посмотреть права доступа приложений к добавленным ресурсам. Для этого выберите добавленный ресурс в левой части окна и Kaspersky Endpoint Security покажет список приложений и права доступа для каждого из приложений. Также вы можете выключить контроль действия приложений на операции с ресурсами кнопкой **Включить контроль** в графе **Статус**.
7. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет контролировать доступ к добавленным ресурсам операционной системы и персональных данных. Kaspersky Endpoint Security контролирует доступ приложения к ресурсам на основании присвоенной группы доверия. Вы также можете изменить группу доверия для приложения (см. раздел "Изменение группы доверия для приложения" на стр. 129).

kaspersky

Удаление информации о неиспользуемых приложениях

Kaspersky Endpoint Security контролирует работу приложений с помощью прав приложений. Права приложения определены группой доверия. Kaspersky Endpoint Security помещает приложение в группу доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 469) при первом запуске. Вы можете изменить группу доверия для приложения вручную (см. раздел "Работа с правами приложений" на стр. 132). Также вы можете настроить права для отдельного приложения вручную (см. раздел "Работа с правами приложений" на стр. 132). Таким образом, Kaspersky Endpoint Security хранит следующую информацию о приложении: группа доверия и права приложения.

Kaspersky Endpoint Security автоматически удаляет информацию о неиспользуемых приложениях для экономии ресурсов компьютера. Kaspersky Endpoint Security удаляет информацию о приложениях по следующим правилам:

- Если группа доверия и права приложения определены автоматически, Kaspersky Endpoint Security удаляет информацию об этом приложении через 30 дней. Изменить время хранения информации о приложении или выключить автоматическое удаление невозможно.
- Если вы вручную поместили приложение в группу доверия или настроили права доступа, Kaspersky Endpoint Security удаляет информацию об этом приложении через 60 дней (значение по умолчанию). Вы можете изменить время хранения информации о приложении или выключить автоматическое удаление (см. инструкцию ниже).

При запуске приложения, информация о которой была удалена, Kaspersky Endpoint Security исследует приложение как при первом запуске.

► *Как настроить автоматическое удаление информации о неиспользуемых приложениях в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. В блоке **Правила обработки приложений** выполните одно из следующих действий:
   - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять правила для приложений, не запускавшихся более N дней (от 1 до 90)** и укажите нужное количество дней.

     Kaspersky Endpoint Security будет удалять информацию о тех приложениях, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, через заданное количество дней. Также Kaspersky Endpoint Security будет удалять информацию о приложениях, для которых группа доверия и права приложения определены автоматически, через 30 дней.
   - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять правила для приложений, не запускавшихся более N дней (от 1 до 90)**.

     Kaspersky Endpoint Security будет хранить информацию о тех приложениях, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, без ограничений по времени. Kaspersky Endpoint Security будет удалять информацию только о приложениях, для которых группа доверия и права приложения определены автоматически, через 30 дней.
4. Сохраните внесенные изменения.

kaspersky

Мониторинг работы Предотвращения вторжений

Вы можете получать отчеты о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.

Для мониторинга работы Предотвращения вторжений вам нужно включить запись в отчет. Например, вы можете включить отправку отчетов для отдельных приложений в параметрах компонента Предотвращение вторжений (см. раздел "Работа с правами приложений" на стр. 132).

При настройке мониторинга работы Предотвращения вторжения учитывайте нагрузку на сеть при отправке событий в Kaspersky Security Center. Также вы можете включить сохранение отчетов только в локальном журнале Kaspersky Endpoint Security.

Защита доступа к аудио и видео

Злоумышленники могут с помощью специальных приложений пытаться получить доступ к устройствам записи аудио и видео (например, микрофоны или веб-камеры). Kaspersky Endpoint Security контролирует получение приложениями аудиосигнала и видеосигнала и защищает данные от несанкционированного перехвата.

По умолчанию Kaspersky Endpoint Security разрешает получение аудиосигнала и видеосигнала только для приложений из группы *Доверенные*. Приложениям из групп *Слабые ограничения*, *Сильные ограничения* и *Недоверенные* доступ к аудиосигналу и видеосигналу запрещен. Вы можете вручную разрешать приложениям получать аудиосигнал и видеосигнал (см. раздел "Работа с правами приложений" на стр. 132).

Особенности защиты аудиосигнала

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Предотвращение вторжений (см. раздел "Включение и выключение Предотвращения вторжений" на стр. 128).
- Если приложение начало получать аудиосигнал до запуска компонента Предотвращение вторжений, то Kaspersky Endpoint Security разрешает приложению получение аудиосигнала и не показывает никаких уведомлений.
- Если вы поместили приложение в группу *Недоверенные* или *Сильные ограничения* после того, как приложение начало получать аудиосигнал, то Kaspersky Endpoint Security разрешает приложению получение аудиосигнала и не показывает никаких уведомлений.
- При изменении параметров доступа приложения к устройствам записи звука (например, приложению было запрещено получение аудиосигнала (см. раздел "Работа с правами приложений" на стр. 132)) требуется перезапуск этого приложения, чтобы она перестала получать аудиосигнал.
- Контроль получения аудиосигнала с устройств записи звука не зависит от параметров доступа приложений к веб-камере.
- Kaspersky Endpoint Security защищает доступ только к встроенным и внешним микрофонам. Другие устройства передачи звука не поддерживаются.
- Kaspersky Endpoint Security не гарантирует защиту аудиосигнала, передаваемого с таких устройств, как DSLR-камеры, портативные видеокамеры, экшн-камеры.

- При первом запуске приложения Kaspersky Endpoint Security с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в приложениях записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа приложений к устройствам записи звука. Системная служба управления средствами работы со звуком будет перезапущена при первом запуске приложения Kaspersky Endpoint Security.

Особенности доступа приложений к веб-камерам

Функциональность защиты доступа к веб-камере имеет следующие особенности и ограничения:

- Приложение контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.
- Приложение контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.
- Приложение контролирует только веб-камеры, подключаемые по интерфейсу USB или IEEE1394 и отображаемые в Диспетчере устройств Windows как Устройства обработки изображений (англ. Imaging Device).
- Kaspersky Endpoint Security поддерживает следующие веб-камеры:
  - Logitech HD Webcam C270;
  - Logitech HD Webcam C310;
  - Logitech Webcam C210;
  - Logitech Webcam Pro 9000;
  - Logitech HD Webcam C525;
  - Microsoft LifeCam VX-1000;
  - Microsoft LifeCam VX-2000;
  - Microsoft LifeCam VX-3000;
  - Microsoft LifeCam VX-800;
  - Microsoft LifeCam Cinema.

  "Лаборатория Касперского" не гарантирует поддержку веб-камер, не указанных в этом списке.

kaspersky

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы в режиме реального времени. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110) и эвристического анализа.

Компонент проверяет файлы, к которым обращается пользователь или приложение. При обнаружении вредоносного файла Kaspersky Endpoint Security блокирует операцию с файлом. Далее приложение лечит или удаляет вредоносный файл, в зависимости от настройки компонента Защита от файловых угроз.

При обращении к файлу, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security загружает и проверяет содержимое этого файла.

В этом разделе

Включение и выключение Защиты от файловых угроз 139
Автоматическая приостановка Защиты от файловых угроз 142
Изменение действия компонента Защита от файловых угроз над зараженными файлами 143
Формирование области защиты компонента Защита от файловых угроз 144
Использование методов проверки 145
Использование технологий проверки в работе компонента Защита от файловых угроз 146
Оптимизация проверки файлов 147
Проверка составных файлов 147
Изменение режима проверки файлов 148
Проверка контейнеров 149

Включение и выключение Защиты от файловых угроз

По умолчанию компонент Защита от файловых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от файловых угроз приложение Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

Компонент Защита от файловых угроз использует данные, полученные от других компонентов приложения. Включение этих компонентов не является обязательным. К компонентам, которые предоставляют дополнительные данные, относятся следующие компоненты:

- Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110).
- Предотвращение вторжений (см. раздел "Включение и выключение Предотвращения вторжений" на стр. 128).
- Анализ поведения (на стр. 115).

► *Как включить или выключить компонент Защита от файловых угроз в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Используйте переключатель **Защита от файловых угроз**, чтобы включить или выключить компонент.
4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Уровень безопасности файлов, при котором компонент Защита от файловых угроз максимально контролирует все открываемые, сохраняемые и запускаемые файлы. Компонент Защита от файловых угроз проверяет все типы файлов на всех жестких, сменных и сетевых дисках компьютера, а также архивы, установочные пакеты и вложенные OLE-объекты.
     - **Рекомендуемый**. Уровень безопасности файлов, который рекомендован для использования специалистами "Лаборатории Касперского". Компонент Защита от файловых угроз проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты, компонент Защита от файловых угроз не проверяет архивы и установочные пакеты.
     - **Низкий**. Уровень безопасности файлов, параметры которого обеспечивают максимальную скорость проверки. Компонент Защита от файловых угроз проверяет только файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера, компонент Защита от файловых угроз не проверяет составные файлы.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

     Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности**.
5. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами:
   - **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.
   - **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security блокирует эти файлы (чтение / запись).

- **Блокировать**. Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить.
- **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.

Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить (см. раздел "Восстановление файлов из резервного хранилища" на стр. 334).

6. Сохраните внесенные изменения.

Таблица 9. Параметры Защиты от файловых угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Типы файлов	**Файлы, проверяемые по формату**	Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.
Эвристический анализ	**Поверхностный**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Проверять только новые и измененные файлы	**Вкл**	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Использовать технологию iSwift	**Вкл**	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

Параметр	Значение	Описание
Использовать технологию iChecker	**Вкл**	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Проверять файлы офисных форматов	**Вкл**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Проверять файлы почтовых форматов	**Вкл**	Проверка файлов почтовых форматов. Приложение проверяет MSG- и EML-файлы. К файлам почтовых форматов также относятся OLE-объекты и MHT-файлы. Kaspersky Endpoint Security проверяет файлы почтовых форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Режим проверки	**Интеллектуальный**	Режим проверки, при котором Защита от файловых угроз проверяет объект на основании анализа операций, выполняемых над объектом. Например, при работе с документом Microsoft Office приложение Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**	Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

Автоматическая приостановка Защиты от файловых угроз

Вы можете настроить автоматическую приостановку Защиты от файловых угроз в указанное время или во время работы с определенными приложениями.

Приостановка работы Защиты от файловых угроз при конфликте с определенными приложениями является экстренной мерой. Если во время работы компонента возникают какие-либо конфликты, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (https://companyaccount.kaspersky.com). Специалисты помогут вам наладить совместную работу компонента Защита от файловых угроз с другими приложениями на вашем компьютере.

► *Чтобы настроить автоматическую приостановку работы Защиты от файловых угроз, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Приостановка Защиты от файловых угроз** перейдите по ссылке **Приостановить Защиту от файловых угроз**.
5. В открывшемся окне настройте параметры приостановки работы Защиты от файловых угроз:
   a. Настройте расписание автоматической приостановки Защиты от файловых угроз.
   b. Сформируйте список приложений, во время работы которых Защиту от файловых угроз следует приостанавливать.
6. Сохраните внесенные изменения.

Изменение действия компонента Защита от файловых угроз над зараженными файлами

По умолчанию компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз удаляет эти файлы.

► *Чтобы изменить действие компонента Защита от файловых угроз над зараженными файлами, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.
   - **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security блокирует эти файлы (чтение / запись).

- **Блокировать**. Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить.

Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить (см. раздел "Восстановление файлов из резервного хранилища" на стр. 334).

4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от файловых угроз

Под областью защиты подразумеваются объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от файловых угроз являются местоположение и тип проверяемых файлов. По умолчанию компонент Защита от файловых угроз проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460), запускаемые со всех жестких, съемных и сетевых дисков компьютера.

Выбирая тип проверяемых файлов, нужно учитывать следующее:

1. Вероятность внедрения вредоносного кода в файлы некоторых форматов и его последующей активации низка (например, формат TXT). В то же время существуют форматы файлов, которые содержат исполняемый код (например, форматы EXE, DLL). Также исполняемый код могут содержать форматы файлов, которые для этого не предназначены (например, формат DOC). Риск внедрения в такие файлы вредоносного кода и его активации высок.
2. Злоумышленник может отправить вирус или другое приложение, представляющее угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки приложение пропускает такой файл. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Kaspersky Endpoint Security анализирует заголовок файла. Если в результате выясняется, что файл имеет формат исполняемого файла (например, EXE), то приложение проверяет его.

► *Чтобы сформировать область защиты, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять компонентом Защита от файловых угроз:
   - **Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений).
   - **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.

- **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Формат файла определяется на основании его расширения.

5. Перейдите по ссылке **Изменить область защиты**.
6. В открывшемся окне выберите объекты, которые вы хотите добавить в область защиты или исключить из нее.

   Вы не можете удалить или изменить объекты, включенные в область защиты по умолчанию.

7. Если вы хотите добавить новый объект в область защиты, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

      Откроется дерево папок.

   b. В поле **Путь** введите путь к папке или файлу.

      Используйте маски:

      - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
      - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
      - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

      Вы можете использовать маски в любом месте пути к файлу или папке. Например, если вы хотите включить в область проверки папку Загрузки для всех учетных записей пользователей компьютера, введите маску `C:\Users\*\Downloads\`.

      Объект **Этот компьютер** в списке файловых ресурсов компьютера включает в себя следующие объекты: **Все жесткие диски**, **Все сетевые диски** и **Все съемные диски**.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области проверки. Для этого снимите флажок рядом с ним.

8. Сохраните внесенные изменения.

Использование методов проверки

Во время своей работы Kaspersky Endpoint Security использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Endpoint Security сравнивает найденный объект с записями в базах приложения. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

► *Чтобы настроить использование эвристического анализа в работе компонента Защита от файловых угроз, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Методы проверки** установите флажок **Эвристический анализ**, если вы хотите, чтобы приложение использовало эвристический анализ для защиты от файловых угроз. Далее при помощи ползунка задайте уровень эвристического анализа: **Поверхностный**, **Средний** или **Глубокий**.
5. Сохраните внесенные изменения.

Использование технологий проверки в работе компонента Защита от файловых угроз

► *Чтобы настроить использование технологий проверки в работе компонента Защита от файловых угроз, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать для защиты от файловых угроз:
   - **Использовать технологию iSwift**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
   - **Использовать технологию iChecker**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
5. Сохраните внесенные изменения.

kaspersky

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов компонентом Защита от файловых угроз: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Вы также можете включить использование технологий iChecker и iSwift (см. раздел "Использование технологий проверки в работе компонента Защита от файловых угроз" на стр. 146), которые позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Чтобы оптимизировать проверку файлов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Оптимизация** установите флажок **Проверять только новые и измененные файлы**.
5. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других приложений, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие приложения, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки.

Способ обработки зараженного составного файла (лечение или удаление) зависит от типа файла. Компонент Защита от файловых угроз лечит составные файлы форматов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и удаляет файлы всех остальных форматов (кроме почтовых баз).

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты, файлы почтовых или офисных форматов.
5. Если режим проверки только новых и измененных файлов выключен (см. раздел "Оптимизация проверки файлов" на стр. 147), настройте параметры проверки каждого типа составных файлов: проверка всех файлов этого типа или только новых файлов.

Если режим проверки только новых и измененных файлов включен, Kaspersky Endpoint Security проверяет только новые и измененные файлы всех типов составных файлов.

6. Настройте дополнительные параметры проверки составных файлов:

   - **Не распаковывать составные файлы большого размера**.

     Если флажок установлен, то Kaspersky Endpoint Security не проверяет составные файлы, размеры которых больше заданного значения.

     Если флажок снят, Kaspersky Endpoint Security проверяет составные файлы любого размера.

     > Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

   - **Распаковывать составные файлы в фоновом режиме**.

     Если флажок установлен, Kaspersky Endpoint Security предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом Kaspersky Endpoint Security в фоновом режиме распаковывает и проверяет составные файлы.

     Kaspersky Endpoint Security предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов.

     Если флажок снят, Kaspersky Endpoint Security предоставляет доступ к составным файлам только после распаковки и проверки файлов любого размера.

7. Сохраните внесенные изменения.

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором компонент Защита от файловых угроз начинает проверять файлы. По умолчанию Kaspersky Endpoint Security использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, компонент Защита от файловых угроз принимает решение о проверке файлов на основании анализа операций, которые пользователь, приложение от имени пользователя (под учетными данными которого был осуществлен вход в операционную систему или другого пользователя) или операционная система выполняет над файлами. Например, работая с документом Microsoft Office Word, Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

► *Чтобы изменить режим проверки файлов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Режим проверки** выберите нужный режим:
   - **Интеллектуальный**. Режим проверки, при котором Защита от файловых угроз проверяет объект на основании анализа операций, выполняемых над объектом. Например, при работе с документом Microsoft Office приложение Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.
   - **При доступе и изменении**. Режим проверки, при котором Защита от файловых угроз проверяет объекты при попытке их открыть или изменить.
   - **При доступе**. Режим проверки, при котором Защита от файловых угроз проверяет объекты только при попытке их открыть.
   - **При выполнении**. Режим проверки, при котором Защита от файловых угроз проверяет объекты только при попытке их запустить.
5. Сохраните внесенные изменения.

Проверка контейнеров

Контейнер – это изолированная среда, где приложение может работать без прямого взаимодействия с операционной системой. Использование контейнеров включает в себя следующие риски:

- Уязвимости в процессе контейнеризации могут быть использованы злоумышленниками для компрометации приложений внутри контейнера.
- Небезопасная конфигурация контейнерной среды может быть использована злоумышленниками для получения несанкционированного доступа к данным компьютера или нарушения целостности системы.
- Взлом контейнера может позволить злоумышленнику получить доступ к данным компьютера.
- Сетевые уязвимости могут быть использованы злоумышленниками для перехвата сетевого трафика.

Kaspersky Endpoint Security проверяет файлы не только на дисках, то и внутри контейнеров. То есть Kaspersky Endpoint Security является внешним инструментом для обнаружения вредоносной активности внутри контейнеров. Это позволяет сохранить производительность контейнеров и избежать конфликтов с другими приложениями внутри контейнера. Установка приложения Kaspersky Endpoint Security внутрь контейнера не поддерживается.

Кроме обеспечения безопасности контейнеров, Kaspersky Endpoint Security позволяет управлять работой приложений внутри контейнеров с помощью Контроля приложений (см. раздел "Контроль приложений" на стр. 191). Настройка Контроля приложения для контейнеров не отличается от настройки компонента для приложений, установленных на компьютере. Контроль целостности системы (на стр. 277) также поддерживает контейнеры.

Требования к контейнерам

- Контейнер создан на платформе Docker. Другие средства контейнеризации не поддерживаются.
- Контейнер запущен в режиме изоляции процессов. Режим изоляции Hyper-V не поддерживается.
- Контейнер расположен на сервере под управлением Windows Server 2016, 2019 или 2022 (Docker Host).
- Контейнер включает в себя образ Windows (Docker Image). ОС Windows 10 и 11 не поддерживаются. Образы Linux не поддерживаются.

Действие при обнаружении угрозы

При обнаружении угрозы внутри контейнера, приложение применяет действие, выбранное для компонента Защита от файловых угроз (см. раздел "Изменение действия компонента Защита от файловых угроз над зараженными файлами" на стр. 143). Также проверка контейнеров имеет дополнительные параметры (см. инструкцию ниже). При обнаружении угрозы, приложение блокирует вредоносную активность и выполняет выбранное действие (например, пытается вылечить объект). Kaspersky Endpoint Security может остановить контейнер, если вылечить обнаруженный объект не удалось. По умолчанию функция остановки контейнеров выключена.

► *Как настроить проверку контейнеров в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. В блоке **Проверка файловых операций, исполняемых в контейнерах Windows** настройте параметры проверки контейнеров:
   - **Останавливать контейнер, если лечение невозможно**. У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект.
   - **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.
4. Сохраните внесенные изменения.

Защита от веб-угроз

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110) и эвристического анализа.

Kaspersky Endpoint Security проверяет HTTP-, HTTPS- и FTP-трафик. Kaspersky Endpoint Security проверяет URL- и IP-адреса.

Для работы Защиты от веб-угроз необходимо выполнить первоначальную настройку приложения:

- Для контроля HTTPS-трафика включите проверку защищенных соединений (см. раздел "Включение проверки защищенных соединений" на стр. 181) (по умолчанию проверка включена).
- Выберите порты, которые Kaspersky Endpoint Security будет контролировать (см. раздел "Контроль сетевых портов" на стр. 273) (по умолчанию приложение контролирует все порты).
- Выберите приложения, трафик которых будет контролировать Kaspersky Endpoint Security (см. раздел "Формирование списка приложений, для которых контролируются все сетевые порты" на стр. 275). Основные браузеры уже добавлены в список, рекомендованный "Лабораторией Касперского". Если вашего браузера нет в списке, добавьте приложение вручную.
- Рекомендуется внедрить в трафик скрипт для взаимодействия с веб-страницами (см. раздел "Мониторинг активности пользователей в интернете" на стр. 264) (по умолчанию внедрение скрипта выключено). Скрипт позволяет регистрировать события работы Защиты от веб-угроз для журнала событий приложения, журнала событий ОС, отчетов (см. раздел "Работа с отчетами" на стр. 342).

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security заблокирует доступ и покажет предупреждение (см. рис. ниже).

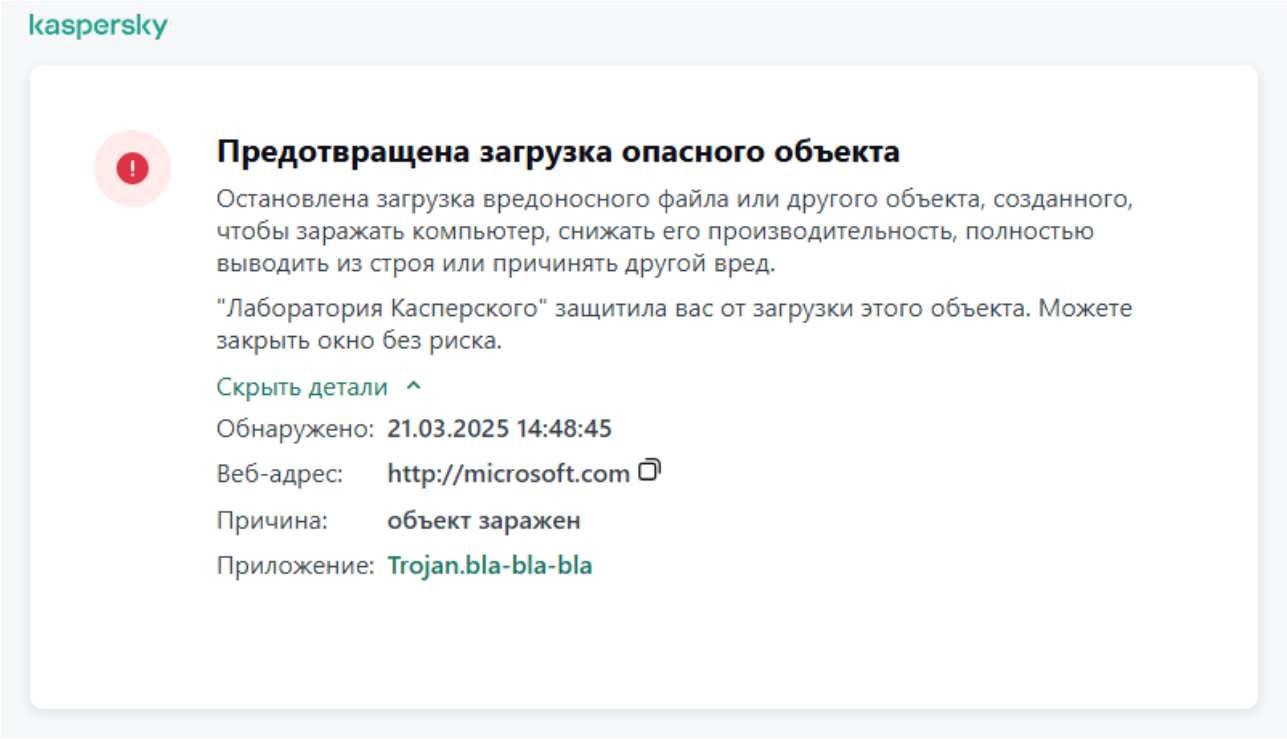


Рисунок 34. Сообщение о запрете доступа к веб-сайту

kaspersky

В этом разделе

Включение и выключение Защиты от веб-угроз 152

Настройка методов обнаружения вредоносных веб-адресов 154

Анти-Фишинг 156

Формирование списка доверенных веб-адресов 157

Включение и выключение Защиты от веб-угроз

По умолчанию компонент Защита от веб-угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от веб-угроз приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности веб-трафика **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности веб-трафика, получаемых или передаваемых по протоколам HTTP и FTP, или настроить уровень безопасности веб-трафика самостоятельно. После того как вы изменили параметры уровня безопасности веб-трафика, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности веб-трафика.

► *Как включить или выключить компонент Защита от веб-угроз в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.
3. Используйте переключатель **Защита от веб-угроз**, чтобы включить или выключить компонент.
4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Уровень безопасности веб-трафика, при котором компонент Защита от веб-угроз максимально проверяет веб-трафик, поступающий на компьютер по HTTP- и FTP-протоколам. Защита от веб-угроз детально проверяет все объекты веб-трафика, используя полный набор баз приложения, а также выполняет максимально глубокий эвристический анализ.
     - **Рекомендуемый**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на среднем уровне. Этот уровень безопасности веб-трафика рекомендован для использования специалистами "Лаборатории Касперского". Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.
     - **Низкий**. Уровень безопасности веб-трафика, параметры которого обеспечивают максимальную скорость проверки веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на поверхностном уровне.

- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности**.

5. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика:

   - **Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.
   - **Информировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта Kaspersky Endpoint Security разрешает загрузку этого объекта на компьютер и добавляет информацию о зараженном объекте в список активных угроз.

6. Сохраните внесенные изменения.

Таблица 10. Параметры Защиты от веб-угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Проверять веб-адрес по базе вредоносных веб-адресов	**Вкл**	Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.
Проверять веб-адрес по базе фишинговых веб-адресов	**Вкл**	В состав базы фишинговых веб-адресов и поддельных криптовалютных бирж включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Специалисты "Лаборатории Касперского" пополняют базу веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов и поддельных криптовалютных бирж входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.

Параметр	Значение	Описание
Использовать эвристический анализ (Защита от веб-угроз)	**Средний**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу, эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Использовать эвристический анализ (Анти-Фишинг)	**Вкл**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.
Действие при обнаружении угрозы	**Блокировать**	Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.

Настройка методов обнаружения вредоносных веб-адресов

Защита от веб-угроз обнаруживает вредоносные веб-адреса с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110) и эвристического анализа.

Вы можете выбрать методы обнаружения вредоносных веб-адресов только в Консоли администрирования (MMC) или в локальном интерфейсе приложения. Выбрать методы обнаружения вредоносных веб-адресов в Web Console или Cloud Console невозможно. По умолчанию проверка по базе вредоносных веб-адресов с использованием эвристического анализа (средний уровень) включена.

Проверка по базе вредоносных адресов

Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.

Kaspersky Endpoint Security проверяет все ссылки по базам вредоносных веб-адресов. Параметры проверки защищенных соединений приложения (см. раздел "Включение проверки защищенных соединений" на стр. 181) не влияют на проверку ссылок. То есть, если проверка защищенных соединений выключена, Kaspersky Endpoint Security проверяет ссылки по базам вредоносных веб-адресов, даже если сетевой трафик передается по защищенному соединению.

► *Как включить или выключить проверку по базе вредоносных адресов в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Методы проверки** используйте флажок **Проверять веб-адрес по базе вредоносных веб-адресов**, чтобы включить или выключить проверку по базе вредоносных адресов.
5. Сохраните внесенные изменения.

Эвристический анализ

В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую приложения производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу, эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

► *Как включить или выключить использование эвристического анализа в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.

3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Методы проверки** установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы приложение использовало эвристический анализ при проверке веб-трафика на наличие вирусов и других приложений, представляющих угрозу.

   Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу, эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
5. Сохраните внесенные изменения.

Анти-Фишинг

Защита от веб-угроз проверяет ссылки на принадлежность к фишинговым веб-адресам. Это позволяет избежать *фишинговых атак*. Частным примером фишинговых атак может служить сообщение электронной почты якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт банка в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его веб-адрес в браузере, однако находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Поскольку ссылка на фишинговый веб-сайт может содержаться не только в сообщении электронной почты, но и, например, в сообщении мессенджера, компонент Защита от веб-угроз отслеживает попытки перейти на фишинговый веб-сайт на уровне проверки веб-трафика и блокирует доступ к таким веб-сайтам. Списки фишинговых веб-адресов включены в комплект поставки Kaspersky Endpoint Security.

► *Как включить или выключить функцию Анти-Фишинг в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Анти-Фишинг** установите флажок **Проверять веб-адрес по базе фишинговых веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам фишинговых веб-адресов. В состав базы фишинговых веб-адресов и поддельных криптовалютных бирж включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Специалисты "Лаборатории Касперского" пополняют базу веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов и поддельных криптовалютных бирж входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.
5. Установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы приложение использовало эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок.

   В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую приложения производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

   Для проверки ссылок кроме антивирусных баз и эвристического анализа вы также можете

использовать репутационные базы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110).

6. Сохраните внесенные изменения.

Формирование списка доверенных веб-адресов

Защита от веб-угроз, кроме вредоносных и фишинговых веб-сайтов, может заблокировать и другие веб-сайты. Например, Защита от веб-угроз блокирует HTTP-трафик, который не соответствует стандартам RFC. Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Компонент Защита от веб-угроз не анализирует информацию, поступающую с доверенных веб-адресов, на присутствие вирусов и других приложений, представляющих угрозу. Такая возможность может быть использована, например, в том случае, если компонент Защита от веб-угроз препятствует загрузке файла с известного вам веб-сайта.

Под веб-адресом подразумевается адрес как отдельной веб-страницы, так и веб-сайта.

► *Как добавить доверенный веб-адрес в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. Установите флажок **Не проверять веб-трафик с доверенных веб-адресов** .

   Если флажок установлен, компонент Защита от веб-угроз не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта.
5. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете.

   Kaspersky Endpoint Security поддерживает символы * и ? для ввода маски.

   Вы также можете импортировать список доверенных веб-адресов из XML-файла.
6. Сохраните внесенные изменения.

В результате Защита от веб-угроз не будет проверять трафик доверенных веб-адресов. Пользователь всегда может открыть доверенный веб-сайт и загрузить файл с веб-сайта. Если получить доступ к веб-сайту не удалось, проверьте параметры компонентов Проверка защищенных соединений (на стр. 181), Веб-Контроль (на стр. 252) и Контроль сетевых портов (на стр. 273). Если Kaspersky Endpoint Security определяет загруженный с доверенного веб-сайта файл как вредоносный, вам нужно добавить этот файл в исключения (см. раздел "Создание исключения из проверки" на стр. 320).

Вы также можете сформировать общий список исключений защищенных соединений (см. раздел "Исключение защищенных соединений из проверки" на стр. 188). В этом случае Kaspersky Endpoint Security не будет проверять HTTPS-трафик доверенных веб-адресов при работе компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль.

kaspersky

Защита от почтовых угроз

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 110) и эвристического анализа.

Защита от почтовых угроз может проверять и получаемые, и отправляемые сообщения. Приложение поддерживает протоколы POP3, SMTP, IMAP, NNTP в следующих почтовых клиентах:

- Microsoft Office Outlook;
- Mozilla Thunderbird;
- Windows Mail;
- МойОфис Почта;
- Органайзер Р7-Офис.

Для проверки трафика в почтовых клиентах Mozilla Thunderbird, МойОфис Почта и Органайзер Р7-Офис вам нужно добавить сертификат "Лаборатории Касперского" в хранилище сертификатов и выбрать собственное хранилище сертификатов (см. раздел "Добавление сертификата "Лаборатории Касперского" в собственное хранилище сертификатов" на стр. 187).

Другие протоколы и почтовые клиенты Защита от почтовых угроз не поддерживает.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security добавляет информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

В этом разделе

Включение и выключение Защиты от почтовых угроз 159

Изменение действия над зараженными сообщениями электронной почты 162

Формирование области защиты компонента Защита от почтовых угроз 163

Проверка составных файлов, вложенных в сообщения электронной почты 164

Фильтрация вложений в сообщениях электронной почты 165

kaspersky

Включение и выключение Защиты от почтовых угроз

По умолчанию компонент Защита от почтовых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от почтовых угроз приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности почты **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности почты или настроить уровень безопасности почты самостоятельно. После того как вы изменили параметры уровня безопасности почты, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности почты.

Работая с почтовым клиентом Mozilla Thunderbird, компонент Защита от почтовых угроз не проверяет на вирусы и другие приложения, представляющие угрозу, сообщения, передаваемые по протоколу IMAP, в случае если используются фильтры, перемещающие сообщения из папки входящих сообщений.

► *Как включить или выключить компонент Защита от почтовых угроз в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.
3. Используйте переключатель **Защита от почтовых угроз**, чтобы включить или выключить компонент.
4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз максимально контролирует сообщения. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет глубокий эвристический анализ. Высокий уровень безопасности почты рекомендуется применять для работы в опасной среде. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованной защиты почты.
     - **Рекомендуемый**. Уровень безопасности почты, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью почты. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет эвристический анализ среднего уровня. Этот уровень безопасности почты рекомендован для использования специалистами "Лаборатории Касперского". Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.
     - **Низкий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз проверяет только входящие сообщения электронной почты, а также выполняет поверхностный эвристический анализ и не проверяет архивы, вложенные в сообщения. Если используется этот уровень безопасности почты, компонент Защита от почтовых угроз проверяет сообщения электронной почты максимально быстро и затрачивает минимум ресурсов операционной системы. Низкий уровень безопасности почты рекомендуется применять для работы в хорошо защищенной среде. Примером такой среды может служить локальная сеть организации с централизованным обеспечением безопасности почты.

- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности**.

5. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами:

   - **Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.
   - **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.
   - **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

6. Сохраните внесенные изменения.

Таблица 11. Параметры Защиты от почтовых угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Область защиты	**Входящие и исходящие сообщения**	*Область защиты* – это объекты, которые проверяет компонент во время своей работы: входящие и исходящие сообщения или только входящие сообщения. Для защиты компьютеров достаточно проверять только входящие сообщения. Вы можете включить проверку исходящих сообщений для предотвращения отправки зараженных файлов в архивах. Вы также можете включить проверку исходящих сообщений, если вы хотите запретить обмен файлами определенных форматов, например, аудио или видео.

Параметр	Значение	Описание
Подключить расширение для Microsoft Outlook	**Вкл**	Если флажок установлен, включена проверка сообщений электронной почты, передающихся по протоколам POP3, SMTP, NNTP, IMAP на стороне расширения, интегрированного в Microsoft Outlook. В случае проверки почты с помощью расширения для Microsoft Outlook рекомендуется использовать режим кеширования Exchange (Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендации по его использованию вы можете найти в базе знаний Microsoft https://technet.microsoft.com/ru-ru/library/cc179175.aspx.
Проверять вложенные архивы	**Вкл**	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять вложенные файлы форматов Microsoft Office	**Вкл**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Фильтр вложений	**Переименовывать вложения указанных типов**	Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл.
Эвристический анализ	**Средний**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

Параметр	Значение	Описание
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**	При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

Изменение действия над зараженными сообщениями электронной почты

По умолчанию компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз удаляет зараженные сообщения электронной почты.

► *Чтобы изменить действие над зараженными сообщениями электронной почты, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое выполняет Kaspersky Endpoint Security при обнаружении зараженного сообщения:
   - **Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.
   - **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.
   - **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.
4. Сохраните внесенные изменения.

kaspersky

Формирование области защиты компонента Защита от почтовых угроз

Область защиты – это объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от почтовых угроз являются параметры интеграции компонента Защита от почтовых угроз в почтовые клиенты, тип сообщений электронной почты и почтовые протоколы, трафик которых проверяет компонент Защита от почтовых угроз. По умолчанию Kaspersky Endpoint Security проверяет как входящие, так и исходящие сообщения электронной почты, трафик почтовых протоколов POP3, SMTP, NNTP и IMAP, а также интегрируется в почтовый клиент Microsoft Office Outlook.

► *Чтобы сформировать область защиты компонента Защита от почтовых угроз, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Область защиты** выберите сообщения для проверки:
   - **Входящие и исходящие сообщения**.
   - **Только входящие сообщения**.

   Для защиты компьютеров достаточно проверять только входящие сообщения. Вы можете включить проверку исходящих сообщений для предотвращения отправки зараженных файлов в архивах. Вы также можете включить проверку исходящих сообщений, если вы хотите запретить обмен файлами определенных форматов, например, аудио или видео.

   Если вы выбираете проверку только входящих сообщений, рекомендуется однократно проверить все исходящие сообщения, поскольку существует вероятность того, что на вашем компьютере есть почтовые черви, которые используют электронную почту в качестве канала распространения. Это позволит избежать проблем, связанных с неконтролируемой рассылкой зараженных сообщений с вашего компьютера.
5. В блоке **Встраивание в операционную систему** выполните следующие действия:
   - Установите флажок **Проверять трафик POP3, SMTP, NNTP, IMAP**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя.

     Снимите флажок **Проверять трафик POP3, SMTP, NNTP, IMAP**, если вы хотите, чтобы компонент Защита от почтовых угроз не проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя. В этом случае сообщения проверяет расширение компонента Защита от почтовых угроз, встроенное в почтовый клиент Microsoft Office Outlook, после их получения на компьютере пользователя, если установлен флажок **Подключить расширение для Microsoft Outlook**.

Если вы используете почтовый клиент, отличный от Microsoft Office Outlook, то при снятом флажке **Проверять трафик POP3, SMTP, NNTP, IMAP** компонент Защита от почтовых угроз не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

- Установите флажок **Подключить расширение для Microsoft Outlook**, если вы хотите открыть доступ к настройке параметров компонента Защита от почтовых угроз из приложения Microsoft Office Outlook и включить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в приложение Microsoft Office Outlook.

  Снимите флажок **Подключить расширение для Microsoft Outlook**, если вы хотите закрыть доступ к настройке параметров компонента Защита от почтовых угроз из приложения Microsoft Office Outlook и выключить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в приложение Microsoft Office Outlook.

  Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

6. Сохраните внесенные изменения.

Проверка составных файлов, вложенных в сообщения электронной почты

Вы можете включить или выключить проверку объектов, вложенных в сообщения, ограничить максимальный размер проверяемых объектов, вложенных в сообщения, и максимальную длительность проверки объектов, вложенных в сообщения.

► *Чтобы настроить проверку составных файлов, вложенных в сообщения электронной почты, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Проверка составных файлов** настройте параметры проверки:
   - **Проверять вложенные файлы форматов Microsoft Office**. Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
   - **Проверять вложенные архивы**. Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).

Если во время проверки приложение обнаружило в тексте сообщения пароль к архиву, пароль будет использован для проверки содержания этого архива на наличие вредоносных приложений. Пароль при этом не сохраняется. При проверке архива выполняется его распаковка. Если во время распаковки архива произошел сбой в работе приложения, вы можете вручную удалить файлы, которые при распаковке сохраняются по следующему пути: %systemroot%\temp. Файлы имеют префикс PR.

- **Не проверять архивы размером более N МБ (от 1 до 9999)**. Если флажок установлен, компонент Защита от почтовых угроз исключает из проверки вложенные в сообщения электронной почты архивы, размер которых больше заданного. Если флажок снят, компонент Защита от почтовых угроз проверяет архивы любого размера, вложенные в сообщения электронной почты.
- **Ограничить время проверки архива до N сек (от 1 до 9999)**. Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом.

5. Сохраните внесенные изменения.

Фильтрация вложений в сообщениях электронной почты

Функциональность фильтрации вложений не применяется для исходящих сообщений электронной почты.

Вредоносные приложения могут распространяться в виде вложений в сообщениях электронной почты. Вы можете настроить фильтрацию по типу вложений в сообщениях, чтобы автоматически переименовывать или удалять файлы указанных типов. Переименовав вложение определенного типа, Kaspersky Endpoint Security может защитить ваш компьютер от автоматического запуска вредоносного приложения.

► *Чтобы настроить фильтрацию вложений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Фильтр вложений** выполните одно из следующих действий:
   - **Не применять фильтр**. Если выбран этот вариант, компонент Защита от почтовых угроз не фильтрует файлы, вложенные в сообщения электронной почты.
   - **Переименовывать вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл.
   - **Удалять вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз удаляет из сообщений электронной почты вложенные файлы указанных типов.

5. Если на предыдущем шаге инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, установите флажки напротив нужных типов файлов.
6. Сохраните внесенные изменения.

kaspersky

Защита от сетевых угроз

Компонент *Защита от сетевых угроз* (также Intrusion Detection System (IDS) – система обнаружения вторжений) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, приложение блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей приложения.

В этом разделе

Включение и выключение Защиты от сетевых угроз 167

Блокирование атакующего компьютера 168

Настройка адресов исключений из блокирования 170

Настройка Защиты от сетевых угроз по типам 171

Включение и выключение Защиты от сетевых угроз

По умолчанию компонент Защита от сетевых угроз включен и работает в оптимальном режиме. Kaspersky Endpoint Security отслеживает во входящем сетевом трафике активность, характерную для сетевых атак, и блокирует атаки.

► *Как включить или выключить Защиту от сетевых угроз в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.

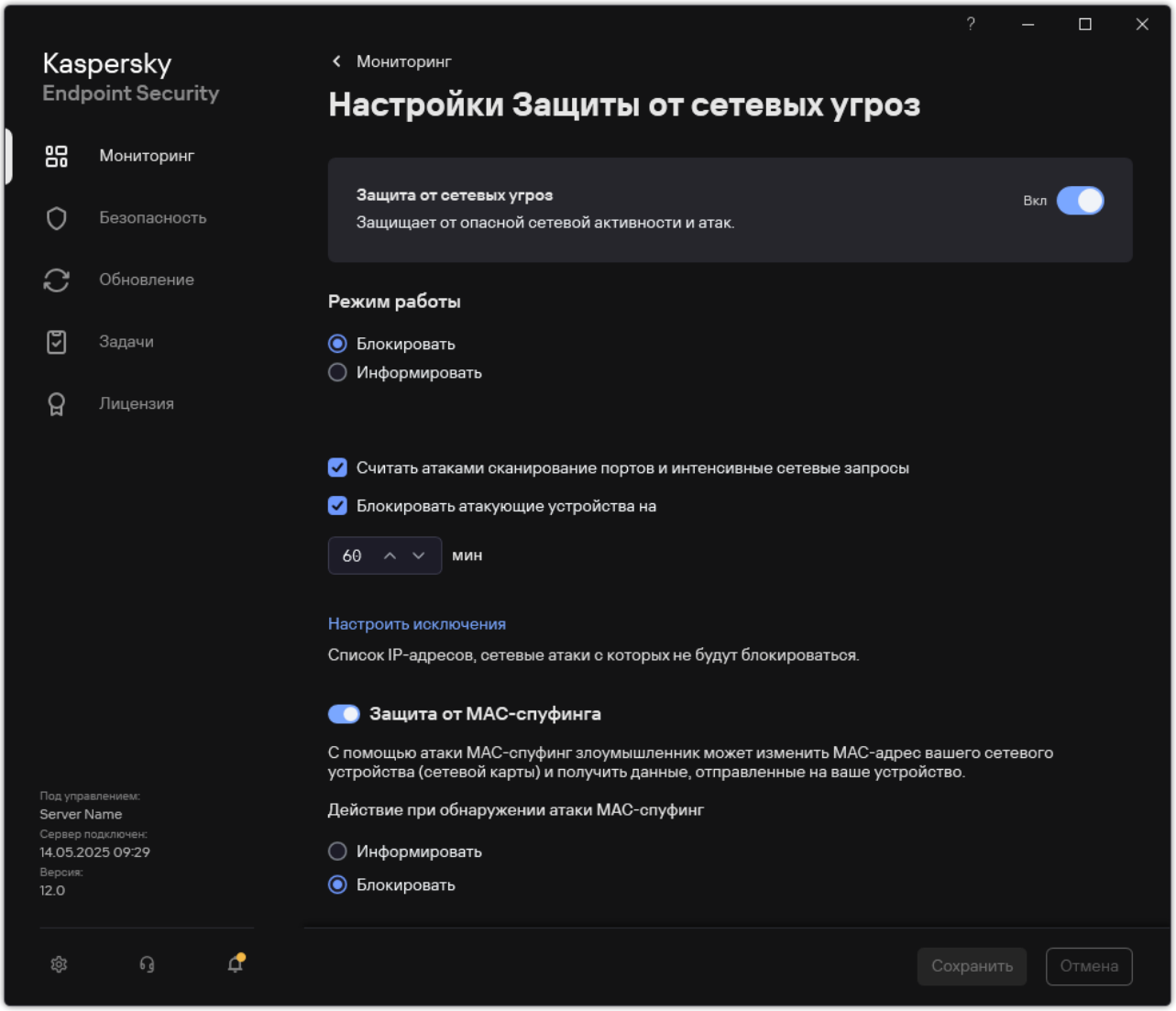


Рисунок 35. Параметры Защиты от сетевых угроз

3. Используйте переключатель **Защита от сетевых угроз**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Блокирование атакующего компьютера

Если компонент Защита от сетевых угроз включен, Kaspersky Endpoint Security автоматически блокирует сетевые атаки. Дополнительно приложение может заблокировать атакующий компьютер и ограничить отправку сетевых пакетов на определенный период времени. По умолчанию Kaspersky Endpoint Security блокирует компьютер на один час.

► *Как заблокировать атакующий компьютер в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.
3. Включите переключатель **Блокировать атакующие устройства на N мин**.

   Если функция включена, компонент Защита от сетевых угроз добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых угроз блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное – 999 минут.
4. Измените время блокирования атакующего компьютера в поле, расположенном снизу от переключателя **Блокировать атакующие устройства на N мин**.
5. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security, обнаружив попытку сетевой атаки на компьютер пользователя, блокирует все соединения с атакующим компьютером. Kaspersky Endpoint Security создает событие *Обнаружена сетевая атака*. Событие содержит информацию об атакующем компьютере: IP- и MAC-адреса.

MAC-адрес атакующего компьютера вы можете просмотреть в интерфейсе приложения и в консоли Kaspersky Security Center версии 15.1 и выше.

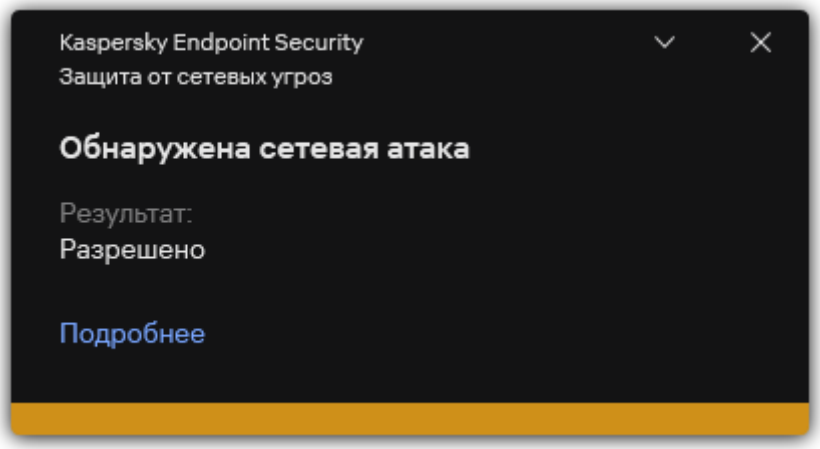


Рисунок 36. Уведомление об обнаружении сетевой атаки

Kaspersky Endpoint Security разблокирует компьютер по истечению заданного периода времени. В консоли Kaspersky Security Center нет инструментов мониторинга заблокированных компьютеров кроме событий *Обнаружена сетевая атака* в отчете. Вы можете просмотреть список заблокированных компьютеров только в интерфейсе приложения. Для этого предназначен инструмент *Мониторинг сети*. Также с помощью инструмента Мониторинг сети вы можете разблокировать компьютер.

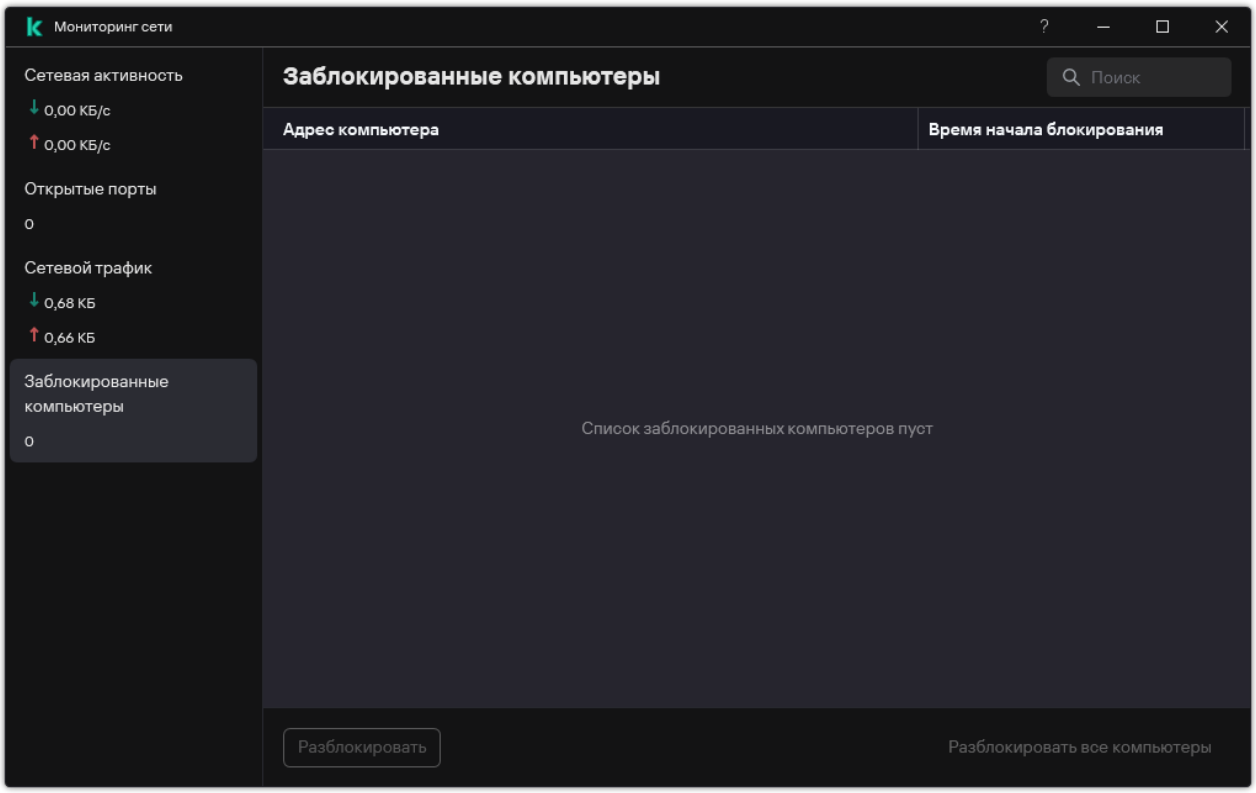
► *Чтобы разблокировать компьютер, выполните следующие действия:*

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Мониторинг сети**.
2. Перейдите на закладку **Заблокированные компьютеры**.

   Откроется список заблокированных компьютеров (см. рис. ниже).

   > Kaspersky Endpoint Security очищает список блокирования при перезапуске приложения и при изменении параметров Защиты от сетевых угроз.

3. Выберите компьютер, который вы хотите разблокировать и нажмите **Разблокировать**.



Настройка адресов исключений из блокирования

Kaspersky Endpoint Security может распознать сетевую атаку и заблокировать безопасное сетевое соединение, по которому передается большое количество пакетов (например, от камер наблюдения). Для работы с доверенными устройствами вы можете добавить IP-адреса этих устройств в список исключений. Также вы можете выбрать протокол и порт, по которым передаются данные, чтобы разрешить отдельную сетевую активность.

Выбор протокола и портов для исключений добавлен в Kaspersky Endpoint Security версии 12.2. Убедитесь, что приложение и плагин управления обновлены до версии 12.2 или выше. Если вы используете более раннюю версию приложения или плагина управления, Kaspersky Endpoint Security разрешает активность компьютеров только по IP-адресу.

► *Как настроить адреса исключений из блокирования в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.
3. Нажмите на ссылку **Настроить исключения**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.

   Если требуется, выберите протокол и порты, по которым передаются данные.
6. Сохраните внесенные изменения.

Настройка Защиты от сетевых угроз по типам

Kaspersky Endpoint Security позволяет управлять защитой от следующих типов сетевых атак:

- *Атака типа Интенсивные сетевые запросы (англ. Network Flooding)* – атака на сетевые ресурсы организации (например, веб-серверы). Атака заключается в отправке большого количества запросов для превышения пропускной способности сетевых ресурсов. Таким образом, пользователи не могут получить доступ к сетевым ресурсам организации.
- *Атака типа Сканирование портов* заключается в сканировании UDP- и TCP-портов, а также сетевых служб на компьютере. Атака позволяет определить степень уязвимости компьютера перед более опасными видами сетевых атак. Сканирование портов также позволяет злоумышленнику определить операционную систему на компьютере и выбрать подходящие для нее сетевые атаки.
- *Атака типа MAC-спуфинг* заключается в изменении MAC-адреса сетевого устройства (сетевой карты). В результате злоумышленник может перенаправить данные, отправленные на устройство, на другое устройство и получить доступ к этим данным. Kaspersky Endpoint Security позволяет блокировать атаки MAC-спуфинга и получать уведомления об атаках.

Вы можете выключить обнаружение этих типов атак, так как некоторые разрешенные приложения выполняют действия, характерные для таких атак. Таким образом, вы можете избежать ложных срабатываний.

По умолчанию Kaspersky Endpoint Security не отслеживает атаки типа Интенсивные сетевые запросы, Сканирование портов и MAC-спуфинг.

На виртуальных машинах в инфраструктуре Microsoft Hyper-V не рекомендуем включать обнаружение атак типа MAC-спуфинг. Из-за особенностей работы платформы Microsoft Hyper-V Kaspersky Endpoint Security может заблокировать гипервизор из-за ложных срабатываний.

► *Как настроить Защиту от сетевых угроз по типам в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.
3. Используйте переключатель **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение атак.

   Если функция включена, Kaspersky Endpoint Security контролирует сетевой трафик на наличие сканирования портов и интенсивных сетевых запросов. При обнаружении такого поведения приложение уведомляет пользователя и отправляет соответствующее событие в Kaspersky Security Center. Приложение предоставляет информацию о компьютере, с которого выполняются запросы. Эта информация нужна для принятия своевременных действий по реагированию. При этом Kaspersky Endpoint Security не блокирует компьютер, с которого выполняются запросы, так как такой трафик может быть штатным поведением в сети организации.
4. Используйте переключатель **Защита от MAC-спуфинга**, чтобы включить или выключить обнаружение атак.
5. В блоке **Действие при обнаружении атаки MAC-спуфинг** выберите один из следующих вариантов:
   - **Информировать**.
   - **Блокировать**.
6. Сохраните внесенные изменения.

kaspersky

Защита от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру. В результате вирус может выполнять команды под вашей учетной записью, например, загрузить вредоносное приложение.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, приложение предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) (см. раздел "Использовании экранной клавиатуры при авторизации USB-устройств" на стр. 174) цифровой код, сформированный приложением (см. рис. ниже). Эта процедура называется авторизацией клавиатуры.

Если код введен правильно, приложение сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

> При подключении авторизованной клавиатуры через другой USB-порт компьютера приложение снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, приложение формирует новый. Вы можете настроить число попыток для ввода цифрового кода (см. раздел "Включение и выключение Защиты от атак BadUSB" на стр. 174). Если цифровой код введен неправильно несколько раз или закрыто окно авторизации клавиатуры (см. рис. ниже), приложение блокирует ввод с этой клавиатуры. По истечении времени блокировки USB-устройства или перезагрузке операционной системы приложение снова предлагает пройти авторизацию клавиатуры.

Приложение разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

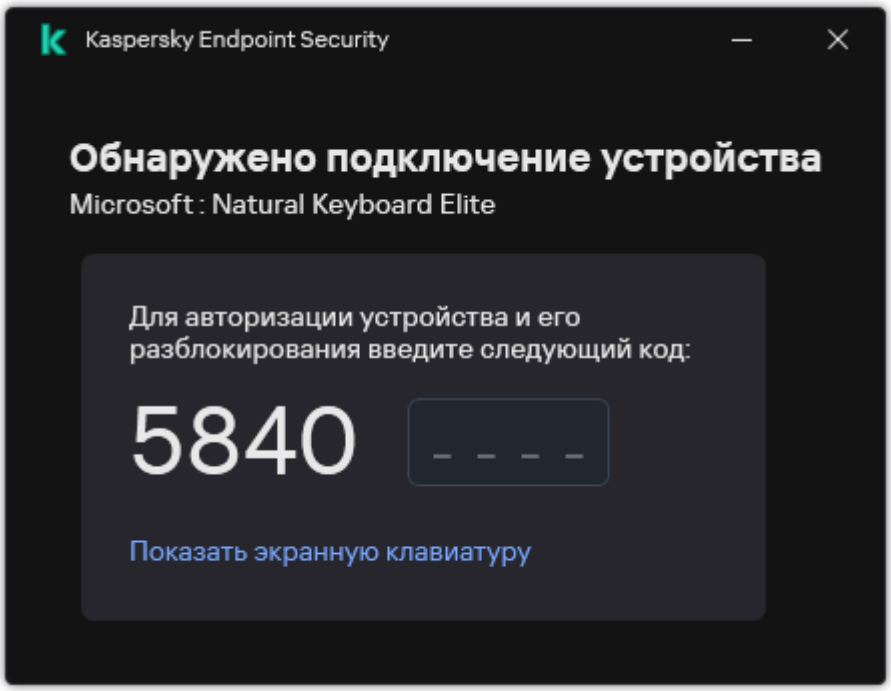


Рисунок 37. Уведомление об авторизации клавиатуры

В этом разделе

Включение и выключение Защиты от атак BadUSB 174
Использовании экранной клавиатуры при авторизации USB-устройств 174
Авторизация сканеров штрихкода 175

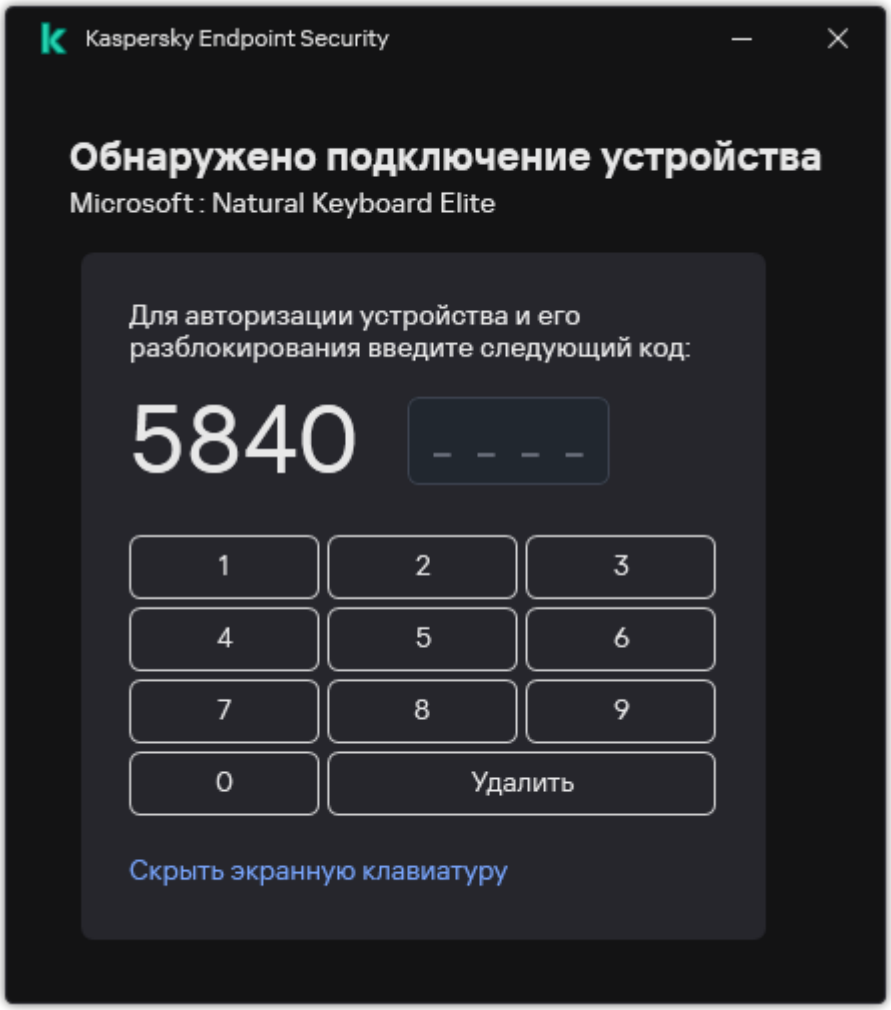
Включение и выключение Защиты от атак BadUSB

USB-устройства, определенные операционной системой как клавиатуры и подключенные к компьютеру до установки компонента Защита от атак BadUSB, считаются авторизованными после его установки.

В результате, если Защита от атак BadUSB включена, Kaspersky Endpoint Security требует авторизацию подключенного USB-устройства, определенного операционной системой как клавиатура. Пользователь не может использовать неавторизованную клавиатуру до тех пор, пока она не будет авторизована.

Использовании экранной клавиатуры при авторизации USB-устройств

Возможность использовать экранную клавиатуру предназначена только для авторизации USB-устройств, не поддерживающих произвольный ввод символов (например, сканеров штрихкодов). Не рекомендуется использовать экранную клавиатуру для авторизации неизвестных вам USB-устройств.



Авторизация сканеров штрихкода

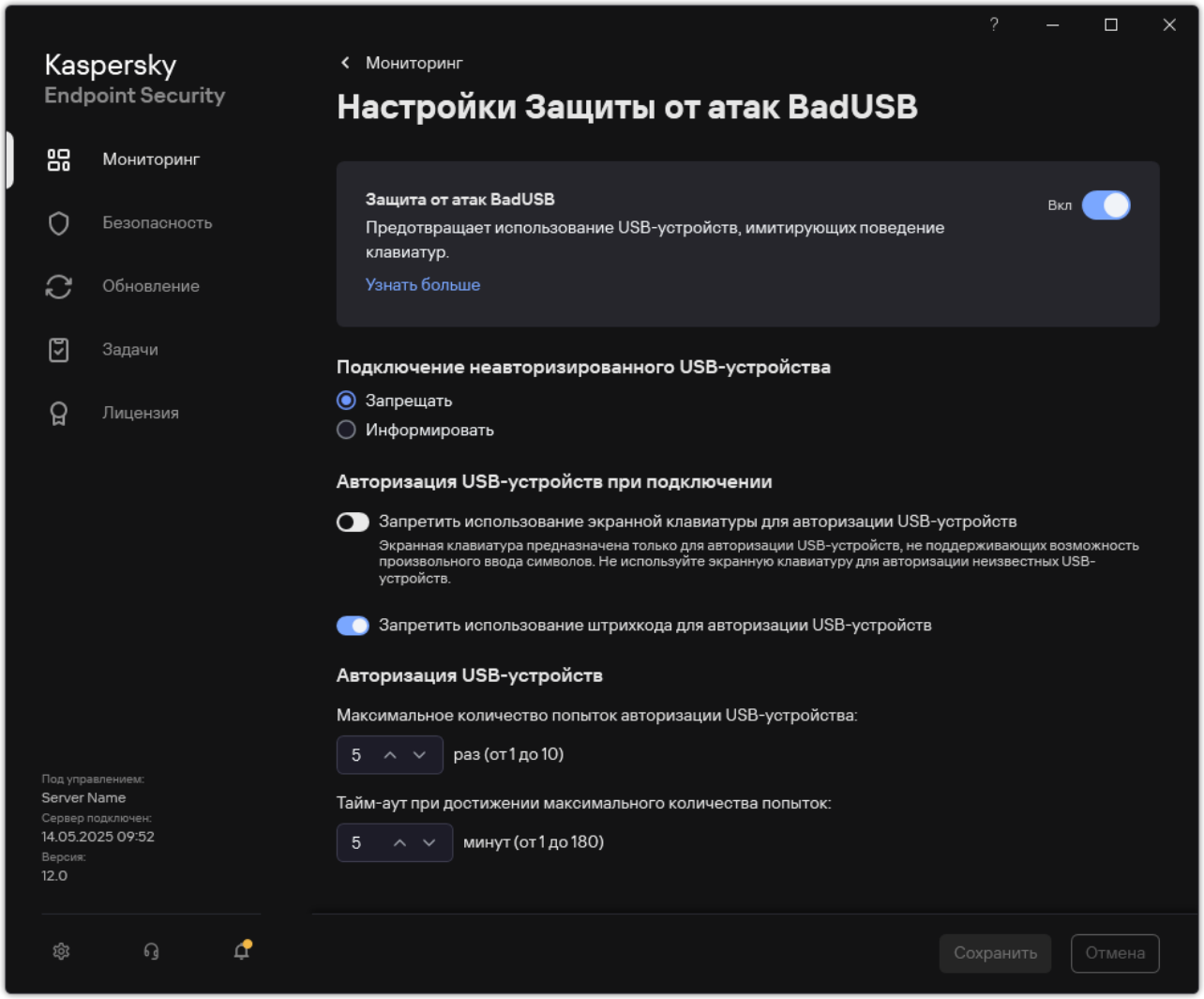
При подключении сканера штрихкодов к компьютеру компонент Защита от атак BadUSB определяет это устройство как устройство ввода и предлагает выполнить процедуру авторизации. Для авторизации сканера штрихкодов вам нужно считать штрихкод с экрана. Приложение формирует штрихкод в формате Code39, который поддерживает большинство сканеров штрихкодов и сканеров QR-кодов.

Kaspersky Endpoint Security также поддерживает другой способ авторизации сканеров штрихкодов. Если вы используете устройства с сенсорным экраном, для авторизации сканера штрихкодов вы можете ввести код с помощью экранной клавиатуры. Для этого вам нужно разрешить использование экранной клавиатуры (см. раздел "Использовании экранной клавиатуры при авторизации USB-устройств" на стр. 174). Этот способ удобен, например, для стационарных сканеров штрихкодов в составе кассовых аппаратов. Другие способы авторизации сканеров штрихкодов запрещены.

По умолчанию приложение не использует штрихкод для авторизации USB-устройств.

► *Как включить авторизацию USB-устройств по штрихкоду в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от атак BadUSB**.



3. Используйте переключатель **Запретить использование штрихкода для авторизации USB-устройств**, чтобы запретить или разрешить использование штрихкодов для авторизации.
4. Сохраните внесенные изменения.

AMSI-защита

Компонент AMSI-защита предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. *Интерфейс Antimalware Scan Interface (AMSI)* позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для дополнительной проверки и получать результаты проверки этих объектов. Сторонними приложениями могут быть, например, приложения Microsoft Office (см. рис. ниже). Подробнее об интерфейсе AMSI см. в документации Microsoft https://docs.microsoft.com/ru-ru/windows/desktop/amsi/antimalware-scan-interface-portal.

AMSI-защита может только обнаруживать угрозу и уведомлять стороннее приложение об обнаруженной угрозе. Стороннее приложение после получения уведомления об угрозе не дает выполнить вредоносные действия (например, завершает работу).

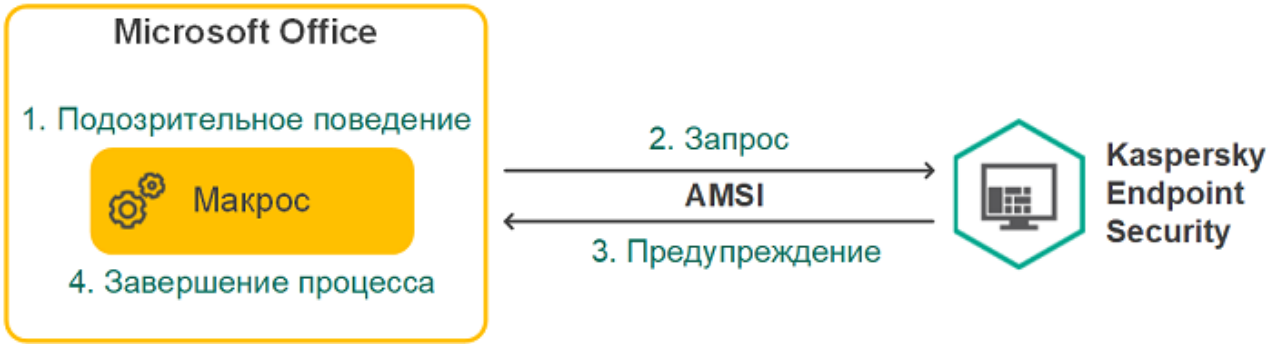


Рисунок 38. Пример работы AMSI

Компонент AMSI-защита может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. Kaspersky Endpoint Security отправляет информацию об отклонении запроса от стороннего приложения на Сервер администрирования. Компонент AMSI-защита не отклоняет запросы от тех сторонних приложений, для которых включена функция постоянного взаимодействия с компонентом AMSI-защита (см. раздел "Формирование списка доверенных приложений" на стр. 326).

AMSI-защита доступна для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise / Enterprise multi-session;
- Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core);
- Windows Server 2025 Standard / Datacenter.

В этом разделе

Включение и выключение AMSI-защиты 178
Оптимизация проверки файлов AMSI-защитой 179

Включение и выключение AMSI-защиты

По умолчанию AMSI-защита включена и работает в рекомендованном специалистами «Лаборатории Касперского» режиме (см. таблицу ниже).

► *Как включить или выключить AMSI-защиту в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **AMSI-защита**.

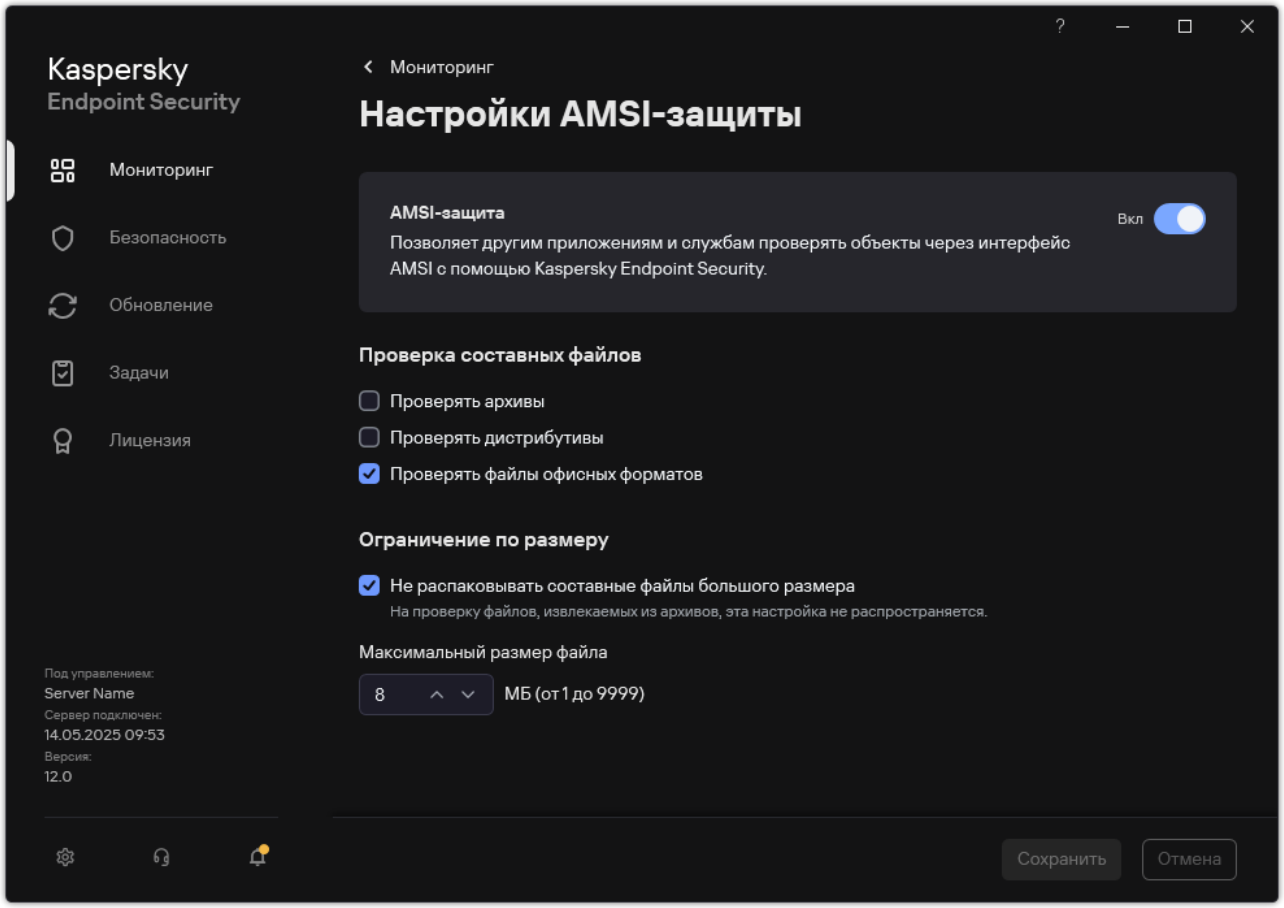


Рисунок 39. Параметры AMSI-защиты

3. Используйте переключатель **AMSI-защита**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Таблица 12. Параметры AMSI-защиты, рекомендованные специалистами "Лаборатории Касперского"

Параметр	Значение	Описание
Проверять архивы	**Выкл**	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	**Выкл**	Проверка дистрибутивов сторонних приложений.
Проверять файлы офисных форматов	**Вкл**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Не распаковывать составные файлы большого размера	**Максимальный размер файла 8 МБ**	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Оптимизация проверки файлов AMSI-защитой

Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Вы можете выбрать составные файлы, которые необходимо проверять: архивы, дистрибутивы или файлы офисных форматов. Вы можете также ограничить размер проверяемых составных файлов. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.

Распространенной практикой сокрытия вирусов и других приложений, представляющих угрозу, является внедрение их в составные файлы, например, архивы. Чтобы обнаружить скрытые таким образом вирусы и другие приложения, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить набор типов проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Как оптимизировать проверку файлов AMSI-защитой в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **AMSI-защита**.
3. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.
4. В блоке **Ограничение по размеру** выполните одно из следующих действий:
   - Чтобы запретить компоненту AMSI-защита распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и укажите нужное значение. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.
   - Чтобы разрешить компоненту AMSI-защита распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Компонент AMSI-защита проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
5. Сохраните внесенные изменения.

kaspersky

Проверка защищенных соединений

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Kaspersky Endpoint Security использует этот сертификат для проверки защищенных соединений. Также Kaspersky Endpoint Security включает использование системного хранилища доверенных сертификатов в приложениях Firefox и Thunderbird для проверки трафика этих приложений.

Компоненты Веб-Контроль (на стр. 252), Защита от почтовых угроз (на стр. 158), Защита от веб-угроз (на стр. 151), Анализ поведения (на стр. 115), Защита от эксплойтов (на стр. 124) могут расшифровывать и проверять сетевой трафик, передаваемый по защищенным соединениям с использованием следующих протоколов:

- SSL 3.0;
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

В этом разделе

Включение проверки защищенных соединений 181

Установка доверенных корневых сертификатов 185

Проверка защищенных соединений с недоверенным сертификатом 186

Добавление сертификата "Лаборатории Касперского" в собственное хранилище сертификатов .. 187

Исключение защищенных соединений из проверки 188

Включение проверки защищенных соединений

По умолчанию Kaspersky Endpoint Security проверяет защищенные соединения не всегда, а только по запросу компонентов защиты.

► *Как включить проверку защищенных соединений в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

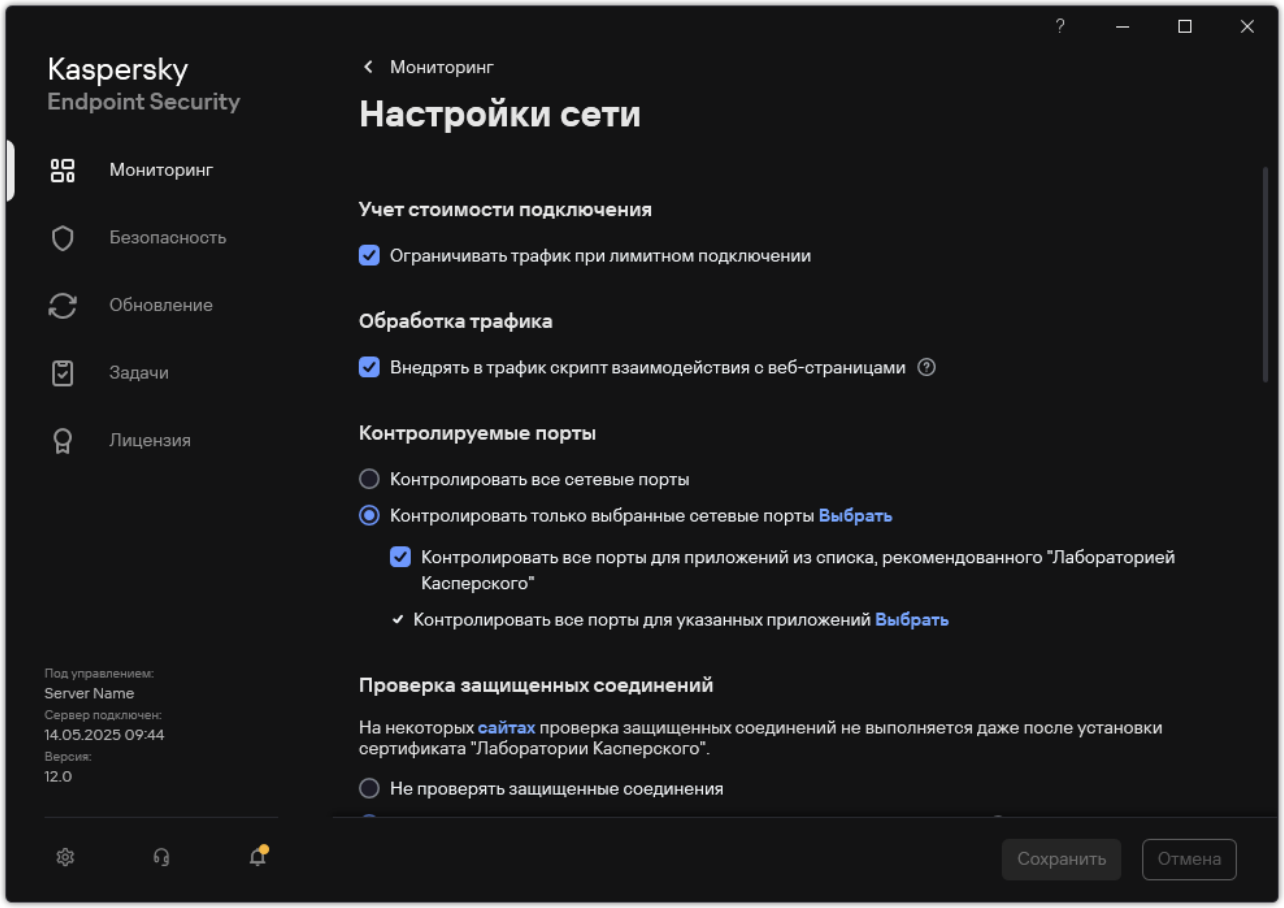


Рисунок 40. Параметры проверки защищенных соединений

3. В блоке **Проверка защищенных соединений** выберите режим проверки защищенных соединений:
   - **Не проверять защищенные соединения**. Kaspersky Endpoint Security не имеет доступ к содержанию сайтов, адрес которых начинается с https://.
   - **Проверять защищенные соединения по запросу компонентов защиты**. Kaspersky Endpoint Security проверяет зашифрованный трафик только по запросу компонентов Защита от веб-угроз, Защита от почтовых угроз и Веб-Контроль.
   - **Всегда проверять защищенные соединения**. Kaspersky Endpoint Security проверяет зашифрованный сетевой трафик, даже если компоненты защиты выключены.

   Kaspersky Endpoint Security не проверяет защищенные соединения, установленные доверенными приложениями, для которых выключена проверка трафика (см. раздел "Формирование списка доверенных приложений" на стр. 326). Также Kaspersky Endpoint Security не проверяет защищенные соединения из предустановленного списка доверенных сайтов. Предустановленный список доверенных сайтов составляют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения. Вы можете просмотреть предустановленный список доверенных сайтов только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center просмотреть список невозможно.

4. Если требуется, добавьте исключения из проверки: доверенные адреса и приложения (см. раздел "Исключение защищенных соединений из проверки" на стр. 188).

5. Настройте параметры проверки защищенных соединений (см. таблицу ниже).

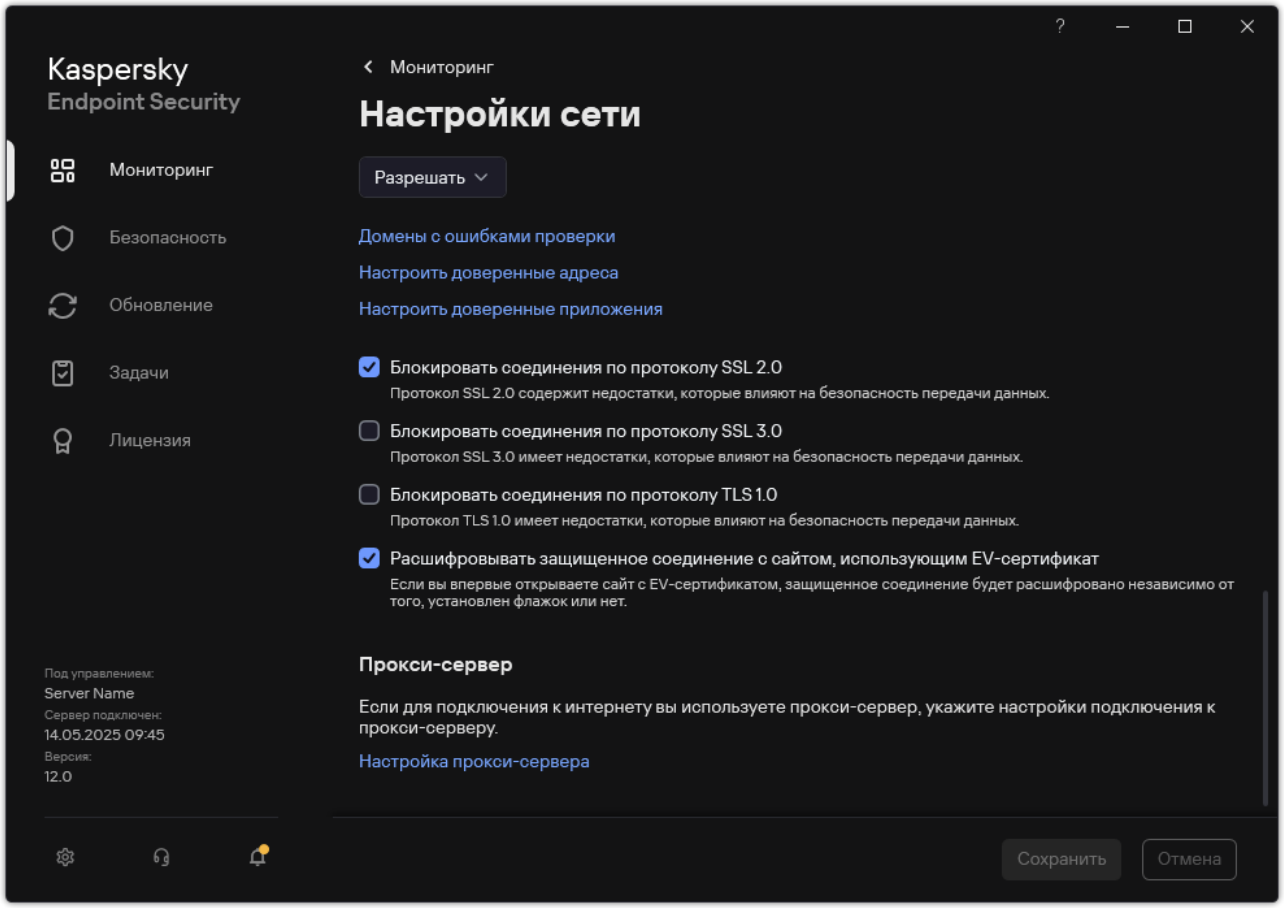


Рисунок 41. Параметры сети приложения

6. Сохраните внесенные изменения.

Таблица 13. Параметры проверки защищенных соединений

Параметр	Описание
Доверенные корневые сертификаты	Список доверенных корневых сертификатов. Kaspersky Endpoint Security позволяет устанавливать доверенные корневые сертификаты на компьютеры пользователей, если, например, вам нужно развернуть новый центр сертификации. Приложение позволяет добавить сертификат в специальное хранилище сертификатов Kaspersky Endpoint Security. При этом сертификат будет доверенным только для приложения Kaspersky Endpoint Security. То есть пользователь будет иметь доступ к веб-сайту с новым сертификатом в браузере. Если другое приложение попытается получить доступ к веб-сайту, вы можете получить ошибку соединения из-за проблем с сертификатом. Для добавления сертификата в системное хранилище сертификатов, вы можете использовать групповые политики Active Directory.

Параметр	Описание
Переход на домен с недоверенным сертификатом	• **Разрешать**. При переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security разрешает установку сетевого соединения (см. раздел "Проверка защищенных соединений с недоверенным сертификатом" на стр. 186). При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения. По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. Если стороннее приложение или служба устанавливает соединение с доменом с недоверенным сертификатом, Kaspersky Endpoint Security создаст собственный сертификат для проверки трафика. Новый сертификат будет иметь статус *Недоверенный*. Это нужно, чтобы предупредить стороннее приложение о недоверенном соединении, так как показать HTML-страницу в этом случае невозможно и соединение может быть установлено в фоновом режиме. • **Блокировать**. При переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security блокирует сетевое соединение. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security отображает HTML-страницу с информацией о причине, по которой переход на этот домен заблокирован.
Переход на домен с ошибкой проверки защищенного соединения	• **Блокировать**. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение. • **Разрешать и добавлять домен в исключения**. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security добавляет домен, при переходе на который возникла ошибка, в список доменов с ошибками проверки и не контролирует зашифрованный сетевой трафик при переходе на этот домен. Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе приложения. Чтобы сбросить содержание списка, нужно выбрать элемент **Блокировать**. Также Kaspersky Endpoint Security формирует событие об ошибке проверки защищенного соединения.
Блокировать соединения по протоколу SSL 2.0	Если флажок установлен, то приложение контролирует и блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. При этом приложение не контролирует сетевой трафик по этому протоколу.
Блокировать соединения по протоколу SSL 3.0	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу SSL 3.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 3.0. Приложение контролирует сетевой трафик по этому протоколу. Все компоненты приложения работают без ограничений.

Параметр	Описание
Блокировать соединения по протоколу TLS 1.0	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу TLS 1.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу TLS 1.0. Приложение контролирует сетевой трафик по этому протоколу. Все компоненты приложения работают без ограничений.
Расшифровывать защищенное соединение с сайтом, использующим EV-сертификат	EV-сертификаты (англ. Extended Validation Certificate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет. Если флажок установлен, приложение расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, приложение не имеет доступа к содержанию HTTPS-трафика. Поэтому приложение контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://bing.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.

Установка доверенных корневых сертификатов

Kaspersky Endpoint Security позволяет устанавливать доверенные корневые сертификаты на компьютеры пользователей, если, например, вам нужно развернуть новый центр сертификации. Приложение позволяет добавить сертификат в специальное хранилище сертификатов Kaspersky Endpoint Security. При этом сертификат будет доверенным только для приложения Kaspersky Endpoint Security. То есть пользователь будет иметь доступ к веб-сайту с новым сертификатом в браузере. Если другое приложение попытается получить доступ к веб-сайту, вы можете получить ошибку соединения из-за проблем с сертификатом. Для добавления сертификата в системное хранилище сертификатов, вы можете использовать групповые политики Active Directory.

► *Как установить доверенные сертификаты в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Показать сертификаты**.
4. В открывшемся окне нажмите на кнопку **Добавить** и выберите доверенный корневой сертификат.

   Kaspersky Endpoint Security поддерживает сертификаты с расширением PEM, DER и CRT.
5. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security при проверке трафика кроме системного хранилища сертификатов будет использовать собственное хранилище сертификатов.

kaspersky

Проверка защищенных соединений с недоверенным сертификатом

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Kaspersky Endpoint Security использует этот сертификат для проверки защищенных соединений. При переходе на домен с недоверенным сертификатом вы можете разрешить или заблокировать пользователю доступ к этому домену (см. инструкцию ниже).

Если вы разрешили пользователю переходить на домены с недоверенным сертификатом, Kaspersky Endpoint Security выполняет следующие действия:

- При переходе на домен с недоверенным сертификатом в *браузере*, Kaspersky Endpoint Security использует сертификат "Лаборатории Касперского" для проверки трафика. Kaspersky Endpoint Security отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения (см. рис. ниже). По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. После перехода по этой ссылке Kaspersky Endpoint Security в течение часа не будет отображать предупреждения о недоверенном сертификате при переходе на другие веб-ресурсы в том же домене. Также Kaspersky Endpoint Security формирует событие об использовании защищенного соединения с недоверенным сертификатом.

  В некоторых случаях у Kaspersky Endpoint Security нет технической возможности показать HTML-страницу с предупреждением в браузере (см. рис. ниже). Например, если веб-ресурс использует устаревшую версию сетевого протокола и нестандартный порт. В этих случаях Kaspersky Endpoint Security заблокирует доступ к этому домену, а браузер покажет стандартное окно `ERR_CONNECTION_RESET`. Для доступа к веб-ресурсу вы можете добавить домен в исключения (см. раздел "Исключение защищенных соединений из проверки" на стр. 188) или использовать доверенный сертификат.

- Если *стороннее приложение или служба* устанавливает соединение с доменом с недоверенным сертификатом, Kaspersky Endpoint Security создаст собственный сертификат для проверки трафика. Новый сертификат будет иметь статус *Недоверенный*. Это нужно, чтобы предупредить стороннее приложение о недоверенном соединении, так как показать HTML-страницу в этом случае невозможно и соединение может быть установлено в фоновом режиме. Поэтому, если стороннее приложение имеет встроенные инструменты проверки сертификатов, соединение может быть разорвано. В этом случае, вам нужно обратиться к владельцу домена и настроить доверенное соединение. Если настроить доверенное соединение невозможно, вы можете добавить это стороннее приложение в список доверенных приложений (см. раздел "Формирование списка доверенных приложений" на стр. 326). Также Kaspersky Endpoint Security формирует событие об использовании защищенного соединения с недоверенным сертификатом.

► *Как настроить проверку защищенных соединений с недоверенным сертификатом в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

3. В блоке **Проверка защищенных соединений** выберите режим работы приложения при переходе на домен с недоверенным сертификатом: **Разрешать** или **Блокировать**.
4. Сохраните внесенные изменения.

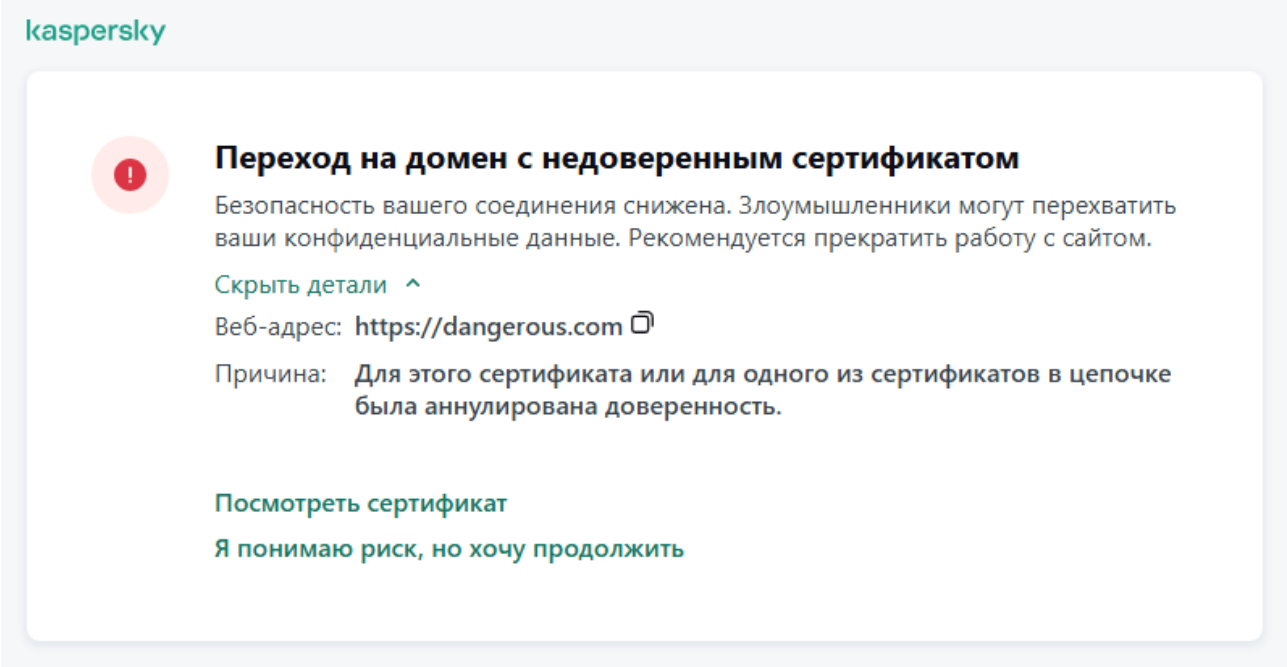


Рисунок 42. Предупреждение о переходе на домен с недоверенным сертификатом

Добавление сертификата "Лаборатории Касперского" в собственное хранилище сертификатов

С помощью сертификата браузеры и почтовые клиенты проверяют безопасность и подлинность веб-ресурсов. Также сертификат обеспечивает шифрование данных между веб-ресурсами и пользователем. Большинство браузеров и почтовых клиентов используют хранилище доверенных сертификатов (хранилище сертификатов Windows), например, Google Chrome. Некоторые браузеры и почтовые клиенты по умолчанию используют собственное хранилище сертификатов, а не хранилище сертификатов Windows, например, Firefox и Thunderbird.

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Если в вашей организации развернуто решение Kaspersky Security Center и к компьютеру применена политика, Kaspersky Endpoint Security автоматически включает использование хранилища сертификатов Windows в браузерах и почтовых клиентах для проверки трафика этих приложений. Если к компьютеру не применена политика, вы можете выбрать хранилище сертификатов, которое будут использовать браузеры и почтовые клиенты. Если вы выбрали собственное хранилище сертификатов, добавьте сертификат "Лаборатории Касперского" в хранилище вручную. Это позволит избежать ошибок при работе с HTTPS-трафиком.

Для проверки трафика в браузере Mozilla Firefox и почтовом клиенте Thunderbird должна быть включена проверка защищенных соединений (см. раздел "Включение проверки защищенных соединений" на стр. 181). Если проверка защищенных соединений выключена, приложение не проверяет трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird. Также проверку защищенных соединений нужно включить для проверки трафика в почтовых клиентах МойОфис Почта и Органайзер Р7-Офис.

Перед добавлением сертификата в собственное хранилище браузера или почтового клиента экспортируйте сертификат "Лаборатории Касперского" из Панели управления Windows (свойства браузера). Подробнее об экспорте сертификата "Лаборатории Касперского" вы можете узнать в базе знаний Службы технической поддержки https://support.kaspersky.ru/14620. Подробнее о добавлении сертификата в хранилище вы можете узнать, например, на сайте Службы технической поддержки Mozilla https://support.mozilla.org/.

Вы можете выбрать хранилище сертификатов только в локальном интерфейсе приложения.

► *Чтобы выбрать хранилище сертификатов для проверки защищенных соединений в браузерах и почтовых клиентах, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Проверка защищенных соединений** установите флажок **В приложениях с собственным хранилищем сертификатов для проверки защищенных соединений использовать**.
4. Выберите хранилище сертификатов:
   - **Хранилище сертификатов Windows (рекомендуется)**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке приложения Kaspersky Endpoint Security.
   - **Собственное хранилище сертификатов**. Приложения Mozilla Firefox и Thunderbird используют собственное хранилище сертификатов. Если выбрано хранилище сертификатов Mozilla, корневой сертификат "Лаборатории Касперского" нужно добавить в это хранилище вручную через свойства браузера.

     Также собственное хранилище сертификатов используют почтовые клиенты МойОфис Почта и Органайзер Р7-Офис.
5. Сохраните внесенные изменения.

Исключение защищенных соединений из проверки

Большинство веб-ресурсов используют защищенное соединение. Специалисты "Лаборатории Касперского" рекомендуют включить проверку защищенных соединений (см. раздел "Включение проверки защищенных соединений" на стр. 181). Если проверка защищенных соединений мешает работе, вы можете добавить веб-сайт в исключения, – *доверенные адреса*. В этом случае Kaspersky Endpoint Security не будет проверять HTTPS-трафик доверенных веб-адресов при работе компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль.

Если доверенное приложение использует защищенное соединение, вы можете выключить проверку защищенных соединений для этого приложения (см. раздел "Формирование списка доверенных приложений" на стр. 326). Например, вы можете выключить проверку защищенных соединений для приложений облачных хранилищ, так как эти приложения используют двухфакторную аутентификацию с собственным сертификатом.

► *Как исключить веб-адрес из проверки защищенных соединений в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

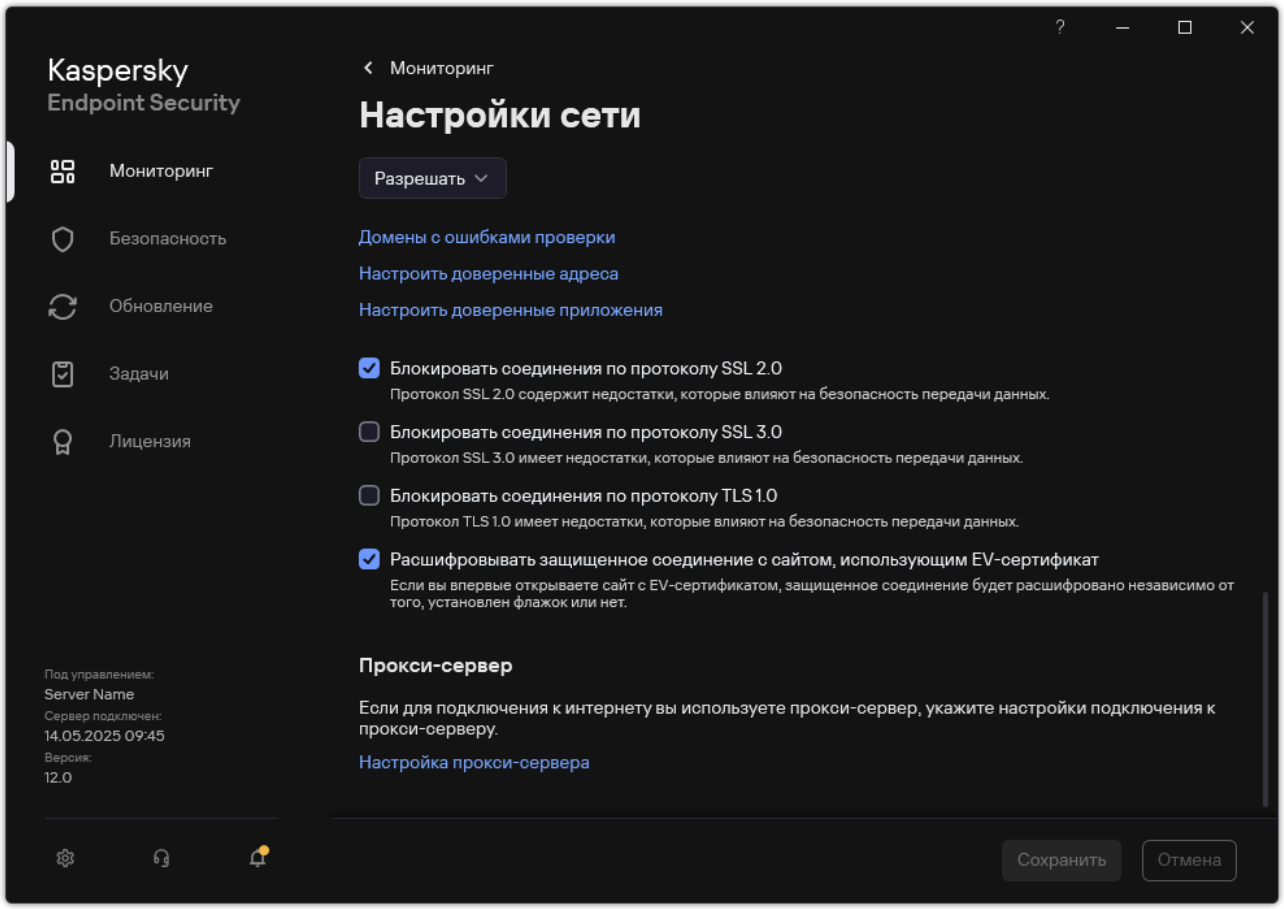


Рисунок 43. Параметры сети приложения

3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Настроить доверенные адреса**.
4. Нажмите на кнопку **Добавить**.
5. Введите имя домена или IP-адрес, если вы хотите, чтобы приложение Kaspersky Endpoint Security не проверяло защищенные соединения, устанавливаемые при переходе на эту веб-страницу.

   Kaspersky Endpoint Security поддерживает символ * для ввода маски в имени домена.

   Kaspersky Endpoint Security не поддерживает символ * для IP-адресов. Вы можете выбрать диапазон IP-адресов с помощью маски подсети (например, 198.51.100.0/24).

Примеры:

- `domain.com` – запись включает в себя следующие адреса: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Запись исключает поддомены (например, `subdomain.domain.com`).
- `subdomain.domain.com` – запись включает в себя следующие адреса: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Запись исключает домен `domain.com`.
- `*.domain.com` – запись включает в себя следующие адреса: `https://movies.domain.com`, `https://images.domain.com/page123`. Запись исключает домен `domain.com`.

6. Сохраните внесенные изменения.

По умолчанию Kaspersky Endpoint Security не проверяет защищенные соединения при возникновении ошибок и добавляет веб-сайт в специальный список – *домены с ошибками проверки*. Kaspersky Endpoint Security составляет список для каждого пользователя отдельно и не передает данные в Kaspersky Security Center. Вы можете включить блокирование соединения при возникновении ошибки (см. раздел "Включение проверки защищенных соединений" на стр. 181). Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе приложения.

► *Чтобы просмотреть список доменов с ошибками проверки, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Домены с ошибками проверки**.

Откроется список доменов с ошибками проверки. Чтобы сбросить список вам нужно включить блокирование соединения при возникновении ошибки в политике, применить политику, вернуть параметр в исходное состояние и снова применить политику.

Специалисты "Лаборатории Касперского" составляют список доверенных веб-сайтов, которые Kaspersky Endpoint Security не проверяет независимо от параметров приложения, – *глобальные исключения*.

► *Чтобы просмотреть глобальные исключения из проверки защищенного трафика, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на ссылку со списком доверенных веб-сайтов.

Откроется список веб-сайтов, составленный специалистами "Лаборатории Касперского". Kaspersky Endpoint Security не проверяет защищенные соединения для сайтов из списка. Список может быть обновлен при обновлении баз и модулей Kaspersky Endpoint Security.

kaspersky

Контроль приложений

Контроль приложений управляет запуском приложений на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании приложений. Также Контроль приложений снижает риск заражения компьютера, ограничивая доступ к приложениям.

Настройка Контроля приложений состоит из следующих этапов:

1. Создание категорий приложений.

   Администратор создает категории приложений, которыми администратор хочет управлять. Категории приложений предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, *Браузеры*), хеш файла, производитель приложения и другие.

2. Создание правил Контроля приложений.

   Администратор создает правила Контроля приложений в политике для группы администрирования. Правило включает в себя категории приложений и статус запуска приложений из этих категорий: запрещен или разрешен. Администратор может создать множество правил. При этом одно приложение может соответствовать критериям нескольких правил. Приоритет запрещающего правила выше разрешающего. Kaspersky Endpoint Security проверяет приложение на принадлежность к правилу при каждом запуске. Kaspersky Endpoint Security последовательно проверяет приложение по всем правилам Контроля приложения.

3. Выбор режима работы Контроля приложений (см. раздел "Контроль приложений на основе эталонного компьютера" на стр. 198).

   Администратор выбирает режим работы с приложениями, которые не входят ни в одно из правил (списки запрещенных и разрешенных приложений).

При попытке пользователя запустить запрещенное приложение, Kaspersky Endpoint Security заблокирует запуск приложения и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля приложений предусмотрен *тестовый режим*. В этом режиме Kaspersky Endpoint Security выполняет следующие действия:

- разрешает запуск приложений, в том числе запрещенных;
- показывает уведомление о запуске запрещенного приложения и добавляет информацию в отчет на компьютере пользователя;

- отправляет данные о запуске запрещенных приложений в Kaspersky Security Center.

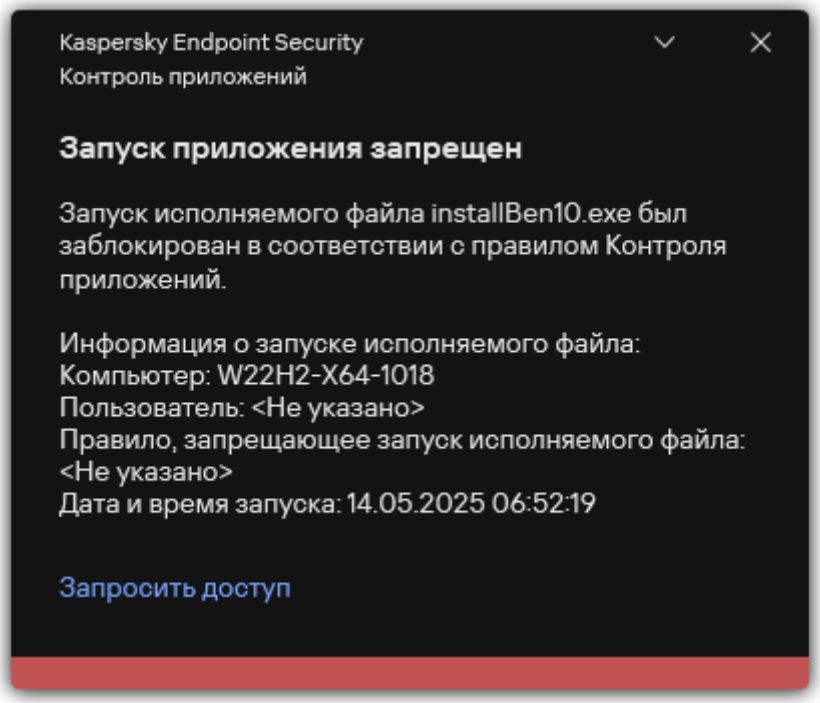


Рисунок 44. Уведомление Контроля программ

Режимы работы Контроля приложений

Компонент Контроль приложений может работать в двух режимах:

- **Список запрещенных**. Режим, при котором Контроль приложений разрешает пользователям запуск любых приложений, кроме тех, которые запрещены в правилах Контроля приложений.

  Этот режим работы Контроля приложений установлен по умолчанию.

- **Список разрешенных**. Режим, при котором Контроль приложений запрещает пользователям запуск любых приложений, кроме тех, которые разрешены и не запрещены в правилах Контроля приложений.

  Если разрешающие правила Контроля приложений сформированы максимально полно, компонент запрещает запуск всех новых приложений, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных приложений, которые нужны пользователям для выполнения должностных обязанностей.

  Вы можете ознакомиться с рекомендациями по настройке правил Контроля приложений в режиме списка разрешенных приложений.

Настройка Контроля приложений для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security, так и с помощью Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security и необходимые для следующих задач:

- Создание категорий приложений.

  Правила Контроля приложений, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях приложений, а не на включающих и

исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.

- Получение информации о приложениях, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль приложений рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля приложений

Kaspersky Endpoint Security использует алгоритм для принятия решения о запуске приложения (см. рис. ниже).

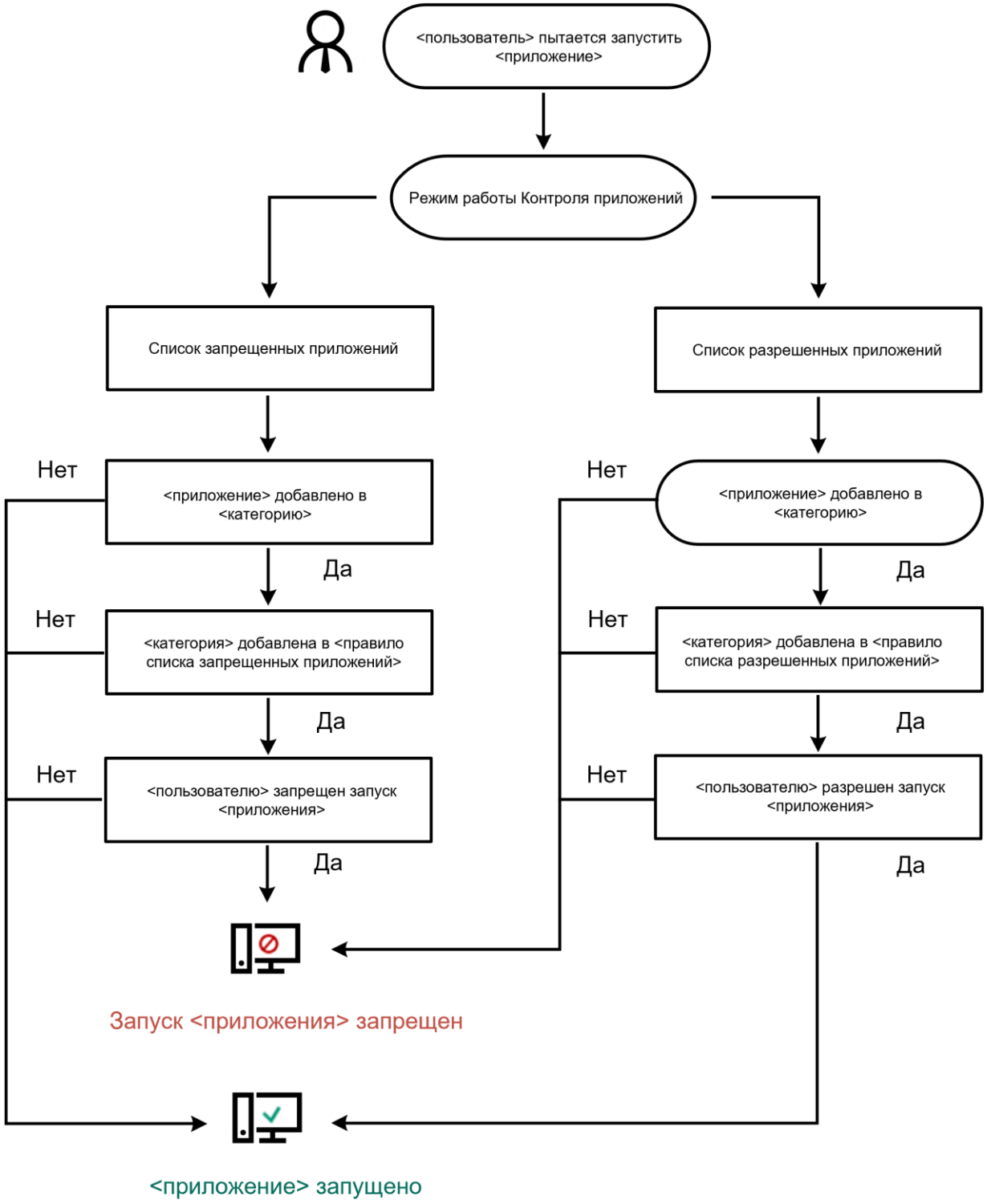


Рисунок 45. Алгоритм работы Контроля программ

kaspersky

В этом разделе

Ограничения функциональности Контроля приложений 195
Включение режима блокирования только запрещенных приложений 196
Контроль приложений на основе эталонного компьютера 198
Действия с правилами Контроля приложений в интерфейсе приложения 201
Тестирование правил Контроля приложений 206
Мониторинг активности приложений 206
Правила формирования масок имен файлов или папок 207
Изменение шаблонов сообщений Контроля приложений 208

Ограничения функциональности Контроля приложений

Работа компонента Контроль приложений ограничена в следующих случаях:

- При обновлении версии приложения импорт параметров компонента Контроль приложений не поддерживается.
- При отсутствии соединения с серверами KSN Kaspersky Endpoint Security получает информацию о репутации приложения и их модулей только из локальных баз.

  Список приложений, для которых Kaspersky Endpoint Security определяет KL-категорию **Другие приложения\Приложения, доверенные согласно репутации в KSN**, при наличии соединения с серверами KSN может отличаться от списка приложений, для которых Kaspersky Endpoint Security определяет KL-категорию **Другие приложения\Приложения, доверенные согласно репутации в KSN**, при отсутствии соединения с KSN.

- В базе данных Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с компьютера, на котором установлено приложение Kaspersky Endpoint Security, файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.
- Компонент не контролирует запуск скриптов, если скрипт передается интерпретатору не через командную строку.

  Если запуск интерпретатора разрешен правилами Контроля приложений, то компонент не блокирует скрипт, запущенный из этого интерпретатора.
  Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля приложений, то компонент блокирует все скрипты, указанные в командной строке интерпретатора.

- Компонент не контролирует запуск скриптов из интерпретаторов, не поддерживаемых приложением Kaspersky Endpoint Security.

Kaspersky Endpoint Security поддерживает следующие интерпретаторы:

- Java;
- PowerShell.

Поддерживаются следующие типы интерпретаторов:

- %ComSpec%;
- %SystemRoot%\system32\regedit.exe;
- %SystemRoot%\regedit.exe;
- %SystemRoot%\system32\regedt32.exe;
- %SystemRoot%\system32\cscript.exe;
- %SystemRoot%\system32\wscript.exe;
- %SystemRoot%\system32\msiexec.exe;
- %SystemRoot%\system32\mshta.exe;
- %SystemRoot%\system32\rundll32.exe;
- %SystemRoot%\system32\wwahost.exe;
- %SystemRoot%\syswow64\cmd.exe;
- %SystemRoot%\syswow64\regedit.exe;
- %SystemRoot%\syswow64\regedt32.exe;
- %SystemRoot%\syswow64\cscript.exe;
- %SystemRoot%\syswow64\wscript.exe;
- %SystemRoot%\syswow64\msiexec.exe;
- %SystemRoot%\syswow64\mshta.exe;
- %SystemRoot%\syswow64\rundll32.exe;
- %SystemRoot%\syswow64\wwahost.exe.

Включение режима блокирования только запрещенных приложений

Режим *Запрещенные приложения* – это режим, при котором Контроль приложений разрешает пользователям запуск любых приложений, кроме тех, которые запрещены в правилах Контроля приложений. То есть, если запрещающего правила нет, Контроль приложений разрешает запуск приложения. Этот режим работы Контроля приложений установлен по умолчанию.

Перед включением режима *Запрещенные приложения* рекомендуется проверить работу правил Контроля приложений. Для этого вы можете включить режим тестирования (см. раздел "Тестирование правил Контроля приложений" на стр. 206).

► *Как включить режим блокирования только запрещенных приложений в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. Включите переключатель **Контроль приложений**.
4. В блоке **Режим контроля запуска приложений** выберите вариант **Список запрещенных. Разрешены все приложения, кроме указанных в списке**.
5. В блоке **Действие при запуске приложений, запрещенных правилами** выберите действие Контроля приложения:
   - **Информировать (тестовый режим) и записывать в отчет**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.
   - **Блокировать**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.
6. Выберите статус для правил Контроля приложений:
   - **Включено**. Статус означает, что правило используется во время работы компонента Контроль приложений.
   - **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль приложений.
   - **Тестовый режим**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск приложений, на которые распространяется действие правила, но заносит информацию о запуске этих приложений в отчет.

   Если требуется, добавьте новые правила Контроля приложений.
7. Настройте дополнительные параметры Контроля приложений:
   - **Контролировать загрузку DLL-модулей**. Если флажок установлен, то Kaspersky Endpoint Security контролирует загрузку DLL-модулей при запуске пользователями приложений. Информация о DLL-модуле и приложении, загрузившей этот DLL-модуль, сохраняется в отчет.

     При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля приложений включено правило по умолчанию **Приложения ОС** или другое правило, которое содержит KL-категорию **Приложения ОС\Доверенные сертификаты** и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле **Приложения ОС** может привести к нестабильности операционной системы.

     Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Рекомендуется перезагрузить компьютер после установки флажка, чтобы приложение контролировало все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.

- **Использовать строгую проверку цифровой подписи**. Вы можете выбрать сертификат в качестве условия срабатывания правила Контроля приложений. Если флажок установлен, то Kaspersky Endpoint Security применяет правила к приложениям, подписанных сертификатом только из доверенного системного хранилища сертификатов приложения (см. раздел "Работа с приложениями, подписанными доверенной цифровой подписью" на стр. 331). Приложения, подписанные таким сертификатом, также являются доверенными для компонентов защиты, например, для задачи *Поиск вредоносного ПО*. При этом, если в правиле Контроля приложений указать сертификат из другого хранилища, Kaspersky Endpoint Security не применит такое правило.

  Если флажок снят, Kaspersky Endpoint Security применяет правила к приложениям, подписанных сертификатом из хранилища доверенных корневых центров Windows (англ. Trusted Root Certificate Store). Такие приложения не входит в доверенную зону. Компоненты защиты контролируют активность таких приложений.

- **Шаблоны сообщений о блокировке приложений**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения.
- **Шаблон сообщения, появляющегося при блокировке запуска приложения**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.

8. Сохраните внесенные изменения.

В результате Контроль приложений будет блокировать запрещенные приложения. Также Kaspersky Endpoint Security формирует события *Запуск приложения запрещен*. На основании этих событий вы можете сформировать в консоли Kaspersky Security Center отчет – *Отчет о запрещенных приложениях*. В сводной информации отчета вы можете просмотреть список приложений и компьютеров, на которых сработало правило Контроля приложений.

Контроль приложений на основе эталонного компьютера

Вы можете использовать эталонный компьютер для создания образа с набором необходимых приложений. Далее вы можете использовать образ для развертывания операционной системы и приложений на других компьютерах. Поддерживать образ в актуальном состоянии не всегда возможно. Контроль приложений позволяет поддерживать список разрешенных приложений на основе эталонного компьютера. Контроль приложений автоматически определяет набор установленных приложений на эталонном компьютере и обновляет категорию. Таким образом, компьютеры получают актуальный список разрешенных приложений.

Настройка Контроля приложений на основе эталонного компьютера состоит из следующих этапов:

1. Создание автоматически пополняемой категории. При создании новой категории вам нужно выбрать тип **Категория, в которую входят исполняемые файлы из указанной папки** и выбрать эталонный компьютер.
2. Выбор режима Контроля приложений. Вам нужно запретить запуск всех приложений кроме разрешенных. Для этого выберите режим *Запрещенные приложения*.
3. Создание правила Контроля приложений. В параметрах правила нужно выбрать категорию, в которую входят исполняемые файлы с эталонного компьютера.

Как создать автоматически пополняемую категорию в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно** → **Управление**

приложениями → Категории приложений.

3. В рабочей области нажмите на кнопку **Новая категория**.

   Запустится мастер создания категории приложений.

4. Следуйте указаниям мастера создания категории приложений.

Шаг 1. Выбор типа категории

Выберите тип категории **Категория, в которую входят исполняемые файлы с выбранных устройств**.

Шаг 2. Ввод названия пользовательской категории

На этом шаге укажите название категории приложений.

Шаг 3. Параметры

> Этот шаг доступен, если вы выбрали тип категории **Категория, в которую входят исполняемые файлы с выбранных устройств**.

На этом шаге нажмите на кнопку **Добавить** и укажите компьютеры, исполняемые файлы с которых Kaspersky Security Center добавит в категорию приложений. Kaspersky Security Center добавит в категорию приложений все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

Также на этом шаге вы можете настроить следующие параметры:

- Алгоритм вычисления хеш-функции. Для выбора алгоритма необходимо установить хотя бы один из следующих флажков:
  - **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**.
  - **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**.
- Флажок **Синхронизировать данные с хранилищем Сервера администрирования**. Установите этот флажок, если вы хотите, чтобы Kaspersky Security Center периодически очищал категорию приложений и добавлял в нее все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

  Если флажок **Синхронизировать данные с хранилищем Сервера администрирования** снят, то после создания категории приложений Kaspersky Security Center не будет вносить в нее изменения.

Шаг 4. Фильтр

На этом шаге настройте фильтр для файлов.

Вы можете указать тип файла, который используется для создания категории приложений.

- **Все файлы**. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.
- **Только файлы вне категорий приложений**. Для создаваемой категории учитываются только файлы вне категорий приложений.

Вы можете указать папки выбранных компьютеров, содержащие файлы, которые используются для создания категории приложений.

- **Все папки**. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

- **Указанная папка**. Для создаваемой категории учитывается только указанная папка. Если вы выбрали этот параметр, вам нужно указать путь к папке.

Шаг 5. Создание пользовательской категории

Завершите работу мастера.

При создании автоматически пополняемой категории может быть удобно разделить файлы на несколько категорий. Например, файлы операционной системы и файлы из папки Program Files. Для этого вы можете использовать фильтр в параметрах категории и выбрать отдельные папки.

Как настроить Контроль приложений на основе эталонного компьютера в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Контроль безопасности** → **Контроль приложений**.
5. Установите флажок **Контроль приложений**.
6. В блоке **Настройки Контроля приложений** в раскрывающемся списке **Режим контроля** выберите вариант **Список запрещенных**.
7. В раскрывающемся списке **Действие** выберите действие Контроля приложения:
   - **Тестировать правила**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.
   - **Применять правила**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.
8. В списке правил Контроля приложений нажмите на кнопку **Добавить**.

   Запустится мастер добавления правила Контроля приложений.
9. В раскрывающемся списке **Категория** выберите автоматически пополняемую категорию на основе эталонного компьютера.
10. Выберите пользователей или группы пользователей, к которым вы хотите применить правило Контроля приложений.
11. Настройте дополнительные параметры правила Контроля приложений:
    - **Запретить остальным пользователям**. Приложение запрещает запуск приложений, принадлежащих к выбранной категории, всем пользователям, которые не указаны в списке.
    - **Доверенные приложения обновления**. Приложения, входящие в выбранную категорию, Kaspersky Endpoint Security считает доверенными приложениями обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.
12. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки  .
13. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку  .
14. В окне параметров приложения в блоке **Контроль безопасности** → **Контроль приложений**.
15. Включите переключатель **Контроль приложений**.
16. В блоке **Режим контроля запуска приложений** выберите вариант **Список запрещенных. Разрешены все приложения, кроме указанных в списке**.

17. В блоке **Действие при запуске приложений, запрещенных правилами** выберите действие Контроля приложения:
    - **Информировать (тестовый режим) и записывать в отчет**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.
    - **Блокировать**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.
18. В списке правил Контроля приложений нажмите на кнопку **Добавить**.

    Запустится мастер добавления правила Контроля приложений.
19. В блоке **Категория** выберите автоматически пополняемую категорию на основе эталонного компьютера.
20. Выберите пользователей или группы пользователей, к которым вы хотите применить правило Контроля приложений.
21. Настройте дополнительные параметры правила Контроля приложений:
    - **Запретить остальным пользователям**. Приложение запрещает запуск приложений, принадлежащих к выбранной категории, всем пользователям, которые не указаны в списке.
    - **Доверенные приложения обновления**. Приложения, входящие в выбранную категорию, Kaspersky Endpoint Security считает доверенными приложениями обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.
22. Сохраните внесенные изменения.

Действия с правилами Контроля приложений в интерфейсе приложения

Kaspersky Endpoint Security контролирует запуск приложений пользователями с помощью правил. В правиле Контроля приложений содержатся условия срабатывания и действия компонента Контроль приложений при срабатывании правила (разрешение или запрещение пользователям запускать приложение).

Условия срабатывания правила

Условие срабатывания правила представляет собой соответствие "тип условия - критерий условия - значение условия". На основании условий срабатывания правила Kaspersky Endpoint Security применяет (или не применяет) правило к приложению.

В правилах используются следующие типы условий:

- *Включающие условия*. Kaspersky Endpoint Security применяет правило к приложению, если приложение соответствует хотя бы одному включающему условию.
- *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к приложению, если приложение соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

Условия срабатывания правила формируются с помощью критериев. Для формирования условий в Kaspersky Endpoint Security используются следующие критерии:

- путь к папке с исполняемым файлом приложения или путь к исполняемому файлу приложения;
- метаданные: название исполняемого файла приложения, версия исполняемого файла приложения, название приложения, версия приложения, производитель приложения;

- хеш исполняемого файла приложения;
- сертификат: издатель, субъект, отпечаток;
- принадлежность приложения к KL-категории;
- расположение исполняемого файла приложения на съемном диске.

Для каждого критерия, используемого в условии, нужно указать его значение. Если параметры запускаемого приложения соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль приложений выполняет действие, прописанное в правиле. Если параметры приложения соответствуют значениям критериев, указанных в исключающем условии, Контроль приложений не контролирует запуск приложения.

Если в качестве условия срабатывания правила вы выбрали сертификат, вам нужно убедиться, что этот сертификат добавлен в доверенное системное хранилище на компьютере, и проверить параметры использования доверенного системного хранилища в приложении (см. раздел "Работа с приложениями, подписанными доверенной цифровой подписью" на стр. 331).

Решения компонента Контроль приложений при срабатывании правила

При срабатывании правила Контроль приложений в соответствии с правилом разрешает или запрещает пользователям (группам пользователей) запускать приложения. Вы можете выбирать отдельных пользователей или группы пользователей, которым разрешен или запрещен запуск приложений, для которых срабатывает правило.

Если в правиле не указан ни один пользователь, которому разрешен запуск приложений, удовлетворяющих правилу, правило называется *запрещающим*.

Если в правиле не указан ни один пользователь, которому запрещен запуск приложений, удовлетворяющих правилу, правило называется *разрешающим*.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей назначено разрешающее правило Контроля приложений и для одного из пользователей этой группы назначено запрещающее правило Контроля приложений, то этому пользователю будет запрещен запуск приложения.

Статус работы правила

Правила Контроля приложений могут иметь один из следующих статусов работы:

- **Включено**. Статус означает, что правило используется во время работы компонента Контроль приложений.
- **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль приложений.
- **Тестовый режим**. Статус означает, что Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но заносит информацию о запуске этих приложений в отчет.

kaspersky

В этом разделе

Добавление правила Контроля приложений 203

Добавление условия срабатывания в правило Контроля приложений 204

Изменение статуса правила Контроля приложений 205

Добавление правила Контроля приложений

► *Чтобы добавить правило Контроля приложений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. Нажмите на кнопку **Запрещенные приложения** или **Разрешенные приложения**.

   Откроется список правил Контроля приложений.
4. Нажмите на кнопку **Добавить**.

   Откроется окно с параметрами правила Контроля приложений.
5. На закладке **Общие настройки** задайте основные параметры правила:
   a. В поле **Название правила** введите название правила.
   b. В поле **Описание** введите описание правила.
   c. В таблице **Пользователи и их права** нажмите на кнопку **Добавить**.

      Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489).

      По умолчанию действие правила распространяется на всех пользователей.

      > Если в таблице не указан ни один пользователь, правило не может быть сохранено.

   d. В таблице **Пользователи и их права** определите право пользователей на запуск приложений с помощью переключателя.
   e. Установите флажок **Запретить остальным пользователям**, если вы хотите, чтобы приложение запрещало запуск приложений, удовлетворяющих условиям срабатывания правила, всем пользователям, которые не указаны в таблице **Пользователи и их права** и не входят в группы пользователей, указанные в таблице **Пользователи и их права**.

Если флажок **Запретить остальным пользователям** снят, Kaspersky Endpoint Security не контролирует запуск приложений пользователями, которые не указаны в таблице **Пользователи и их права** и не входят в группы пользователей, указанные в таблице **Пользователи и их права**.

f. Установите флажок **Доверенные приложения обновления**, если вы хотите, чтобы приложения, удовлетворяющие условиям срабатывания правила, Kaspersky Endpoint Security считал доверенными приложения обновления. *Доверенные приложения обновления* – приложения с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

Если приложение соответствует условиям срабатывания нескольких правил, Kaspersky Endpoint Security устанавливает признак *Доверенные приложения обновления* при выполнении следующих требований:

- запуск приложения разрешен во всех правилах;
- хотя бы в одном правиле установлен флажок **Доверенные приложения обновления**.

6. На закладке **Условия: N** сформируйте (см. раздел "Добавление условия срабатывания в правило Контроля приложений" на стр. 204) или измените список включающих условий срабатывания правила.
7. На закладке **Исключения: N** сформируйте или измените список исключающих условий срабатывания правила.

При миграции параметров Kaspersky Endpoint Security осуществляется также миграция списка исполняемых файлов, созданных доверенными приложениями обновления.

8. Сохраните внесенные изменения.

Добавление условия срабатывания в правило Контроля приложений

► *Чтобы добавить новое условие срабатывания в правило Контроля приложений в интерфейсе приложения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. Нажмите на кнопку **Запрещенные приложения** или **Разрешенные приложения**.

Откроется список правил Контроля приложений.

4. Выберите правило, для которого вы хотите добавить условие срабатывания.

Откроются свойства правила Контроля приложений.

5. Перейдите на закладку **Условия: N** или **Исключения: N** и нажмите на кнопку **Добавить**.
6. Выберите условия срабатывания правила Контроля приложений:

- **Условия из свойств запускавшихся приложений**. Вы можете выбрать приложения, к которым будет применено правило Контроля приложений, из списка запущенных приложений. Kaspersky Endpoint Security также добавляет в этот список приложения, которые когда-либо были запущены на компьютере. Вам нужно выбрать критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к файлу или папке**.

- **Условия "KL-категория"**. *KL-категория* – сформированный специалистами "Лаборатории Касперского" список приложений, обладающих общими тематическими признаками. Например, KL-категория "Офисные приложения" включает в себя приложения из пакетов Microsoft Office, Adobe® Acrobat® и другие.
- **Условие вручную**. Вы можете выбрать файл приложения и выбрать одно из условий срабатывания правила: **Хеш файла**, **Сертификат**, **Метаданные** или **Путь к файлу или папке**.
- **Условие по носителю файла (съемный диск)**. Правило Контроля приложений применяется только к файлам, которые запускаются на съемном диске.
- **Условия из свойств файлов указанной папки**. Правило Контроля приложений применяется только к файлам, которые расположены в указанной папке. Вы также можете включить или исключить файлы из вложенных папок. Вам нужно выбрать критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к файлу или папке**.

7. Сохраните внесенные изменения.

При добавлении условий учитывайте следующие особенности работы Контроля приложений:

- Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски в метаданных: **Имя файла**, **Название программы**, **Поставщик**.
- Kaspersky Endpoint Security не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.
- Не рекомендуется использовать в качестве условий срабатывания правил только критерии **Издатель** и **Субъект сертификата**. Использование этих критериев является ненадежным.
- Если вы используете символьную ссылку в поле **Путь к файлу или папке**, рекомендуется развернуть символьную ссылку для корректной работы правила Контроля приложений. Для этого нажмите на кнопку **Развернуть символьную ссылку**.

Изменение статуса правила Контроля приложений

► *Чтобы изменить статус правила Контроля приложений в интерфейсе приложения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. Нажмите на кнопку **Запрещенные приложения** или **Разрешенные приложения**.

   Откроется список правил Контроля приложений.
4. В графе **Статус** откройте контекстное меню и выберите один из следующих пунктов:
   - **Включено**. Статус означает, что правило используется во время работы компонента Контроль приложений.
   - **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль приложений.
   - **Тестовый режим**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск приложений, на которые распространяется действие этого правила, но заносит информацию о запуске этих приложений в отчет.
5. Сохраните внесенные изменения.

kaspersky

Тестирование правил Контроля приложений

Чтобы убедиться, что правила Контроля приложений не блокируют приложения, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля приложений и проанализировать их работу. При включении тестирования правил Контроля приложений Kaspersky Endpoint Security не будет блокировать приложения, запуск которых запрещен Контролем приложений, но будет отправлять уведомления об их запуске на Сервер администрирования.

Для анализа работы правил Контроля приложений требуется изучить события по результатам работы компонента Контроль приложений, приходящие в Kaspersky Security Center. Если для всех приложений, которые необходимы для работы пользователю компьютера, отсутствуют события о запрете запуска в тестовом режиме, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами правил, создать дополнительные или удалить существующие правила.

По умолчанию Kaspersky Endpoint Security разрешает запуск всех приложений, кроме приложений, запрещенных правилами.

Мониторинг активности приложений

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Мониторинг активности приложений – это инструмент, предназначенный для просмотра информации об активности приложений на компьютере пользователя в режиме реального времени.

Для работы Мониторинга активности приложений вам нужно установить компоненты Контроль приложений и Предотвращение вторжений. Если эти компоненты не установлены, в главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) раздел Мониторинг активности приложений скрыт.

► *Чтобы запустить Мониторинг активности приложений,*

в главном окне приложения в разделе **Мониторинг** нажмите на плитку **Мониторинг активности приложений**.

В открывшемся окне информация об активности приложений на компьютере пользователя представлена на трех закладках:

- На закладке **Все приложения** отображается информация о всех приложениях, установленных на компьютере.
- На закладке **Работающие** отображается информация о потреблении ресурсов компьютера каждого из приложений в режиме реального времени. На этой закладке вы можете, а также перейти к настройке разрешений для отдельного приложения.
- На закладке **Запускаемые при старте** отображается список приложений, которые запускаются при старте операционной системы.

Если вы хотите скрыть данные об активности приложений на компьютере пользователя, вы можете ограничить доступ пользователя к инструменту Мониторинг активности приложений.

► *Как скрыть Мониторинг активности приложений в интерфейсе приложения через Консоль администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Интерфейс**.
4. Используйте флажок **Скрыть раздел Мониторинг активности приложений**, чтобы включить или выключить доступ к инструменту.
5. Сохраните внесенные изменения.

Правила формирования масок имен файлов или папок

Маска имени файла или папки – это представление имени папки или имени и расширения файла с использованием общих символов.

Для формирования маски имени файла или папки вы можете использовать следующие общие символы:

- Символ `*`, который заменяет любой набор символов, в том числе пустой. Например, маска `C:\*.txt` будет включать все пути к файлам с расширением `txt`, расположенным в папках и подпапках на диске (C:).
- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Изменение шаблонов сообщений Контроля приложений

Когда пользователь пытается запустить приложение, запрещенное правилом Контроля приложений, Kaspersky Endpoint Security выводит сообщение о блокировке запуска приложения. Специалисты "Лаборатории Касперского" составили шаблон сообщения пользователю, которое описывает причины блокировки приложения (см. рис. ниже). Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.

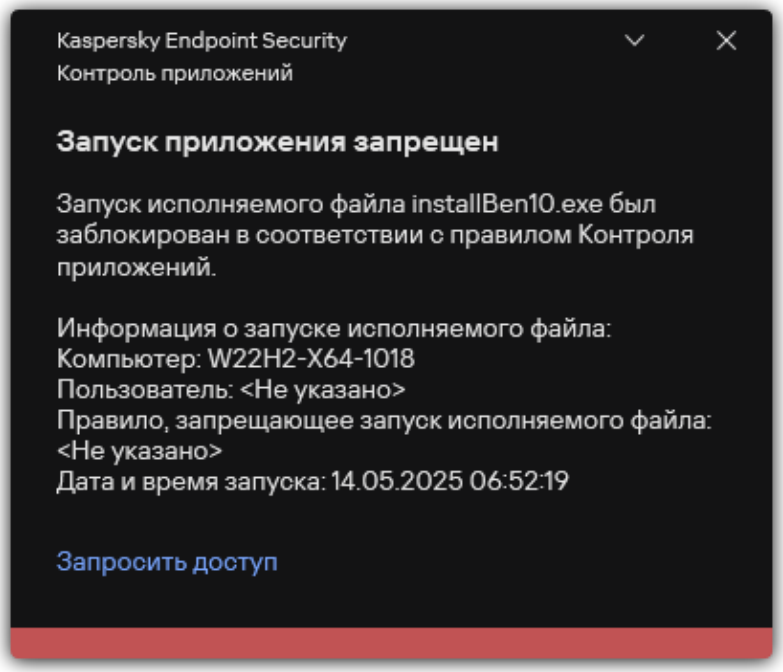


Рисунок 46. Уведомление Контроля программ

Если блокировка запуска приложения, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации. Для этого пользователю нужно нажать на кнопку **Запросить доступ** и отправить администратору сообщение с описанием ситуации. Вы также можете подготовить шаблон сообщения администратору и добавить в текст сообщения данные, которые могут быть вам нужны для принятия решения о разрешении доступа к приложению. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете запуска приложения**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

► *Как изменить шаблон сообщений Контроля приложения в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.

3. В блоке **Шаблоны сообщений о блокировке приложений** настройте шаблоны сообщений Контроля приложений:

   - **Сообщение о блокировке**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения.

     Настроить шаблоны сообщения для Контроля приложений в тестовом режиме (см. раздел "Тестирование правил Контроля приложений" на стр. 206) невозможно. Контроль приложений в тестовом режиме показывает предустановленные уведомления.

   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **Сбросить**.

4. Сохраните внесенные изменения.

См. также:

Изменение шаблонов сообщений Веб-Контроля 268

Изменение шаблонов сообщений Контроля устройств 237

Изменение шаблонов сообщений Адаптивного контроля аномалий 248

kaspersky

Контроль устройств

Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.

Если Контроль устройств включен, приложение передает в Kaspersky Security Center информацию о подключенных устройствах. Вы можете просмотреть список подключенных устройств в Kaspersky Security Center в папке **Дополнительно** → **Хранилища** → **Оборудование**.

Уровни доступа к устройствам

Контроль устройств управляет доступом на следующих уровнях:

- **Тип устройства**. Например, принтеры, съемные диски, CD/DVD-приводы.

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – ✓.
  - Запрещать – ⊘.
  - По правилам (только принтеры и портативные устройства) – .
  - Зависит от шины подключения (кроме Wi-Fi) – .
  - Запрещать с исключениями (только Wi-Fi) – .

- **Шина подключения**. *Шина подключения* – интерфейс, с помощью которого устройства подключаются к компьютеру (например, USB, FireWire). Если для типа устройств выбран режим **Зависит от шины подключения**, приложение разрешает или запрещает доступ к устройству в зависимости от интерфейса подключения (например, через USB).

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – ✓.
  - Запрещать – ⊘.

- **Доверенные устройства**. *Доверенные устройства* – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

  Вы можете добавить доверенные устройства по следующим данным:

  - **Устройства по идентификатору**. Каждое устройство имеет уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы. Пример идентификатора устройства: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств.
  - **Устройства по модели**. Каждое устройство имеет идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы. Шаблон для ввода VID и PID: `VID_1234&PID_5678`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.

- **Устройства по маске идентификатора**. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `WDC_C*`.
- **Устройства по маске модели**. Если вы используете несколько устройств с похожими VID или PID (например, устройства одного производителя), вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `VID_05AC&PID_*`.

Контроль устройств регулирует доступ пользователей к устройствам с помощью *правил доступа*. Также Контроль устройств позволяет сохранять события подключения / отключения устройств. Для сохранения событий вам нужно настроить отправку событий в политике.

Если доступ к устройству зависит от шины подключения (статус), Kaspersky Endpoint Security не сохраняет события подключения / отключения устройства. Чтобы приложение Kaspersky Endpoint Security сохраняла события подключения / отключения устройства, разрешите доступ к соответствующему типу устройств (статус) или добавьте устройство в список доверенных.

При подключении к компьютеру устройства, доступ к которому запрещен Контролем устройств, Kaspersky Endpoint Security заблокирует доступ и покажет уведомление (см. рис. ниже).

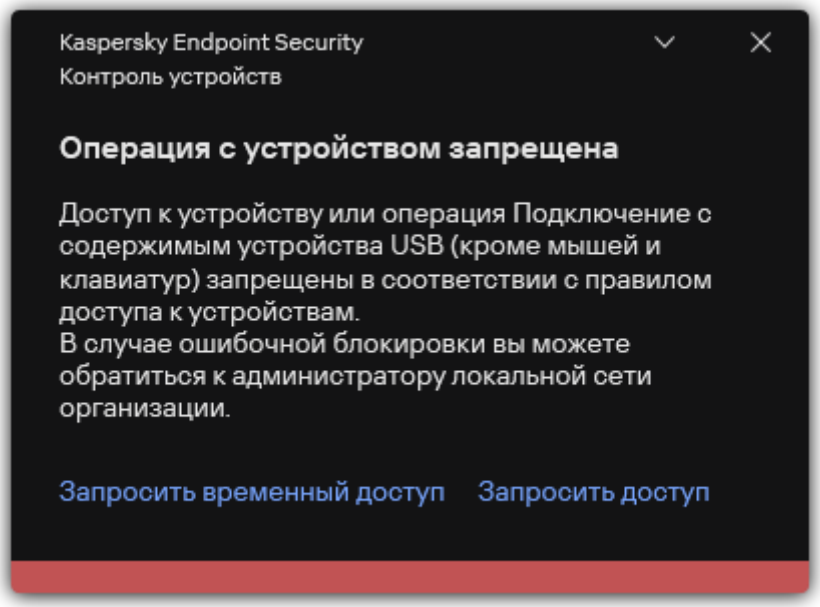


Рисунок 47. Уведомление Контроля устройств

Алгоритм работы Контроля устройств

Kaspersky Endpoint Security принимает решение о доступе к устройству после того, как пользователь подключил это устройство к компьютеру (см. рис. ниже).

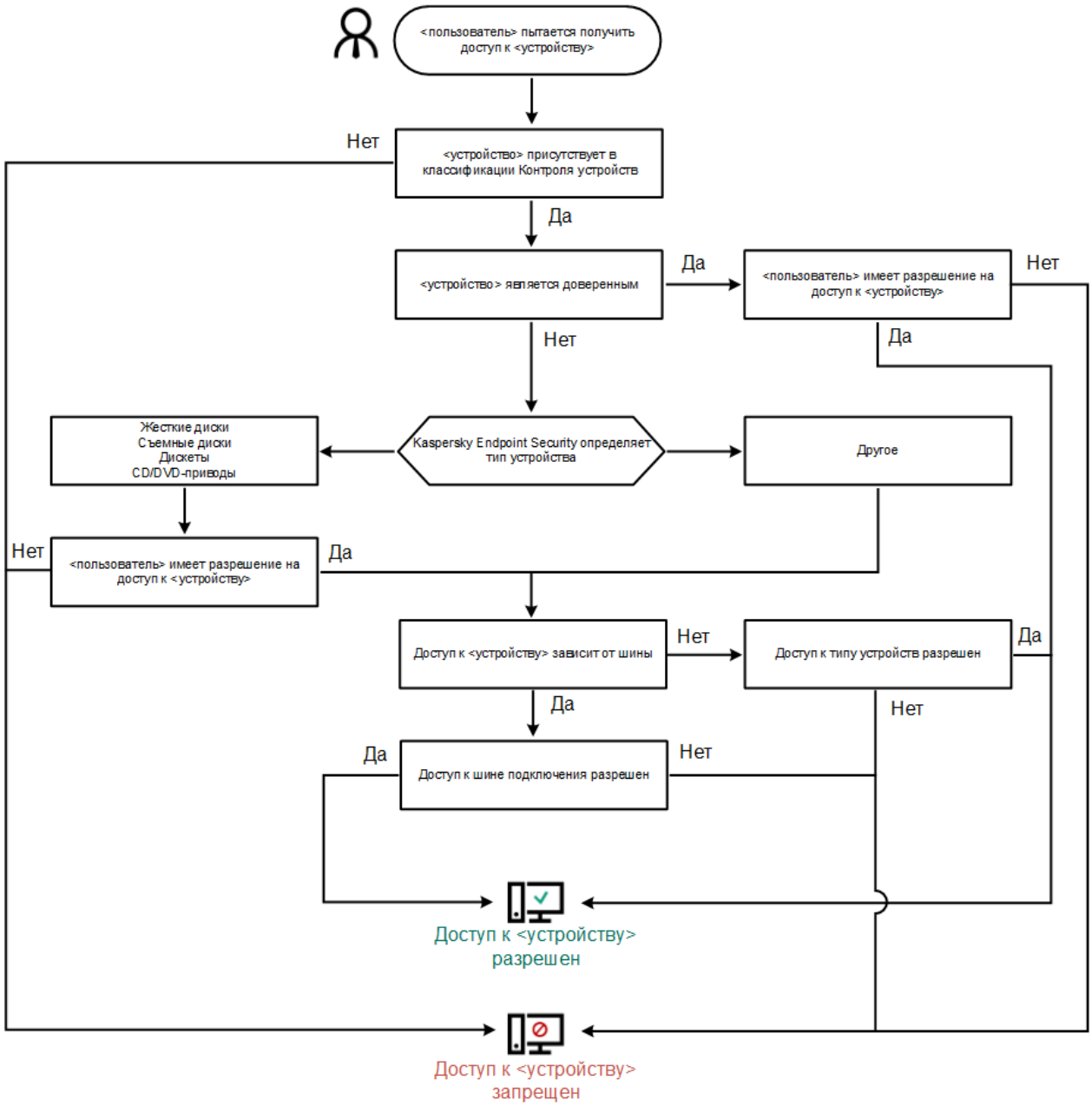


Рисунок 48. Алгоритм работы Контроля устройств

Если устройство подключено и доступ разрешен, вы можете изменить правило доступа и запретить доступ. В этом случае при очередном обращении к устройству (просмотр дерева папок, чтение, запись) Kaspersky Endpoint Security блокирует доступ. Блокирование устройства без файловой системы произойдет только при последующем подключении устройства.

Если пользователю компьютера с установленным приложением Kaspersky Endpoint Security требуется запросить доступ к устройству, которое, по его мнению, было заблокировано ошибочно, передайте ему инструкцию по запросу доступа (см. раздел "Получение доступа к заблокированному устройству" на стр. 232).

kaspersky

В этом разделе

Контроль доступа к устройствам по типу ... 213
О правилах доступа ... 214
Разграничение прав доступа пользователей к устройствам ... 215
Контроль доступа к устройствам по шине подключения ... 216
Контроль доступа к мобильным устройствам ... 217
Контроль доступа к Bluetooth-устройствам ... 221
Контроль печати ... 222
Контроль подключения к Wi-Fi ... 225
Мониторинг использования съемных дисков ... 229
Изменение периода кеширования ... 231
Добавление устройства в список доверенных из интерфейса приложения ... 232
Получение доступа к заблокированному устройству ... 232
Изменение шаблонов сообщений Контроля устройств ... 237
Анти-Бриджинг ... 239

Контроль доступа к устройствам по типу

Контроль устройств позволяет управлять доступом к устройствам по типу. Тип устройства определяет операционная система при подключении устройства. Вы можете узнать тип устройства с помощью встроенного в операционную систему инструмента Менеджер устройств. Для управления доступом к устройствам вам нужно настроить правила. *Правило доступа к устройствам* – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам: доступ к устройству, расписание доступа, разрешение на чтение или запись. Невозможно добавить устройство, которое выходит за рамки классификации Контроля устройств. Доступ к этим устройствам разрешен для всех пользователей.

По умолчанию Контроль устройств разрешает доступ ко всем устройствам для всех пользователей.

Вы можете настроить доступ к устройствам следующим образом:

- **Разрешать**.

  Kaspersky Endpoint Security предоставляет полный доступ к устройствам для всех пользователей.

- **Запрещать**.

  Kaspersky Endpoint Security блокирует подключение устройств. Приложение разрешает подключение только доверенных устройств.

- **Зависит от шины подключения**.

  Kaspersky Endpoint Security определяет интерфейс подключения устройства и ограничивает доступ к устройствам в соответствии со статусом подключения к шине. Также приложение разрешает подключение доверенных устройств.

- **По правилам**.

  Для некоторых типов устройств вы можете выбрать пользователей или группу пользователей, которым будет разрешено использование устройств, задать расписание для доступа к устройствам и настроить разрешения на чтение и запись. Также приложение разрешает подключение доверенных устройств.

Будьте осторожны при настройке доступа к типу устройств **Жесткие диски**. Если вы запретите доступ к системному диску, приложение может вызвать сбой при загрузке операционной системы (BSOD).

Если устройство выходит за рамки классификации Контроля устройств, ограничить доступ к таким устройствам невозможно.

В результате при попытке пользователя получить доступ к устройству приложение заблокирует доступ в соответствии с правилами. Также Kaspersky Endpoint Security зарегистрирует соответствующее событие. Если вы хотите предоставить доступ к отдельным устройствам, вы можете добавить эти устройства в список доверенных.

О правилах доступа

Правило доступа к устройствам – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам: доступ к устройству, расписание доступа, разрешение на чтение или запись. Невозможно добавить устройство, которое выходит за рамки классификации Контроля устройств. Доступ к этим устройствам разрешен для всех пользователей.

Правила доступа к устройствам

Набор параметров правила доступа отличается в зависимости от типа устройств (см. таблицу ниже).

Таблица 14. Параметры правила доступа

Устройства	Управление доступом	Расписание доступа к устройству	Назначение пользователей / группы пользователей	Приоритет	Разрешение на чтение / запись
Жесткие диски	✓	✓	✓	✓	✓
Съемные диски (включая USB-флешки)	✓	✓	✓	✓	✓
Дискеты	✓	✓	✓	✓	✓
CD/DVD-приводы	✓	✓	✓	✓	✓
Портативные устройства (MTP)	✓	✓	✓	✓	✓
Локальные принтеры	✓	–	✓	✓	–
Сетевые принтеры	✓	–	✓	✓	–
Модемы	✓	–	–	–	–

Устройства	Управление доступом	Расписание доступа к устройству	Назначение пользователей / группы пользователей	Приоритет	Разрешение на чтение / запись
Стримеры	✓	–	–	–	–
Многофункциональные устройства	✓	–	–	–	–
Устройства чтения смарт-карт	✓	–	–	–	–
Windows CE USB ActiveSync устройства	✓	–	–	–	–
Внешние сетевые адаптеры	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Камеры и сканеры	✓	–	–	–	–

Правило доступа к сетям Wi-Fi

Правило доступа к сетям Wi-Fi определяет разрешение (статус ✓) или запрет (статус ⊘) на использование сетей Wi-Fi. Вы можете добавить в правило *доверенную сеть Wi-Fi* (статус). Использование доверенной сети Wi-Fi разрешено без ограничений. По умолчанию правило доступа к сетям Wi-Fi разрешает доступ к любым сетям Wi-Fi.

Правила доступа к шинам подключения

Если для правила доступа по типу устройств выбрано значение **Зависит от шины подключения**, то приложение разрешает или запрещает доступ к устройству в зависимости интерфейса подключения. Для всех шин подключения из классификации компонента Контроль устройств по умолчанию созданы правила, разрешающие доступ к шинам.

Правила доступа к шинам определяют только разрешение (статус ✓) или запрет (статус ⊘) на подключение устройств. Приоритет правил доступа по типу устройств выше, чем приоритет правил доступа к шине.

Клавиатуры и мыши невозможно заблокировать средствами Контроля устройств. Если вы запретили доступ к шине подключения USB, пользователь продолжит работу с клавиатурой и мышью, подключенными через USB. Для предотвращения подключения к компьютеру зараженных USB-устройств, имитирующих клавиатуры, предназначен компонент Защита от атак BadUSB (на стр. 173).

kaspersky

Разграничение прав доступа пользователей к устройствам

Вы можете настроить права доступа пользователей по типу устройств или к доверенным устройствам.

Разграничение прав доступа пользователей по типу устройств

Контроль устройств позволяет настроить права доступа пользователей к данным на *запоминающих устройствах*. Для этих устройств вы можете настроить разрешения на запись и чтение. Контроль устройств поддерживает следующие типы *запоминающих устройств*:

- Жесткие диски.
- Съемные диски (включая USB-флешки).
- Дискеты.
- CD/DVD-приводы.
- Портативные устройства (MTP). К портативным устройствам (MTP) относятся, например, мобильные устройства, фотокамеры, медиаплееры и другие.

Таким образом, вы можете, например, разрешить использование съемных дисков только группе администраторов. Для других типов устройств вы можете или запретить, или разрешить доступ для всех пользователей. Также вы можете настроить права доступа пользователей при работе с принтерами (см. раздел "Контроль печати" на стр. 222).

Разграничение прав доступа пользователей к доверенным устройствам

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства. Для работы с доверенными устройствами вы можете предоставить доступ отдельному пользователю, группе пользователей или всем пользователям организации. Вы можете настроить права доступа пользователей в свойствах доверенного устройства.

Контроль доступа к устройствам по шине подключения

► *Чтобы изменить правило доступа к шине подключения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Шины подключения**.

   В открывшемся окне находятся правила доступа для всех шин подключения, которые есть в классификации компонента Контроль устройств.
4. Выберите правило доступа, которое хотите изменить.

5. В графе **Доступ** выберите доступ к шине подключения: **Разрешать** или **Запрещать**.

   Если вы изменили доступ к шине подключения **Последовательный порт** (COM) или **Параллельный порт** (LPT), для активации правила доступа вам нужно перезагрузить компьютер.

6. Сохраните внесенные изменения.

Контроль доступа к мобильным устройствам

Kaspersky Endpoint Security позволяет управлять доступом к данным на мобильных устройствах под управлением Android и iOS. Мобильные устройства относятся к портативным устройствам (MTP). Поэтому, чтобы настроить доступ к данным на мобильных устройствах вам нужно перейти в настройки доступа к портативным устройствам (MTP).

При подключении мобильного устройства к компьютеру операционная система определяет тип устройства. Если на компьютере установлены приложения Android Debug Bridge (ADB), iTunes или их аналоги, операционная система определяет мобильные устройства как ADB- или iTunes-устройства. В остальных случаях операционная система может определить тип мобильного устройства как портативное устройство (MTP) для передачи файлов, PTP-устройство (камера) для передачи изображений или другое устройство. Тип устройства зависит от модели мобильного устройства и выбранного режима подключения по USB. Kaspersky Endpoint Security позволяет настроить отдельные права доступа к данным на мобильных устройствах в приложениях ADB, iTunes или файловом менеджере. В остальных случаях Контроль устройств предоставляет доступ к мобильным устройствам согласно правилам доступа к портативным устройствам (MTP).

Доступ к мобильным устройствам

Так как мобильные устройства относятся к портативным устройствам (MTP), настройки доступа у этих устройств общие. Вы можете выбрать один из следующих режимов доступа к мобильным устройствам (см. раздел "Контроль доступа к устройствам по типу" на стр. 213):

- **Разрешать**. Kaspersky Endpoint Security предоставляет полный доступ к мобильным устройствам. Вы можете открывать, создавать, изменять, копировать или удалять файлы на мобильных устройствах с помощью файлового менеджера или приложений ADB и iTunes. Также вы можете заряжать батарею устройства, подключив мобильное устройств через USB к компьютеру.
- **Запрещать**. Kaspersky Endpoint Security ограничивает доступ к мобильным устройствам в файловом менеджере и приложениях ADB и iTunes. Приложение разрешает доступ только к доверенным мобильным устройствам. Также вы можете заряжать батарею устройства, подключив мобильное устройство через USB к компьютеру.
- **Зависит от шины подключения**. Kaspersky Endpoint Security ограничивает доступ к мобильным устройствам в соответствии со статусом подключения к шине USB (см. раздел "Контроль доступа к устройствам по шине подключения" на стр. 216) (**Разрешать** или **Запрещать**).
- **По правилам**. Kaspersky Endpoint Security ограничивает доступ к мобильным устройствам в соответствии с правилами. В правилах вы можете настроить права доступа (чтение / запись), выбрать пользователей или группу пользователей, которые имеют доступ к мобильным устройствам и задать расписание доступа к мобильным устройствам. Также вы можете ограничить доступ к данным на мобильных устройствах через приложения ADB и iTunes.

Настройка правил доступа к мобильным устройствам

Настройка правил доступа для портативных устройств (MTP), ADB- и iTunes-устройств отличается. Для портативных устройств (MTP) и ADB-устройств вы можете назначать правила для отдельных пользователей или групп пользователей и составлять расписание работы правил. Для iTunes-устройств таких возможностей нет. Вы можете только разрешить или запретить доступ к данным через приложение iTunes для всех пользователей.

► *Как настроить правила доступа к мобильным устройствам в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

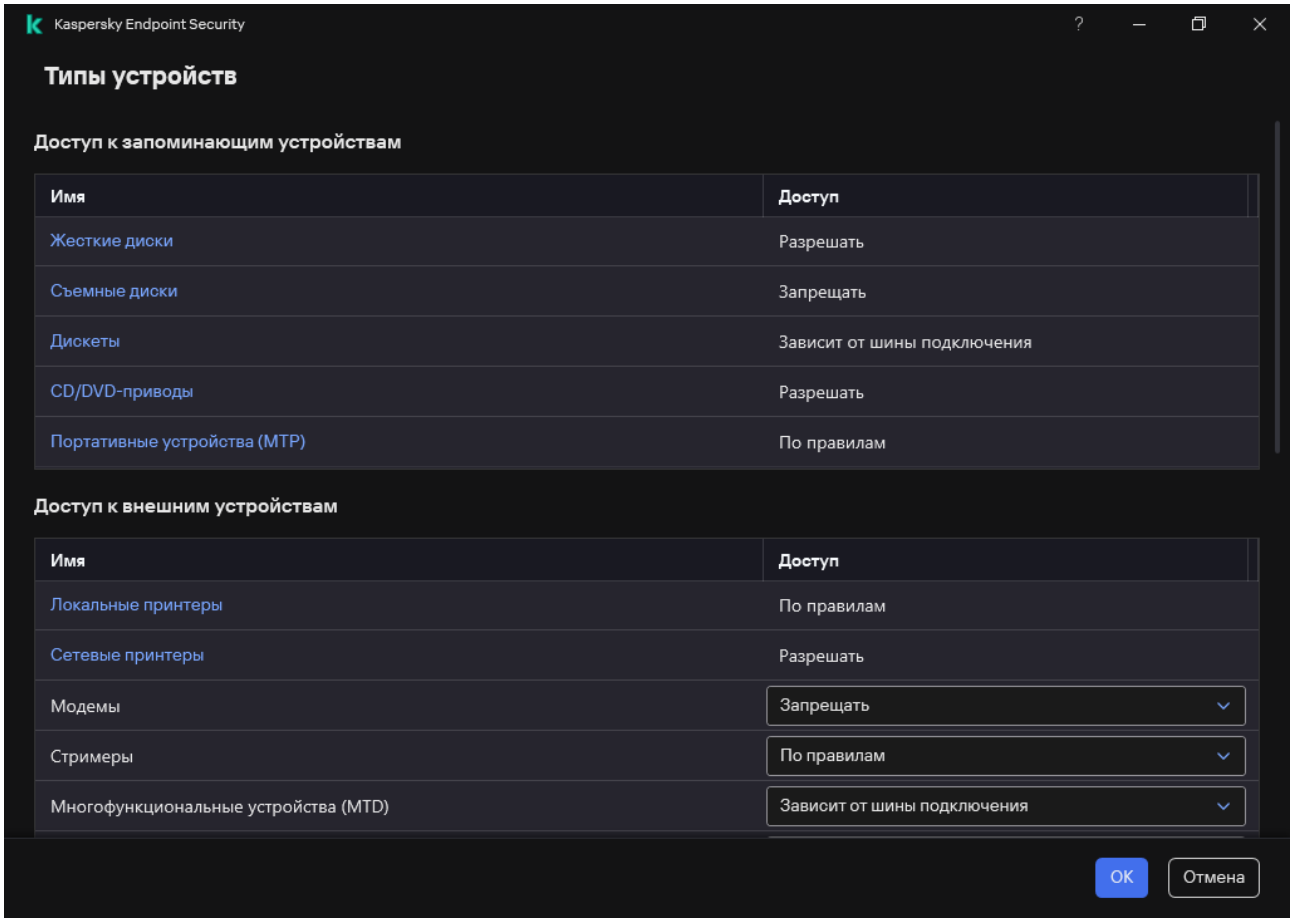


Рисунок 49. Типы устройств Контроля устройств

4. В блоке **Доступ к запоминающим устройствам** перейдите по ссылке **Портативные устройства (MTP)**.

   В открывшемся окне находятся правила доступа к портативным устройствам (MTP).

5. В блоке **Доступ** настройте режим доступа к мобильным устройствам: **Разрешать**, **Запрещать**, **Зависит от шины подключения** или **По правилам**.
6. Если вы выбрали режим **По правилам**, вам нужно добавить правила доступа к устройствам:
   a. В блоке **Права пользователей** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к мобильным устройствам.

   b. В поле **Приоритет** задайте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись / доступ через ADB) и приоритет.

      Запись правила имеет приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи, запрещающей доступ к устройству.

   c. В блоке **Состояние** включите правило доступа к мобильным устройствам.
   d. В блоке **Права доступа** настройте разрешения пользователей для доступа к мобильным устройствам.
      - Настройте разрешения пользователей для доступа к мобильным устройствам в файловом менеджере (**Чтение** / **Запись**).
      - Настройте доступ к данным мобильного устройства через приложение ADB с помощью флажка **Доступ через ADB**.

        Если флажок снят, при подключении мобильного устройства приложение ADB не сможет обнаружить устройство.
   e. В блоке **Пользователи** выберите пользователей или группы пользователей для доступа к мобильным устройствам. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489).
   f. В блоке **Расписание доступа к устройствам** настройте расписание доступа к устройствам для пользователей.

      Настроить отдельное расписание доступа к ADB-устройствам невозможно. Вы можете настроить общее расписание для ADB-устройств и портативных устройств (MTP).

g. В блоке **Доступ через iTunes** настройте доступ к данным мобильного устройства через приложение iTunes.

> Kaspersky Endpoint Security применяет настройки доступа к мобильным устройствам через приложение iTunes для всех пользователей. Настроить отдельное расписание доступа к iTunes-устройствам невозможно.

7. Сохраните внесенные изменения.

В результате пользователям будет ограничен доступ к мобильным устройствам согласно правилам. Если вы запретили доступ к мобильным устройствам в приложениях ADB и iTunes, при подключении мобильного устройства приложения ADB и iTunes не смогут обнаружить мобильное устройство.

Доверенные мобильные устройства

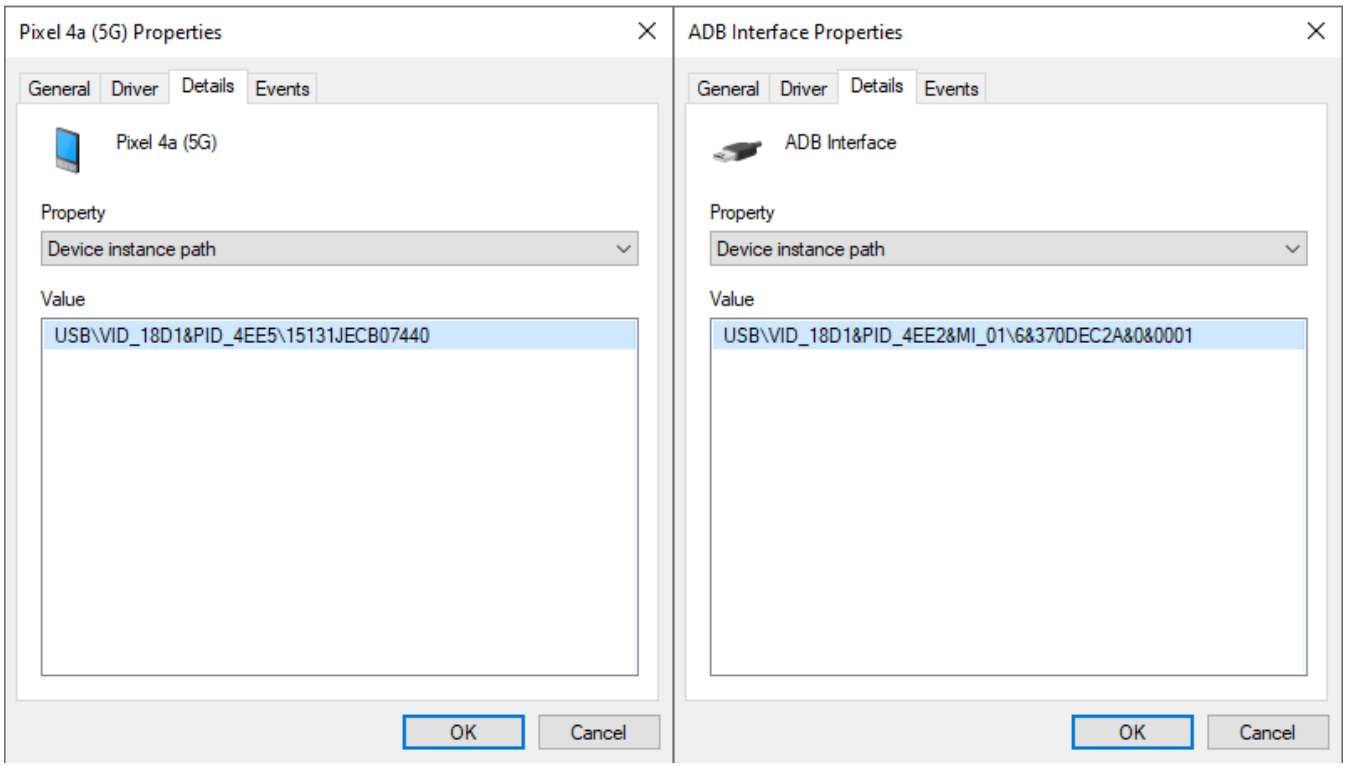
Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Добавление доверенного мобильного устройства ничем не отличается от добавления других типов доверенных устройств. Вы можете добавить мобильное устройство по идентификатору или модели устройства.

Для добавления доверенного мобильного устройства по идентификатору, вам понадобится уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы (см. рис. ниже). Для этого предназначен инструмент Диспетчер устройств (англ. Device Manager). Идентификаторы для портативных устройств (MTP) и ADB-, iTunes-устройств отличаются, даже если это одно мобильное устройство. Пример идентификатора портативного устройства (MTP): `15131JECB07440`. Пример идентификатора ADB-устройства: `6&370DEC2A&0&0001`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств. Также вы можете использовать маски.

> Если вы установили приложение ADB или iTunes после подключения устройства к компьютеру, уникальный идентификатор устройства может быть сброшен. То есть, Kaspersky Endpoint Security определит это устройство как новое. Если устройство доверенное, добавьте устройство в список доверенных повторно.

Для добавления доверенного мобильного устройства по модели, вам понадобятся идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы (см. рис. ниже). Шаблон для ввода VID и PID: `VID_18D1&PID_4EE5`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.



Контроль доступа к Bluetooth-устройствам

Kaspersky Endpoint Security позволяет управлять доступом к устройствам, подключенным по Bluetooth. К Bluetooth-устройствам относятся беспроводные клавиатуры, мыши, гарнитуры, принтеры и т.д. Также вы можете использовать Bluetooth для обмена данными, например, с мобильным устройством.

При подключении или отключении Bluetooth-устройств приложение может создавать несколько событий о действиях с устройством. Это связано с тем, что операционная система может определять Bluetooth-устройство как несколько устройств разных типов. Также Kaspersky Endpoint Security контролирует Bluetooth-адаптер, через который подключено устройство, как отдельное устройство. Поэтому приложение создает событие для всех обнаруженных устройств.

Вы можете выбрать один из следующих режимов доступа к Bluetooth-устройствам:

- **Разрешать и не записывать в отчет** . Kaspersky Endpoint Security позволяет подключать любые Bluetooth-устройства и не сохраняет информацию о подключении в журнал событий. Вы можете подключать устройства ввода по Bluetooth (клавиатуры, мыши и т.п.), передавать данные по Bluetooth, управлять другими устройствами по Bluetooth (гарнитура, наушники и т.п.).
- **Разрешать** . Kaspersky Endpoint Security позволяет подключать любые Bluetooth-устройства. Вы можете подключать устройства ввода по Bluetooth (клавиатуры, мыши и т.п.), передавать данные по Bluetooth, управлять другими устройствами по Bluetooth (гарнитура, наушники и т.п.).
- **Запрещать** . Kaspersky Endpoint Security ограничивает доступ к Bluetooth-устройствам. Вы можете разрешить подключение только устройств ввода по Bluetooth (класс HID-устройств – Human Interface Devices). К этим устройствам относятся клавиатуры, мыши, джойстики и т.п.

Сформировать список доверенных Bluetooth-устройств невозможно. Если вы ограничили доступ к Bluetooth-устройствам, вы можете разрешить подключение только устройств ввода по Bluetooth.

Вы можете разрешить подключение устройств ввода только в интерфейсе приложения или в Web Console. Разрешить подключение устройств ввода в Консоли администрирования (MMC) невозможно.

► *Как настроить правила доступа к Bluetooth-устройствам в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
4. В блоке **Доступ к внешним устройствам** перейдите по ссылке **Bluetooth**.

   Откроются настройки доступа к Bluetooth-устройствам.
5. В блоке **Доступ** настройте режим доступа к Bluetooth-устройствам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.
6. Если вы выбрали режим **Запрещать**, вы можете разрешить подключение только устройств ввода по Bluetooth (клавиатуры, мыши и т.п.). Для этого в блоке **Исключения** установите флажок **Устройства ввода (мыши и клавиатуры)**.
7. Сохраните внесенные изменения.

Контроль печати

С помощью Контроля печати вы можете настроить доступ пользователей к локальным и сетевым принтерам.

Контроль локальных принтеров

Kaspersky Endpoint Security позволяет настроить доступ к локальным принтерам на двух уровнях: *подключение* и *печать*.

Kaspersky Endpoint Security управляет подключением локальных принтеров по следующим шинам: USB, Последовательный порт (COM), Параллельный порт (LPT).

Kaspersky Endpoint Security контролирует подключение локальных принтеров через COM и LPT только на уровне шины. То есть, чтобы запретить подключение принтеров через COM и LPT вам нужно выбрать режим доступа к локальным принтерам Зависит от шины подключения (см. раздел "Контроль доступа к устройствам по типу" на стр. 213) и запретить подключение к шинам COM и LPT (см. раздел "Контроль доступа к устройствам по шине подключения" на стр. 216).

Принтеры, подключенные через USB, приложение контролирует на двух уровнях: тип устройств (локальные принтеры) и шина подключения (USB).

Вы можете выбрать один следующих режимов доступа к локальным принтерам через USB (см. раздел "Контроль доступа к устройствам по типу" на стр. 213):

- **Разрешать**. Kaspersky Endpoint Security предоставляет полный доступ к локальным принтерам для всех пользователей. Пользователи могут подключать принтеры и печатать документы средствами операционной системы.
- **Запрещать**. Kaspersky Endpoint Security блокирует подключение локальных принтеров. Приложение разрешает подключить только доверенные принтеры.
- **Зависит от шины подключения**. Kaspersky Endpoint Security ограничивает доступ к локальным принтерам в соответствии со статусом подключения к шине USB (см. раздел "Контроль доступа к устройствам по шине подключения" на стр. 216) (**Разрешать** или **Запрещать**).
- **По правилам**. Для контроля печати вам нужно добавить *правила печати*. В правилах вы можете выбрать пользователей или группу пользователей, которым будет разрешено или запрещено печатать документы на локальных принтерах.

Контроль сетевых принтеров

Kaspersky Endpoint Security позволяет настроить доступ к печати на сетевых принтерах. Вы можете выбрать один следующих режимов доступа к сетевым принтерам (см. раздел "Контроль доступа к устройствам по типу" на стр. 213):

- **Разрешать и не записывать в отчет**. Kaspersky Endpoint Security не контролирует печать на сетевых принтерах. Приложение предоставляет доступ к печати на сетевых принтерах для всех пользователей и не сохраняет информацию о печати в журнал событий.
- **Разрешать**. Kaspersky Endpoint Security предоставляет доступ к печати на сетевых принтерах для всех пользователей.
- **Запрещать**. Kaspersky Endpoint Security ограничивает доступ к печати на сетевых принтерах для всех пользователей. Приложение разрешает доступ только к доверенным принтерам.
- **По правилам**. Kaspersky Endpoint Security предоставляет доступ к печати для в соответствии с правилами печати. В правилах вы можете выбрать пользователей или группу пользователей, которым будет разрешено или запрещено печатать документы на сетевых принтерах.

Добавление правил печати для принтеров

► *Как добавить правила печати в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.

3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. В блоке **Доступ к внешним устройствам** перейдите по ссылке **Локальные принтеры** или **Сетевые принтеры**.

   В открывшемся окне находятся правила доступа к принтерам.

5. В блоке **Доступ к локальным принтерам** или **Доступ к сетевым принтерам** настройте режим доступа к принтерам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет** (только для сетевых принтеров), **Зависит от шины подключения** (только для локальных принтеров) или **По правилам**.

6. Если вы выбрали режим **По правилам**, вам нужно добавить правила печати для принтеров. Выберите пользователей или группы пользователей, к которым вы хотите применить правило печати:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила печати.

   b. Назначьте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, разрешения (разрешено / запрещено) и приоритет.

      Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи, запрещающей доступ к устройству.

   c. В блоке **Действие** настройте разрешения пользователей для доступа печати.

   d. В блоке **Пользователи и группы** выберите пользователей или группы пользователей для доступа к печати. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489).

7. Сохраните внесенные изменения.

Доверенные принтеры

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Добавление доверенных принтеров ничем не отличается от добавления других типов доверенных устройств. Локальные принтеры вы можете добавить по идентификатору или модели устройства. Сетевые принтеры вы можете добавить только по идентификатору устройства.

Для добавления доверенного локального принтера по идентификатору, вам понадобится уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы (см. рис. ниже). Для этого предназначен инструмент Диспетчер устройств (англ. Device Manager). Пример идентификатора локального принтера: `6&2D09F5AF&1&C000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств. Также вы можете использовать маски.

Для добавления доверенного локального принтера по модели, вам понадобятся идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы (см. рис. ниже). Шаблон для ввода VID и PID: `VID_04A9&PID_27FD`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.

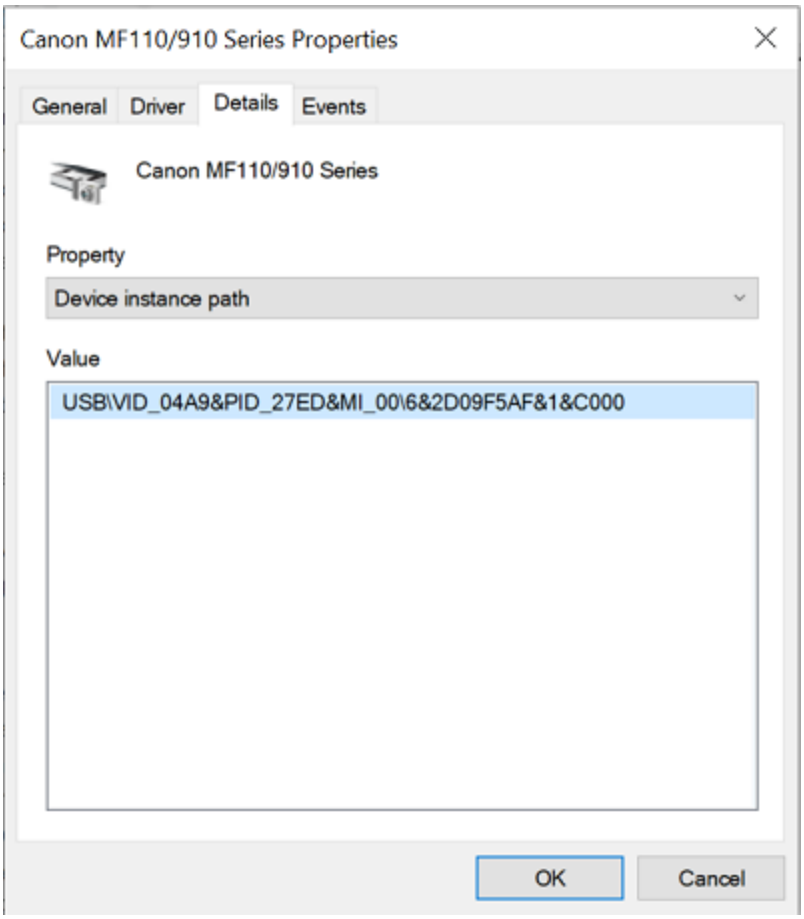


Рисунок 50. Идентификатор устройств в Диспетчере устройств

Для добавления доверенного сетевого принтера, вам понадобится идентификатор устройства. Для сетевых принтеров идентификатором может быть сетевое имя принтера (имя общего принтера), IP-адрес принтера или URL-адрес принтера.

kaspersky

Контроль подключения к Wi-Fi

Контроль устройств позволяет управлять подключением компьютера (ноутбука) к сетям Wi-Fi. Публичные сети Wi-Fi могут быть не защищены, и использование таких сетей может привести к потере данных. С помощью Контроля устройств вы можете запретить пользователю подключение к Wi-Fi или разрешить подключение только к доверенным сетям. Например, вы можете разрешить подключение только к корпоративной сети Wi-Fi, которая достаточно защищена. Контроль устройств будет блокировать доступ ко всем сетям Wi-Fi, кроме тех, которые указаны в списке доверенных.

На компьютерах под управлением Windows 11 для контроля подключения к Wi-Fi нужно включить службы определения местоположения. Для этого вам нужно включить переключатель **Службы определения местоположения** в параметрах операционной системы (**Настройки** → **Конфиденциальность и защита** → **Расположение**). Если службы определения местоположения выключены, Kaspersky Endpoint Security не контролирует подключение к сетям Wi-Fi.

► *Как ограничить подключение к Wi-Fi в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
4. В блоке **Доступ к сетям Wi-Fi** перейдите по ссылке **Wi-Fi**.

В открывшемся окне находятся правила доступа к сетям Wi-Fi.

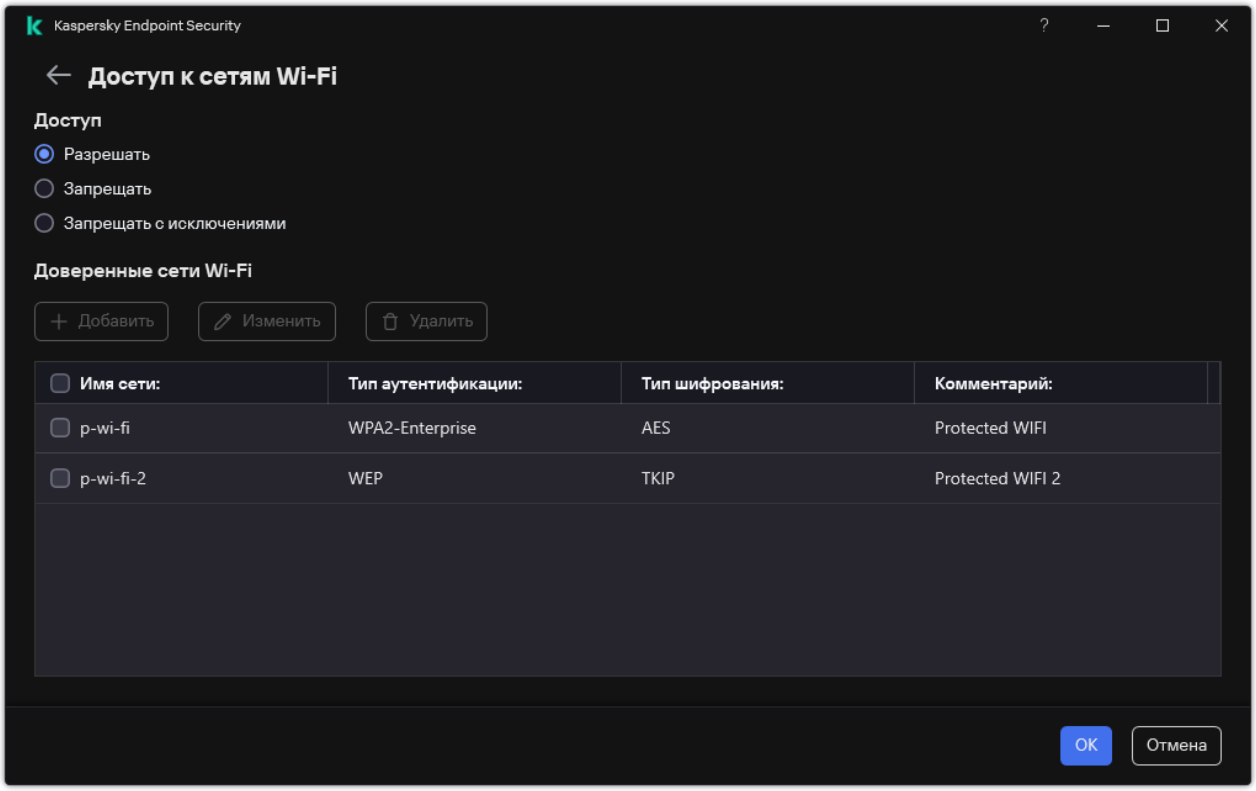


Рисунок 51. Настройки доступа к Wi-Fi

5. В блоке **Доступ** выберите действие Контроля устройств при подключения к Wi-Fi: **Разрешать**, **Запрещать** или **Запрещать с исключениями**.
6. Если вы выбрали вариант **Запрещать с исключениями**, сформируйте список доверенных сетей Wi-Fi:
   a. В блоке **Доверенные сети Wi-Fi** нажмите на кнопку **Добавить**.
   b. В открывшемся окне задайте параметры доверенной сети Wi-Fi (см. рис. ниже):
      - **Имя сети**. Имя сети Wi-Fi или SSID (Service Set Identifier).
      - **Тип аутентификации**. Тип аутентификации при подключении к сети Wi-Fi.

        Начиная с версии Kaspersky Endpoint Security для Windows 12.0 в приложение добавлена поддержка протокола WPA3. Если на компьютере применена политика Kaspersky Endpoint Security версии 12.2, на компьютерах с установленным приложением Kaspersky Endpoint Security версии 11.11.0 и более ранних версий будет выбран протокол WPA2, для версий 12.0 – 12.1 будет выбран протокол WPA2 / WPA3, для версии 12.2 и выше – WPA3.

      - **Тип шифрования**. Тип шифрования, используемый для защиты трафика сети Wi-Fi.
      - **Комментарий**. Дополнительная информация о добавленной сети Wi-Fi.

      Вы можете посмотреть параметры доверенной сети Wi-Fi в параметрах роутера.

Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.

7. Сохраните внесенные изменения.

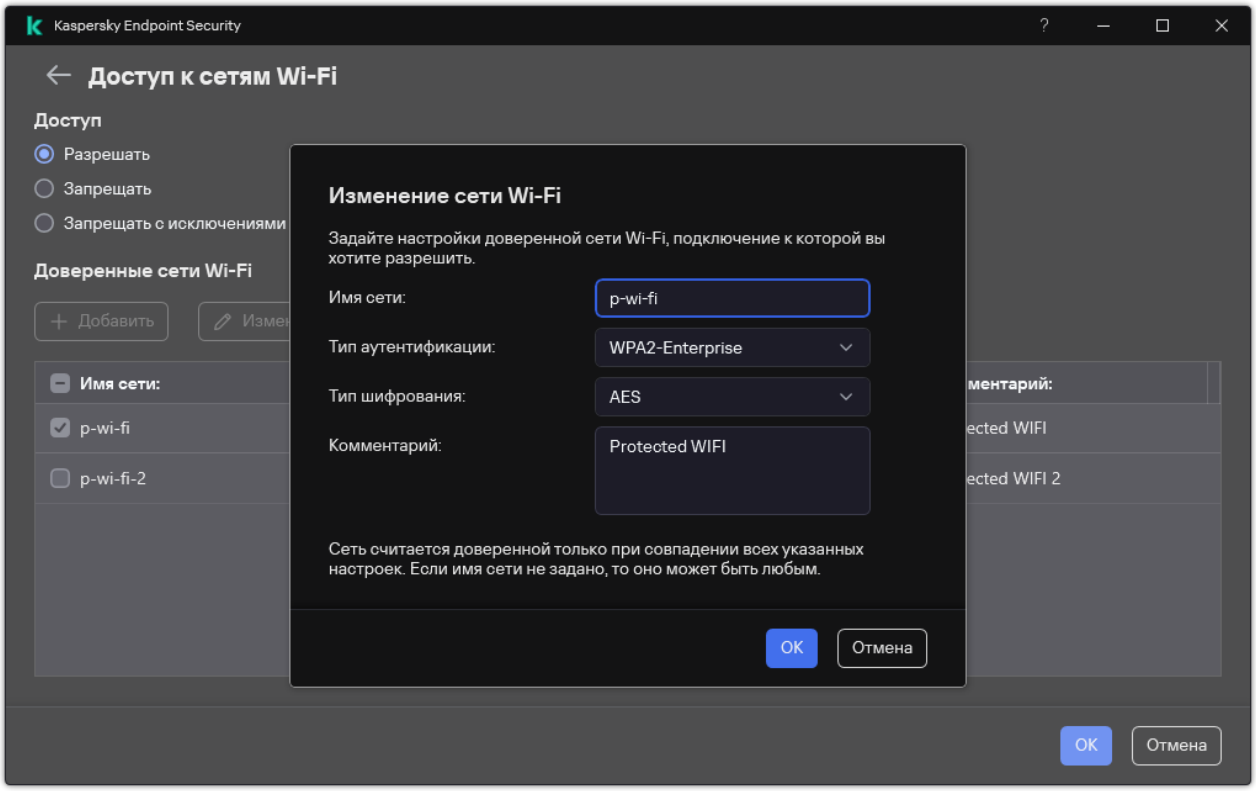


Рисунок 52. Параметры доверенной сети Wi-Fi

В результате при попытке пользователя подключиться к сети Wi-Fi, которая не указана в списке доверенных, приложение заблокирует подключение и покажет уведомление (см. рис. ниже).

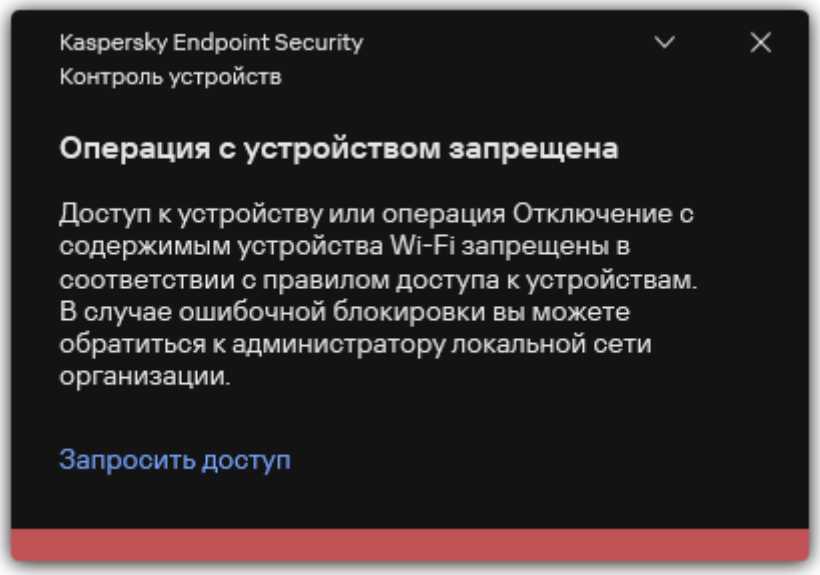


Рисунок 53. Уведомление Контроля устройств

Мониторинг использования съемных дисков

Мониторинг использования съемных дисков включает в себя следующие инструменты:

- Контроль операций с файлами на съемных дисках.
- Контроль подключения и отключения доверенных съемных дисков.

  Kaspersky Endpoint Security позволяет контролировать подключение и отключение всех доверенных устройств, не только съемных дисков. Вы можете включить запись событий в параметрах уведомлений (см. раздел "Настройка параметров журналов событий" на стр. 339) для компонента Контроль устройств. События имеют уровень важности *Информационное сообщение*.

► *Чтобы включить мониторинг использования съемных дисков, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
4. В блоке **Доступ к запоминающим устройствам** выберите элемент **Съемные диски**.

5. В открывшемся окне перейдите на закладку **Запись событий в журнал**.

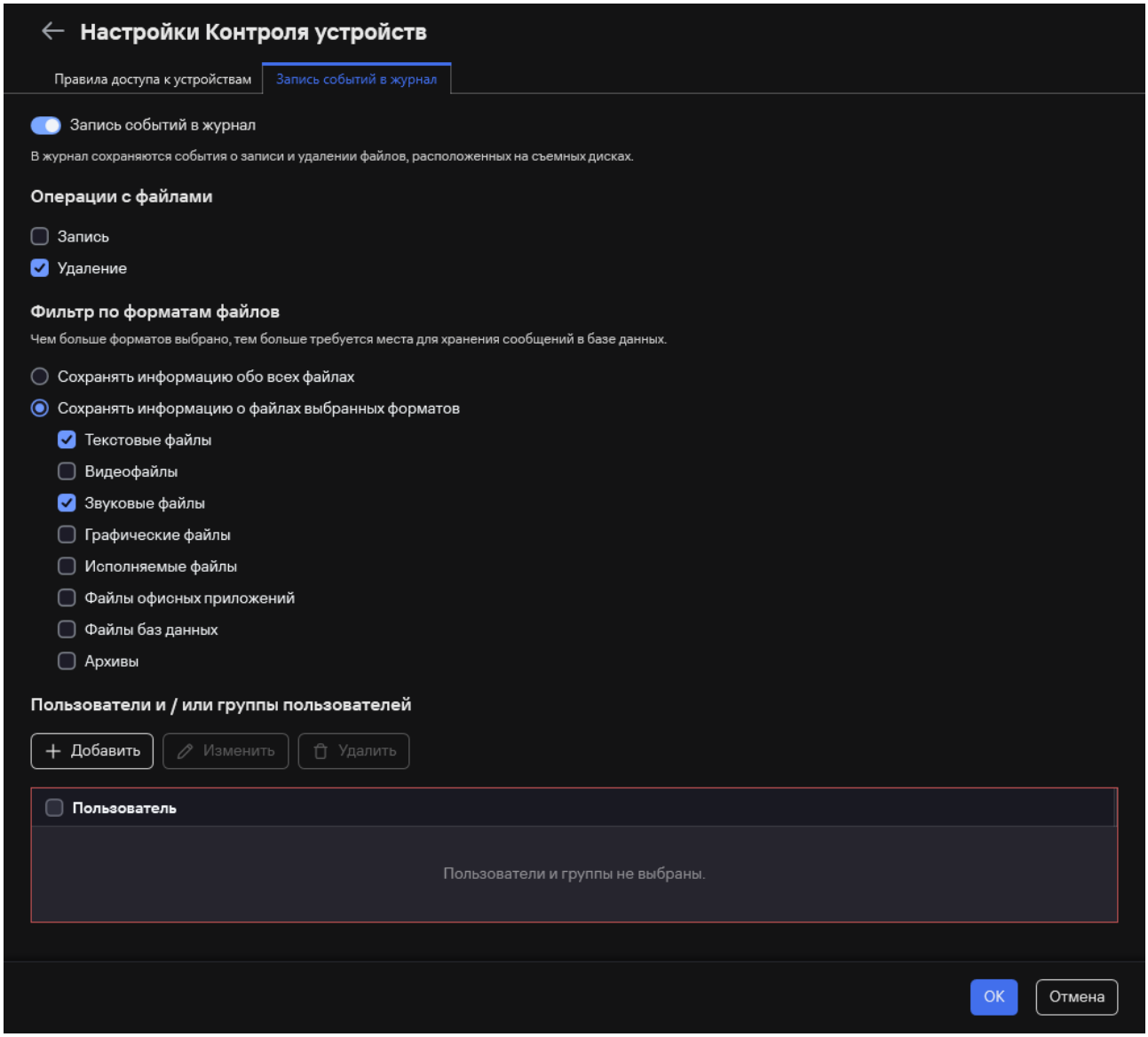


Рисунок 54. Параметры мониторинга использования съемных дисков

6. Включите переключатель **Запись событий в журнал**.
7. В блоке **Операции с файлами** выберите операции, которые вы хотите контролировать: **Запись**, **Удаление**.
8. В блоке **Фильтр по форматам файлов** выберите форматы файлов, информацию об операциях с которыми Контроль устройств должен записывать в журнал.
9. Выберите пользователей или группы пользователей, использование съемных дисков которых вы хотите контролировать.
10. Сохраните внесенные изменения.

В результате, когда пользователи будут производить запись в файлы, расположенные на съемных дисках, или удалять файлы со съемных дисков, Kaspersky Endpoint Security будет сохранять информацию о совершенной операции в журнал событий и отправлять события в Kaspersky Security Center. Вы можете просмотреть события, связанные с файлами на съемных дисках, в Консоли

администрирования Kaspersky Security Center в рабочей области для узла **Сервер администрирования** на закладке **События**. Чтобы события отображались в локальном журнале событий Kaspersky Endpoint Security, требуется установить флажок **Выполнена операция с файлом** в параметрах уведомлений (см. раздел "Настройка параметров журналов событий" на стр. 339) для компонента Контроль устройств.

Изменение периода кеширования

Компонент Контроль устройств регистрирует события, связанные с контролируемыми устройствами, такие как подключение и отключение устройства, чтение файла с устройства, запись файла на устройство и другие события. Далее Контроль устройств разрешает или запрещает выполнение действия в соответствии с параметрами Kaspersky Endpoint Security.

Контроль устройств хранит информацию о событиях в течение определенного времени, которое называется *периодом кеширования*. Кеширование информации о событии позволяет при повторении этого события не уведомлять Kaspersky Endpoint Security о нем и не запрашивать повторно доступ на выполнение соответствующего действия, например, подключение устройства. Это позволяет ускорить работу с устройством.

Событие считается повторяющимся, если все следующие параметры события совпадают с записью в кеше:

- идентификатор устройства;
- SID пользователя, от имени которого происходит обращение;
- класс устройства;
- действие с устройством;
- разрешение приложения для этого действия: разрешено или запрещено;
- путь к процессу, от имени которого совершается действие;
- файл, к которому происходит обращение.

Перед изменением периода кеширования выключите самозащиту Kaspersky Endpoint Security (см. раздел "Включение и выключение механизма самозащиты" на стр. 348). После изменения периода кеширования включите самозащиту.

► *Чтобы изменить период кеширования, выполните следующие действия:*

1. Откройте редактор реестра на компьютере.
2. В редакторе реестра перейдите в раздел:
   - для 64-битных операционных систем: `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`;
   - для 32-битных операционных систем: `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`.
3. Откройте параметр `DeviceControlEventsCachePeriod` на редактирование.
4. Укажите количество минут, по истечении которых информация о событии в Контроле устройств должна удаляться.

Добавление устройства в список доверенных из интерфейса приложения

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей "Все").

► *Чтобы добавить устройство в список доверенных из интерфейса приложения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Доверенные устройства**.

   Откроется список доверенных устройств.
4. Нажмите на кнопку **Выбрать**.

   Откроется список подключенных устройств. Список устройств зависит от того, какое значение выбрано в раскрывающемся списке **Отображать подключенные устройства**.
5. В списке устройств выберите устройство, которое вы хотите добавить в список доверенных.

   > Kaspersky Endpoint Security не поддерживает добавление устройств типа **Дискеты** в список доверенных.
6. В поле **Комментарий** вы можете указать любую информацию о доверенном устройстве.
7. Выберите пользователей или группы пользователей, для которых вы хотите разрешить доступ к доверенным устройствам.

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489).
8. Сохраните внесенные изменения.

Получение доступа к заблокированному устройству

При настройке Контроля устройств вы можете случайно запретить доступ к необходимому для работы устройству.

Если в вашей организации не развернуто решение Kaspersky Security Center, то вы можете предоставить доступ к устройству в параметрах Kaspersky Endpoint Security. Например, вы можете добавить устройство в список доверенных или временно выключить Контроль устройств (см. раздел "Контроль доступа к устройствам по типу" на стр. 213).

Если в вашей организации развернуто решение Kaspersky Security Center и к компьютерам применена политика, вы можете предоставить доступ к устройству в Консоли администрирования.

Онлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в онлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. Компьютер должен иметь возможность установить связь с Сервером администрирования.

Предоставление доступа в онлайн-режиме состоит из следующих этапов:

1. Пользователь отправляет администратору сообщение с запросом на предоставление доступа (см. раздел "Онлайн-режим предоставления доступа" на стр. 234).
2. Администратор получает сообщение с запросом в консоли Kaspersky Security Center.

   В консоли Kaspersky Security Center предустановлена выборка событий *Запросы пользователей* для удобного поиска сообщений от пользователей.
3. Администратор добавляет устройство в список доверенных.

   Вы можете добавить доверенное устройство в политике для группы администрирования или в локальных параметрах приложения для отдельного компьютера.
4. Администратор обновляет параметры Kaspersky Endpoint Security на компьютере пользователя.

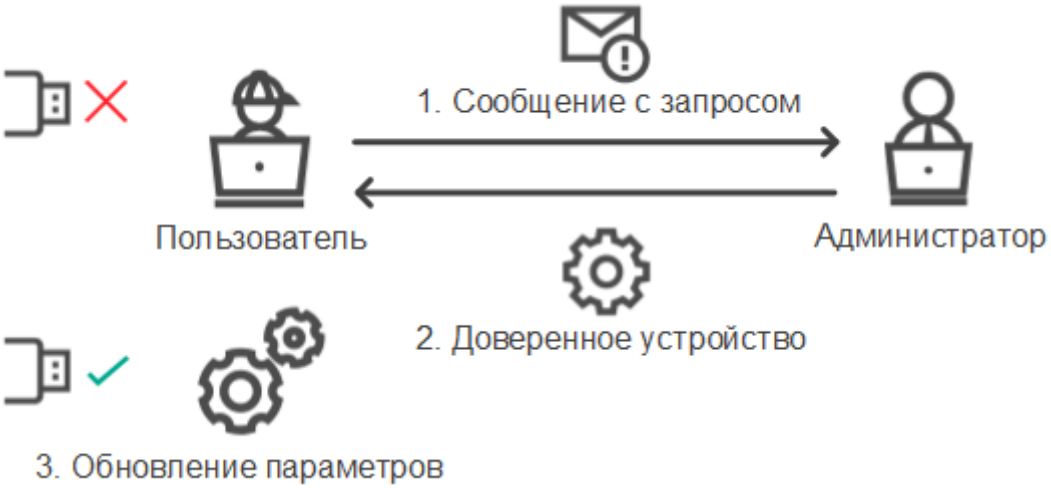


Рисунок 55. Схема предоставления доступа к устройству в онлайн-режиме

Офлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в офлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. В параметрах политики в разделе **Контроль устройств** должен быть установлен флажок **Разрешать запрашивать временный доступ**.

Если вам необходимо предоставить временный доступ к заблокированному устройству, а добавить устройство в список доверенных невозможно, вы можете предоставить доступ к устройству в офлайн-режиме. Таким образом, вы можете предоставить доступ к заблокированному устройству, если у компьютера отсутствует доступ к сети или компьютер находится за пределами сети организации.

Предоставление доступа в офлайн-режиме состоит из следующих этапов:

1. Пользователь создает файл запроса и передает его администратору.
2. Администратор создает из файла запроса ключ доступа и передает его пользователю.
3. Пользователь активирует ключ доступа.

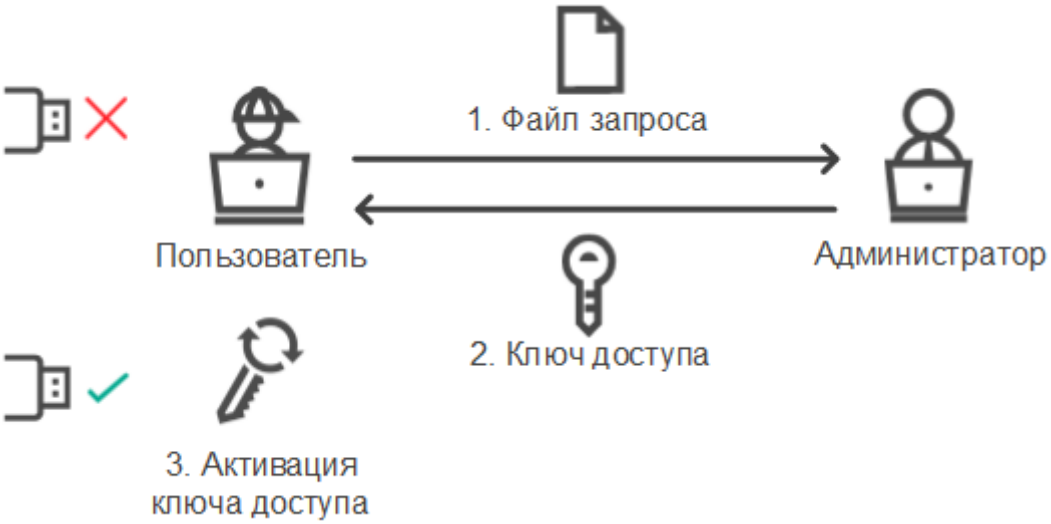


Рисунок 56. Схема предоставления доступа к устройству в офлайн-режиме

Онлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в онлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. Компьютер должен иметь возможность установить связь с Сервером администрирования.

► *Чтобы пользователю запросить доступ к заблокированному устройству, выполните следующие действия:*

1. Подключите устройство к компьютеру.

   Kaspersky Endpoint Security покажет уведомление блокировки доступа к устройству (см. рис. ниже).

2. Нажмите на ссылку **Запросить доступ**.

   Откроется окно с сообщением для администратора. В сообщении содержится информация о заблокированном устройстве.

3. Нажмите на кнопку **Отправить**.

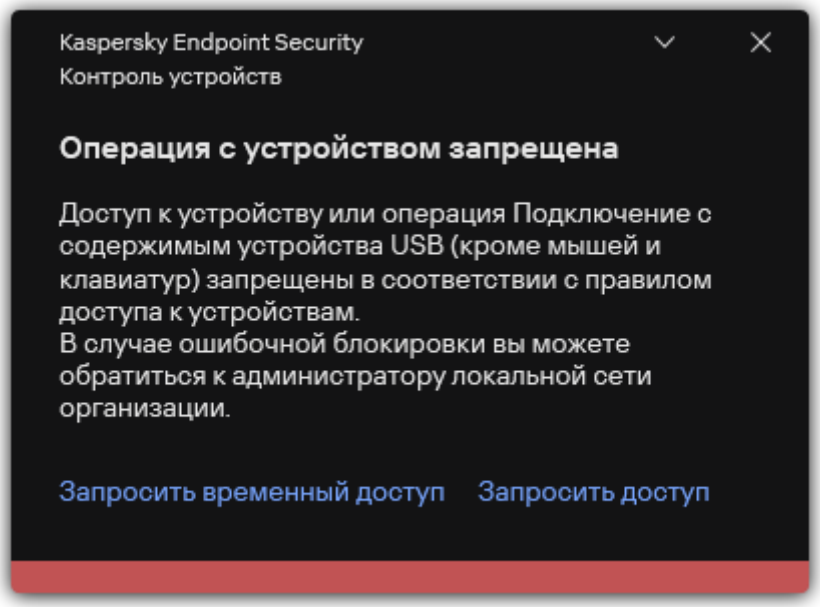


Рисунок 57. Уведомление Контроля устройств

Далее администратор в консоли Kaspersky Security Center получит событие *Сообщение администратору о запрете доступа к устройству*. Событие содержит имя пользователя, имя компьютера, данные об устройстве, к которому пользователь пытается получить доступ, и другие данные. Вы можете настроить способ уведомления администратора о получении таких событий и, например, выбрать уведомление по электронной почте. В консоли Kaspersky Security Center предустановлена выборка событий *Запросы пользователей* для удобного поиска сообщений от пользователей.

Для того, чтобы предоставить доступ вам нужно добавить устройство в список доверенных. После обновления параметров Kaspersky Endpoint Security на компьютере пользователь получит доступ к устройству.

Офлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в офлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. В параметрах политики в разделе **Контроль устройств** должен быть установлен флажок **Разрешать запрашивать временный доступ**.

► *Чтобы пользователю запросить доступ к заблокированному устройству, выполните следующие действия:*

1. Подключите устройство к компьютеру.

   Kaspersky Endpoint Security покажет уведомление блокировки доступа к устройству (см. рис. ниже).
2. Нажмите на ссылку **Запросить временный доступ**.

   Откроется окно со списком подключенных устройств.

3. В списке подключенных устройств выберите устройство, к которому вы хотите получить доступ.
4. Нажмите на кнопку **Сформировать файл запроса**.
5. В поле **Длительность доступа к устройству** укажите, на какое время вы хотите получить доступ к устройству.
6. Сохраните файл в память компьютера.

В результате в память компьютера будет загружен файл запроса с расширением *.akey. Передайте файл запроса доступа к устройству администратору локальной сети организации любым доступным способом.

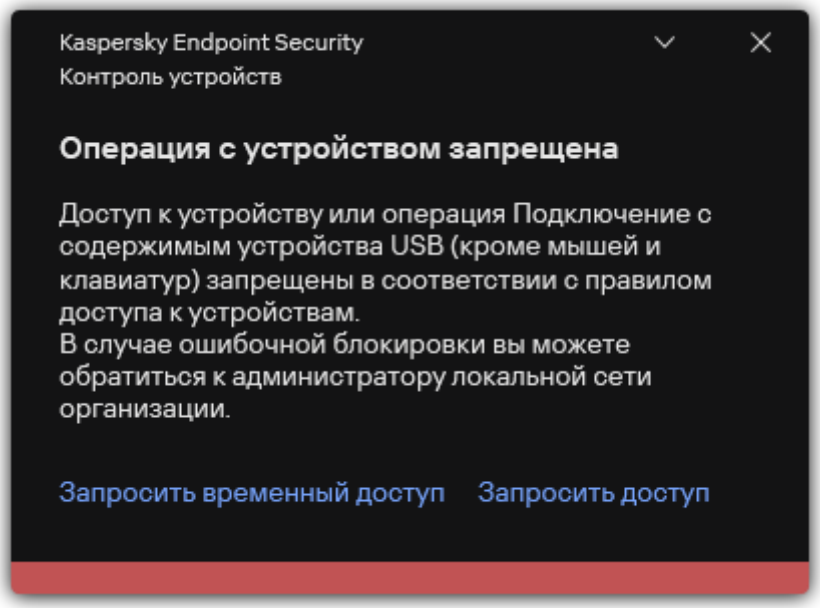


Рисунок 58. Уведомление Контроля устройств

Как администратору создать ключ доступа к заблокированному устройству в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, пользователю которого вы хотите дать временный доступ к заблокированному устройству.
5. В контекстном меню компьютера выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Контроль устройств**.
7. Нажмите на кнопку **Обзор** и загрузите полученный от пользователя файл запроса.

   Отобразится информация о заблокированном устройстве, к которому пользователь запросил доступ.
8. Если требуется, измените значение параметра **Длительность доступа к устройству**.

   По умолчанию для параметра **Длительность доступа к устройству** выбрано значение, указанное пользователем при формировании файла запроса.

9. Укажите значение параметра **Срок активации**.

   Параметр содержит период времени, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью предоставленного ключа доступа.

10. Сохраните файл ключа доступа в память компьютера.

В результате в память компьютера будет загружен ключ доступа к заблокированному устройству. Файл ключа доступа имеет расширение *.acode. Передайте ключ доступа к заблокированному устройству пользователю любым доступным способом.

► *Чтобы пользователю активировать ключ доступа, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Запрос доступа** нажмите на кнопку **Запросить доступ к устройству**.
4. В открывшемся окне нажмите на кнопку **Активировать ключ доступа**.
5. В открывшемся окне выберите файл с ключом доступа к устройству, полученный от администратора локальной сети организации.

   Откроется окно с информацией о предоставленном доступе.

6. Нажмите на кнопку **ОК**.

В результате пользователь получит доступ к устройству на срок, установленный администратором. Пользователь получит полный набор прав доступа к устройству (запись и чтение). По истечении срока действия ключа доступ к устройству будет заблокирован. Если пользователю требуется постоянный доступ к устройству, добавьте устройство в список доверенных.

Изменение шаблонов сообщений Контроля устройств

Когда пользователь пытается обратиться к заблокированному устройству, Kaspersky Endpoint Security выводит сообщение о блокировке доступа к устройству или о запрете операции над содержимым устройства. Специалисты "Лаборатории Касперского" составили шаблон сообщения пользователю, которое описывает причины блокировки доступа к устройству (см. рис. ниже).

Для работы с шаблонами сообщений предусмотрены специальные переменные (например, %USER_NAME%). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.

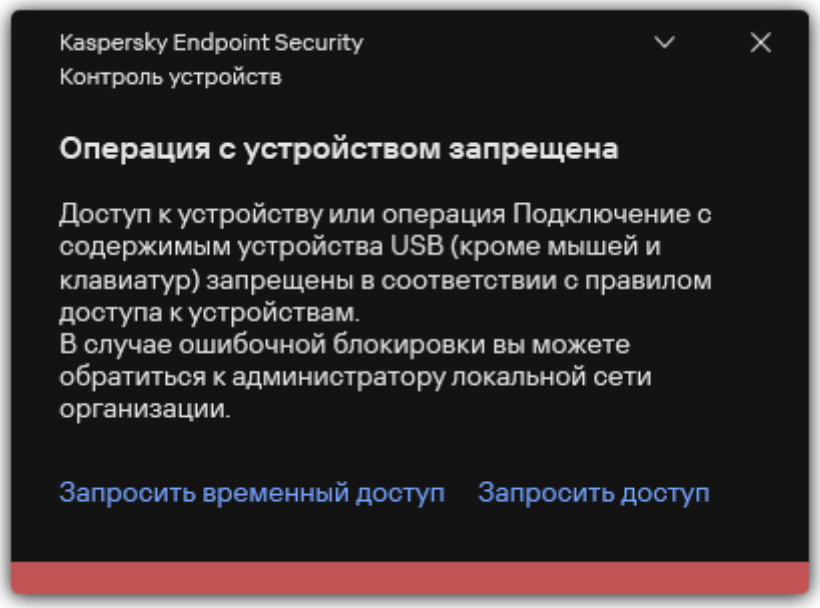


Рисунок 59. Уведомление Контроля устройств

Если блокировка доступа к устройству или запрет операции с содержимым устройства, по мнению пользователя, произошло ошибочно, пользователь может отправить сообщение администратору локальной сети организации по ссылке из текста сообщения о блокировке. Для этого пользователю нужно нажать на кнопку **Запросить доступ** или **Запросить временный доступ** и отправить администратору сообщение с описанием ситуации. Вы также можете подготовить шаблон сообщения администратору и добавить в текст сообщения данные, которые могут быть вам нужны для принятия решения о разрешении доступа к устройству. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете доступа к устройству**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

► *Как изменить шаблоны сообщений Контроля устройств в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. В блоке **Шаблоны сообщений** настройте шаблоны сообщений Контроля приложений:
   - **Сообщение о блокировке**. Шаблон сообщения, которое появляется при обращении пользователя к заблокированному устройству. Также сообщение появляется при попытке пользователя совершить операцию над содержимым устройства, которая запрещена для этого пользователя.

- **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к устройству или запрет операции над содержимым устройства, по мнению пользователя, произошли ошибочно.

Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

Также вы можете восстановить текст шаблона по умолчанию.

4. Сохраните внесенные изменения.

См. также:

Изменение шаблонов сообщений Веб-Контроля 268

Изменение шаблонов сообщений Контроля приложений 208

Изменение шаблонов сообщений Адаптивного контроля аномалий 248

Анти-Бриджинг

Анти-Бриджинг предотвращает создание сетевых мостов, исключая возможность одновременной установки нескольких сетевых соединений для компьютера. Это позволяет защитить корпоративную сеть от атак через незащищенные, несанкционированные сети.

Анти-Бриджинг регулирует установку сетевых соединений с помощью *правил установки соединений*.

Правила установки соединений созданы для следующих предустановленных типов устройств:

- сетевые адаптеры;
- адаптеры Wi-Fi;
- модемы.

Если правило установки соединений включено, то Kaspersky Endpoint Security выполняет следующие действия:

- блокирует активное соединение при установке нового соединения, если для обоих соединений используется указанный в правиле тип устройств;
- блокирует соединения, установленные или устанавливаемые с помощью тех типов устройств, для которых используются правила с более низким приоритетом.

В этом разделе

Включение Анти-Бриджинга 240

Изменение статуса правила установки соединений 240

Изменение приоритета правила установки соединений 240

Включение Анти-Бриджинга

По умолчанию функция Анти-Бриджинг выключена.

► *Чтобы включить функцию Анти-Бриджинг, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Анти-Бриджинг**.
4. Используйте переключатель **Включить Анти-Бриджинг**, чтобы включить или выключить функцию.
5. Сохраните внесенные изменения.

После включения функции Анти-Бриджинг Kaspersky Endpoint Security блокирует уже установленные соединения в соответствии с правилами установки соединений.

Изменение статуса правила установки соединений

► *Чтобы изменить статус правила установки соединений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Анти-Бриджинг**.
4. В блоке **Правила устройств** выберите правило, статус которого вы хотите изменить.
5. Используйте переключатели в графе **Контроль**, чтобы включить или выключить правило.
6. Сохраните внесенные изменения.

Изменение приоритета правила установки соединений

► *Чтобы изменить приоритет правила установки соединений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Анти-Бриджинг**.
4. В блоке **Правила устройств** выберите правило, приоритет которого вы хотите изменить.
5. Кнопками **Вверх** / **Вниз** установите приоритет правила установки соединений.

   Чем выше правило в таблице правил, тем выше у него приоритет. Функция Анти-Бриджинг блокирует все соединения, кроме одного соединения, установленного с помощью того типа устройств, для которого используется правило с наиболее высоким приоритетом.
6. Сохраните внесенные изменения.

kaspersky

Адаптивный контроль аномалий

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Компонент Адаптивный контроль аномалий отслеживает и блокирует действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило *Запуск Windows PowerShell из офисного приложения*). Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач. Kaspersky Endpoint Security обновляет набор правил с базами приложения. Обновление набора правил нужно подтверждать вручную (см. раздел "Применение обновлений для правил Адаптивного контроля аномалий" на стр. 248).

Настройка Адаптивного контроля аномалий

Настройка Адаптивного контроля аномалий состоит из следующих этапов:

1. Обучение Адаптивного контроля аномалий.

   После включения Адаптивного контроля аномалий правила работают в *обучающем режиме*. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты "Лаборатории Касперского". Обычно срок действия обучающего режима составляет 2 недели.

   Если в ходе обучения правило ни разу не сработало, Адаптивный контроль аномалий будет считать действия, связанные с этим правилом, нехарактерным. Kaspersky Endpoint Security будет блокировать все действия, связанные с этим правилом.

   Если в ходе обучения правило сработало, Kaspersky Endpoint Security регистрирует события в отчете о срабатываниях правил (см. раздел "Мониторинг работы Адаптивного контроля аномалий" на стр. 249) и в хранилище **Правила срабатываний в статусе Интеллектуальное обучение**.

2. Анализ отчета о срабатывании правил.

   Администратор анализирует отчет о срабатываниях правил (см. раздел "Мониторинг работы Адаптивного контроля аномалий" на стр. 249) или содержание хранилища **Правила срабатываний в статусе Интеллектуальное обучение**. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу приложения в обучающем режиме. Если администратор не предпринимает никаких мер, приложение также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени и осуществляется по следующим каналам:

- Адаптивный контроль аномалий автоматически начинает блокировать действия, связанные с правилами, которые не сработали в течение обучающего режима.

- Kaspersky Endpoint Security добавляет новые правила или удаляет неактуальные.
- Администратор настраивает работу Адаптивного контроля аномалий после анализа отчета о срабатывании правил и содержимого хранилища **Правила срабатываний в статусе Интеллектуальное обучение**. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища **Правила срабатываний в статусе Интеллектуальное обучение**.

При попытке вредоносного приложения выполнить действие, Kaspersky Endpoint Security заблокирует действие и покажет уведомление (см. рис. ниже).

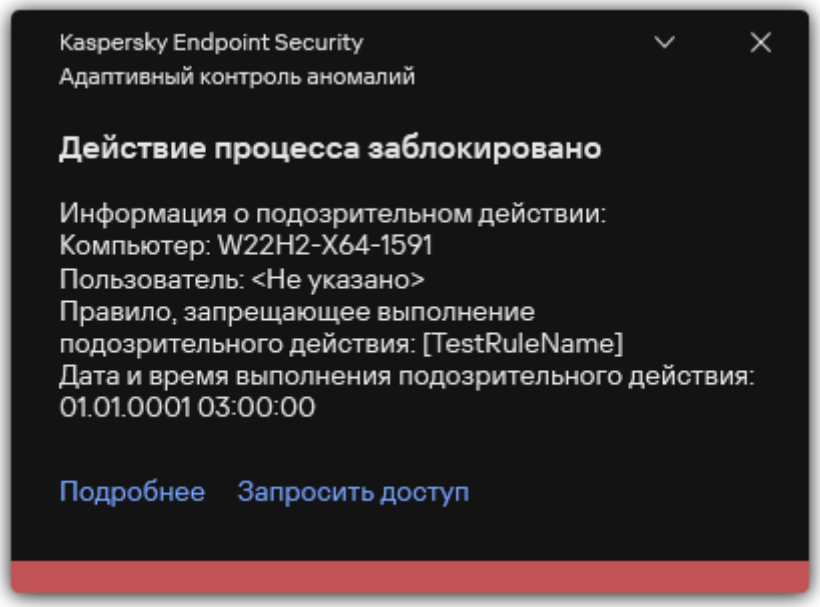


Рисунок 60. Уведомление Адаптивного контроля аномалий

Алгоритм работы Адаптивного контроля аномалий

Kaspersky Endpoint Security принимает решение о выполнении действия, связанного с правилом, по следующему алгоритму (см. рис. ниже).

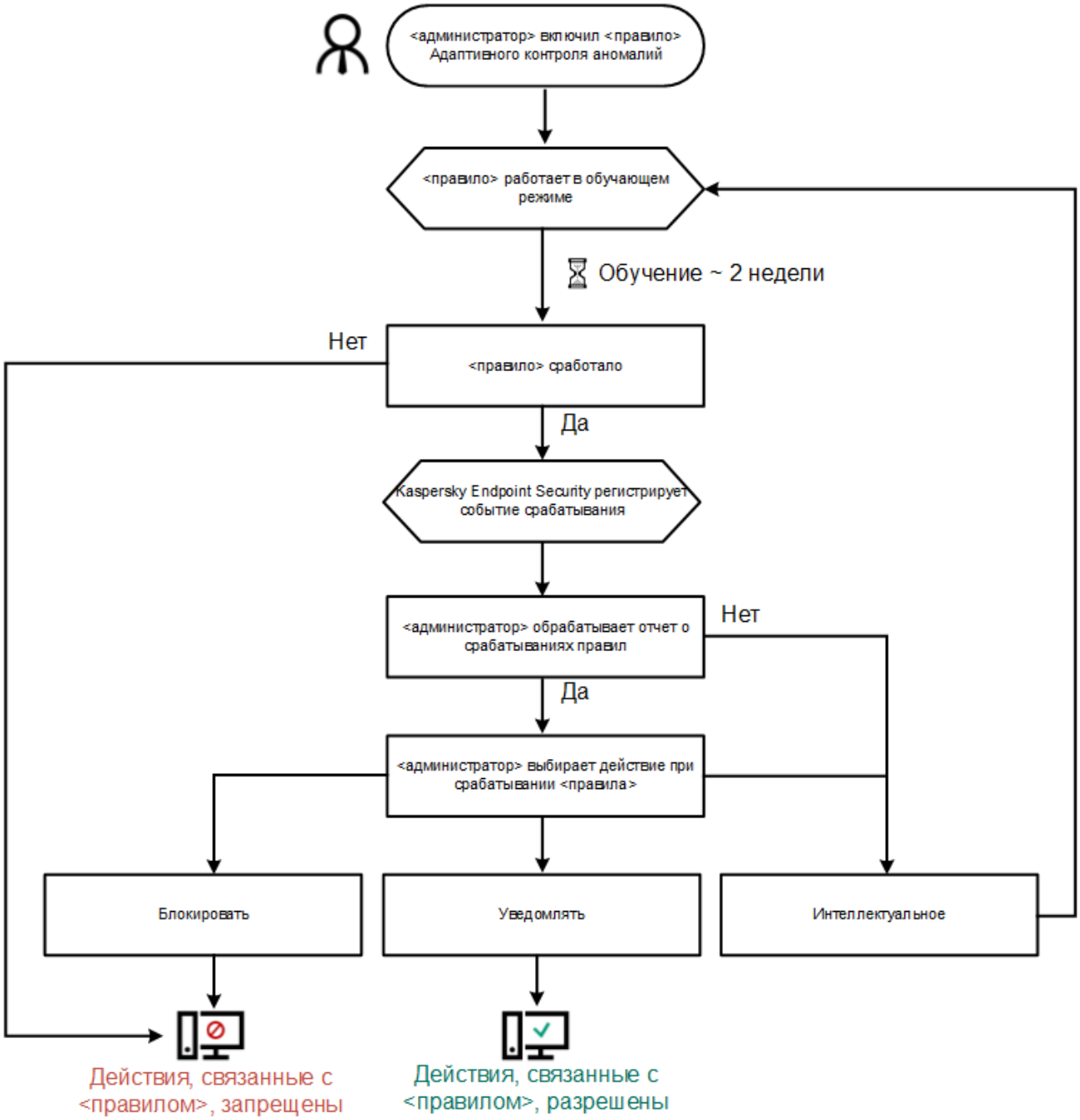


Рисунок 61. Алгоритм работы Адаптивного контроля аномалий

kaspersky

В этом разделе

Обучение Адаптивного контроля аномалий 244
Включение и выключение правила Адаптивного контроля аномалий 245
Изменение действия при срабатывании правила Адаптивного контроля аномалий 245
Создание исключения для правила Адаптивного контроля аномалий 246
Применение обновлений для правил Адаптивного контроля аномалий 248
Изменение шаблонов сообщений Адаптивного контроля аномалий 248
Мониторинг работы Адаптивного контроля аномалий 249

Обучение Адаптивного контроля аномалий

Адаптивный контроль аномалий включает в себя набор правил (шаблонов поведения). После включения Адаптивного контроля аномалий правила работают в *обучающем режиме*. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Адаптивный контроль аномалий не блокирует активность приложений на компьютере, а только информирует администратора. Вы также можете вручную выбрать действие при срабатывании правила Адаптивного контроля аномалий.

► *Как просмотреть список правил Адаптивного контроля аномалий в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. Включите переключатель **Адаптивный контроль аномалий**.
4. В блоке **Правила** перейдите по ссылке **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий. По умолчанию все правила работают в режиме **Интеллектуальное**.
5. Если требуется, подтвердите обновление правила Адаптивного контроля аномалий.
6. Если требуется, выберите действие при срабатывании правил Адаптивного контроля аномалий:
   - **Блокировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
   - **Информировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
7. Если требуется, выключите правила, которые вы не хотите использовать.
8. Сохраните внесенные изменения.

Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты «Лаборатории Касперского». Обычно срок действия обучающего режима составляет две недели.

Если в течение срока действия обучающего режима правило ни разу не сработало, то Адаптивный контроль аномалий считает такое поведение нетипичным и меняет статус правила на **Интеллектуальное блокирование**. Далее приложение будет блокировать активность, которая соответствует этому правилу.

Если в течение срока действия обучающего режима правило сработало, вам нужно вручную задать действие приложения при обнаружении активности, которая соответствует этому правилу. Если вы не выберите действие при срабатывании правила, Адаптивный контроль аномалий продолжит работать в режиме обучения.

Включение и выключение правила Адаптивного контроля аномалий

► *Чтобы включить или выключить правило Адаптивного контроля аномалий, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В таблице выберите набор правил (например, *Активность офисных приложений*) и разверните набор.
5. Выберите правило (например, *Запуск Windows PowerShell из офисного приложения*).
6. Используйте переключатель в графе **Состояние**, чтобы включить или выключить правило Адаптивного контроля аномалий.
7. Сохраните внесенные изменения.

Изменение действия при срабатывании правила Адаптивного контроля аномалий

► *Чтобы изменить действие при срабатывании правила Адаптивного контроля аномалий, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В таблице выберите правило.

5. Нажмите на кнопку **Изменить**.

   Откроется окно свойств правила Адаптивного контроля аномалий.

6. В блоке **Действие** выберите один из следующих пунктов:

   - **Интеллектуальное**. Если выбран этот вариант, то правило Адаптивного контроля аномалий работает в обучающем режиме в течение периода, определенного специалистами "Лаборатории Касперского". В этом режиме при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает запись в хранилище **Правила срабатываний в статусе Интеллектуальное обучение** Сервера администрирования Kaspersky Security Center. По истечении периода работы обучающего режима Kaspersky Endpoint Security блокирует активность, подпадающую под правило Адаптивного контроля аномалий, и создает в журнале запись, содержащую информацию об этой активности.
   - **Блокировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
   - **Информировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.

7. Сохраните внесенные изменения.

Создание исключения для правила Адаптивного контроля аномалий

Для правил Адаптивного контроля аномалий невозможно создать более 1000 исключений. Не рекомендуется создавать более 200 исключений. Чтобы уменьшить количество используемых исключений, рекомендуется использовать маски в параметрах исключений.

Исключение для правила Адаптивного контроля аномалий включает в себя описание исходных и целевых объектов. *Исходный объект* – объект, который выполняет действия. *Целевой объект* – объект, над которым выполняются действия. Например, вы открыли файл `file.xlsx`. В результате в память компьютера была добавлена библиотека с расширением dll, которую использует браузер (исполняемый файл `browser.exe`). В этом примере `file.xlsx` – исходный объект, Excel – исходный процесс, `browser.exe` – целевой объект, Browser – целевой процесс.

► *Чтобы создать исключение для правила Адаптивного контроля аномалий, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.

3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.

4. В таблице выберите правило.
5. Нажмите на кнопку **Изменить**.

   Откроется окно свойств правила Адаптивного контроля аномалий.

6. В блоке **Исключения** нажмите на кнопку **Добавить**.

   Откроется окно свойств исключения.

7. Выберите пользователя, для которого вы хотите настроить исключение.

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489).

   > Адаптивный контроль аномалий не поддерживает исключения для групп пользователей. Если вы выберите группу пользователей, Kaspersky Endpoint Security не применит исключение.

8. В поле **Описание** введите описание исключения.
9. Задайте параметры исходного объекта или исходного процесса, запущенных объектом:

   - **Исходный процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`).
   - **Хеш исходного процесса**. Хеш файла.
   - **Исходный объект**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`). Например, путь к файлу `document.docm`, который запускает целевые процессы с помощью скрипта или макроса.

     Вы также можете указать другие объекты для исключения, например, веб-адрес, макрос, команду в командной строке, путь реестра и другие. Укажите объект по следующему шаблону: `object://<object>`, где `<object>` – название объекта, например, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Вы также можете использовать маски, например, `object://*C:\Windows\temp\*`.
   - **Хеш исходного объекта**. Хеш файла.

   Правило Адаптивного контроля аномалий не распространяется на действия, выполняемые объектом, или на процессы, запущенные объектом.

10. Задайте параметры целевого объекта или целевых процессов, запущенных над объектом.

    - **Целевой процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`).
    - **Хеш целевого процесса**. Хеш файла.
    - **Целевой объект**. Команда запуска целевого процесса. Укажите команду по следующему шаблону `object://<command>`, например, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Также вы можете использовать маски, например, `object://*C:\Windows\temp\*`.

- **Хеш целевого объекта**. Хеш файла.

  Правило Адаптивного контроля аномалий не распространяется на действия над объектом или на процессы, запущенные над объектом.

11. Сохраните внесенные изменения.

Применение обновлений для правил Адаптивного контроля аномалий

Новые правила Адаптивного контроля аномалий могут быть добавлены в таблицу правил и существующие правила Адаптивного контроля аномалий могут быть удалены из таблицы правил по результату обновления антивирусных баз. Kaspersky Endpoint Security выделяет удаляемые и добавляемые правила Адаптивного контроля аномалий в таблице, если для этих правил обновление не было применено.

До тех пор, пока обновление не применено, Kaspersky Endpoint Security отображает удаленные в результате обновления правила Адаптивного контроля аномалий в таблице правил и присваивает этим правилам статус *Выключено*. Изменение параметров этих правил невозможно.

► *Чтобы применить обновления для правил Адаптивного контроля аномалий, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В открывшемся окне нажмите на кнопку **Подтвердить обновления**.

   Кнопка **Подтвердить обновления** доступна, если доступно обновление для правил Адаптивного контроля аномалий.
5. Сохраните внесенные изменения.

Изменение шаблонов сообщений Адаптивного контроля аномалий

Когда пользователь пытается выполнить действие, запрещенное правилами Адаптивного контроля аномалий, Kaspersky Endpoint Security выводит сообщение о блокировке потенциально опасных действий. Если блокировка, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщений администратору о блокировке потенциально опасных действий предусмотрены шаблоны. Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной

из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.

► *Чтобы изменить шаблон сообщения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Адаптивного контроля аномалий:
   - **Сообщение о блокировке**. Шаблон сообщения для пользователя, которое появляется при срабатывании правила Адаптивного контроля аномалий, блокирующего нехарактерное действие.
   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка действия, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете действия приложения**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **Сбросить**.
4. Сохраните внесенные изменения.

См. также:

Изменение шаблонов сообщений Веб-Контроля..... 268
Изменение шаблонов сообщений Контроля устройств..... 237
Изменение шаблонов сообщений Контроля приложений..... 208

Мониторинг работы Адаптивного контроля аномалий

Адаптивный контроль аномалий включает в себя несколько инструментов мониторинга. Мониторинг работы Адаптивного контроля аномалий нужен в первую очередь для настройки компонента во время обучения.

Отчеты Адаптивного контроля аномалий

Адаптивный контроль аномалий использует следующие отчеты:

- **Отчет о состоянии правил Адаптивного контроля аномалий**. Отчет содержит информацию о статусе правил Адаптивного контроля аномалий (*Выключено*, *Интеллектуальное обучение*, *Интеллектуальное блокирование*, *Уведомлять*, *Блокировать*). Отчет позволяет проанализировать уровень обучения Адаптивного контроля аномалий и оценить количество правил, которые перешли из режима *Интеллектуальное обучение* в рабочий режим (например, *Интеллектуальное блокирование*).

- **Отчет о срабатываниях правил Адаптивного контроля аномалий**. Отчет содержит информацию о срабатываниях правил. Также отчет показывает режим срабатывания правила: *Блокировать* (включая *Интеллектуальное блокирование*) или *Уведомлять*. Отчет позволяет оценить активность Адаптивного контроля аномалий на компьютерах пользователей.

► *Как посмотреть отчеты Адаптивного контроля аномалий в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Адаптивный контроль аномалий**.
4. Выполните одно из следующих действий:
   - Если вы хотите просмотреть отчет о параметрах правил Адаптивного контроля аномалий, перейдите по ссылке **Отчет о состоянии правил Адаптивного контроля аномалий**.
   - Если вы хотите просмотреть отчет о срабатываниях правил Адаптивного контроля аномалий, перейдите по ссылке **Отчет о срабатываниях правил Адаптивного контроля аномалий**.
5. Запустится процесс формирования отчета.

Отчет отобразится в новом окне.

Для формирования отчетов в консоли Kaspersky Security Center необходимо включить передачу данных на Сервер администрирования. По умолчанию передача данных включена.

► *Как включить передачу данных для отчетов Адаптивного контроля аномалий в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Отчеты и хранилище**.
4. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Настройка**.
5. Установите следующие флажки:
   - **Отчет о состоянии правил Адаптивного контроля аномалий**.
   - **Отчет о срабатываниях правил Адаптивного контроля аномалий**.
6. Сохраните внесенные изменения.

Хранилище Правила срабатываний в статусе Интеллектуальное обучение

В режиме обучения Адаптивный контроль аномалий отправляет информацию о срабатывании правил в отдельное хранилище **Правила срабатываний в статусе Интеллектуальное обучение**. Информация о срабатывании правил представлена в хранилище в виде списка событий. Для настройки Адаптивного контроля аномалий вы можете или подтвердить нетипичное поведение на компьютере, или добавить исключение для правила (см. раздел "Создание исключения для правила Адаптивного контроля аномалий" на стр. 246).

kaspersky

События Адаптивного контроля аномалий

Адаптивный контроль аномалий регистрирует события срабатывания правил в режимах *Блокировать* (включая *Интеллектуальное блокирование*) и *Уведомлять*. Для этого предусмотрены следующие события:

 **Действие процесса заблокировано**;

 **Действие процесса пропущено**.

События содержат информацию о подозрительной активности, включая контрольные суммы файлов, учетные записи пользователей, время срабатывания правила и имя компьютера. После анализа события вы можете сразу добавить исключения для правила, если активность является легитимной.

kaspersky

Веб-Контроль

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security заблокирует доступ или покажет предупреждение (см. рис. ниже).

Для работы Веб-Контроля необходимо выполнить первоначальную настройку приложения:

- Для контроля HTTPS-трафика включите проверку защищенных соединений (см. раздел "Включение проверки защищенных соединений" на стр. 181) (по умолчанию проверка включена).
- Выберите порты, которые Kaspersky Endpoint Security будет контролировать (см. раздел "Контроль сетевых портов" на стр. 273) (по умолчанию приложение контролирует все порты).
- Выберите приложения, трафик которых будет контролировать Kaspersky Endpoint Security (см. раздел "Формирование списка приложений, для которых контролируются все сетевые порты" на стр. 275). Основные браузеры уже добавлены в список, рекомендованный "Лабораторией Касперского". Если вашего браузера нет в списке, добавьте приложение вручную.
- Рекомендуется внедрить в трафик скрипт для взаимодействия с веб-страницами (см. раздел "Мониторинг активности пользователей в интернете" на стр. 264) (по умолчанию внедрение скрипта выключено). Скрипт позволяет регистрировать события работы Веб-Контроля для журнала событий приложения, журнала событий ОС, отчетов (см. раздел "Работа с отчетами" на стр. 342).

Способы управления доступом к веб-сайтам

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- **Категория веб-сайта**. Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей, например, к категории *Социальные сети* или другим категориям (https://support.kaspersky.com/Legal/WebCategories/ru-RU/206917.htm).
- **Тип данных**. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению.

  Kaspersky Endpoint Security не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security определит тип данных *Архивы*, а не *Графические файлы*.

- **Отдельный адрес**. Вы можете ввести веб-адрес или использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 270).

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных *Файлы офисных приложений* только для категории веб-сайтов *Веб-почта*.

kaspersky

Правила доступа к веб-сайтам

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью *правил доступа*. Вы можете настроить следующие дополнительные параметры правила доступа к веб-сайтам:

- Пользователи, на которых распространяется правило.

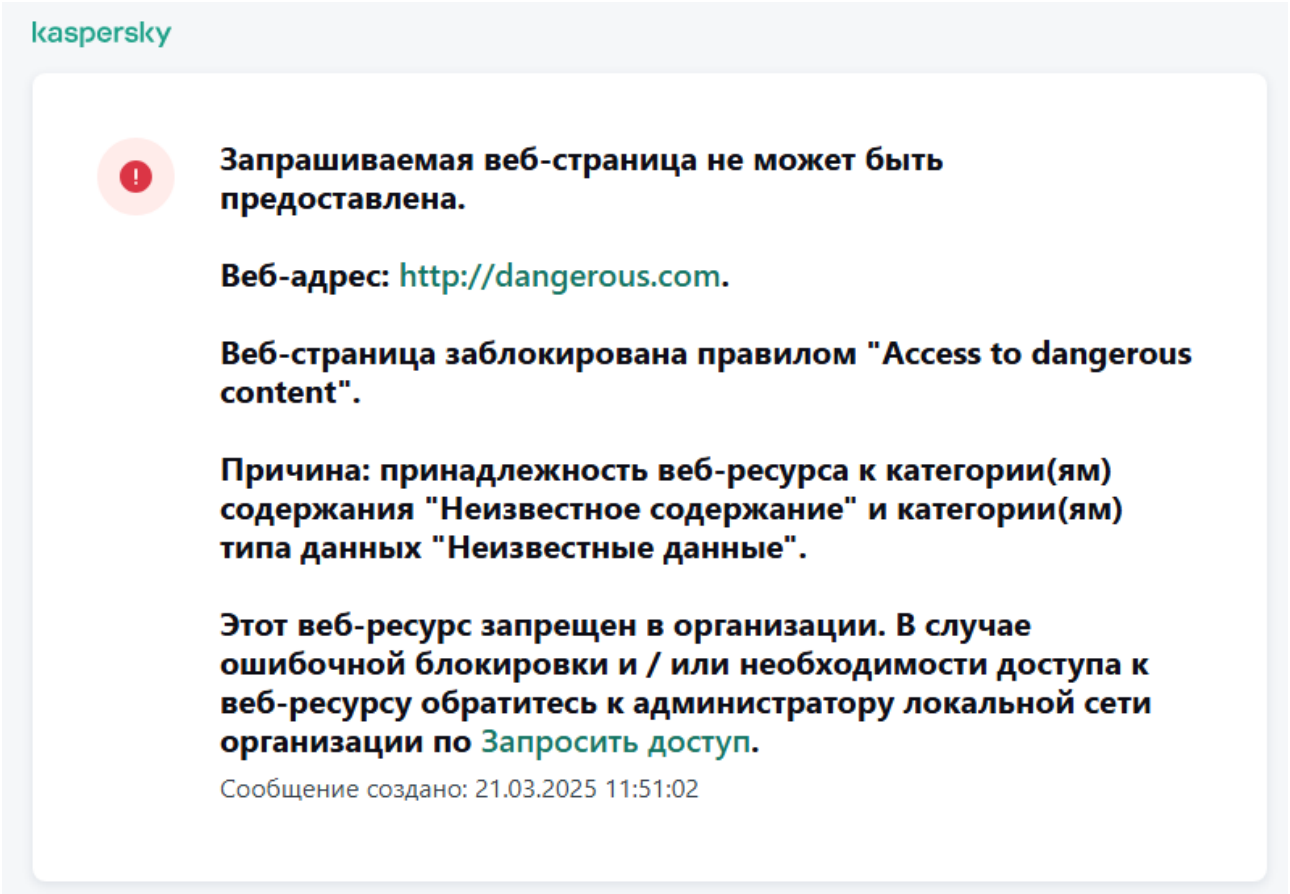
  Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

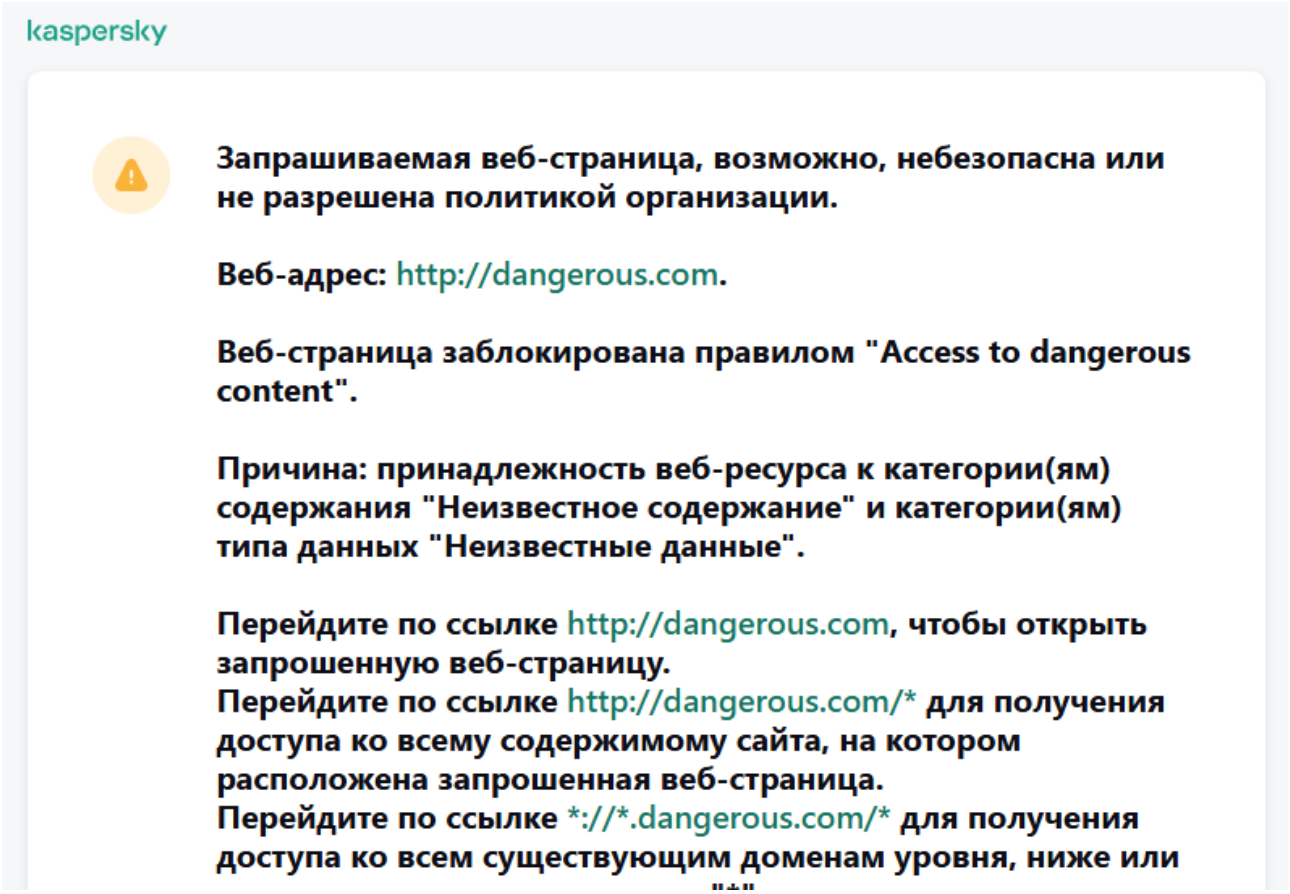
- Расписание работы правила.

  Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Приоритеты правил доступа

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов *Социальные сети* и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.





В этом разделе

Добавление правила доступа к веб-ресурсам 254
Фильтр по содержанию веб-ресурсов 258
Фильтр по адресам веб-ресурсов 260
Проверка работы правил доступа к веб-ресурсам 262
Мониторинг активности пользователей в интернете 264
Изменение шаблонов сообщений Веб-Контроля 268
Правила формирования масок адресов веб-ресурсов 270

Добавление правила доступа к веб-ресурсам

Правило доступа к веб-ресурсам – набор фильтров и действий, которое Kaspersky Endpoint Security выполняет при посещении пользователями веб-ресурсов. Правила доступа могут включать в себя расписание работы правила.

Не рекомендуется создавать более 1000 правил доступа к веб-ресурсам, поскольку это может привести к нестабильности системы.

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое Kaspersky Endpoint Security выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют точно задать круг веб-ресурсов, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по содержанию**. Веб-Контроль разделяет веб-ресурсы по категориям содержания (https://support.kaspersky.com/Legal/WebCategories/ru-RU/206917.htm) и категориям типа данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящихся к определенными этими категориями типам данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания и / или категории типа данных, Kaspersky Endpoint Security выполняет действие, указанное в правиле.
- **Фильтр по адресам веб-ресурсов**. Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

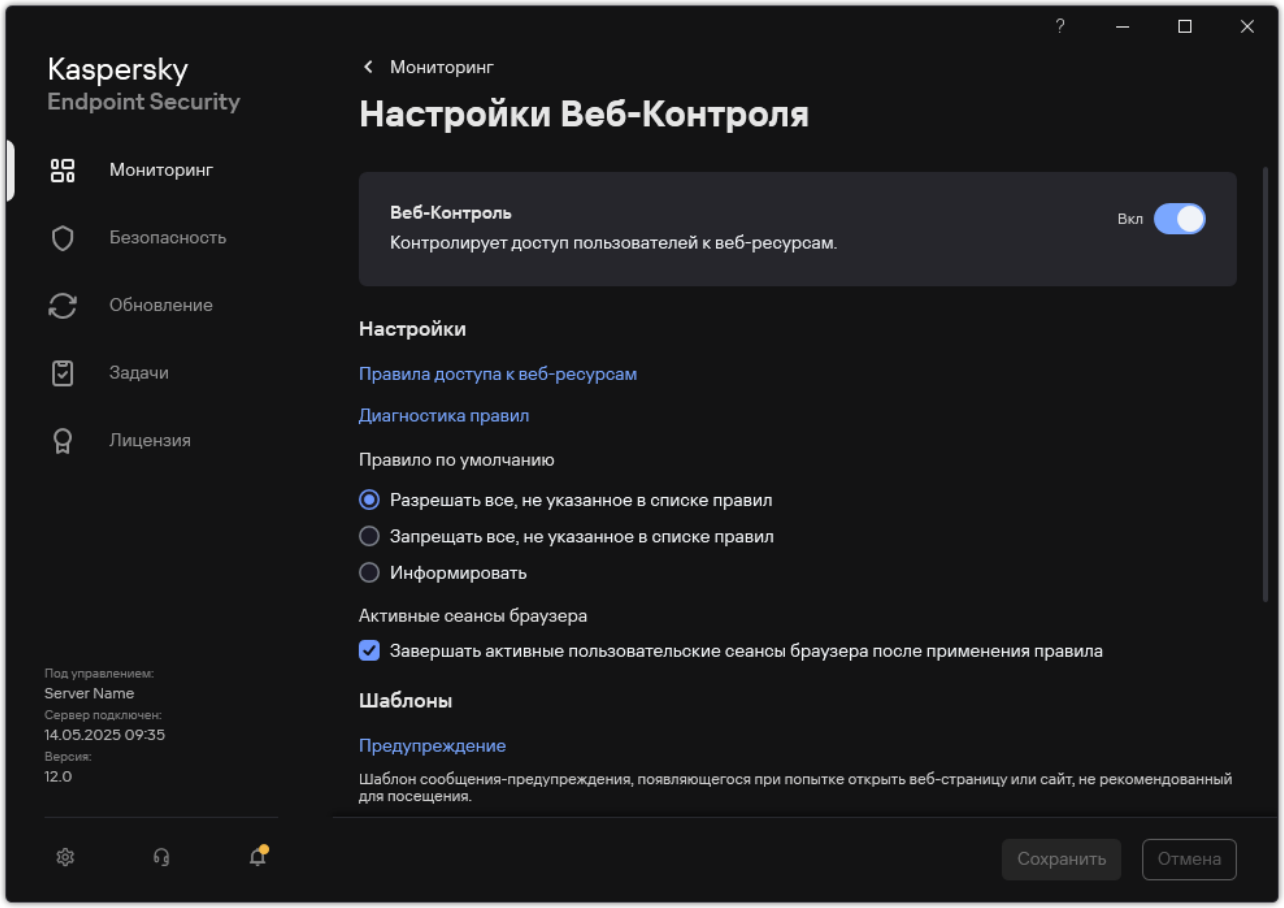
  Если задан и фильтр по содержанию, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и / или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типа данных, Kaspersky Endpoint Security контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и / или категорий типа данных, а только к заданным адресам веб-ресурсов и / или группам адресов веб-ресурсов.
- **Фильтр по именам пользователей и групп пользователей**. Вы можете задавать пользователей и / или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.
- **Расписание работы правила**. Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда Kaspersky Endpoint Security контролирует доступ к веб-ресурсам, указанным в правиле.

После установки приложения Kaspersky Endpoint Security список правил компонента Веб-Контроль не пуст. Предустановлено *Правило по умолчанию*. Это правило в зависимости от выбранного действия разрешает или запрещает всем пользователям доступ ко всем веб-ресурсам, которые не попадают под действие других правил.

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов *Социальные сети* и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.

► *Как добавить правило доступа к веб-ресурсам в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.



3. Включите переключатель **Веб-Контроль**.
4. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
5. В открывшемся окне нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
6. Настройте правило доступа к веб-ресурсам (см. таблицу ниже).
7. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

   Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

   Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.
8. Сохраните внесенные изменения.

В результате новое правило Веб-Контроля будет добавлено в список. Если требуется, измените приоритет правила Веб-Контроля. Также вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя, не удаляя его из списка правил.

Таблица 15. Параметры правила Веб-Контроля

Параметр	Описание
Название правила	Название правила Веб-Контроля.
Состояние	• **Активно**. • **Не активно**. Вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя.
Действие	• **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила. • **Запрещать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа. • **Предупреждать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
Содержимое фильтра	• **По категориям содержания**. Вы можете контролировать доступ пользователей к веб-ресурсам по категориям (https://support.kaspersky.com/Legal/WebCategories/ru-RU/206917.htm) (например, категория *Социальные сети*). • **По типам данных**. Вы можете контролировать доступ пользователей к веб-ресурсам по размещенным данным, относящихся к определенным типам данных (например, *Графические файлы*).
Адреса	• **Ко всем адресам**. Веб-Контроль не фильтрует веб-ресурсы по адресам. • **К отдельным адресам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 270). Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489). Если Проверка защищенных соединений отключена (см. раздел "Проверка защищенных соединений" на стр. 181), для протокола HTTPS доступна фильтрация только по имени сервера.

Параметр	Описание
Пользователи	• **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы для отдельных пользователей. • **К отдельным пользователям и / или группам**. Веб-Контроль фильтрует веб-ресурсы только для отдельных пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489).
Расписание работы правила	Расписание работы правила определяет время, когда Kaspersky Endpoint Security контролирует доступ к веб-ресурсам, указанным в правиле. Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Фильтр по содержанию веб-ресурсов

Для контроля доступа по содержанию веб-ресурсов в Веб-Контроле предусмотрены следующие фильтры: фильтр по категориям и фильтр по типу данных.

Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей, например, к категории *Социальные сети* или другим категориям (https://support.kaspersky.com/Legal/WebCategories/ru-RU/206917.htm).

Вы можете ограничить доступ пользователей по типу данных и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению. Веб-Контроль определяет следующие типы данных:

- Видео;
- Звуковые данные;
- Файлы офисных приложений;
- Исполняемые файлы;
- Архивы;
- Графические файлы;
- Скрипты.

Kaspersky Endpoint Security не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security определит тип данных *Архивы*, а не *Графические файлы*.

Правила могут включать в себя расписание работы правила и список пользователей, которым это правило назначено. Например, вы можете ограничить доступ к веб-сайтам только в рабочее время или разрешить посещение веб-сайтов только пользователям определенных групп.

► *Как включить фильтр по содержанию веб-ресурсов в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
5. В поле **Название правила** введите название правила.
6. Установите статус правила доступа к веб-ресурсам **Активно**.

   Вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя.
7. В блоке **Действие** выберите нужный вариант:
   - **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Запрещать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа.
   - **Предупреждать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
8. В блоке **Содержимое фильтра** выберите нужный фильтр по содержанию:
   - **По категориям содержания**. Вы можете контролировать доступ пользователей к веб-ресурсам по категориям (https://support.kaspersky.com/Legal/WebCategories/ru-RU/206917.htm) (например, категория *Социальные сети*).
   - **По типам данных**. Вы можете контролировать доступ пользователей к веб-ресурсам по размещенным данным, относящихся к определенным типам данных (например, *Графические файлы*).

   Для настройки фильтра по содержанию выполните следующие действия:
   a. Нажмите на ссылку **Настроить**.
   b. Установите флажки напротив названий желаемых категорий содержания и / или типов данных.

      Установка флажка напротив названия категории содержания и / или типа данных означает, что Kaspersky Endpoint Security, в соответствии с правилом, контролирует доступ к веб-ресурсам, принадлежащим к выбранным категориям содержания и / или типам данных.
   c. Вернитесь в окно настройки правила доступа к веб-ресурсам.

9. В блоке **Пользователи** выберите нужный фильтр для пользователей:
   - **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы по адресам.
   - **К отдельным пользователям и / или группам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 270). Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489). Для создания списка пользователей, к которым вы хотите применить правило, выполните следующие действия:
     a. Нажмите на кнопку **Добавить**.
     b. В открывшемся окне выберите пользователей или группы пользователей, к которым вы хотите применить правило доступа к веб-ресурсам.
     c. Вернитесь в окно настройки правила доступа к веб-ресурсам.
10. Выберите из раскрывающегося списка **Расписание работы правила** название нужного расписания или сформируйте новое расписание на основе выбранного расписания работы правила. Для этого выполните следующие действия:
    a. Нажмите на кнопку **Изменить или добавить новое**.
    b. В открывшемся окне нажмите на кнопку **Добавить**.
    c. В открывшемся окне введите название расписания работы правила.
    d. Настройте расписание доступа к веб-ресурсам для пользователей.
    e. Вернитесь в окно настройки правила доступа к веб-ресурсам.
11. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

    Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

    Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.
12. Сохраните внесенные изменения.

В результате новое правило Веб-Контроля будет добавлено в список. Если требуется, измените приоритет правила Веб-Контроля. Также вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя, не удаляя его из списка правил.

kaspersky

Фильтр по адресам веб-ресурсов

Для контроля доступа к отдельным веб-ресурсам вам нужно создать правило Веб-Контроля, сформировать список веб-адресов и выбрать действие Веб-Контроля. При формировании списка веб-адресов вы можете ввести URL-адрес или использовать маски.

Правила могут включать в себя расписание работы правила и список пользователей, которым это правило назначено. Например, вы можете ограничить доступ к веб-сайтам только в рабочее время или разрешить посещение веб-сайтов только пользователям определенных групп.

► *Как включить фильтр по адресам веб-ресурсов в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
5. В поле **Название правила** введите название правила.
6. Установите статус правила доступа к веб-ресурсам **Активно**.

   Вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя.
7. В блоке **Действие** выберите нужный вариант:
   - **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Запрещать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа.
   - **Предупреждать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
8. В блоке **Адреса** выберите **К отдельным адресам**.

   Сформируйте список адресов веб-ресурсов. Вы можете ввести веб-адрес или использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 270). Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла.

   > Если Проверка защищенных соединений отключена (см. раздел "Проверка защищенных соединений" на стр. 181), для протокола HTTPS доступна фильтрация только по имени сервера.
9. В блоке **Пользователи** выберите нужный фильтр для пользователей:
   - **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы для отдельных пользователей.

- **К отдельным пользователям и / или группам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 270). Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489).

10. В раскрывающемся списке **Расписание работы правила** выберите расписание или сформируйте новое расписание.
11. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

    Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

    Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.
12. Сохраните внесенные изменения.

В результате новое правило Веб-Контроля будет добавлено в список. Если требуется, измените приоритет правила Веб-Контроля. Также вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя, не удаляя его из списка правил.

Проверка работы правил доступа к веб-ресурсам

При настройке Веб-Контроля вы можете случайно заблокировать доступ к веб-ресурсам, необходимым пользователям для работы. Для определения правила Веб-Контроля, которое блокирует доступ к веб-ресурсам, предназначен инструмент *Диагностика правил Веб-Контроля*. Диагностика правил Веб-Контроля доступна только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center определить правило Веб-Контроля, которое включает в себя веб-ресурс, невозможно.

Если блокировка доступа к веб-ресурсу, по мнению пользователя, была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение администратору локальной сети организации (см. раздел "Изменение шаблонов сообщений Веб-Контроля" на стр. 268).

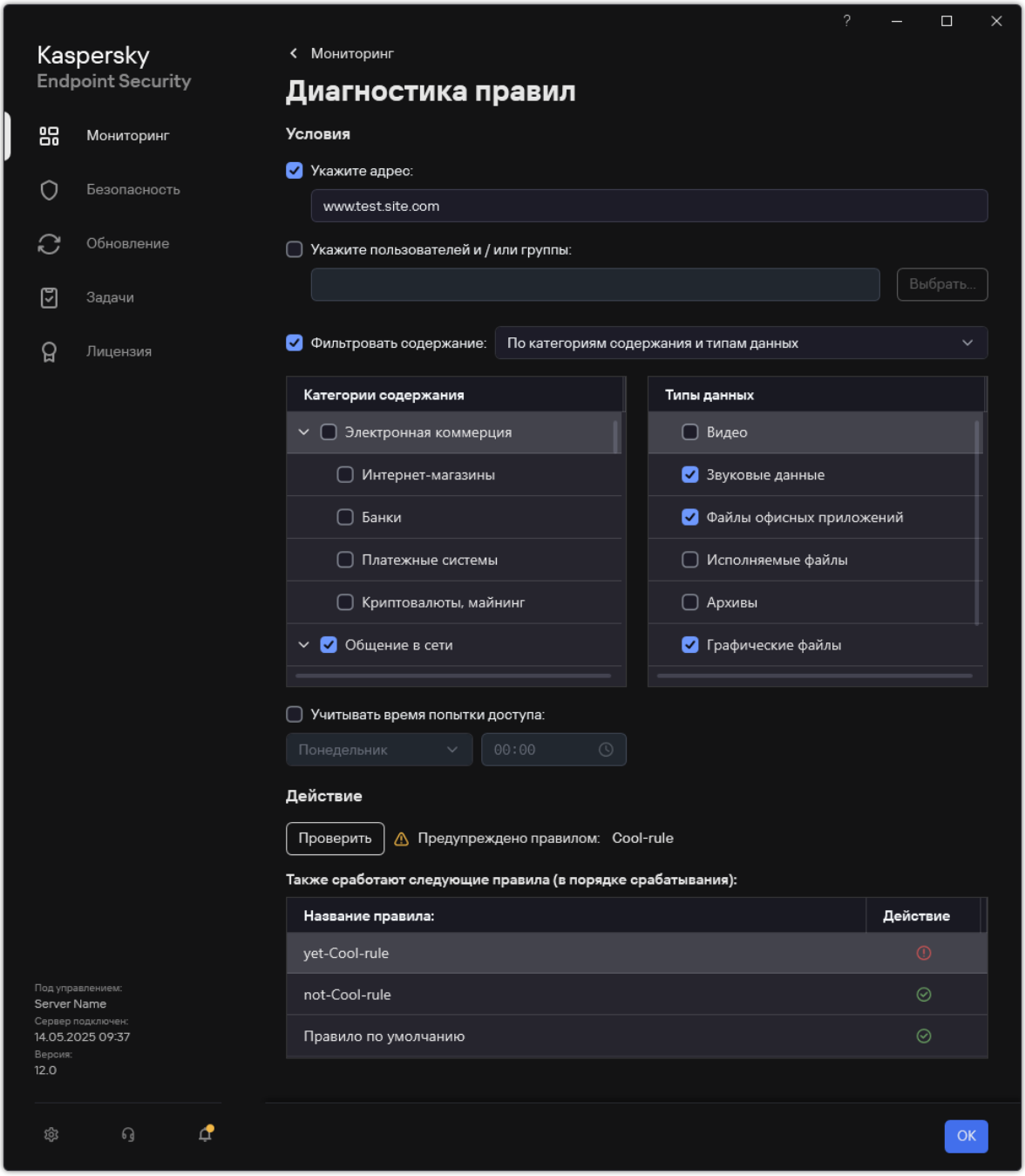
► *Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.
3. В блоке **Настройки** нажмите на ссылку **Диагностика правил**.

   Откроется окно **Диагностика правил**.

4. Установите флажок **Укажите адрес**, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к определенному веб-ресурсу. В поле ниже введите адрес веб-ресурса.
5. Задайте список пользователей и / или групп пользователей, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к веб-ресурсам для определенных пользователей и / или групп пользователей.
6. Установите флажок **Фильтровать содержание** и в раскрывающемся списке выберите нужный элемент (**По категориям содержания**, **По типам данных** или **По категориям содержания и типам данных**), если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к веб-ресурсам определенных категорий содержания и / или категорий типа данных.
7. Установите флажок **Учитывать время попытки доступа**, если вы хотите проверить работу правил с учетом дня недели и времени совершения попытки доступа к веб-ресурсам, указанным в условиях диагностики правил. Далее укажите день недели и время.
8. Нажмите на кнопку **Проверить**.

В результате проверки выводится сообщение о действии Kaspersky Endpoint Security в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу (разрешение, запрет, предупреждение). Первым срабатывает правило, которое находится в списке правил Веб-Контроля выше других правил, удовлетворяющих условиям диагностики. Сообщение выводится справа от кнопки **Проверить**. В таблице ниже выводится список остальных сработавших правил с указанием действия, которое выполняет Kaspersky Endpoint Security. Правила выводятся в порядке убывания приоритета.



Мониторинг активности пользователей в интернете

Kaspersky Endpoint Security позволяет записывать данные о посещении пользователями всех веб-сайтов, в том числе и разрешенных. Таким образом, вы можете получить полную историю просмотров в браузере. Kaspersky Endpoint Security отправляет события активности пользователя в Kaspersky Security Center, локальный журнал Kaspersky Endpoint Security (см. раздел "Работа с отчетами" на стр. 342), журнал событий Windows. Для получения событий в Kaspersky Security Center нужно настроить параметры событий в политике в Консоли администрирования или Web Console. Также вы можете настроить отправку событий Веб-Контроля по электронной почте и отображение уведомлений на экране компьютера пользователя.

Браузеры, которые поддерживают функцию мониторинга: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Яндекс.Браузер, Mozilla Firefox. Мониторинг активности пользователей не работает в других браузерах.

Kaspersky Endpoint Security создает следующие события активности пользователя в интернете:

- блокировка веб-сайта (статус *Критическое*);
- посещение нерекомендованного веб-сайта (статус *Предупреждение*);
- посещение разрешенного веб-сайта (статус *Информационное сообщение*).

Для мониторинга активности необходимо выполнить следующие действия:

- Внедрите в трафик скрипт взаимодействия с веб-страницами (см. инструкцию ниже). Скрипт позволяет регистрировать события работы Веб-Контроля.
- Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Включение проверки защищенных соединений" на стр. 181).

Внедрение скрипта взаимодействия с веб-страницами

► *Как внедрить в трафик скрипт взаимодействия с веб-страницами в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

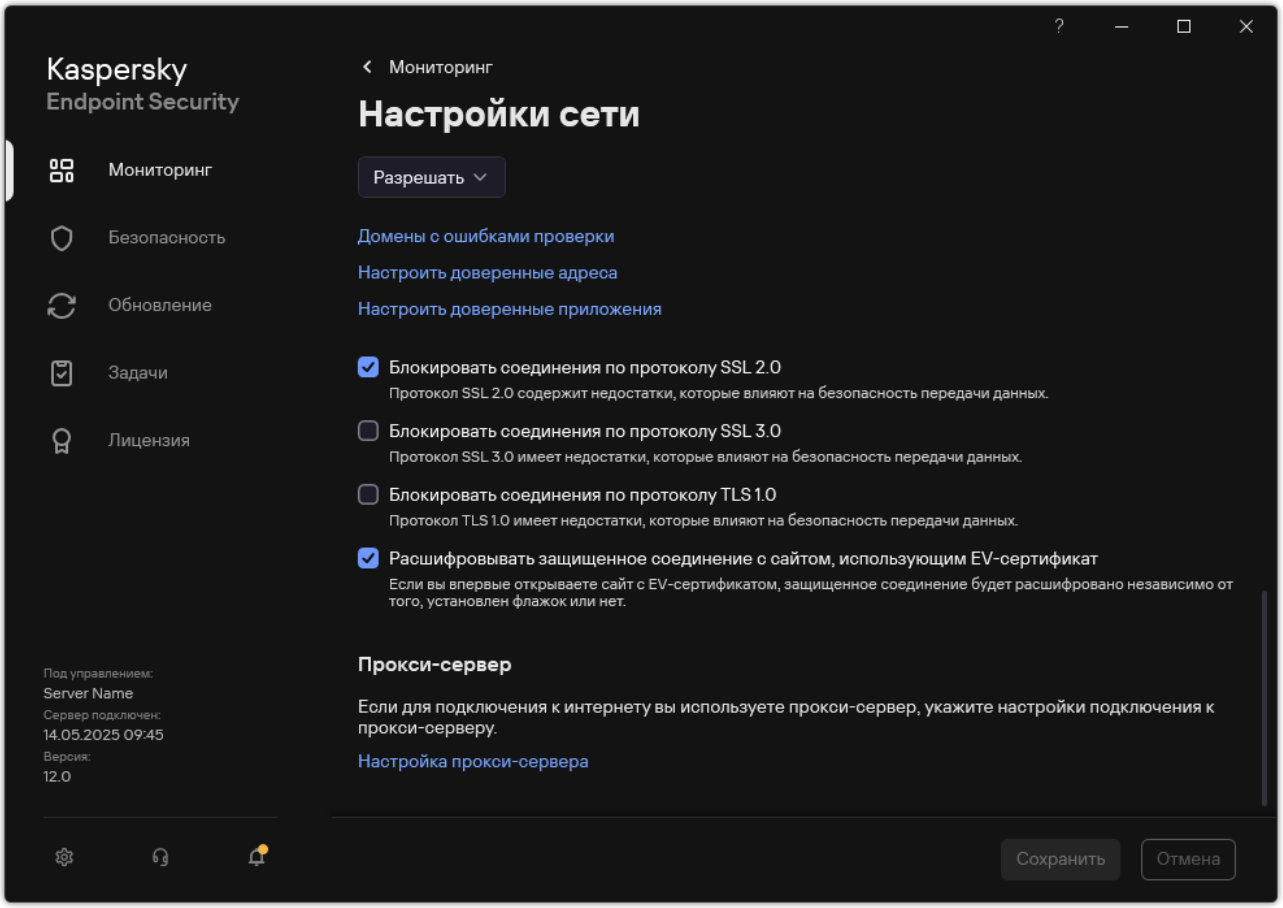


Рисунок 62. Параметры сети приложения

3. В блоке **Обработка трафика** установите флажок **Внедрять в трафик скрипт взаимодействия с веб-страницами**.
4. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security внедрит в трафик скрипт взаимодействия с веб-страницами. Скрипт позволяет регистрировать события работы Веб-Контроля для журнала событий приложения, журнала событий ОС, отчетов (см. раздел "Работа с отчетами" на стр. 342).

Настройка записи событий Веб-Контроля

► *Чтобы настроить запись событий Веб-Контроля на компьютере пользователя, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настроить уведомления**.
4. В открывшемся окне выберите раздел **Веб-Контроль**.

   Откроется таблица событий Веб-Контроля и способов уведомлений.

5. Настройте для каждого события способ уведомления: **Сохранять в локальном отчете** и **Сохранять в журнале событий Windows**.

   Для записи событий посещения разрешенных веб-сайтов нужно дополнительно настроить Веб-Контроль (см. инструкцию ниже).

   Также в таблице событий вы можете включить уведомление на экране и уведомление по электронной почте. Для отправки уведомлений по почте нужно настроить параметры SMTP-сервера. Подробнее об отправке уведомлений по почте см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm.

6. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security начинает записывать события активности пользователя в интернете.

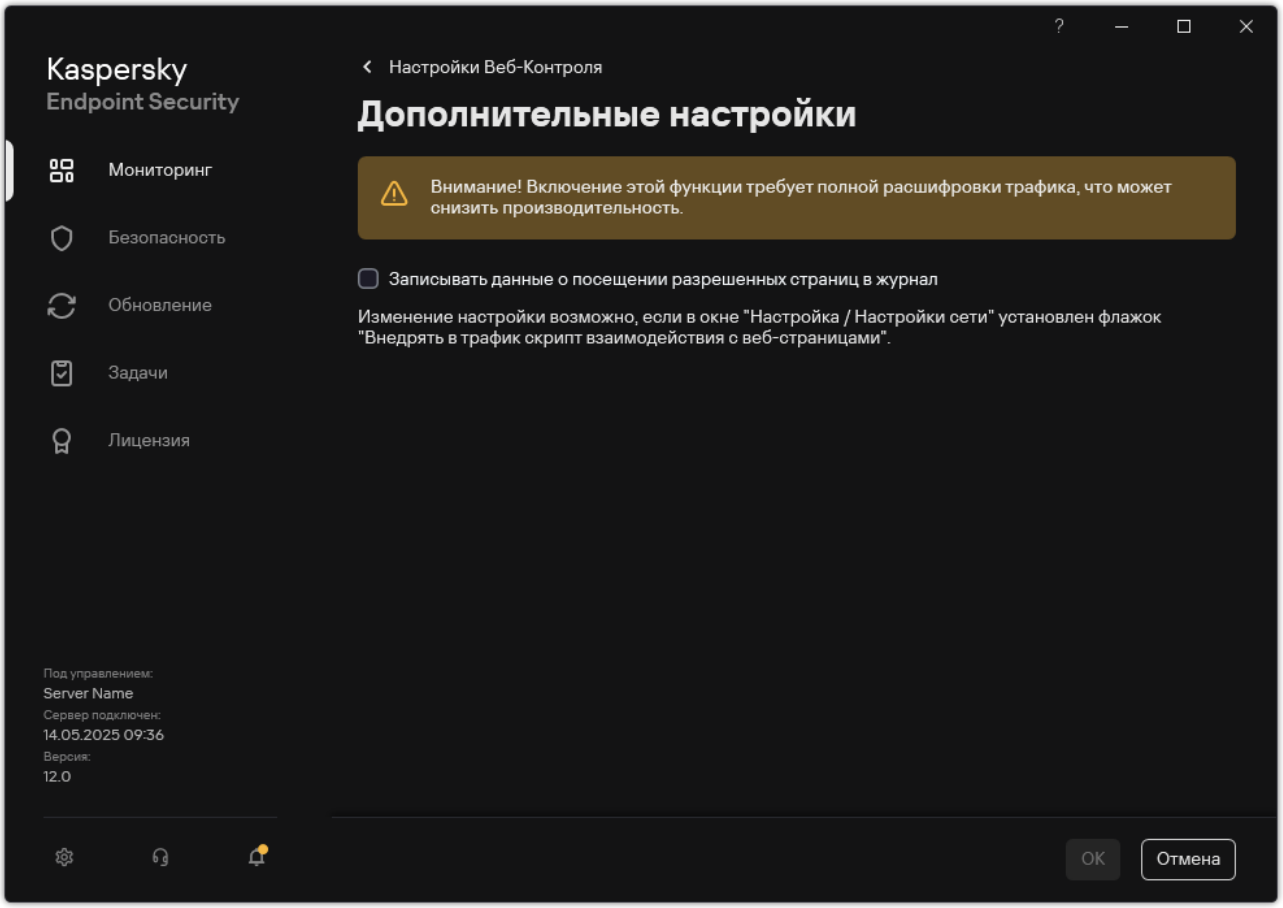
Веб-Контроль отправляет события активности пользователя в Kaspersky Security Center следующим образом:

- Если вы используете Kaspersky Security Center, Веб-Контроль отправляет события по всем объектам, из которых состоит веб-страница. Поэтому при блокировании одной веб-страницы может быть создано несколько событий. Например, при блокировании веб-страницы http://www.example.com Kaspersky Endpoint Security может отправить события по следующим объектам: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js и так далее.
- Если вы используете Kaspersky Security Center Cloud Console, Веб-Контроль группирует события и отправляет только протокол и домен веб-сайта. Например, если пользователь посетил нерекомендованные веб-страницы http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, то Kaspersky Endpoint Security отправит только одно событие с объектом http://www.example.com.

Запись событий посещения разрешенных веб-сайтов

► *Чтобы включить запись событий посещения разрешенных веб-сайтов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.
3. В блоке **Дополнительно** нажмите на кнопку **Дополнительные настройки**.
4. В открывшемся окне установите флажок **Записывать данные о посещении разрешенных страниц в журнал**.



5. Сохраните внесенные изменения.

В результате вам будет доступна полная история просмотров в браузере.

Изменение шаблонов сообщений Веб-Контроля

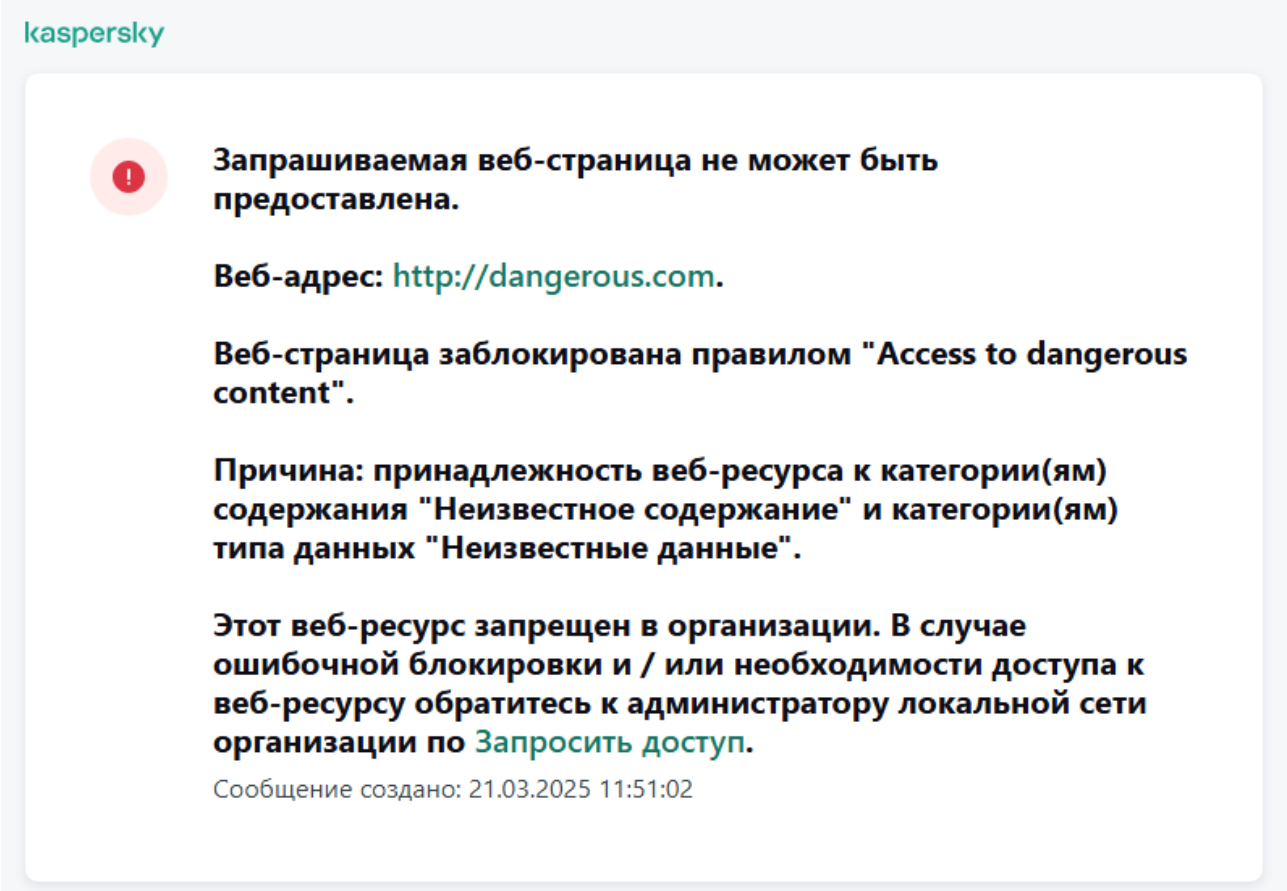
В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователей получить доступ к веб-ресурсам Kaspersky Endpoint Security выводит сообщение (подменяет ответ HTTP-сервера HTML-страницей с сообщением) одного из следующих типов:

- Сообщение-предупреждение. Такое сообщение предупреждает пользователя о том, что посещение веб-ресурса не рекомендуется и / или не соответствует корпоративной политике безопасности. Kaspersky Endpoint Security выводит сообщение-предупреждение, если в параметрах правила, описывающего этот веб-ресурс, выбрано действие **Предупреждать**.

  Если, по мнению пользователя, предупреждение ошибочно, по ссылке из предупреждения пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

- Сообщение о блокировке веб-ресурса. Kaspersky Endpoint Security выводит сообщение о блокировке веб-ресурса (см. рис. ниже), если в параметрах правила, которое описывает этот веб-ресурс, выбрано действие **Запрещать**.

  Если блокировка доступа к веб-ресурсу, по мнению пользователя, была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение администратору локальной сети организации.



Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения для отправки администратору локальной сети организации предусмотрены шаблоны. Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.

► *Как изменить шаблон сообщений Веб-Контроля в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Веб-Контроля:
   - **Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.
   - **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.

- **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете доступа к веб-странице**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **Сбросить**.

4. Сохраните внесенные изменения.

См. также:

Изменение шаблонов сообщений Контроля устройств 237

Изменение шаблонов сообщений Контроля приложений 208

Изменение шаблонов сообщений Адаптивного контроля аномалий 248

Правила формирования масок адресов веб-ресурсов

Использование *маски адреса веб-ресурса* (далее также "маски адреса") может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует использовать следующие правила:

1. Символ `*` заменяет любую последовательность из нуля или более символов.

   Например, при вводе маски адреса `*abc*` правило доступа к веб-ресурсам применяется ко всем адресам, содержащим последовательность `abc`. Пример: `http://www.example.com/page_0-9abcdef.html`.

2. Последовательность символов `*.` позволяет выбрать все домены адреса – *маска домена*. Маска домена `*.` трактуется как любое имя домена, имя поддомена или пустая строка.

   Пример: под действие маски `*.example.com` попадают следующие адреса:

   - `http://pictures.example.com` – маска домена `*.` применена для `pictures.`.
   - `http://user.pictures.example.com` – маска домена `*.` применена для `pictures.` и `user.`.
   - `http://example.com` – маска домена `*.` трактуется как пустая строка.

3. Последовательность символов `www.` в начале маски адреса трактуется как последовательность `*.`.

   Пример: маска адреса `www.example.com` трактуется как `*.example.com`. Под действие маски попадают адреса `www2.example.com` и `www.pictures.example.com`.

4. Если маска адреса начинается не с символа `*`, то содержание маски адреса эквивалентно тому же содержанию с префиксом `*.`.

5. Если маска адреса заканчивается символом, отличным от `/` или `*`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

   Пример: под действие маски адреса `http://www.example.com` попадают адреса вида `http://www.example.com/abc`, где `a`, `b`, `c` – любые символы.

6. Если маска адреса заканчивается символом `/`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

7. Последовательность символов `/*` в конце маски адреса трактуется как `/*` или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):

   - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес с любым сетевым протоколом.

     Пример: под действие маски адреса `example.com` попадают адреса http://example.com и https://example.com.

   - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса с таким же сетевым протоколом, как у маски адреса.

     Пример: под действие маски адреса `http://*.example.com` попадает адрес `http://www.example.com` и не попадает адрес `https://www.example.com`.

9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа `*`, если он изначально включен в состав маски адреса. Для масок адреса, заключенных в двойные кавычки, не выполняются правила 5 и 7 (см. примеры 14 – 18 в таблице ниже).

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Таблица 16. Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.
2	*.example.com	http://www.123.example.com	Да	См. правило 2.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.
6	www.example.com	http://www.example.com	Да	См. правила 3, 2, 1.

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
7	www.example.com	https://www.example.com	Да	См. правила 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 3, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	"example.com"	http://www.example.com	Нет	См. правило 9.
15	"http://www.example.com"	http://www.example.com/abc	Нет	См. правило 9.
16	"*.example.com"	http://www.example.com	Да	См. правила 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Да	См. правила 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес веб-ресурса.

kaspersky

Контроль сетевых портов

Во время работы Kaspersky Endpoint Security компоненты Веб-Контроль (на стр. 252), Защита от почтовых угроз (на стр. 158), Защита от веб-угроз (на стр. 151), Анализ поведения (на стр. 115), Защита от эксплойтов (на стр. 124) контролируют потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты компьютера пользователя. Например, компонент Защита от почтовых угроз анализирует информацию, передаваемую по SMTP-протоколу, а компонент Защита от веб-угроз анализирует информацию, передаваемую по протоколам HTTP и FTP.

Kaspersky Endpoint Security подразделяет TCP- и UDP-порты компьютера пользователя на несколько групп в соответствии с вероятностью их взлома. Сетевые порты, отведенные для уязвимых служб, рекомендуется контролировать более тщательно, так как эти сетевые порты с большей вероятностью могут являться целью сетевой атаки. Если вы используете нестандартные службы, которым отведены нестандартные сетевые порты, эти сетевые порты также могут являться целью для атакующего компьютера. Вы можете задать список сетевых портов и список приложений, запрашивающих сетевой доступ, на которые компоненты Защита от почтовых угроз и Защита от веб-угроз должны обращать особое внимание во время слежения за сетевым трафиком.

Компоненты Анализ поведения (на стр. 115) и Защита от эксплойтов (на стр. 124) также контролируют потоки данных через сетевые порты для обеспечения безопасности компьютера. Компоненты постоянно контролируют сетевой трафик для отдельных процессов, которые могут представлять угрозу.

В этом разделе

Включение контроля всех сетевых портов 273

Формирование списка контролируемых сетевых портов 274

Формирование списка приложений, для которых контролируются все сетевые порты 275

Включение контроля всех сетевых портов

► *Чтобы включить контроль всех сетевых портов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

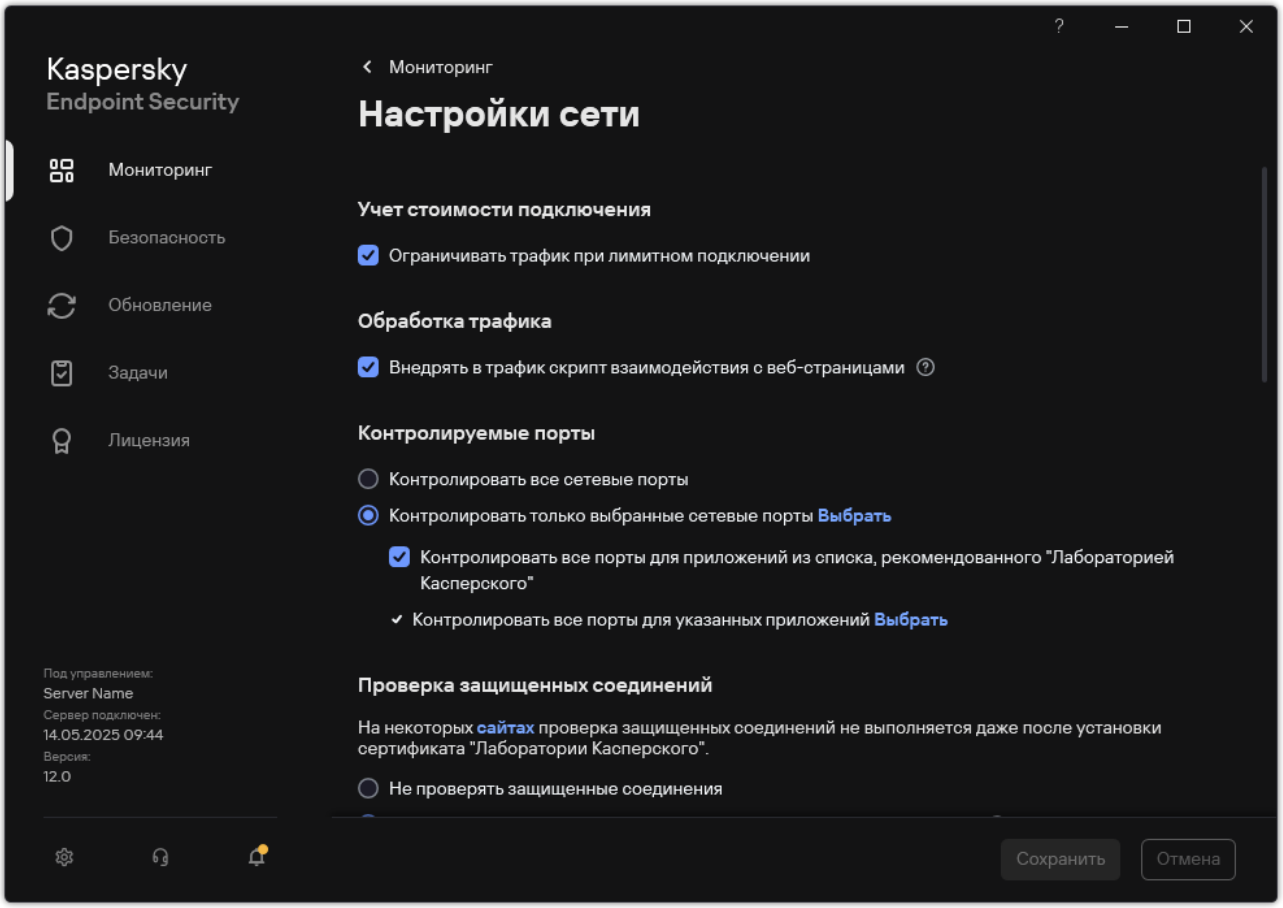


Рисунок 63. Параметры проверки защищенных соединений

3. В блоке **Контролируемые порты** выберите вариант **Контролировать все сетевые порты**.
4. Сохраните внесенные изменения.

Формирование списка контролируемых сетевых портов

► *Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.
4. Нажмите на кнопку **Выбрать**.

   Откроется список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Endpoint Security.
5. Используйте переключатель в графе **Статус**, чтобы включить или выключить контроль сетевых портов.

6. Если сетевой порт отсутствует в списке сетевых портов, добавьте его следующим образом:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне введите номер сетевого порта и короткое описание.
   c. Установите статус контроля сетевого порта **Активно** или **Неактивно**.
7. Сохраните внесенные изменения.

При работе протокола FTP в пассивном режиме соединение может устанавливаться через случайный сетевой порт, который не добавлен в список контролируемых сетевых портов. Чтобы защищать такие соединения, включите контроль всех сетевых портов (см. раздел "Включение контроля всех сетевых портов" на стр. 273) или настройте контроль сетевых портов для приложений, с помощью которых устанавливается FTP-соединение (см. раздел "Формирование списка приложений, для которых контролируются все сетевые порты" на стр. 275).

Формирование списка приложений, для которых контролируются все сетевые порты

Вы можете сформировать список приложений, для которых Kaspersky Endpoint Security контролирует все сетевые порты.

В список приложений, для которых Kaspersky Endpoint Security контролирует все сетевые порты, рекомендуется включить приложения, которые принимают или передают данные по протоколу FTP.

► *Чтобы сформировать список приложений, для которых контролируются все сетевые порты, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.
4. Установите флажок **Контролировать все порты для приложений из списка, рекомендованного "Лабораторией Касперского"**.

   Если установлен этот флажок, приложение Kaspersky Endpoint Security контролирует все порты для следующих приложений:

   - Adobe Acrobat Reader.
   - Apple Application Support.
   - Google Chrome.
   - Microsoft Edge.
   - Mozilla Firefox.

- Internet Explorer.
- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.
- Агент Mail.ru.
- Яндекс.Браузер.

5. Установите флажок **Контролировать все порты для указанных приложений**.
6. Нажмите на кнопку **Выбрать**.

   Откроется список приложений, сетевые порты которых контролирует Kaspersky Endpoint Security.
7. Используйте переключатель в графе **Статус**, чтобы включить или выключить контроль сетевых портов.
8. Если приложение отсутствует в списке приложений, добавьте ее следующим образом:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне укажите путь к исполняемому файлу приложения и короткое описание.
   c. Установите статус контроля сетевых портов **Активно** или **Неактивно**.
9. Сохраните внесенные изменения.

kaspersky

Контроль целостности системы

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций.

Начиная с версии Kaspersky Endpoint Security для Windows 12.6 вместо компонента Мониторинг файловых операций https://support.kaspersky.com/help/KESWin/12.5/ru-RU/236372.htm добавлен компонент Контроль целостности системы. Контроль целостности системы включает в себя все функции Мониторинга файловых операций, а также позволяет контролировать изменения в реестре и подключение внешних устройств.

Контроль целостности системы отслеживает изменения в операционной системе, которые могут указывать на нарушения безопасности компьютера. Обнаружив такие изменения, Kaspersky Endpoint Security формирует соответствующие события и предупреждает администратора. Контроль целостности системы может работать в режиме реального времени, а также выполнять проверку целостности системы по запросу.

Контроль целостности системы в режиме реального времени

При работе в режиме реального времени (см. раздел "Контроль целостности системы в режиме реального времени" на стр. 280) Контроль целостности системы отслеживает изменения в объектах, которые вы включили в область действия компонента (*область мониторинга*). Также Контроль целостности системы позволяет блокировать несанкционированный доступ к этим объектам в режиме реального времени.

Проверка целостности системы по запросу

Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Для выполнения задачи *Проверка целостности системы* (см. раздел "*Проверка целостности системы по запросу*" на стр. 283) требуется настроить область действия компонента (*область мониторинга*) и создать снимок состояния системы. *Снимок состояния системы* – зафиксированное состояние объектов системы, с которым приложение сравнивает текущее состояние.

Миграция параметров Мониторинга файловых операций

При обновлении Kaspersky Endpoint Security до версии 12.6 миграция параметров Мониторинга файловых операций будет выполнена автоматически. Во время миграции приложение переносит правила мониторинга в Контроль целостности системы. Также при миграции с KSWS на KES правила компонента Мониторинг файловых операций будут перенесены в Контроль целостности системы.

Для корректной работы Контроля целостности системы нужно обновить приложение Kaspersky Endpoint Security и плагин управления до версии 12.6. Если у вас установлен плагин управления более ранней версии, настроить параметры Контроля целостности системы невозможно, так как в плагине управления отсутствует раздел **Контроль целостности системы**.

kaspersky

В этом разделе

О правилах Контроля целостности системы 278

Контроль целостности системы в режиме реального времени 280

Проверка целостности системы по запросу 283

Просмотр отчетов о работе Контроля целостности системы 289

Сброс статуса целостности системы 289

О правилах Контроля целостности системы

Для работы Контроля целостности системы требуется добавить хотя бы одно правило (см. раздел "Контроль целостности системы в режиме реального времени" на стр. 280). *Правило Контроля целостности системы* – набор критериев, которые определяют доступ пользователей к файлам и реестру. Контроль целостности системы обнаруживает изменения в файлах и реестре в заданной *области мониторинга*. Область мониторинга является одним из критериев правила Контроля целостности системы.

Контроль целостности системы позволяет контролировать следующие объекты:

- файлы;
- реестр;
- внешние устройства.

Особенности мониторинга файлов

Контроль целостности системы осуществляет мониторинг изменений в файлах и папках, а также добавление и удаление файлов в области мониторинга. Эти изменения могут указывать на нарушение безопасности компьютера. Рекомендуется добавлять в область мониторинга объекты, изменения в которых происходят редко, или, доступ к которым имеет только администратор. Это позволит уменьшить количество событий Контроля целостности системы.

Контроль целостности системы не осуществляет мониторинг изменений в файлах в общих папках сервера. Контроль целостности системы предназначен только для локального использования.

Kaspersky Endpoint Security отслеживает изменения файлов и папок только на тех дисках, которые подключены в момент начала работы Контроля целостности системы в режиме реального времени. Если диск отключен в момент начала работы Контроля целостности системы в режиме реального времени, приложение не отслеживает изменения файлов и папок на этом диске, даже если эти файлы и папки добавлены в область мониторинга.

Особенности мониторинга реестра

Контроль целостности системы осуществляет мониторинг реестра. Эти изменения могут указывать на нарушение безопасности компьютера.

Контроль целостности системы осуществляет мониторинг следующих корневых разделов реестра:

- HKCR;
- HKLM;
- HKU;
- HKCC;
- HKEY_CLASSES_ROOT;
- HKEY_LOCAL_MACHINE;
- HKEY_USERS;
- HKEY_CURRENT_CONFIG (только для Контроля целостности системы в режиме реального времени);
- HKEY_CURRENT_USER (только для Контроля целостности системы в режиме реального времени).

> Задача *Проверка целостности системы* не поддерживает ключ HKEY_CURRENT_USER. Вы можете указывать путь к ключу в реестре через раздел HKEY_USERS в виде HKEY_USERS\<user profile ID>\<key>.

Особенности мониторинга внешних устройств

Контроль целостности системы осуществляет мониторинг подключения и отключения внешних устройств. Это нужно для защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с этими устройствами. Контроль целостности системы не контролирует доступ к внешним устройствам и не запрещает обмен файлами. Вы можете настроить доступ к устройствам с помощью другого компонента приложения – Контроль устройств (на стр. 210).

> При выполнении задачи *Мониторинг целостности системы на основе эталона* (см. раздел "*Проверка целостности системы по запросу*" на стр. 283) приложение пропускает переключение внешних устройств, если устройства имеют одинаковую букву диска в операционной системе. Для регистрации переключения внешних устройств необходимо, чтобы эти устройства имели разные буквы диска.

Контроль целостности системы осуществляет мониторинг подключения следующих типов внешних устройств:

- Съемный диск (включая USB-флешки).
- Жесткий диск.
- Внешний сетевой адаптер.
- Привод CD/DVD/Blu-ray.
- Сканер / камера.

kaspersky

Контроль целостности системы в режиме реального времени

Контроль целостности системы позволяет отслеживать изменения в операционной системе в режиме реального времени. Вы можете отслеживать изменения, которые могут указывать на нарушения безопасности на компьютере. Компонент позволяет или блокировать эти изменения, или только регистрировать события об изменениях.

Для работы Контроля целостности системы требуется добавить хотя бы одно правило (см. раздел "О правилах Контроля целостности системы" на стр. 278). *Правило Контроля целостности системы* – набор критериев, которые определяют доступ пользователей к файлам и реестру. Контроль целостности системы обнаруживает изменения в файлах и реестре в заданной *области мониторинга*. Область мониторинга является одним из критериев правила Контроля целостности системы.

Режимы работы Контроля целостности системы в режиме реального времени

Чтобы убедиться, что правила Контроля целостности системы не блокируют действия с ресурсами, необходимые для работы операционной системы или других сервисов, рекомендуется после создания правил включить Тестовый режим и проанализировать работу компонента. При включении Тестового режима Kaspersky Endpoint Security не будет блокировать действия пользователя, запрещенные в правилах, но будет формировать события со статусом *Предупреждение* ⚠.

Компонент Контроль целостности системы в режиме реального времени работает в двух режимах:

- Блокировать.

  В этом режиме Контроль целостности системы отслеживает изменения в системе и выполняет действие согласно правилам: **Разрешать** или **Запрещать**. Также Контроль целостности системы формирует соответствующее событие и меняет статус устройства в консоли Kaspersky Security Center.

- Информировать.

  В этом режиме Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга. Если действие с файлами или реестром запрещено, приложение формирует событие *Запрещенное действие разрешено в тестовом режиме*. Для анализа работы правил предназначены отчеты (см. раздел "Просмотр отчетов о работе Контроля целостности системы" на стр. 289).

Включение Контроля целостности системы в режиме реального времени

► *Как включить Контроль целостности системы в режиме реального времени в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль целостности системы**.
3. Включить переключатель **Контроль целостности системы**.
4. В блоке **Режим работы для блокирующих правил** выберите режим работы Контроля целостности системы в режиме реального времени:
   - **Блокировать**. В этом режиме Контроль целостности системы блокирует действия с файлами и реестром в области мониторинга и формирует соответствующее событие.
   - **Информировать**. В этом режиме Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга и формирует соответствующее событие.

5. В блоке **Контроль целостности системы в режиме реального времени** установите флажок **Контроль целостности системы в режиме реального времени**.
6. Настройте мониторинг внешних устройств:
   a. Установите флажок **Следить за устройствами**.
   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационные*  , *Предупреждение*  , *Критические*  .

   Контроль целостности системы фиксирует текущее подключение внешних устройств. Приложение начинает контролировать подключение и отключение внешних устройств после включения компонента в параметрах приложения. Далее при подключении или отключении внешних устройств приложение формирует соответствующее событие.
7. Настройте мониторинг файлов и реестра:
   a. Установите флажок **Следить за файлами и реестром**.
   b. Нажмите на кнопку **Настроить**.

      Откроется список правил Контроля целостности системы.
   c. Нажмите на кнопку **Добавить**.

      Вы также можете импортировать правила из другого источника.
8. Настройте правило Контроля целостности системы (см. таблицу ниже).
9. Сохраните внесенные изменения.

Таблица 17. Параметры правила Контроля целостности системы в режиме реального времени

Параметр	Описание
Имя правила	Название правила Контроля целостности системы в режиме реального времени.
Действия с файлами и реестром	• **Разрешать**. Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга. • **Запрещать**. Поведение Контроля целостности системы отличается в зависимости от выбранного режима работы. Если вы выбрали *Режим защиты системы*, Контроль целостности системы блокирует действия с файлами и реестром из области мониторинга, формирует соответствующее событие и меняет статус устройства в консоли Kaspersky Security Center. Если вы выбрали *Тестовый режим*, Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга.
Уровень важности событий	Kaspersky Endpoint Security регистрирует события изменения файлов и реестра в области мониторинга. Доступны следующие уровни важности событий: *Информационные*  , *Предупреждение*  , *Критические*  .

Параметр	Описание
Область мониторинга	• **Файл**. Список файлов и папок, которые контролирует компонент. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. Используйте маски: Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов. • **Реестр**. Список ключей реестра и значений ключей, которые контролирует компонент. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.
Исключения	• **Файл**. Список исключений из области мониторинга. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. Например, `C:\Folder\Application\*.log`. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга. Используйте маски: Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов. • **Реестр**. Список исключений из области мониторинга. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга.

Параметр	Описание
Доверенные пользователи и / или группы пользователей	*Доверенный пользователь* – пользователь, которому разрешено выполнение действий с файлами и реестром в области мониторинга. Если Kaspersky Endpoint Security обнаруживает действие, выполненное доверенным пользователем, Контроль целостности системы формирует событие с уровнем важности *Информационные* . Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489).
Маркеры файловых операций / Контролируемые действия	Маркеры, характеризующие действие над файлами или реестром, которые будет контролировать приложение.
Хеширование	Вычисление хеша файла при изменении. Kaspersky Endpoint Security добавляет информацию о хеше файла при формировании события.

Проверка целостности системы по запросу

Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Во время выполнения задачи *Проверка целостности системы* приложение сравнивает текущее состояние объектов, включенных в область мониторинга, с состоянием этих объектов, зафиксированных в *снимке состояния системы*. В отличие от Контроля целостности системы в режиме реального времени задача *Проверка целостности системы* позволяет уменьшить количество событий и сформировать общий отчет об изменениях в операционной системе.

Для работы Контроля целостности системы требуется добавить хотя бы одно правило (см. раздел "О правилах Контроля целостности системы" на стр. 278). *Правило Контроля целостности системы* – набор критериев, которые определяют доступ пользователей к файлам и реестру. Контроль целостности системы обнаруживает изменения в файлах и реестре в заданной *области мониторинга*. Область мониторинга является одним из критериев правила Контроля целостности системы. Вы можете настроить общие правила для Контроля целостности системы в режиме реального времени и задачи *Проверка целостности системы* или создать отдельные правила для задачи. Kaspersky Endpoint Security применяет область мониторинга из задачи *Проверка целостности системы* к задаче *Обновление снимка состояния системы* для создания снимка состояния системы.

Создание и обновление снимка состояния системы

Для работы задачи *Проверка целостности системы* вам нужно создать снимок состояния системы. *Снимок состояния системы* – зафиксированное состояние объектов системы, с которым приложение сравнивает текущее состояние. Если текущее состояние системы отличается от состояния системы, зафиксированного в снимке состояния системы, Kaspersky Endpoint Security формирует соответствующее событие. Вы можете создать и обновить снимок состояния системы с помощью задачи *Обновление снимка состояния системы*.

Вы можете обновлять список состояния системы в следующих режимах:

- Полное обновление.

  Приложение обновляет все объекты из области мониторинга.

- Инкрементальное обновление.

  Приложение обнаруживает и обновляет только измененные или новые объекты.

► *Как создать и обновить снимок состояния системы в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (12.12)** → **Обновление снимка состояния системы**.

Шаг 2. Выбор режима обновления снимка состояния системы

Выберите режим обновления снимка состояния системы:

- **Полное обновление**. Приложение обновляет все объекты из области мониторинга.
- **Инкрементальное обновление**. Приложение обнаруживает и обновляет только измененные или новые объекты.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Снимок состояния системы 2024*.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:
   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 12.12.0**.
   b. В раскрывающемся списке **Тип задачи** выберите **Обновление снимка состояния системы**.
   c. В поле **Название задачи** введите короткое описание, например, *Снимок состояния системы 2024*.
   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.
5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.
6. Завершите работу мастера.

   В списке задач отобразится новая задача.
7. Нажмите на новую задачу.

   Откроется окно свойств задачи.
8. Выберите закладку **Параметры приложения**.
9. Выберите режим обновления снимка состояния системы:
   - **Полное обновление**. Приложение обновляет все объекты из области мониторинга.
   - **Инкрементальное обновление**. Приложение обнаруживает и обновляет только измененные или новые объекты.
10. Сохраните внесенные изменения.
11. Установите флажок напротив задачи.
12. Нажмите на кнопку **Запустить**.

Настройка области мониторинга для задачи Проверка целостности системы

По умолчанию область мониторинга для задачи *Проверка целостности системы* совпадает с областью мониторинга Контроля целостности системы в режиме реального времени (см. раздел "Контроль целостности системы в режиме реального времени" на стр. 280). Вы можете задать отдельную область мониторинга для задачи.

Контроль целостности системы не поддерживает импорт ключей `HKEY_CURRENT_USER` и `HKEY_CURRENT_CONFIG` для задачи *Проверка целостности системы*. Если область мониторинга задачи содержит эти ключи, приложение формирует событие *Область мониторинга содержит некорректные объекты*.

► *Как задать отдельную область мониторинга для задачи Проверка целостности системы в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Контроль безопасности → Контроль целостности системы**.
4. Установите флажок **Контроль целостности системы**.
5. В блоке **Проверка целостности системы** выберите режим настройки задачи **Настройки пользователя**.
6. Настройте мониторинг внешних устройств:
   a. Установите флажок **Следить за устройствами**.
   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*  , *Предупреждение*  , *Критическое*  .

   Контроль целостности системы фиксирует подключенные внешние устройства на момент создания снимка состояния системы. Далее при подключении внешних устройств приложение формирует соответствующее событие. При выполнении задачи *Проверка целостности системы* приложение не отслеживает отключение внешних устройств.
7. Настройте мониторинг файлов и реестра:
   a. Установите флажок **Следить за файлами и реестром**.
   b. Нажмите на кнопку **Настройка**.

      Откроется список правил Контроля целостности системы.
   c. Нажмите на кнопку **Добавить**.

      Вы также можете импортировать правила из другого источника.
   d. Настройте правило Контроля целостности системы (см. таблицу ниже).
8. Сохраните внесенные изменения.

Таблица 18. Параметры правила задачи Проверка целостности системы

Параметр	Описание
Имя правила	Название правила задачи *Проверка целостности системы*.
Уровень важности событий	Kaspersky Endpoint Security регистрирует события изменения файлов и реестра в области мониторинга. Доступны следующие уровни важности событий: *Информационные*  , *Предупреждение*  , *Критические*  .

Параметр	Описание
Область мониторинга	• **Файл**. Список файлов и папок, которые контролирует компонент. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски. Используйте маски: Символ *, который заменяет любой набор символов, в том числе пустой, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:**.txt будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. Два введенных подряд символа * заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:\Folder***.txt будет включать все пути к файлам с расширением txt в папках, вложенных в папку Folder, кроме самой папки Folder. Маска должна включать хотя бы один уровень вложенности. Маска C:***.txt не работает. Символ ?, который заменяет любой один символ, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:\Folder\???.txt будет включать пути ко всем расположенным в папке Folder файлам с расширением txt и именем, состоящим из трех символов. • **Реестр**. Список ключей реестра и значений ключей, которые контролирует компонент. Kaspersky Endpoint Security поддерживает символы * и ? для ввода маски.
Исключения	• **Файл**. Список исключений из области мониторинга. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски. Например, C:\Folder\Application*.log. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга. Используйте маски: Символ *, который заменяет любой набор символов, в том числе пустой, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:**.txt будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. Два введенных подряд символа * заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:\Folder***.txt будет включать все пути к файлам с расширением txt в папках, вложенных в папку Folder, кроме самой папки Folder. Маска должна включать хотя бы один уровень вложенности. Маска C:***.txt не работает. Символ ?, который заменяет любой один символ, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска C:\Folder\???.txt будет включать пути ко всем расположенным в папке Folder файлам с расширением txt и именем, состоящим из трех символов. • **Реестр**. Список исключений из области мониторинга. Kaspersky Endpoint Security поддерживает символы * и ? для ввода маски. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга.

Запуск задачи Проверка целостности системы

Задача *Проверка целостности системы* позволяет проверять изменения в файлах, реестре, а также контролировать подключение внешних устройств. Для контроля изменений файлов вы можете запустить задачу *Проверка целостности системы* в следующих режимах:

- Быстрая проверка.

  При проверке изменений в файлах приложение проверяет только атрибуты файлов. Изменения в содержании файлов приложение не проверяет.

- Полная проверка.

  При проверке изменений в файлах приложение проверяет все атрибуты и содержание файлов.

Режим запуска задачи не влияет на контроль приложением реестра или внешних устройств.

► *Как запустить задачу Проверка целостности системы в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте его указаниям.

3. Выберите **Kaspersky Endpoint Security → Мониторинг целостности системы на основе эталона**. Выберите режим мониторинга целостности системы:

   - **Полная проверка**. В этом режиме приложение проверяет все атрибуты и хеши файлов.
   - **Быстрая проверка**. В этом режиме приложение проверяет только атрибуты файлов.

4. Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

   - Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
   - Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
   - Задать выборку устройств, для которой требуется запускать задачу.
   - Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.
6. Настройте расписание запуска задачи, например, вручную или в определенный день недели.
7. Введите название задачи.
8. Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Для успешного выполнения задачи *Проверка целостности системы* требуется, чтобы снимок состояния системы полностью соответствовал области мониторинга задачи *Проверка целостности системы*. Если область мониторинга отличается, задача завершается с ошибкой. Для синхронизации областей мониторинга запустите задачу *Обновление снимка состояния системы* с новой областью мониторинга.

kaspersky

Просмотр отчетов о работе Контроля целостности системы

Для анализа работы правил Контроля целостности системы вы можете изучать отчеты, а также просматривать события, сформированные приложением. Kaspersky Endpoint Security формирует следующие отчеты о работе компонента:

- В интерфейсе приложения (см. раздел "Работа с отчетами" на стр. 342):
  - Отчет Контроль целостности системы.
  - Отчет Проверка целостности системы.
  - Отчет Обновление снимка состояния системы.

  Отчеты содержат события о работе Контроля целостности системы.
- В консоли Kaspersky Security Center:
  - Отчет о компьютерах, на которых произошло максимальное количество срабатываний правил мониторинга.
  - Отчет о наиболее часто срабатывающих правилах мониторинга.

  По умолчанию отчет создается за последние 30 дней, включая дату создания отчета.

Как просмотреть отчеты о работе Контроля целостности системы в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. На шаге **Выбор типа шаблона отчета** выберите отчет о работе Контроля целостности системы (раздел **Другое**):
   - **Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего**.
   - **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах**.

   После завершения работы мастера создания шаблона отчета в таблице на закладке **Отчеты** появится новый шаблон отчета.
5. Откройте отчет двойным щелчком мыши.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Также вы можете просматривать события, сформированные приложением, в консоли Kaspersky Security Center с помощью выборок событий.

kaspersky

Сброс статуса целостности системы

Компьютеры в консоли Kaspersky Security Center имеют статус: *ОК*  , *Предупреждение*  или *Критический*  . Если Контроль целостности системы обнаруживает изменения файлов или реестра в области мониторинга, компьютер меняет статус на *Предупреждение* или *Критический*. Статус, назначенный Контролем целостности системы, называется *статусом целостности системы*. Вы можете сбросить статус целостности системы, если, например, после анализа вы убедились в том, что обнаруженные изменения объектов не влияют на безопасность компьютера.

► *Как сбросить статус целостности системы в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (12.12)** → **Сброс статуса целостности системы**.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Сброс статуса после изменения области мониторинга*.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

В результате, если причиной изменения статуса компьютера на *Предупреждение* или *Критический* были события Контроля целостности системы, статус компьютера будет изменен на *ОК*. Если статус компьютера был изменен также по причине других событий, статус компьютера останется прежним.

Анализ журналов

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций.

Начиная с версии Kaspersky Endpoint Security для Windows 11.11.0 добавлена поддержка компонента Анализ журналов. Анализ журналов контролирует целостность защищаемой среды на основе журналов событий Windows. При обнаружении признаков нетипичного поведения в системе приложение информирует администратора, так как это поведение может указывать на попытки кибератак.

Kaspersky Endpoint Security анализирует журналы событий Windows и выявляет нарушения в соответствии с правилами. В компонент включены предустановленные правила (см. раздел "Настройка предустановленных правил" на стр. 292). Для работы предустановленных правил приложение использует эвристический анализ. Также вы можете добавить собственные правила (см. раздел "Добавление пользовательских правил" на стр. 293) (пользовательские правила). При срабатывании правила, приложение создает событие со статусом *Критическое* (см. рис. ниже).

Для работы Анализа журналов убедитесь, что параметры политики аудита безопасности настроены и система регистрирует нужные события (подробнее см. на сайте Службы технической поддержки Microsoft https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/audit-policy).

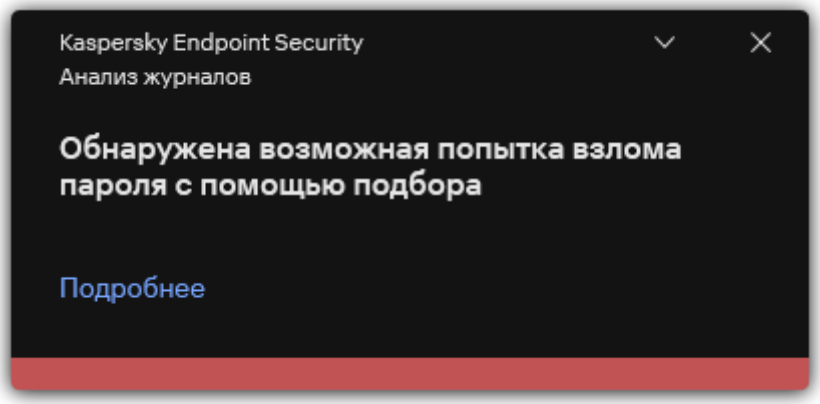


Рисунок 64. Уведомление Анализа журналов

В этом разделе

Настройка предустановленных правил 292
Добавление пользовательских правил 293

kaspersky

Настройка предустановленных правил

Предустановленные правила включают шаблоны аномальной активности на защищаемом компьютере. Аномальная активность может являться признаком попытки атаки. Для работы предустановленных правил приложение использует эвристический анализ. Для Анализа журналов доступно семь предустановленных правил. Вы можете включать и выключать любые правила. Удалить предустановленные правила невозможно.

Вы можете настроить критерии срабатывания правил, которые контролируют события для следующих операций:

- обработка подбора пароля;
- обработка сетевого входа.

► *Как настроить предустановленные правила в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Анализ журналов**.
3. Убедитесь, что переключатель **Анализ журналов** включен.
4. В блоке **Предустановленные правила** нажмите на кнопку **Настроить**.
5. Настройте работу предустановленных правил с помощью флажков:
   - **Обнаружена возможная попытка взлома пароля с помощью подбора**.
   - **Обнаружена подозрительная активность во время сетевого сеанса входа**.
   - **Обнаружены признаки компрометации журналов Windows**.
   - **Обнаружена подозрительная активность со стороны новой установленной службы**.
   - **Обнаружена подозрительная аутентификация с явным указанием учетных данных**.
   - **Обнаружены признаки атаки Kerberos forged PAC (MS14-068)**.

   a. **Обнаружены подозрительные изменения привилегированной группы Администраторы**.
6. Если требуется, настройте параметры правила **Обнаружена возможная попытка взлома пароля с помощью подбора**:
   a. Нажмите **Настройка** под правилом.
   b. В открывшемся окне укажите количество попыток и промежуток времени, в течение которого выполнялись попытки ввода пароля, для срабатывания правила.
7. Если вы выбрали правило **Обнаружена подозрительная активность во время сетевого сеанса входа**, вам нужно настроить параметры правила:
   a. Нажмите **Настройка** под правилом.
   b. В блоке **Обработка атипичной аутентификации** укажите начало и конец временного интервала.

      Kaspersky Endpoint Security будет считать аномальной активностью выполненные попытки входа в течение заданного интервала.

      По умолчанию интервал не задан и приложение не контролирует попытки входа. Чтобы приложение постоянно контролировало попытки входа, задайте интервал 12:00 AM – 11:59 PM. Начало и конец интервала не должны совпадать. Если они совпадают, приложение не контролирует попытки входа.

c. В блоке **Исключения** добавьте доверенных пользователей и доверенные IP-адреса компьютеров (IPv4 и IPv6).

Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно (см. раздел "Приложение 11. Учетные записи пользователей в правилах компонентов приложения" на стр. 489). Kaspersky Endpoint Security не будет контролировать попытки входа для этих пользователей и компьютеров.

8. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security при срабатывании правила будет создавать события со статусом *Критическое событие*.

Добавление пользовательских правил

Вы можете задать собственные критерии срабатывания правила Анализа журналов. Для этого вам нужно ввести идентификатор события и выбрать источник событий. Вы можете узнать идентификатор события на сайте Службы технической поддержки Microsoft https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor. Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*. Также вы можете указать журнал стороннего приложения. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал *Windows PowerShell*).

Приложение не выполняет проверок на фактическое наличие заданного журнала в журнале событий Windows. Если название журнала введено с ошибкой, приложение не будет контролировать события из этого журнала.

В список пользовательских правил уже добавлено три правила, которые созданы специалистами "Лаборатории Касперского".

► *Как добавить пользовательское правило в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Анализ журналов**.
3. Убедитесь, что переключатель **Анализ журналов** включен.
4. В блоке **Пользовательские правила** нажмите на кнопку **Настроить**.
5. В открывшемся окне установите флажки напротив тех пользовательских правил, которые вы хотите включить.
6. Если требуется, создайте собственные пользовательские правила по кнопке **Добавить**.
7. В открывшемся окне настройте параметры пользовательского правила:
   - **Название правила**.
   - **Имя журнала**. Журналы событий Windows. Доступны следующие журналы: *Application*, *Security*, *System*.

- **Источник**. Журналы событий сторонних приложений. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал *Windows PowerShell*).
- **Идентификатор событий**. Идентификаторы событий в журнале событий Windows. Вы можете узнать идентификатор события в справке Microsoft https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor.

8. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security при срабатывании правила будет создавать события со статусом *Критическое*.

kaspersky

Endpoint Detection and Response Optimum

Встроенный агент Endpoint Detection and Response Optimum (EDR Optimum) в составе приложения Kaspersky Endpoint Security доступен только в составе решения Kaspersky Endpoint Detection and Response Optimum. Для работы встроенного агента EDR Optimum необходимо активировать приложение с помощью лицензии, которая включает в себя эту функциональность.

Для работы решения Kaspersky Endpoint Detection and Response Optimum в приложение добавлен встроенный агент. Встроенный агент EDR Optimum предоставляет *Сотруднику службы безопасности* или *Администратору* информацию о потенциальной атаке, необходимую для принятия своевременных действий по реагированию. В качестве действий по реагированию встроенный агент позволяет изолировать компьютер от сети, блокировать запуск объектов, завершать процессы, а также выполнять другие действия. Для обнаружения угроз встроенные агент EDR Optimum выполняет поиск индикаторов компрометации. *Индикатор компрометации (Indicator of Compromise, IOC)* – набор данных об объекте или активности, который указывает на несанкционированный доступ к компьютеру (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача *Поиск IOC* позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

В этом разделе

Интеграция с Kaspersky Endpoint Detection and Response 295
Поиск индикаторов компрометации (стандартная задача) 298
Расширенный сбор телеметрии для поиска IOC 303
Помещение файла на карантин 304
Получение файла 306
Удаление файла 308
Запуск процесса 309
Завершение процесса 310
Запрет запуска объектов 312
Сетевая изоляция компьютера 315

Интеграция с Kaspersky Endpoint Detection and Response

Для интеграции с Kaspersky Endpoint Detection and Response Optimum вам нужно добавить компонент Endpoint Detection and Response Optimum (EDR Optimum) и настроить параметры Kaspersky Endpoint Security.

Компоненты EDR Optimum, EDR Expert и EDR (KATA) несовместимы между собой.

Для работы Endpoint Detection and Response Optimum должны быть выполнены следующие условия:

- Kaspersky Security Center версии 13.2 или выше. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Endpoint Detection and Response Optimum.
- Плагин управления Kaspersky Endpoint Detection and Response.

  Начиная с Kaspersky Endpoint Security версии 12.6 отображение деталей алерта перенесено из плагина управления Kaspersky Endpoint Security в плагин управления EDR. Плагин управления EDR является единым плагином для работы с агентами на операционных системах Windows, Mac и Linux. Теперь для работы с EDR Optimum вам нужен плагин управления Kaspersky Endpoint Security для создания задач реагирования на угрозы и плагин управления EDR для просмотра деталей алерта.
- Компонент EDR Optimum в составе Kaspersky Endpoint Security поддерживает работу с решением Kaspersky Endpoint Detection and Response Optimum версии 2.0. Работа с решением Kaspersky Endpoint Detection and Response Optimum версии 1.0 не поддерживается.
- Управление EDR Optimum доступно в Kaspersky Security Center Web Console. Управлять функциональностью в Консоли администрирования (MMC) невозможно.
- Приложение активировано и функциональность входит в лицензию.
- Компонент Endpoint Detection and Response включен.
- Компоненты приложения, которые обеспечивают работу Endpoint Detection and Response Optimum, включены и работают. Работу Endpoint Detection and Response Optimum обеспечивают следующие компоненты:
  - Защита от файловых угроз (см. раздел "Включение и выключение Защиты от файловых угроз" на стр. 139).
  - Защита от веб-угроз (см. раздел "Включение и выключение Защиты от веб-угроз" на стр. 152).
  - Защита от почтовых угроз (см. раздел "Включение и выключение Защиты от почтовых угроз" на стр. 159).
  - Защита от эксплойтов (см. раздел "Включение и выключение Защиты от эксплойтов" на стр. 124).
  - Анализ поведения (на стр. 115).
  - Предотвращение вторжений (см. раздел "Включение и выключение Предотвращения вторжений" на стр. 128).
  - Откат вредоносных действий (на стр. 122).
  - Адаптивный контроль аномалий (см. раздел "Обучение Адаптивного контроля аномалий" на стр. 244).

Интеграция с Kaspersky Endpoint Detection and Response Optimum состоит из следующих этапов:

1. Установка компонента Endpoint Detection and Response Optimum

   Вы можете выбрать компонент EDR Optimum во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

   Для завершения обновления приложения с новыми компонентами нужно перезагрузить компьютер.

a. **Активация Kaspersky Endpoint Detection and Response Optimum**

Вы можете приобрести лицензию на использование Kaspersky Endpoint Detection and Response Optimum следующими способами:

- Функциональность Endpoint Detection and Response Optimum включена в состав лицензии на использование Kaspersky Endpoint Security для Windows.

  Функциональность будет доступна сразу после активации Kaspersky Endpoint Security для Windows.

- Приобретение отдельной лицензии на использование EDR Optimum (Kaspersky Endpoint Detection and Response Optimum Add-on).

  Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response Optimum. В результате на компьютере будет установлено два ключа: ключ для Kaspersky Endpoint Security и ключ для Kaspersky Endpoint Detection and Response Optimum.

  Лицензирование отдельной функциональности Endpoint Detection and Response Optimum не отличается от лицензирования Kaspersky Endpoint Security.

Убедитесь, что функциональность EDR Optimum включена в лицензию и работает в локальном интерфейсе приложения.

b. **Включение компонента Endpoint Detection and Response**

Вы можете включить или выключить компонент в настройках политики Kaspersky Endpoint Security для Windows.

Как включить или выключить компонент Endpoint Detection and Response в Web Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Включите переключатель **Endpoint Detection and Response ВКЛЮЧЕН**.
6. Сохраните внесенные изменения.

   В результате компонент Endpoint Detection and Response будет включен. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах (см. раздел "Просмотр отчетов" на стр. 343). В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Endpoint Detection and Response Optimum**.

c. **Включение передачи данных на Сервер администрирования**

Для работы всех функций Endpoint Detection and Response Optimum должна быть включена передача следующих данных:

- Данные о файлах карантина.

  Данные нужны для получения информации о помещенных на компьютере файлах на карантин в Web Console. В Web Console вы можете, например, загрузить файл из карантина на компьютер для анализа.

- Данные о цепочке развития угрозы.

  Данные нужны для получения информации об обнаруженных на компьютере угрозах в Web

Console. В Web Console вы можете просматривать детали обнаружения и выполнять действия по реагированию.

Как включить передачу данных на Сервер администрирования в Web Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Отчеты и хранилище**.
5. В блоке **Передача данных на Сервер администрирования** установите следующие флажки:
   - **О файлах карантина**.
   - **О цепочке развития угрозы**.
6. Сохраните внесенные изменения.

Поиск индикаторов компрометации (стандартная задача)

Индикатор компрометации (Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к компьютеру (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача *Поиск IOC* позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

Для поиска индикаторов компрометации Kaspersky Endpoint Security использует IOC-файлы. *IOC-файлы* – файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. IOC-файлы должны соответствовать стандарту описания OpenIOC.

Режим запуска задачи Поиск IOC

Kaspersky Endpoint Detection and Response позволяет создавать стандартные задачи поиска IOC для обнаружения компрометации данных. *Стандартная задача поиска IOC* – групповая или локальная задача, которые создаются и настраиваются вручную в Web Console. Для запуска задач используются IOC-файлы, подготовленные пользователем. Если вы хотите добавить индикатор компрометации вручную, ознакомьтесь с требованиями к IOC-файлам.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC.

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX
https://support.kaspersky.com/Help/KESWin/12.12/IOC_Terms/IOC_TERMS.xlsx

Kaspersky Endpoint Security также поддерживает автономные задачи поиска IOC при работе приложения в составе решения Kaspersky Sandbox.

Создание IOC-файла

Начиная с версии Kaspersky Endpoint Security для Windows 12.10 добавлена возможность создавать IOC-файлы прямо в свойствах задачи. Для создания IOC-файла вам нужно подготовить TXT-файл со списком индикаторов компрометации. В качестве индикаторов компрометации вы можете добавить списки следующих объектов:

- Хеши файлов (MD5 / SHA256).

  Приложение подготовит IOC-файл с областью поиска FileItem/Md5sum или FileItem/Sha256sum.

- IP-адреса (IPv4, IPv6).

  Приложение подготовит IOC-файл с областью поиска PortItem/RemoteIP.

- DNS-имена.

  Приложение подготовит IOC-файл с областью поиска DnsEntryItem/RecordName.

Как создать IOC-файл в Web Console

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Выберите задачу **Поиск IOC**.

   Откроется окно свойств задачи. Если требуется, создайте задачу **Поиск IOC**.

3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Настройки поиска IOC**.
5. Нажмите на кнопку **Переопределить IOC-файлы**.
6. Откроется форма для создания IOC-файла:

   a. В блоке **Источник IOC-файлов** выберите **Создать из файла**.
   b. Введите имя для IOC-файла.
   c. Выберите TXT-файл со списком индикаторов компрометации.
   d. Выберите тип IOC-файла: **DNS-имена**, **Хеши файлов**, **IP-адреса**.
   e. Нажмите на кнопку **Создать**.

   Kaspersky Endpoint Security добавит IOC-файлы в IOC-коллекцию. Если требуется, вы можете временно выключить IOC-файлы из области действия задачи.

7. Сохраните внесенные изменения.

Создание задачи Поиск IOC

Вы можете создавать задачи *Поиск IOC* вручную следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали обнаружения – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали обнаружения содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями обнаружения см. в справке Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).

- С помощью мастера создания задач.

Вы можете настроить параметры задачи только в Web Console.

► *Чтобы создать задачу Поиск IOC, выполните следующие действия:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 12.12.0**.

   b. В раскрывающемся списке **Тип задачи** выберите **Поиск IOC**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Перейдите к следующему шагу.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

   У системной учетной записи (SYSTEM) отсутствуют права на выполнение задачи *Поиск IOC* на сетевых дисках. Если вы хотите выполнить задачу на сетевом диске, выберите учетную запись пользователя, у которого есть доступ к этому диску.

   Для работы автономных задач поиска IOC на сетевых дисках вам нужно вручную выбрать учетную запись пользователя, у которого есть доступ к этом диску, в свойствах задачи.

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите закладку **Параметры приложения**.

9. Перейдите в раздел **Настройки поиска IOC**.

10. Загрузите IOC-файлы для поиска индикаторов компрометации.

    После загрузки IOC-файлов приложение покажет сводную информацию о файле, включая список индикаторов, которые не прошли проверку. После загрузки IOC-файлов вы можете вручную изменять содержание файлов во встроенном редакторе прямо в свойствах задачи. Kaspersky Endpoint Security поддерживает изменение содержания IOC-файлов, которые соответствуют стандарту OpenIOC версии 1.1. Изменить содержание IOC-файлов, соответствующие стандарту OpenIOC версии 1.0, невозможно.

    Kaspersky Endpoint Security добавит IOC-файлы в IOC-коллекцию. Если требуется, вы можете временно выключить IOC-файлы из области действия задачи.

Не рекомендуется добавлять или удалять IOC-файлы после запуска задачи. Это может привести к некорректному отображению результатов поиска IOC для предыдущих запусков задачи. Для поиска индикаторов компрометации по новым IOC-файлам рекомендуется добавлять новые задачи.

11. Настройте действия при обнаружении индикатора компрометации:

    - **Изолировать компьютер от сети**. Если выбран этот вариант действия, то Kaspersky Endpoint Security изолирует компьютер от сети для предотвращения распространения угрозы. Вы можете настроить время изоляции в параметрах компонента Endpoint Detection and Response.

      Если флажок снят, вы можете изолировать компьютер от сети после выполнения задачи вручную. Если в результате выполнения задачи *Поиск IOC* обнаружен IOC, то вы можете изолировать компьютер от сети прямо из результатов поиска IOC (свойства задачи *Поиск IOC* → **Параметры приложения** → **Результаты поиска IOC**). Также Kaspersky Endpoint Security позволяет сразу настроить дополнительные параметры: период выключения Сетевой изоляции и исключения из Сетевой изоляции.

    - **Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин.

      Если флажок снят, вы можете поместить файл на карантин после выполнения задачи вручную. Если в результате выполнения задачи *Поиск IOC* обнаружен файл, который может вызывать компрометацию данных, то вы можете поместить этот файл на карантин прямо из результатов поиска IOC (**Параметры приложения** → **Результаты поиска IOC**). В результате Kaspersky Endpoint Security запустит мастер создания задач с предустановленными данными об обнаруженном файле. Вам нужно только настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

    - **Запустить проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей* (см. раздел "*Поиск вредоносного ПО*" на стр. 62). По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

12. Перейдите в раздел **Дополнительно**.

13. Выберите типы данных (IOC-документы), которые необходимо анализировать во время выполнения задачи.

    Kaspersky Endpoint Security автоматически выбирает типы данных (IOC-документы) для задачи *Поиск IOC* в соответствии с содержанием загруженных IOC-файлов. Не рекомендуется самостоятельно отменять выбор типов данных.

    В сертифицированной конфигурации программы исключите из анализа тип данных **История браузера - UrlHistoryItem**.

Дополнительно вы можете настроить области поиска для следующих типов данных:

- **Файлы - FileItem**. Задайте область поиска IOC на компьютере с помощью предустановленных областей.

  По умолчанию Kaspersky Endpoint Security выполняет поиск IOC только в важных областях компьютера, таких как папки Загрузки, Рабочий стол, папка с временными файлами операционной системы и другие. Также вы можете добавить области поиска вручную.

- **Журналы событий Windows - EventLogItem**. Задайте период времени, в течение которого зафиксированы события. Также вы можете выбрать журналы событий Windows для поиска IOC. По умолчанию выбраны следующие журналы событий: журнал событий приложений, журнал системных событий и журнал событий безопасности.

- **Реестр Windows - RegistryItem**. Задайте область поиска IOC в реестре.

  По умолчанию Kaspersky Endpoint Security анализирует определенный набор разделов реестра (см. раздел "Приложение 9. Область поиска IOC в реестре (RegistryItem)" на стр. 485).

14. В окне свойств задачи выберите закладку **Расписание**.
15. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

16. Сохраните внесенные изменения.
17. Установите флажок напротив задачи.
18. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security запустит поиск индикаторов компрометации на компьютере. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**. Информацию об обнаруженных индикаторах компрометации вы можете посмотреть в свойствах задачи **Параметры приложения → Результаты поиска IOC**. Также в результатах поиска IOC вы можете вручную поместить обнаруженный файл на карантин (см. раздел "Помещение файла на карантин" на стр. 304) или изолировать компьютер от сети (см. раздел "Сетевая изоляция компьютера" на стр. 315).

Kaspersky Endpoint Security выполняет поиск дубликатов среди записей, полученных по одному IOC-файлу, и сохраняет в результатах задачи только уникальные записи. Дубликатами считаются записи одного типа, у которых совпадают значения всех сравниваемых полей. Также приложение может не создавать записи при отсутствии у них значений одного или нескольких полей (см. таблицу ниже).

Таблица 19.

Тип	Сравниваемые поля	Условие, при котором запись не создается
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• У записи отсутствуют значения полей FullPath, Md5sum, Sha256sum. • У записей отсутствует значение поля FullPath и совпадают значения полей Md5sum, Sha256sum.

Тип	Сравниваемые поля	Условие, при котором запись не создается
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	У записи отсутствует значение какого-либо из следующих полей: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	У записи отсутствуют значения полей startTime или PID.

В окне **Детали алерта** могут присутствовать записи RegistryItem с одинаковыми значениями полей. Данные записи не являются дубликатами, так как различаются значением поля Text, не отображающегося в интерфейсе.
Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет старые записи.

Расширенный сбор телеметрии для поиска IOC

Для ретроспективного поиска IOC (см. раздел "Поиск индикаторов компрометации (стандартная задача)" на стр. 298) рекомендуется включить расширенный сбор телеметрии на компьютере. Расширенный сбор телеметрии позволяет более точно определять индикаторы компрометации, но требует больше ресурсов компьютера.

Расширенный сбор телеметрии дополнительно включает в себя поддержку следующих терминов:

- FileItem/Md5sum;
- FileItem/Sha256sum;
- FileItem/SizeInBytes;
- FileItem/Created;
- FileItem/Modified;
- FileItem/Changed;
- FileItem/Accessed;
- FileItem/FileAttributes.

Если расширенный сбор телеметрии выключен, то Kaspersky Endpoint Security может выполнять ротацию данных об обнаруженных индикаторах компрометации.

► *Чтобы включить расширенный сбор телеметрии, выполните следующие действия:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response** и нажмите **Настроить**.
5. Установите флажок **Включить расширенное логирование активности в системе**.
6. Сохраните внесенные изменения.

Помещение файла на карантин

При реагировании на угрозы Kaspersky Endpoint Detection and Response может создавать задачи *Помещение файла на карантин*. Это нужно, чтобы минимизировать последствия угрозы. *Карантин* – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Endpoint Security использует карантин при работе с решениями Kaspersky Endpoint Detection and Response Optimum. В остальных случаях Kaspersky Endpoint Security помещает файл в резервное хранилище (см. раздел "Работа с резервным хранилищем" на стр. 332). Подробнее о работе с карантином в составе решения см. в Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).

Вы можете создавать задачи *Помещение файла на карантин* следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали обнаружения – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали обнаружения содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями обнаружения см. в справке Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).
- С помощью мастера создания задач.

  Вам нужно ввести путь к файлу или хеш файла (SHA256 или MD5), или путь к файлу и хеш файла.
- В свойствах задачи *Поиск IOC*.

  Если в результате выполнения задачи *Поиск IOC* обнаружен файл, который может вызывать компрометацию данных, то вы можете поместить этот файл на карантин прямо из результатов поиска IOC (**Параметры приложения** → **Результаты поиска IOC**). В результате Kaspersky Endpoint Security запустит мастер создания задач с предустановленными данными об обнаруженном файле. Вам нужно только настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

Задача *Помещение файла на карантин* имеет следующие ограничения:

1. Размер файла не должен превышать 100 МБ.
2. Критически важные системные объекты (англ. System Critical Object, SCO) поместить на карантин невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.

3. Вы можете настроить параметры задачи только в Web Console.
4. Невозможно выполнить проверку объекта, помещенного на карантине в результате выполнения задачи *Помещение файла на карантин*.

► *Чтобы создать задачу Помещение файла на карантин, выполните следующие действия:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. Настройте параметры задачи:
   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 12.12.0**.
   b. В раскрывающемся списке **Тип задачи** выберите **Помещение файла на карантин**.
   c. В поле **Название задачи** введите короткое описание задачи.
   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.
5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).
6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.
7. Нажмите на новую задачу.

   Откроется окно свойств задачи.
8. Выберите закладку **Параметры приложения**.
9. В списке файлов нажмите на кнопку **Добавить**.

   Запустится мастер добавления файла.
10. Для добавления файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

    Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.
11. В окне свойств задачи выберите закладку **Расписание**.
12. Настройте расписание запуска задачи.

Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

13. Сохраните внесенные изменения.
14. Установите флажок напротив задачи.
15. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security переместит файл в карантин.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Задача *Помещение файла на карантин* может быть завершена с ошибкой *Доступ запрещен*, если вы пытаетесь поместить на карантин запущенный исполняемый файл. Создайте задачу завершения процесса (см. раздел "Завершение процесса" на стр. 310) для этого файла, а затем повторите попытку.

Задача *Помещение файла на карантин* может быть завершена с ошибкой *Недостаточно места в хранилище карантина*, если вы пытаетесь поместить на карантин большой файл. Очистите карантин или увеличьте размер карантина (см. раздел "Настройка максимального размера карантина" на стр. 336). Затем повторите попытку.

Вы можете восстановить файл из карантина или очистить карантин в Web Console. Восстановление объектов доступно на компьютере локально из командной строки (см. раздел "RESTORE. Восстановление файлов из карантина" на стр. 419).

Получение файла

Вы можете получать файлы с компьютеров пользователей. Например, вы можете настроить получение файла журнала событий, который создает стороннее приложение. В результате выполнения задачи файл будет сохранен в карантине (см. раздел "Работа с карантином" на стр. 336). *Карантин* – это специальное локальное хранилище на компьютере. Вы можете загрузить этот файл на компьютер из карантина в Web Console (**Операции** → **Хранилища** → **Карантин**). При этом на компьютере пользователя файл остается в исходной папке.

Размер файла не должен превышать 100 МБ.
Вы можете настроить параметры задачи только в Web Console.

► *Чтобы создать задачу Получение файла, выполните следующие действия:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:
   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 12.12.0**.
   b. В раскрывающемся списке **Тип задачи** выберите **Получение файла**.
   c. В поле **Название задачи** введите короткое описание задачи.
   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.
5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.
7. Нажмите на новую задачу.

   Откроется окно свойств задачи.
8. Выберите закладку **Параметры приложения**.
9. В списке файлов нажмите на кнопку **Добавить**.

   Запустится мастер добавления файла.
10. Для добавления файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

    Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

11. В окне свойств задачи выберите закладку **Расписание**.
12. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

13. Сохраните внесенные изменения.
14. Установите флажок напротив задачи.
15. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security создаст копию файла и поместит копию в карантин. Вы можете загрузить файл из карантина в Web Console.

kaspersky

Удаление файла

Вы можете удаленно удалять файлы с помощью задачи *Удаление файла*. Например, вы можете удаленно удалить файл при реагировании на угрозы.

Задача *Удаление файла* имеет следующие ограничения:

- Критически важные системные объекты (англ. System Critical Object, SCO) удалить невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.
- Вы можете настроить параметры задачи только в Web Console.

► *Чтобы создать задачу Удаление файла, выполните следующие действия:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 12.12.0**.

   b. В раскрывающемся списке **Тип задачи** выберите **Удаление файла**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите закладку **Параметры приложения**.

9. В списке файлов нажмите на кнопку **Добавить**.

   Запустится мастер добавления файла.

10. Для добавления файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

Если файл расположен на сетевом диске, введите путь к файлу начиная с символов \\, а не с буквы диска. Например, \\server\shared_folder\file.exe. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

11. В окне свойств задачи выберите закладку **Расписание**.
12. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

13. Сохраните внесенные изменения.
14. Установите флажок напротив задачи.
15. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security удалит файл с компьютера. Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Задача *Удаление файла* может быть завершена с ошибкой *Доступ запрещен*, если вы пытаетесь удалить запущенный исполняемый файл. Создайте задачу завершения процесса (см. раздел "Завершение процесса" на стр. 310) для этого файла, а затем повторите попытку.

Запуск процесса

Вы можете удаленно запускать файлы с помощью задачи *Запуск процесса*. Например, вы можете удаленно запускать утилиту, которая создает файл с конфигурацией компьютера. Далее с помощью задачи *Получение файла* (см. раздел "*Получение файла*" на стр. 306), вы можете получить созданный файл в Kaspersky Security Center Web Console.

Вы можете настроить параметры задачи только в Web Console.

► *Чтобы создать задачу Запуск процесса, выполните следующие действия:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 12.12.0**.

   b. В раскрывающемся списке **Тип задачи** выберите **Запуск процесса**.

c. В поле **Название задачи** введите короткое описание задачи.

d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.
5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.
7. Нажмите на новую задачу.
8. Откроется окно свойств задачи.
9. Выберите закладку **Параметры приложения**.
10. Введите команду запуска процесса.

    Например, вы хотите запустить утилиту (`utility.exe`), которая сохраняет информацию о конфигурации компьютера в файл `conf.txt` в текущую папку (по умолчанию). Утилита расположена в папке `C:\Users\admin\Diagnostic\`. Конфигурационный файл необходимо сохранить в папке `C:\Users\admin\Documents\Configuration`. Введите следующие значения:

    - **Исполняемая команда** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Аргументы командной строки (необязательно)** – `/R conf.txt`
    - **Путь к рабочей папке (необязательно)** – `C:\Users\admin\Documents\Configuration`
11. В окне свойств задачи выберите закладку **Расписание**.
12. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

13. Сохраните внесенные изменения.
14. Установите флажок напротив задачи.
15. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security выполнит команду в тихом режиме и запустит процесс. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты выполнения**.

kaspersky

Завершение процесса

Вы можете удаленно завершать процессы с помощью задачи *Завершение процесса*. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи *Запуск процесса* (см. раздел "*Запуск процесса*" на стр. 309).

Если вы хотите запретить запуск файла, вы можете настроить компонент Запрет запуска объектов (см. раздел "Запрет запуска объектов" на стр. 312). Вы можете запретить запуск исполняемых файлов, скриптов, файлов офисного формата.

Задача *Завершение процесса* имеет следующие ограничения:

- Завершить процессы критически важных системных объектов (англ. System Critical Object, SCO) невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.
- Вы можете настроить параметры задачи только в Web Console.

► *Чтобы создать задачу Завершение процесса, выполните следующие действия:*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 12.12.0**.

   b. В раскрывающемся списке **Тип задачи** выберите **Завершение процесса**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите закладку **Параметры приложения**.

9. Для завершения процесса вам нужно выбрать файл, работу которого вы хотите завершить. Вы можете выбрать файл следующими способами:
   - Введите полный путь к файлу.
   - Введите хеш файла и путь к файлу.
   - Введите идентификатор процесса PID (только для локальных задач).

   Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.
10. В окне свойств задачи выберите закладку **Расписание**.
11. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.
12. Нажмите на кнопку **Сохранить**.
13. Установите флажок напротив задачи.
14. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security завершит процесс на компьютере. Например, если на компьютере запущено приложение GAME и вы завершили процесс game.exe, приложение будет закрыто без сохранения данных. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**.

Запрет запуска объектов

Запрет запуска объектов позволяет контролировать запуск исполняемых файлов и скриптов, а также открытие файлов офисного формата. Таким образом, вы можете, например, запретить запуск приложений, использование которых считаете небезопасным. В результате распространение угрозы может быть остановлено. Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата (см. раздел "Приложение 7. Поддерживаемые расширения файлов для Запрета запуска объектов" на стр. 481) и определенный набор интерпретаторов скриптов (см. раздел "Приложение 8. Поддерживаемые интерпретаторы скриптов для Запрета запуска объектов" на стр. 483).

Правило запрета запуска

Запрет запуска объектов управляет доступом пользователей к файлам с помощью правил запрета запуска. *Правило запрета запуска* – это набор критериев, которые приложение учитывает при реагировании на запуск объекта, например, при блокировании запуска объекта. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Вы можете создавать правила запрета запуска следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали обнаружения – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали обнаружения содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями обнаружения см. в справке Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).

- С помощью групповой политики или локальных параметров приложения.

  Вам нужно ввести путь к файлу или хеш файла (SHA256 или MD5), или путь к файлу и хеш файла.

Вы также можете управлять Запретом запуска объектов локально из командной строки (см. раздел "PREVENTION. Управление Запретом запуска объектов" на стр. 418).

Запрет запуска объектов имеет следующие ограничения:

1. Правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Приложение не будет блокировать исполнение или открытие этих файлов.
2. Невозможно запретить запуск критически важных системных объектов (англ. System Critical Object, SCO). К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.
3. Не рекомендуется создавать более 5000 правил запрета запуска, поскольку это может привести к нестабильности системы.

Режимы применения правил запрета запуска

Компонент Запрет запуска объектов может работать в двух режимах:

- **Только статистика**.

  В этом режиме Kaspersky Endpoint Security публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

- **Активный**.

  В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска объектов или открытия документов.

Управление Запретом запуска объектов

Вы можете настроить параметры компонента только в Web Console.

Чтобы запретить запуск объектов, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Выберите закладку **Запрет запуска**.
6. Включите переключатель **Запрет запуска ВКЛЮЧЕН**.
7. В блоке **Действие при запуске или открытии объекта** выберите режим работы компонента:
   - **Заблокировать и записать в журнал событий**. В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска объектов или открытия документов.

- **Записать в журнал событий**. В этом режиме Kaspersky Endpoint Security публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

8. Сформируйте список правил запрета запуска:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне введите имя правила запрета запуска (например, *Приложение А*).
   c. В раскрывающемся списке **Тип** выберите объект, который вы хотите заблокировать: **Исполняемый файл**, **Скрипт**, **Файл Microsoft Office**.

      Если вы выберите неверный тип объекта, Kaspersky Endpoint Security не заблокирует файл или скрипт.
   d. Для добавления файла вам нужно ввести хеш файла (SHA256 или MD5) или полный путь к файлу, или хеш файла и путь к файлу.

      > Если файл расположен на сетевом диске, введите путь к файлу начиная с символов \\, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, Kaspersky Endpoint Security не заблокирует файл или скрипт.

      Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата (см. раздел "Приложение 7. Поддерживаемые расширения файлов для Запрета запуска объектов" на стр. 481) и определенный набор интерпретаторов скриптов (см. раздел "Приложение 8. Поддерживаемые интерпретаторы скриптов для Запрета запуска объектов" на стр. 483).
9. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет блокировать запуск объектов: запуск исполняемых файлов, скриптов и открытие файлов офисного формата. При этом вы можете, например, открыть файл скрипта в текстовом редакторе, даже если запуск скрипта запрещен. При блокировании запуска объекта Kaspersky Endpoint Security покажет пользователю стандартное уведомление приложения (см. рис. ниже), если уведомления включены в настройках приложения (см. раздел "Настройка отображения и доставки уведомлений" на стр. 340).

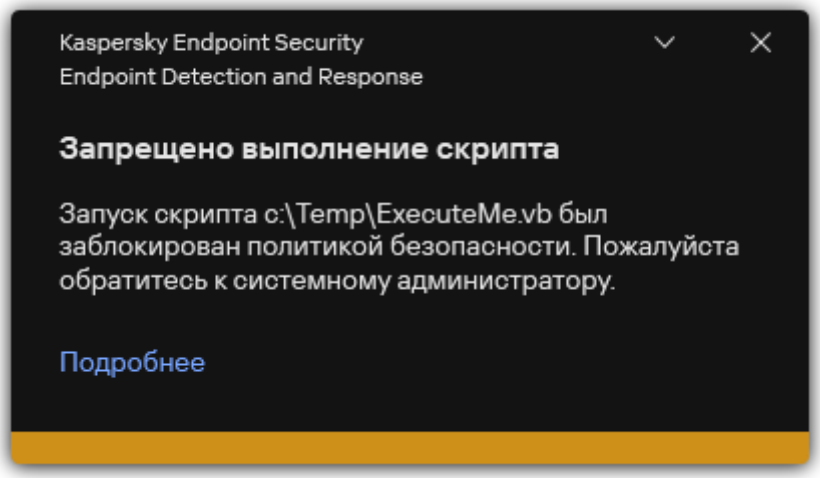


Рисунок 65. Уведомление Запрета запуска объектов

Сетевая изоляция компьютера

Сетевая изоляция позволяет автоматически изолировать компьютеры от сети, в результате реагирования на обнаружение индикатора компрометации (IOC) – *автоматический режим*. Также вы можете включить Сетевую изоляцию вручную на время исследования обнаруженной угрозы – *ручной режим*.

После включения Сетевой изоляции приложение разрывает все активные и блокирует все новые сетевые соединения TCP/IP на компьютере, кроме следующих соединений:

- соединения, указанные в исключениях из Сетевой изоляции;
- соединения, инициированные службами Kaspersky Endpoint Security;
- соединения, инициированные Агентом администрирования Kaspersky Security Center;
- соединения с SVM и Сервером интеграции, если приложение используется в режиме Легкого агента.

Вы можете настроить параметры компонента только в Web Console.

Автоматический режим Сетевой изоляции

Вы можете настроить автоматическое включение Сетевой изоляции, в результате реагирования на обнаружение IOC. Для настройки автоматического режима Сетевой изоляции предназначена групповая политика.

► *Как настроить автоматическое включение Сетевой изоляции компьютера при*

обнаружении IOC

1. В главном окне Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Поиск IOC**.

   Откроется окно свойств задачи.

   Если требуется, создайте задачу *Поиск IOC* (см. раздел "*Поиск индикаторов компрометации (стандартная задача)*" на стр. 298).

3. Выберите закладку **Параметры приложения**.

4. В блоке **Действия при обнаружении IOC** установите флажки **Применять действия по реагированию при обнаружении IOC** и **Изолировать компьютер от сети**.

5. Сохраните внесенные изменения.

В результате при обнаружении IOC приложение изолирует компьютер от сети для предотвращения распространения угрозы.

Вы можете настроить автоматическое выключение Сетевой изоляции по истечении заданного периода времени. По умолчанию приложение выключает Сетевую изоляцию через 8 часов с момента включения. Также вы можете выключить Сетевую изоляцию вручную (см. инструкцию ниже). После выключения Сетевой изоляции компьютер может работать в сети без ограничений.

► *Как задать период выключения Сетевой изоляции компьютера в автоматическом режиме*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Выберите закладку **Сетевая изоляция**.
6. Задайте период времени, по истечении которого Сетевая изоляция должна быть выключена.
7. Сохраните внесенные изменения.

Ручной режим Сетевой изоляции

Вы можете включать или выключать Сетевую изоляцию вручную. Для настройки ручного режима Сетевой изоляции предназначены свойства компьютера в консоли Kaspersky Security Center.

Вы можете включить Сетевую изоляцию следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали обнаружения – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали обнаружения содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями обнаружения см. в справке Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).

- С помощью локальных параметров приложения.
- В свойствах задачи *Поиск IOC*.

  Если в результате выполнения задачи *Поиск IOC* обнаружен IOC, то вы можете изолировать компьютер

от сети прямо из результатов поиска IOC (свойства задачи *Поиск IOC* → **Параметры приложения** → **Результаты поиска IOC**). Также Kaspersky Endpoint Security позволяет сразу настроить дополнительные параметры: период выключения Сетевой изоляции и исключения из Сетевой изоляции.

► *Как вручную включить Сетевую изоляцию компьютера*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите закладку **Приложения**.
4. Нажмите на **Kaspersky Endpoint Security для Windows**.

   Откроются локальные параметры приложения.
5. Выберите закладку **Параметры приложения**.
6. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response**.
7. В блоке параметров **Сетевая изоляция** нажмите на кнопку **Изолировать компьютер от сети**.

Вы можете настроить автоматическое выключение Сетевой изоляции по истечении заданного периода времени. По умолчанию приложение выключает Сетевую изоляцию через 8 часов с момента включения. После выключения Сетевой изоляции компьютер может работать в сети без ограничений.

► *Как задать период выключения Сетевой изоляции компьютера в ручном режиме*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите закладку **Задачи**.

   Откроется список задач, доступных на компьютере.
4. Выберите задачу **Сетевая изоляция**.
5. Выберите закладку **Параметры приложения**.
6. В открывшемся окне задайте период времени, по истечении которого Сетевая изоляция должна быть выключена.
7. Сохраните внесенные изменения.

► *Как вручную выключить Сетевую изоляцию компьютера*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите закладку **Приложения**.
4. Нажмите на **Kaspersky Endpoint Security для Windows**.

   Откроются локальные параметры приложения.
5. Выберите закладку **Параметры приложения**.

6. Перейдите в раздел **Detection and Response → Endpoint Detection and Response**.
7. В блоке параметров **Сетевая изоляция** нажмите на кнопку **Разблокировать изолированный от сети компьютер**.

Вы также можете выключить Сетевую изоляцию локально из командной строки (см. раздел "ISOLATION. Управление Сетевой изоляцией" на стр. 419).

Начиная с версии Kaspersky Endpoint Security для Windows 12.10 добавлена возможность управлять Сетевой изоляцией в деталях алерта. Также в деталях алерта вы можете задавать срок Сетевой изоляции компьютера. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm) и в справке Kaspersky Endpoint Detection and Response Expert (https://support.kaspersky.com/KEDR_Expert/ru-RU/index.htm).

Исключения из Сетевой изоляции

Вы можете задать исключения из Сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на компьютере после включения Сетевой изоляции.

Для настройки исключений из Сетевой изоляции в приложении доступен список *стандартных сетевых профилей*. По умолчанию в исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент. Также вы можете изменить параметры стандартных сетевых профилей или задать исключения вручную (см. инструкцию ниже).

Исключения, заданные в свойствах политики, применяются, только если Сетевая изоляция включена приложением автоматически, в результате реагирования на обнаружение угрозы. Исключения, заданные в свойствах компьютера, применяются, только если Сетевая изоляция включена вручную в свойствах компьютера в консоли Kaspersky Security Center или в деталях алерта.

Активная политика не блокирует применение исключений из Сетевой изоляции, заданных в свойствах компьютера, так как сценарии применения этих параметров разные.

► *Как добавить исключение из Сетевой изоляции в автоматическом режиме*

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response**.
5. Выберите закладку **Сетевая изоляция**.
6. В блоке **Исключения из сетевой изоляции** нажмите **Исключения**.
7. В открывшемся окне нажмите на кнопку **Добавить → Добавить из профиля** и выберите стандартные сетевые профили для настройки исключений.

   Сетевые соединения из профиля будут добавлены в список исключений из Сетевой изоляции. Вы можете просмотреть свойства сетевых соединений. При необходимости, вы можете изменить параметры сетевого соединения.
8. Если требуется, добавьте исключение из Сетевой изоляции вручную. Для этого в окне со списком исключений нажмите на кнопку **Добавить → Добавить** и задайте параметры сетевого соединения

вручную.

9. Сохраните внесенные изменения.

► *Как добавить исключение из Сетевой изоляции в ручном режиме*

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите закладку **Задачи**.

   Откроется список задач, доступных на компьютере.
4. Выберите задачу **Сетевая изоляция**.
5. Выберите закладку **Параметры приложения**.
6. В открывшемся окне нажмите **Исключения**.
7. В открывшемся окне нажмите на кнопку **Добавить из профиля** и выберите стандартные сетевые профили для настройки исключений.

   Сетевые соединения из профиля будут добавлены в список исключений из Сетевой изоляции. Вы можете просмотреть свойства сетевых соединений. При необходимости, вы можете изменить параметры сетевого соединения.
8. Если требуется, добавьте исключение из Сетевой изоляции вручную. Для этого в окне со списком исключений нажмите на кнопку **Добавить** и задайте параметры сетевого соединения вручную.
9. Сохраните внесенные изменения.

Вы также можете просмотреть список исключений из Сетевой изоляции локально из командной строки (см. раздел "ISOLATION. Управление Сетевой изоляцией" на стр. 419). При этом компьютер должен быть изолирован.

Начиная с версии Kaspersky Endpoint Security для Windows 12.10 добавлена возможность добавлять исключения из Сетевой изоляции в деталях алерта. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm) и в справке Kaspersky Endpoint Detection and Response Expert (https://support.kaspersky.com/KEDR_Expert/ru-RU/index.htm).

kaspersky

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые Kaspersky Endpoint Security не контролирует в процессе работы.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от приложений, установленных на компьютере. Включение объектов и приложений в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или приложению, в то время как вы уверены, что этот объект или приложение безвредны. Также администратор может разрешить пользователю формировать собственную локальную доверенную зону для отдельного компьютера. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений и доверенных приложений.

Начиная с версии Kaspersky Endpoint Security для Windows 12.5 вы можете добавить EDR-телеметрию в доверенную зону. Это позволяет оптимизировать данные, которые приложение отправляет на Сервер сбора телеметрии для решения Kaspersky Anti Targeted Attack Platform (EDR).

Начиная с версии Kaspersky Endpoint Security для Windows 12.6 в доверенную зону добавлены предустановленные исключения из проверки (см. раздел "Создание исключения из проверки" на стр. 320) и доверенные приложения (см. раздел "Формирование списка доверенных приложений" на стр. 326). Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах.

Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена установка приложения в режиме Легкого агента для защиты виртуальных сред. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMware.

В этом разделе

Создание исключения из проверки 320

Создание исключения по типу обнаруживаемых объектов 326

Формирование списка доверенных приложений 326

Работа с приложениями, подписанными доверенной цифровой подписью 331

Создание исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие приложения, представляющие угрозу. Исключения из проверки позволяют работать с легальными приложениями, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие приложения сами по себе не имеют вредоносных функций, но эти приложения могут быть использованы злоумышленниками. Подробную информацию о легальных приложениях, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского" https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/.

В результате работы Kaspersky Endpoint Security такие приложения могут быть заблокированы. Чтобы избежать блокирования, для используемых приложений вы можете настроить исключения из проверки. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского". Например, вы часто используете в своей работе приложение Radmin, предназначенное для удаленного управления компьютерами. Такая активность приложения рассматривается Kaspersky Endpoint Security как подозрительная и может быть заблокирована. Чтобы исключить блокировку приложения, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Если у вас на компьютере установлено приложение, выполняющее сбор и отправку информации на обработку, приложение Kaspersky Endpoint Security может классифицировать такое приложение как вредоносное. Чтобы избежать этого, вы можете исключить приложение из проверки, настроив приложение Kaspersky Endpoint Security способом, описанным в этом документе.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач приложения, заданных администратором системы:

- Анализ поведения (см. раздел "Анализ поведения" на стр. 115).
- Защита от эксплойтов (см. раздел "Защита от эксплойтов" на стр. 124).
- Предотвращение вторжений (см. раздел "Предотвращение вторжений" на стр. 127).
- Защита от файловых угроз (см. раздел "Защита от файловых угроз" на стр. 139).
- Защита от веб-угроз (см. раздел "Защита от веб-угроз" на стр. 151).
- Защита от почтовых угроз (см. раздел "Защита от почтовых угроз" на стр. 158).
- Задача *Поиск вредоносного ПО* (см. раздел "*Поиск вредоносного ПО*" на стр. 62).

Kaspersky Endpoint Security не проверяет объект, если при запуске одной из задач проверки в область проверки включен диск, на котором находится объект, или папка, в которой находится объект. Однако при запуске задачи выборочной проверки именно для этого объекта исключение из проверки не применяется.

► *Как создать исключение из проверки в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.

Kaspersky Endpoint Security скрывает для просмотра список исключений из проверки в интерфейсе приложения, если администратор в консоли запретил настройку исключений из проверки ("замок" закрыт) и запретил использование локальных исключений из проверки (флажок **Разрешить использование локальных исключений** снят).

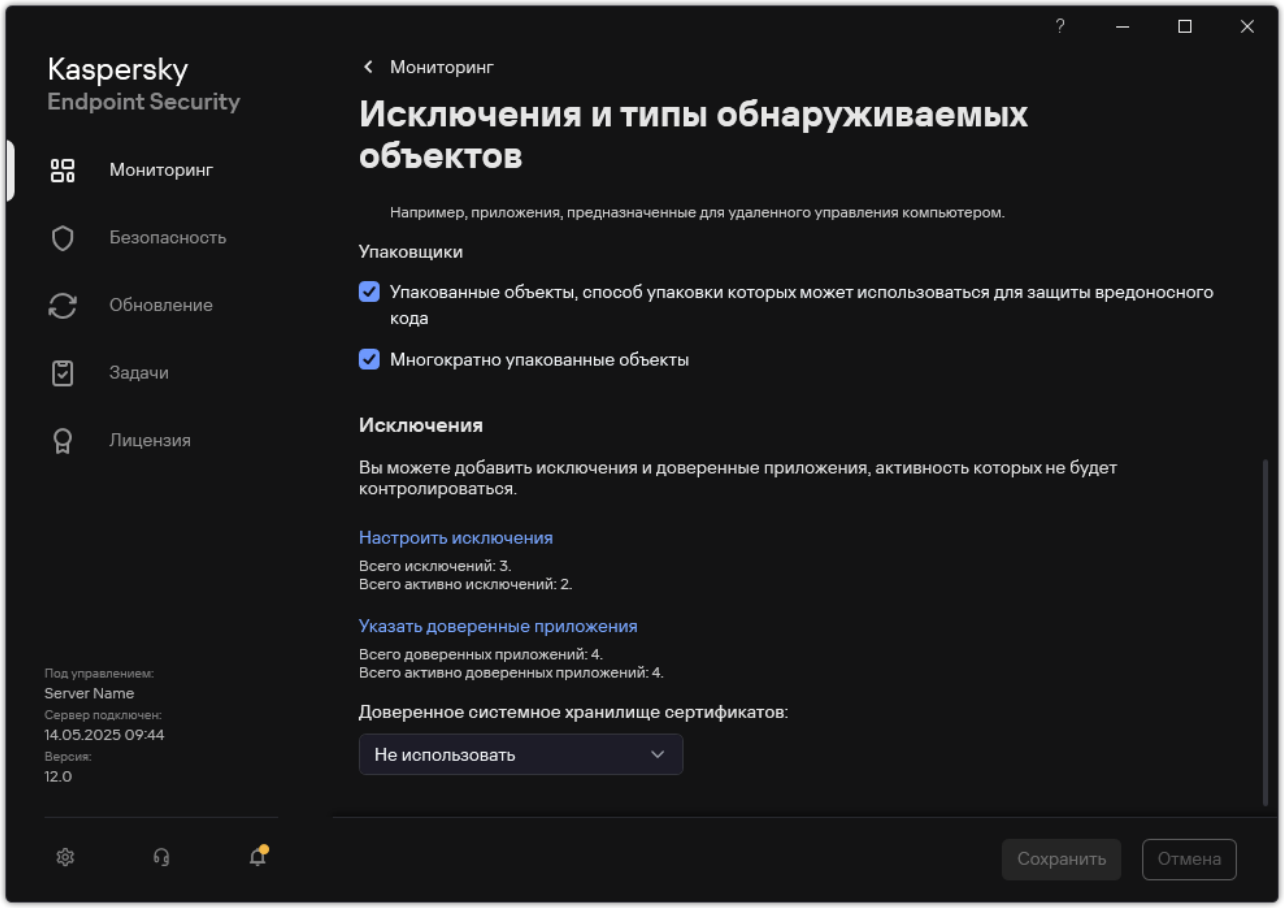


Рисунок 66. Параметры исключений

4. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.
   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое исключение из проверки в корень списка.
   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные исключения из проверки*. Также в приложение добавлены предустановленные исключения из проверки для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные исключения из проверки.

   Для добавления нового исключения из проверки в отдельную категорию установите флажок рядом с этой категорией и выберите вариант **Новое исключение**.

5. Если вы хотите исключить из проверки файл или папку, выберите файл или папку, нажав на кнопку **Обзор**.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски:

   - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
   - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
   - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

     Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

     Вы можете исключать сетевые папки. Для этого введите путь к сетевой папке вручную (например, `\\Network Share\*`).

6. Если вы хотите исключить из проверки тип объектов, в поле **Тип обнаруживаемого объекта** введите название типа объекта по классификации Энциклопедии "Касперского" https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/ (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

   Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Endpoint Security исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

7. Если вы хотите исключить из проверки отдельный файл, в поле **Хеш объекта** введите хеш файла.

   Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

8. В блоке **Компоненты защиты** выберите компоненты, на работу которых должно распространяться исключение из проверки.

9. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

10. Установите статус для исключения **Активно**.

11. Нажмите на кнопку **Добавить**.

    Новое исключение будет добавлено в список. Вы можете в любое время остановить работу исключения с помощью флажка в графе **Статус**.

12. Сохраните внесенные изменения.

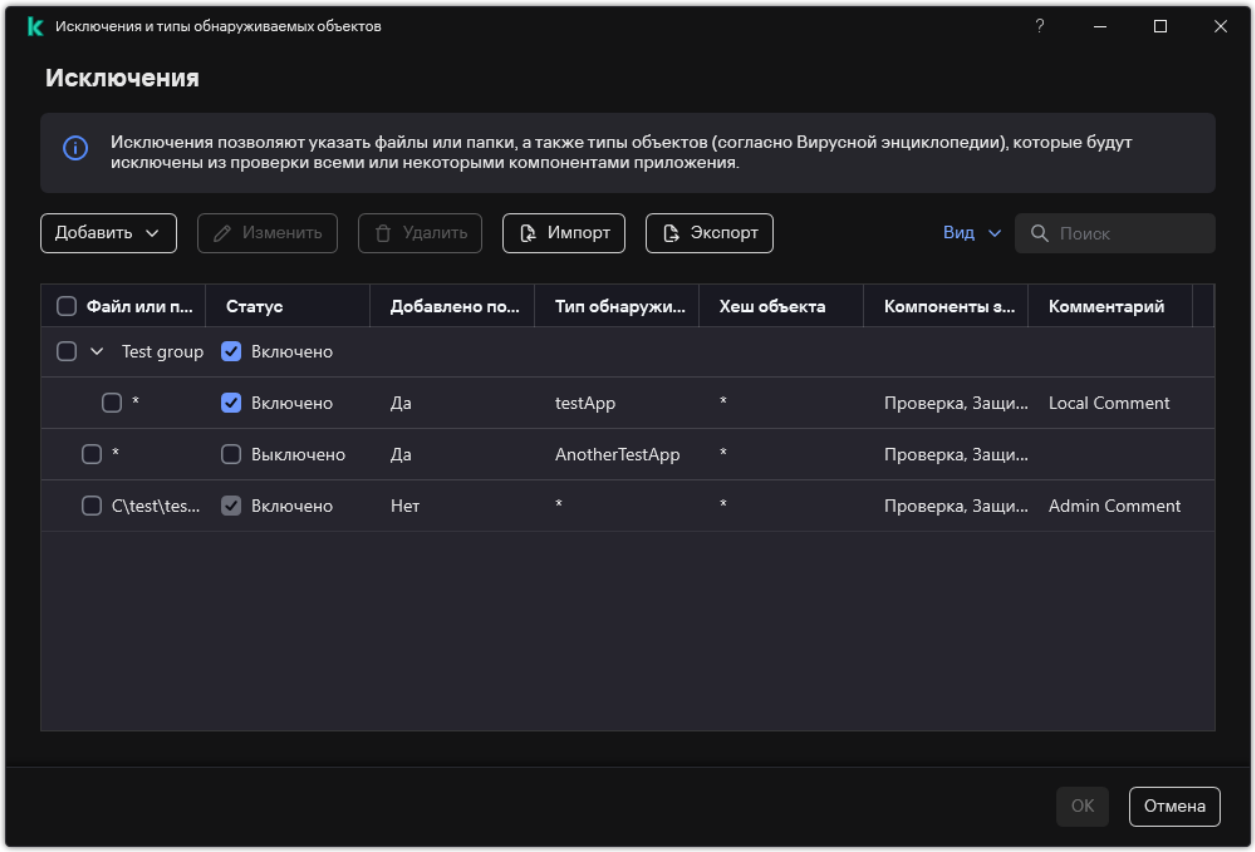


Рисунок 67. Список исключений

Примеры масок пути:

Рекомендуется указывать относительные пути вместо абсолютных. Это позволяет исключить из проверки не только объекты файловой системы, но и безфайловые объекты. Например, `*\Program Files (x86)\Folder\Subfolder`.

Пути к файлам, расположенным в любой из папок:

- Маска `*.exe` будет включать все пути к файлам с расширением exe.
- Маска `example*` будет включать все пути к файлам с именем EXAMPLE.

Пути к файлам, расположенным в указанной папке:

- маска `C:\dir\*.*` будет включать все пути к файлам в папке `C:\dir\`, но не в подпапках папки `C:\dir\`;
- маска `C:\dir\*` будет включать все пути к файлам в папке `C:\dir\`, включая подпапки;
- маска `C:\dir\` будет включать все пути к файлам в папке `C:\dir\`, включая подпапки;
- маска `C:\dir\*.exe` будет включать все пути к файлам с расширением exe в папке `C:\dir\`, но не в подпапках папки `C:\dir\`;
- маска `C:\dir\test` будет включать все пути к файлам с именем test в папке `C:\dir\`, но не в подпапках папки `C:\dir\`;
- маска `C:\dir\*\test` будет включать все пути к файлам с именем test в папке `C:\dir\` и в подпапках папки `C:\dir\`;
- маска `C:\dir1\*\dir3\` будет включать все пути к файлам в подпапках dir3 в папке `C:\dir1\` через один уровень;
- маска `C:\dir1\**\dirN\` будет включать все пути к файлам в подпапках dirN в папке `C:\dir1\` на любом уровне.

Пути к файлам, расположенным во всех папках с указанным именем:

- маска `dir\*.*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*.exe` будет включать все пути к файлам с расширением exe в папках с именем dir, но не в подпапках этих папок;
- маска `dir\test` будет включать все пути к файлам с именем test в папках с именем dir, но не в подпапках этих папок.

kaspersky

Создание исключения по типу обнаруживаемых объектов

Kaspersky Endpoint Security классифицирует обнаруживаемые объекты следующим образом:

- **Вирусы и черви**
- **Троянские приложения (в том числе приложения-вымогатели)**
- **Вредоносные утилиты**
- **Рекламные приложения**
- **Приложения автодозвона**
- **Легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**
- **Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода**
- **Многократно упакованные объекты**

По умолчанию Kaspersky Endpoint Security обнаруживает все типы объектов. Рекомендуется оставить обнаружение всех типов объектов для обеспечения безопасности компьютера. Если вы используете собственные утилиты, которые приложение обнаруживает как вредоносные, добавьте эти утилиты в список исключений (см. раздел "Формирование списка доверенных приложений" на стр. 326), но не выключайте обнаружение этого типа объектов.

► *Как выбрать типы обнаруживаемых объектов в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Типы обнаруживаемых объектов** установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security.
4. Сохраните внесенные изменения.

Формирование списка доверенных приложений

Список доверенных приложений – это список приложений, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активности (в том числе и вредоносную), а также обращения этих приложений к системному реестру. По умолчанию Kaspersky Endpoint Security контролирует объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех приложений и создаваемый ими сетевой трафик. После добавления приложения в список доверенных приложений Kaspersky Endpoint Security перестает контролировать активность приложения.

Отличие исключений из проверки от доверенных приложений заключается в том, что для исключений Kaspersky Endpoint Security не проверяет файлы, а для доверенных приложений инициируемые процессы. То есть, если доверенное приложение создаст вредоносный файл в папке, которая не включена в исключения, Kaspersky Endpoint Security обнаружит этот файл и устранит угрозу. Если папка добавлена в исключения, Kaspersky Endpoint Security пропустит этот файл.

Например, если вы считаете объекты, используемые приложением Microsoft Windows Блокнот, безопасными, то есть доверяете этому приложению, вам следует добавить приложение Microsoft Windows Блокнот в список доверенных приложений, чтобы не контролировать объекты, используемые этим приложением. Это позволит увеличить производительность компьютера, что особенно важно при использовании серверных приложений.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда приложений. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием приложения автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких приложений и отключить контроль их активности, рекомендуется добавить их в список доверенных приложений.

Доверенные приложения позволяют избежать проблемы совместимости Kaspersky Endpoint Security с другими приложениями (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security и другого антивирусного приложения).

В то же время исполняемый файл и процесс доверенного приложения по-прежнему проверяются на наличие в них вирусов и других приложений, представляющих угрозу. Для полного исключения приложения из проверки Kaspersky Endpoint Security следует пользоваться исключениями из проверки (см. раздел "Создание исключения из проверки" на стр. 320).

► *Как добавить приложение в список доверенных в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные приложения**.

   Kaspersky Endpoint Security скрывает для просмотра список доверенных приложений в интерфейсе приложения, если администратор в консоли запретил настройку доверенных приложений ("замок" закрыт) и запретил использование локальных доверенных приложений (флажок **Разрешить использование локальных доверенных приложений** снят).

4. Нажмите на кнопку **Добавить** и выберите нужное действие:
   - **Категорию**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.
   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое доверенное приложение в корень списка.
   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные доверенные приложения*. Также в приложение добавлены предустановленные доверенные приложения для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные доверенные приложения.

Для добавления нового доверенного приложения в отдельную категорию установите флажок рядом с этой категорией и выберите вариант **Новое исключение**.

5. Выберите критерий доверенности:

   - **Использовать полный путь для определения доверенности процессов**. Введите путь к исполняемому файлу доверенного приложения.

     Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

     Kaspersky Endpoint Security учитывает регистр имени файла доверенного приложения. Если вы ввели имя файла в неверном регистре, Kaspersky Endpoint Security не распознает доверенное приложение.

   - **Использовать хеш файла для определения доверенности процессов**.

   Kaspersky Endpoint Security поддерживает переменные среды. При этом Kaspersky Endpoint Security конвертирует путь в локальном интерфейсе приложения. То есть, если вы ввели путь к файлу `%userprofile%\Documents\File.exe`, в локальном интерфейсе приложения для пользователя Fred123 будет добавлена запись `C:\Users\Fred123\Documents\File.exe`. Соответственно, Kaspersky Endpoint Security игнорирует доверенное приложение `File.exe` для других пользователей. Чтобы применить запись ко всем учетным записям, вы можете использовать символ * (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.

6. В окне свойств доверенного приложения настройте дополнительные параметры (см. раздел "Формирование списка доверенных приложений" на стр. 326).

7. Нажмите на кнопку **OK**.

   Новое доверенное приложение будет добавлено в список. Вы можете в любое время исключить приложение из доверенной зоны с помощью флажка в графе **Статус**.

8. Сохраните внесенные изменения.

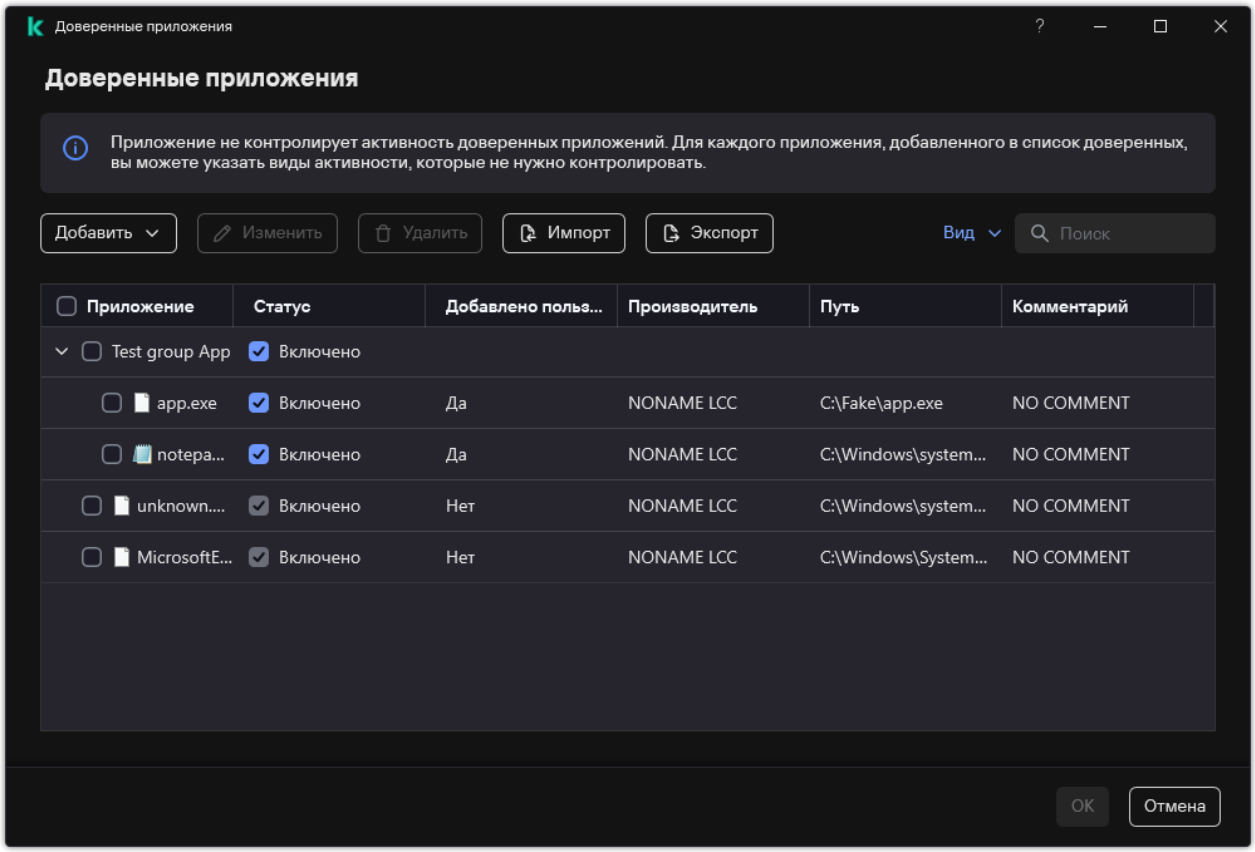


Рисунок 68. Список доверенных приложений

Таблица 20. Параметры доверенного приложения

Параметр	Описание
Не проверять открываемые файлы	Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью приложения. Например, если вы используете приложения резервного копирования файлов, функция позволит снизить потребление ресурсов компьютера Kaspersky Endpoint Security.

Параметр	Описание
Не контролировать активность приложения	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложения в операционной системе. Вы можете настроить контроль активности приложения для разных компонентов Kaspersky Endpoint Security: • **Не контролировать для компонентов защиты и контроля**. Контроль за активностью приложения выполняют следующие компоненты: Анализ поведения (на стр. 115), Защита от эксплойтов (на стр. 124), Предотвращение вторжений (на стр. 127), Откат вредоносных действий (на стр. 122) и Сетевой экран. • **Не контролировать для Managed Detection and Response и Endpoint Detection and Response**. Контроль за активностью приложения выполняют встроенный агент MDR и встроенный агент EDR (KATA). • **Не перехватывать консольный ввод для Endpoint Detection and Response**. Kaspersky Endpoint Security не отправляет данные телеметрии об управлении приложением через консоль. Данные телеметрии использует Kaspersky Anti Targeted Attack Platform (EDR).
Не контролировать активность дочерних приложений	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложений, которые запускает приложение. Вы можете применить исключение рекурсивно. То есть приложение не контролирует активность всей цепочки дочерних приложений.
Не наследовать ограничения родительского процесса (приложения)	Kaspersky Endpoint Security не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает приложение, для которой настроены права приложения (см. раздел "Работа с правами приложений" на стр. 132) (Предотвращение вторжений) и сетевые правила приложения (Сетевой экран).
Не контролировать активность дочерних приложений	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложений, которые запускает приложение. Вы можете применить исключение рекурсивно. То есть приложение не контролирует активность всей цепочки дочерних приложений.
Разрешить взаимодействие с интерфейсом приложения	Самозащита Kaspersky Endpoint Security (на стр. 347) блокирует все попытки управления службами приложения с удаленного компьютера. Если флажок установлен, то приложению удаленного доступа к компьютеру разрешено управлять параметрами Kaspersky Endpoint Security через интерфейс Kaspersky Endpoint Security.
Не блокировать взаимодействие с компонентом AMSI-защита	Kaspersky Endpoint Security не контролирует запросы доверенного приложения на проверку объектов компонентом AMSI-защита (см. раздел "AMSI-защита" на стр. 177).
Не проверять сетевой трафик	Kaspersky Endpoint Security исключает из проверки сетевой трафик, инициируемый приложением. Вы можете исключить из проверки весь трафик или только зашифрованный трафик. Также вы можете исключить из проверки отдельные IP-адреса или номера портов.

Параметр	Описание
Не перехватывать изменения файлов *(доступен только в консоли Kaspersky Security Center)*	Kaspersky Endpoint Security не контролирует изменения в файлах из области мониторинга Контроля целостности системы (см. раздел "Контроль целостности системы" на стр. 277). Приложение применяет исключение для всех режимов работы Контроля целостности системы: режим реального времени (см. раздел "Контроль целостности системы в режиме реального времени" на стр. 280) и проверка целостности системы по запросу (на стр. 283).
Не перехватывать изменения реестра *(доступен только в консоли Kaspersky Security Center)*	Kaspersky Endpoint Security не контролирует изменения ключей реестра из области мониторинга Контроля целостности системы (см. раздел "Контроль целостности системы" на стр. 277). Приложение применяет исключение для всех режимов работы Контроля целостности системы: режим реального времени (см. раздел "Контроль целостности системы в режиме реального времени" на стр. 280) и проверка целостности системы по запросу (на стр. 283).
Комментарий	Если необходимо, вы можете ввести краткий комментарий к доверенному приложению. Комментарий позволяет упростить поиск и сортировку доверенных приложений.
Статус	Статус доверенного приложения: • **Активно** – приложение в доверенной зоне. • **Неактивно** – приложение исключено из доверенной зоны.

Работа с приложениями, подписанными доверенной цифровой подписью

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки приложения, подписанные доверенной цифровой подписью. Kaspersky Endpoint Security автоматически помещает такие приложения в группу *Доверенные*.

► *Как начать использование доверенного системного хранилища сертификата в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В раскрывающемся списке **Доверенное системное хранилище сертификатов** выберите, какое системное хранилище Kaspersky Endpoint Security должен считать доверенным.
4. Сохраните внесенные изменения.

kaspersky

Работа с резервным хранилищем

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.12.12\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл из его резервной копии в папку исходного размещения файла.

Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то резервные копии файлов могут быть передана на Сервер администрирования Kaspersky Security Center. Подробнее о работе резервными копиями файлов в Kaspersky Security Center можно прочитать в Справочной системе Kaspersky Security Center.

В этом разделе

Настройка максимального срока хранения файлов в резервном хранилище 332

Настройка максимального размера резервного хранилища 333

Восстановление файлов из резервного хранилища 334

Удаление резервных копий файлов из резервного хранилища 335

Настройка максимального срока хранения файлов в резервном хранилище

По умолчанию максимальный срок хранения копий файлов в резервном хранилище составляет 30 дней. По истечении максимального срока хранения Kaspersky Endpoint Security удаляет наиболее старые файлы из резервного хранилища.

► *Чтобы настроить максимальный срок хранения файлов в резервном хранилище, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.

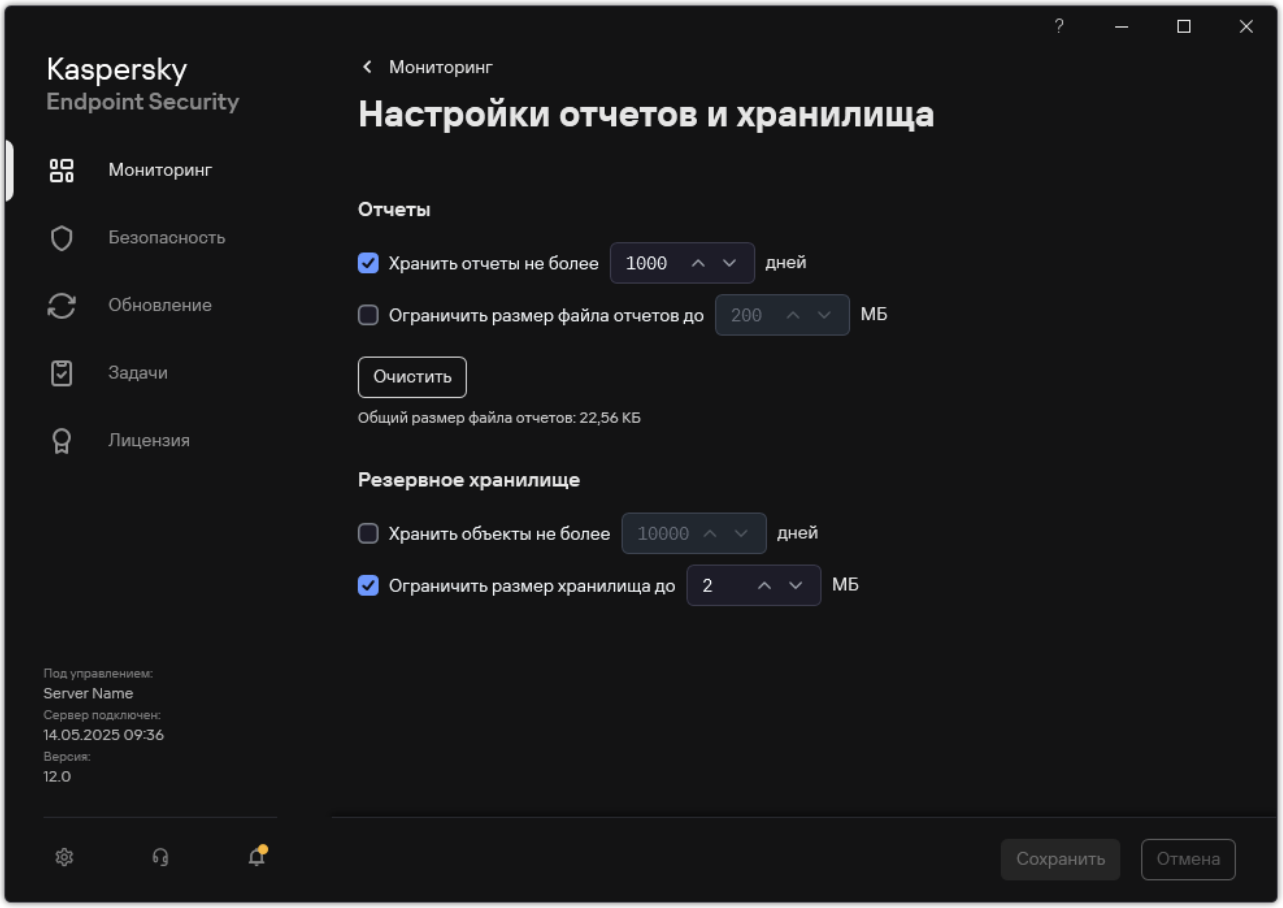


Рисунок 69. Параметры резервного хранилища

3. В блоке **Резервное хранилище** установите флажок **Хранить объекты не более N дней**, если хотите ограничить срок хранения копий файлов в резервном хранилище. Укажите максимальный срок хранения копий файлов в резервном хранилище.
4. Сохраните внесенные изменения.

Настройка максимального размера резервного хранилища

Вы можете указать максимальный размер резервного хранилища. По умолчанию размер резервного хранилища не ограничен. После достижения максимального размера Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы из резервного хранилища.

► *Чтобы настроить максимальный размер резервного хранилища, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.

3. В блоке **Резервное хранилище** установите флажок **Ограничить размер хранилища до N МБ**. Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 1024 МБ. После достижения максимального размера резервного хранилища приложение Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.
4. Сохраните внесенные изменения.

Восстановление файлов из резервного хранилища

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security блокирует файл, присваивает ему статус *Не вылечен*, помещает его копию в резервное хранилище и пытается провести лечение. Если файл удается вылечить, то статус резервной копии файла изменяется на *Вылечен*. Файл становится доступен в папке исходного размещения. Если файл не удается вылечить, то Kaspersky Endpoint Security удаляет его из папки исходного размещения. Вы можете восстановить файл из его резервной копии в папку исходного размещения.

Файлы со статусом *Будет удален при перезагрузке компьютера* восстановить невозможно. Перезагрузите компьютер и статус файла изменится на *Вылечен* или *Удален*. При этом вы можете восстановить файл из его резервной копии в папку исходного размещения.

В случае обнаружения вредоносного кода в файле, который является частью приложения Windows Store, Kaspersky Endpoint Security не помещает копию файла в резервное хранилище, а сразу удаляет его. При этом восстановить целостность приложения Windows Store вы можете средствами операционной системы (подробную информацию о восстановлении приложения Windows Store читайте в Справочной системе к Microsoft Windows).

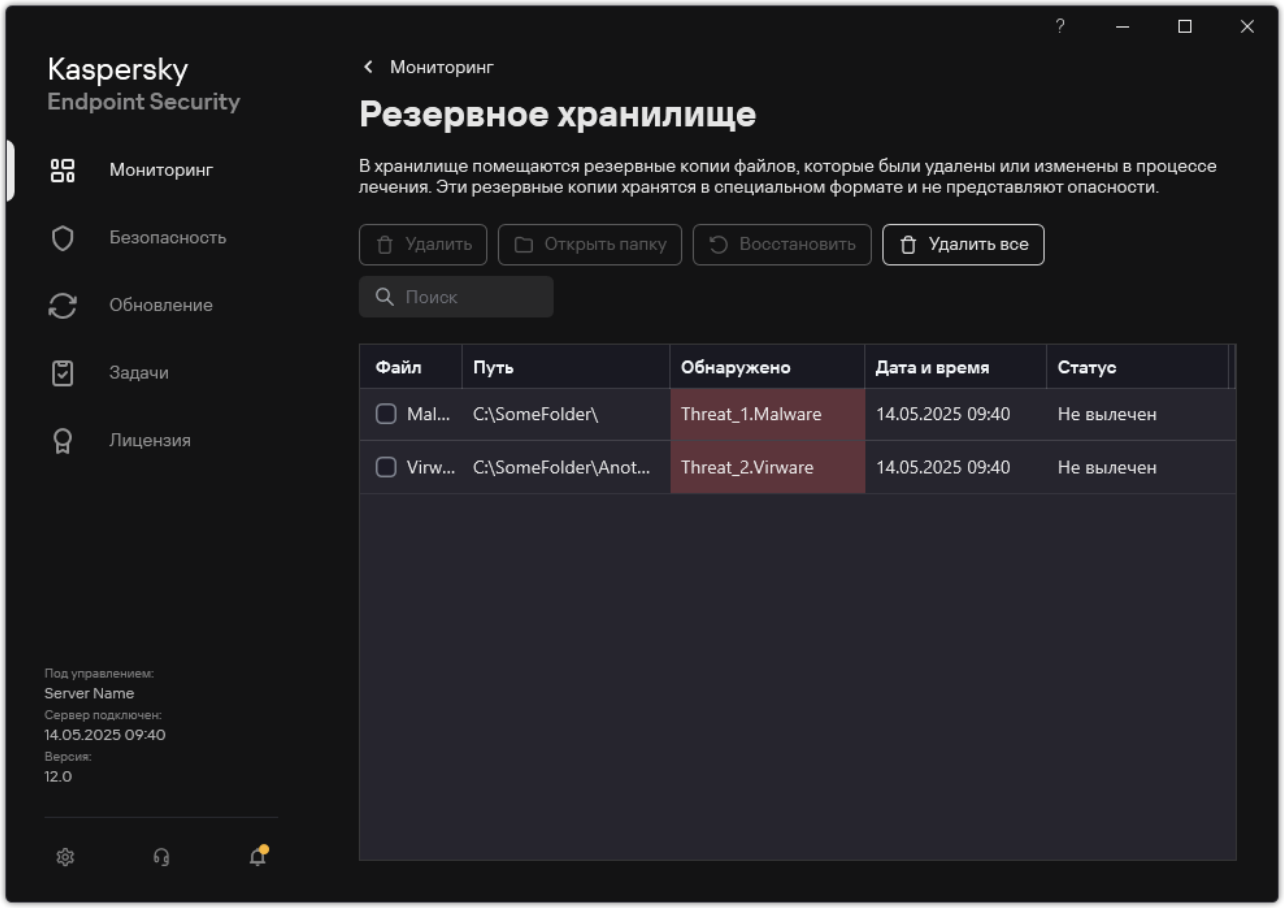
Набор резервных копий файлов представлен в виде таблицы. Для резервной копии файла отображается путь к папке исходного размещения этого файла. Путь к папке исходного размещения файла может содержать персональные данные.

Если в резервное хранилище помещено несколько расположенных в одной и той же папке файлов с одинаковыми именами и различным содержимым, то для восстановления доступен только тот файл, который был помещен в резервное хранилище последним.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Резервное хранилище**.
2. В открывшемся списке файлов резервного хранилища выберите файлы, которые вы хотите восстановить, и нажмите на кнопку **Восстановить**.

Kaspersky Endpoint Security восстановит файлы из выбранных резервных копий в папки их исходного размещения.



Удаление резервных копий файлов из резервного хранилища

Kaspersky Endpoint Security удаляет резервные копии файлов с любым статусом из резервного хранилища автоматически по истечении времени, заданного в параметрах приложения. Также вы можете самостоятельно удалить любую копию файла из резервного хранилища.

► *Чтобы удалить резервные копии файлов из резервного хранилища, выполните следующие действия:*

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Резервное хранилище**.
2. В открывшемся списке файлов резервного хранилища выберите файлы, которые вы хотите удалить из резервного хранилища, и нажмите на кнопку **Удалить**.

Kaspersky Endpoint Security удалит выбранные резервные копии файлов из резервного хранилища.

kaspersky

Работа с карантином

Карантин – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Endpoint Security использует карантин при работе с решениями Kaspersky Endpoint Detection and Response Optimum. В остальных случаях Kaspersky Endpoint Security помещает файл в резервное хранилище (см. раздел "Работа с резервным хранилищем" на стр. 332). Подробнее о работе с карантином в составе решения см. в Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).

Kaspersky Endpoint Security помещает файлы на карантин под системной учетной записью (SYSTEM).

Вы можете настроить параметры карантина только в консоли Kaspersky Security Center. Также в консоли Kaspersky Security Center вы можете выполнить действия с объектами на карантине (восстановить, удалить, добавить и другие). Локально на компьютере вы можете только восстановить объект из командной строки (см. раздел "RESTORE. Восстановление файлов из карантина" на стр. 419).

В этом разделе

Настройка максимального размера карантина 336

Передача данных о файлах на карантине в Kaspersky Security Center 337

Восстановление файлов из карантина 338

Настройка максимального размера карантина

По умолчанию размер карантина ограничен 1024 МБ. После достижения максимального размера Kaspersky Endpoint Security прекращает отправлять файлы и формирует событие *Недостаточно места в хранилище карантина*. Чтобы не допустить переполнение карантина вы можете задать пороговое значение, при котором Kaspersky Endpoint Security будет формировать событие *В хранилище карантина скоро закончится место*. Настроить срок хранения файлов в карантине для автоматического удаления файлов невозможно.

Если в вашей организации развернуто решение Kaspersky Anti Targeted Attack Platform (EDR), мы рекомендуем увеличить размер карантина. При сканировании YARA приложение может обнаружить дамп памяти большого размера. Если размер дампа памяти превышает размер карантина, приложение завершит сканирование YARA с ошибкой и дамп памяти не будет помещен на карантин. Мы рекомендуем задать размер карантина равным размеру оперативной памяти компьютера (например, 8 Гб) или выключить ограничение размера карантина.

► *Как настроить максимальный размер карантина в Web Console и Cloud Console*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Отчеты и хранилище**.
5. В блоке **Карантин** настройте размер карантина:
   - **Ограничить размер карантина**. Если флажок установлен, то размер карантина ограничен указанным значением. Если флажок снят, размер карантина ограничен свободным пространством на диске. Это может понадобится при YARA-проверке, так как приложение может сохранять дамп памяти большого размера.
   - **Максимальный размер карантина (МБ)**. Если флажок установлен, то максимальный размер карантина ограничен заданным значением. По умолчанию максимальный размер составляет 1024 МБ. При достижении максимального размера карантина Kaspersky Endpoint Security отправляет событие в Kaspersky Security Center *Недостаточно места в хранилище карантина* и публикует событие в Журнале событий Windows. При этом приложение прекращает помещать новые объекты на карантин. Вам нужно вручную очистить карантин.

     Если флажок снят, размер карантина ограничен размером свободного пространства на диске.
   - **Уведомлять при заполнении карантина на (%)**. Пороговое значение карантина. Например, вы можете задать пороговое значение карантина 50 %. При достижении порогового значения карантина, Kaspersky Endpoint Security отправляет соответствующее событие в Kaspersky Security Center и публикует событие в Журнале событий Windows. При этом приложение продолжает помещать новые объекты на карантин.
6. Сохраните внесенные изменения.

Передача данных о файлах на карантине в Kaspersky Security Center

Для выполнения действий с объектами на карантине в Web Console вам нужно включить передачу данных на Сервер администрирования о файлах на карантине. В Web Console вы можете, например, загрузить файл из карантина на компьютер для анализа. Передача данных о файлах на карантине должна быть включена для работы всех функций решений Kaspersky Sandbox и Kaspersky Endpoint Detection and Response.

► *Как включить передачу данных о файлах на карантине в Web Console*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Интеграция с KSC**.
5. В блоке **Передача данных на Сервер администрирования** установите флажок **О файлах карантина**.
6. Сохраните внесенные изменения.

В результате вы можете в консоли Kaspersky Security Center просматривать список файлов, помещенных на карантин на компьютере. В консоли Kaspersky Security Center вы можете выполнить действия с объектами на карантине (восстановить, удалить, добавить и другие). Подробнее о работе с карантином см. в справке Kaspersky Security Center https://support.kaspersky.com/KSC/14/ru-RU/12429.htm.

kaspersky

Восстановление файлов из карантина

По умолчанию Kaspersky Endpoint Security восстанавливает файл в папку его исходного размещения. Если папка назначения удалена или у пользователя нет прав доступа к этой папке, приложение помещает файл в папку `%DataRoot%\QB\Restored`. Далее вам нужно вручную переместить файл в папку назначения.

► *Чтобы восстановить файлы из карантина, выполните следующие действия:*

1. В главном окне Web Console выберите **Операции** → **Хранилища** → **Карантин**.
2. В открывшемся списке файлов карантина выберите файлы, которые вы хотите восстановить, и нажмите на кнопку **Восстановить**.

Kaspersky Endpoint Security восстановит файл. Если в папке восстановление уже есть файл с таким же именем, приложение отменит восстановление файла. Приложение удаляет файл из карантина после восстановления.

kaspersky

Служба уведомлений

В процессе работы Kaspersky Endpoint Security возникают различного рода события. Уведомления об этих событиях могут иметь информационный характер или нести важную информацию. Например, уведомление может информировать об успешно выполненном обновлении баз и модулей программы, а может фиксировать ошибку в работе некоторого компонента, которую вам требуется устранить.

Kaspersky Endpoint Security позволяет вносить информацию о событиях, возникающих в работе программы, в журнал событий Microsoft Windows и / или в журнал Kaspersky Endpoint Security.

Kaspersky Endpoint Security может доставлять уведомления следующими способами:

- с помощью всплывающих уведомлений в области уведомлений панели задач Microsoft Windows;
- по электронной почте.

Вы можете настроить способы доставки уведомлений. Способ доставки уведомлений устанавливается для каждого типа событий.

Работая с таблицей событий для настройки службы уведомлений, вы можете выполнять следующие действия:

- фильтровать события службы уведомлений по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска событий службы уведомлений;
- сортировать события службы уведомлений;
- изменять порядок и набор граф, отображаемых в списке событий службы уведомлений.

В этом разделе

Настройка параметров журналов событий 339

Настройка отображения и доставки уведомлений 340

Настройка отображения предупреждений о состоянии приложения в области уведомлений 341

Настройка параметров журналов событий

► *Чтобы настроить параметры журналов событий, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настроить уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

События могут содержать следующие данные пользователя:

- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
- пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
- имя пользователя Microsoft Windows;
- адреса веб-страниц, открываемых пользователем.

4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить параметры журналов событий.
5. В графах **Сохранять в локальном отчете** и **Сохранять в журнале событий Windows** установите флажки напротив нужных событий.

   События, напротив которых установлен флажок в графе **Сохранять в локальном отчете**, отображаются в отчетах приложения (см. раздел "Работа с отчетами" на стр. 342). События, напротив которых установлен флажок в графе **Сохранять в журнале событий Windows**, отображаются в журналах Windows в канале `Application`.
6. Сохраните внесенные изменения.

Настройка отображения и доставки уведомлений

► *Чтобы настроить отображение и доставку уведомлений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настроить уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

   События могут содержать следующие данные пользователя:

   - пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
   - пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
   - имя пользователя Microsoft Windows;
   - адреса веб-страниц, открываемых пользователем.
4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить доставку уведомлений.
5. В графе **Уведомлять на экране** установите флажки напротив нужных событий.

   Информация о выбранных событиях отображается на экране в виде всплывающих уведомлений в области уведомлений панели задач Microsoft Windows.
6. В графе **Уведомлять по почте** установите флажки напротив нужных событий.

   Информация о выбранных событиях доставляется по электронной почте, если заданы параметры доставки почтовых уведомлений.
7. Нажмите на кнопку **OK**.

8. Если вы включили уведомления по почте, настройте параметры доставки электронных сообщений:
   a. Нажмите на кнопку **Настроить почтовые уведомления**.
   b. Установите флажок **Уведомлять о событиях**, чтобы включить доставку информации о событиях в работе Kaspersky Endpoint Security, отмеченных в графе **Уведомлять по почте**.
   c. Укажите параметры доставки почтовых уведомлений.
   d. Нажмите на кнопку **OK**.
9. Сохраните внесенные изменения.

Настройка отображения предупреждений о состоянии приложения в области уведомлений

► *Чтобы настроить отображение предупреждений о состоянии приложения в области уведомлений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. В блоке **Отображать состояние приложения в области уведомлений** установите флажки напротив тех категорий событий, уведомления о которых вы хотите видеть в области уведомлений Microsoft Windows.
4. Сохраните внесенные изменения.

При возникновении событий, относящихся к выбранным категориям, значок приложения (см. раздел "Значок приложения в области уведомлений" на стр. 53) в области уведомлений будет меняться на или в зависимости от важности предупреждения.

kaspersky

Работа с отчетами

Информация о работе каждого компонента Kaspersky Endpoint Security, о событиях шифрования данных, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе приложения в целом сохраняется в отчетах.

Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.12.12\Report`.

Отчеты могут содержать следующие данные пользователя:

- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
- пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
- имя пользователя Microsoft Windows;
- адреса веб-страниц, открываемых пользователем.

Данные в отчете представлены в виде таблицы. Каждая строка таблицы содержит информацию об отдельном событии, атрибуты события находятся в графах таблицы. Некоторые графы являются составными и содержат вложенные графы с дополнительными атрибутами. Чтобы просмотреть дополнительные атрибуты, нажмите на кнопку  рядом с названием графы. События, зарегистрированные в работе разных компонентов или при выполнении разных задач, имеют разный набор атрибутов.

Доступны следующие отчеты:

- Отчет **Аудит системы**. Содержит информацию о событиях, возникающих в процессе взаимодействия пользователя с приложением, а также в ходе работы приложения в целом и не относящихся к каким-либо отдельным компонентам или задачам Kaspersky Endpoint Security.
- Отчеты о работе компонентов Kaspersky Endpoint Security.
- Отчеты о выполнении задач Kaspersky Endpoint Security.
- Отчет **Шифрование данных**. Содержит информацию о событиях, возникающих при шифровании и расшифровке данных.

В отчетах применяются следующие уровни важности событий:

 **Информационные сообщения**. События справочного характера, как правило, не несущие важной информации.

 **Предупреждения**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе приложения Kaspersky Endpoint Security.

 **Критические события**. События критической важности, указывающие на проблемы в работе приложения Kaspersky Endpoint Security или на уязвимости в защите компьютера пользователя.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- фильтровать список событий по различным критериям;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке;
- сортировать список событий по каждой графе отчета;

- отображать и скрывать сгруппированные с помощью фильтра события по кнопке ⊞;
- изменять порядок и набор граф, отображаемых в отчете.

При необходимости вы можете сохранить сформированный отчет в текстовый файл. Также вы можете удалять информацию из отчетов (см. раздел "Удаление информации из отчетов" на стр. 346) по компонентам и задачам Kaspersky Endpoint Security, объединенным в группы.

Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то информация о событиях может быть передана на Сервер администрирования Kaspersky Security Center (подробнее см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/15.1/ru-RU/index.htm).

В этом разделе

Просмотр отчетов 343

Настройка максимального срока хранения отчетов 344

Настройка максимального размера файла отчета 345

Сохранение отчета в файл 345

Удаление информации из отчетов 346

Просмотр отчетов

Если для пользователя доступен просмотр отчетов, то для этого пользователя доступен просмотр всех событий, отраженных в отчетах.

► *Чтобы просмотреть отчеты, выполните следующие действия:*

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Отчеты**.

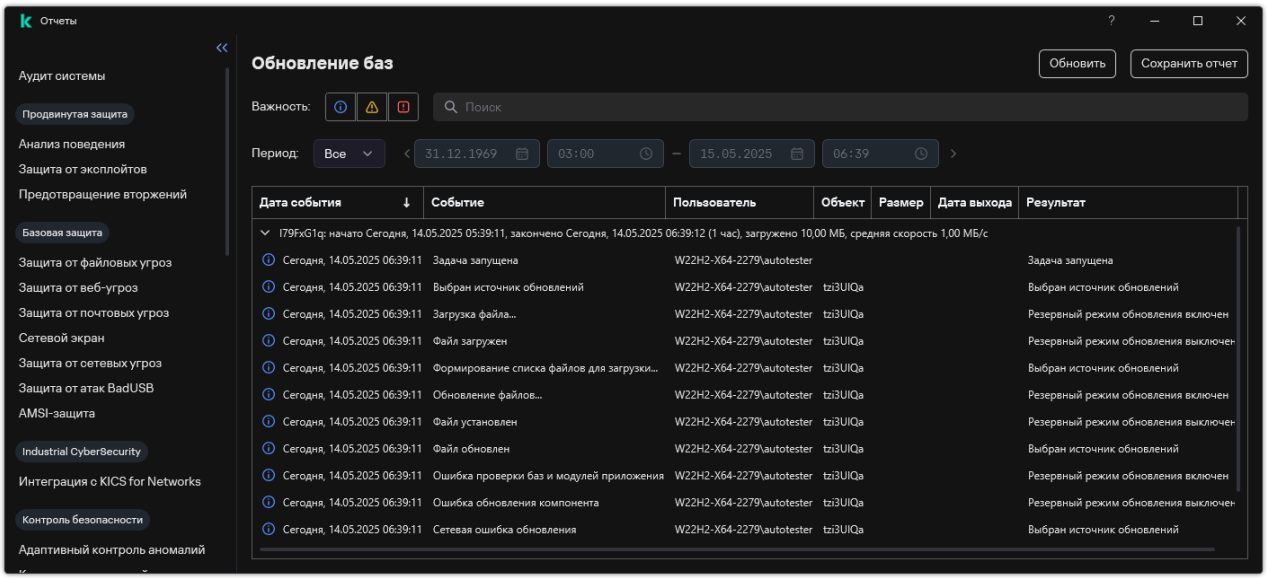


Рисунок 70. Отчеты

2. В списке компонентов и задач выберите компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий по результатам работы выбранного компонента или выбранной задачи Kaspersky Endpoint Security. Вы можете отсортировать события в отчете по значениям в ячейках одной из граф.

3. Если требуется просмотреть подробную информацию о событии, выберите в отчете нужное событие.

В нижней части окна отобразится блок со сводной информацией о событии.

Настройка максимального срока хранения отчетов

По умолчанию максимальный срок хранения отчетов о событиях, фиксируемых Kaspersky Endpoint Security, составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета.

► *Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.
3. В блоке **Отчеты** установите флажок **Хранить отчеты не более N дней**, если хотите ограничить срок хранения отчетов. Укажите максимальный срок хранения отчетов.
4. Сохраните внесенные изменения.

Настройка максимального размера файла отчета

Вы можете указать максимальный размер файла, содержащего отчет. По умолчанию максимальный размер файла отчета составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета таким образом, чтобы размер файла отчетов не превышал максимального значения.

► *Чтобы настроить максимальный размер файла отчета, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.
3. В блоке **Отчеты** установите флажок **Ограничить размер файла отчетов до N МБ**, если хотите ограничить размер файла отчета. Укажите максимальный размер файла отчета.
4. Сохраните внесенные изменения.

Сохранение отчета в файл

Пользователь сам несет ответственность за обеспечение безопасности информации из сохраненного в файл отчета и, в частности, за контроль и ограничение доступа к этой информации.

Сформированный отчет вы можете сохранить в файл текстового формата TXT или CSV.

Kaspersky Endpoint Security сохраняет событие в отчет в том виде, в каком событие отображается на экране, то есть с тем же составом и с той же последовательностью атрибутов события.

► *Чтобы сохранить отчет в файл, выполните следующие действия:*

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Отчеты**.
2. В открывшемся окне выберите компонент или задачу.

В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи Kaspersky Endpoint Security.

3. Если требуется, измените представление данных в отчете с помощью следующих способов:
   - фильтрация событий;
   - поиск событий;
   - изменение расположения граф;
   - сортировка событий.
4. Нажмите на кнопку **Сохранить отчет**, расположенную в верхней правой части окна.
5. В открывшемся окне укажите папку, в которую вы хотите сохранить файл отчета.
6. Введите название файла отчета.
7. Выберите нужный формат файла отчета: TXT или CSV.
8. Сохраните внесенные изменения.

Удаление информации из отчетов

► *Чтобы удалить информацию из отчетов, выполните следующие действия*:

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.
3. В блоке **Отчеты** нажмите на кнопку **Очистить**.
4. Если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355), Kaspersky Endpoint Security может запросить учетные данные пользователя. Приложение запрашивает учетные данные, если у пользователя нет необходимого разрешения.

Kaspersky Endpoint Security удалит все отчеты для всех компонентов и задач приложения.

kaspersky

Самозащита Kaspersky Endpoint Security

Самозащита предотвращает выполнение другими приложениями действий, которые могут нарушить работу Kaspersky Endpoint Security и, например, удалить Kaspersky Endpoint Security с компьютера. Набор доступных технологий самозащиты Kaspersky Endpoint Security зависит от разрядности операционной системы (см. таблицу ниже). Также к средствам самозащиты относятся Защита паролем и Защита подключения к Серверу администрирования.

Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы приложения).

Защита подключения к Серверу администрирования предотвращает несанкционированное переподключение компьютера к недоверенному серверу.

Таблица 21. Технологии самозащиты Kaspersky Endpoint Security

Технология	Описание	x86	x64
Механизм самозащиты	Технология блокирует доступ к следующим компонентам приложения: • файлы в папке установки Kaspersky Endpoint Security и другие файлы приложения; • раздел реестра с ключами приложения; • процессы, которые запускает приложение.	✓	✓
AM-PPL (Antimalware Protected Process Light)	Технология защищает процессы Kaspersky Endpoint Security от вредоносных действий. Подробнее о технологии AM-PPL см. на сайте Microsoft (https://learn.microsoft.com/ru-ru/windows/win32/services/protecting-anti-malware-services-/). Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.	✓	✓
Механизм защиты от внешнего управления	Технология блокирует другим приложениям доступ к Kaspersky Endpoint Security (например, приложения TeamViewer или RemotelyAnywhere).	✓	– (кроме Windows 7)

kaspersky

В этом разделе

Включение и выключение механизма самозащиты 348
Включение и выключение поддержки AM-PPL 349
Защита служб приложения от внешнего управления 351
Обеспечение работы приложений удаленного администрирования 352
Защита паролем 352
Защита подключения к Серверу администрирования 364

Включение и выключение механизма самозащиты

Kaspersky Endpoint Security предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти и записей в системном реестре.

Технология блокирует доступ к следующим компонентам приложения:

- файлы в папке установки Kaspersky Endpoint Security и другие файлы приложения;
- раздел реестра с ключами приложения;
- процессы, которые запускает приложение.

По умолчанию механизм самозащиты Kaspersky Endpoint Security включен.

► *Как включить или выключить механизм самозащиты в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

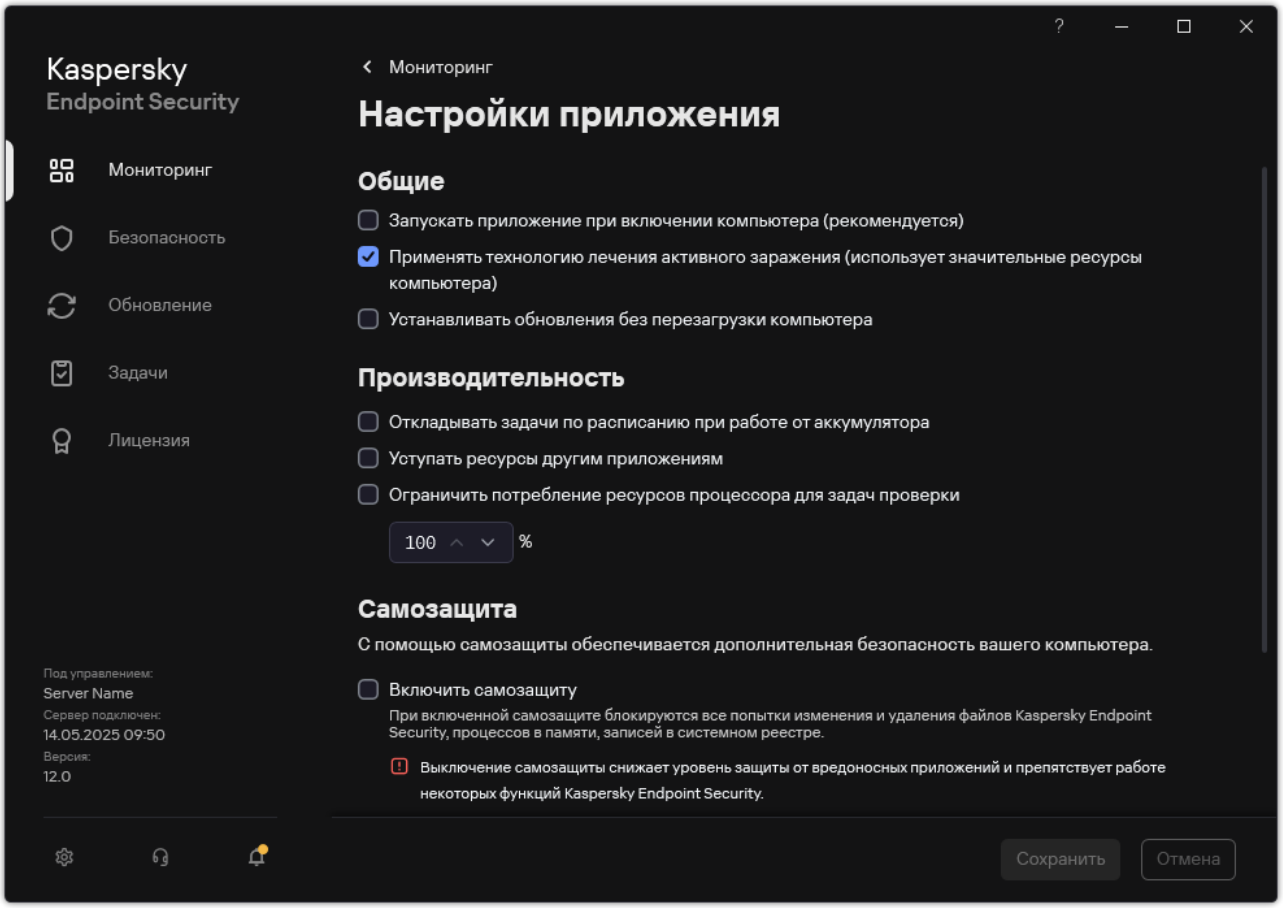


Рисунок 71. Параметры приложения Kaspersky Endpoint Security для Windows

3. Используйте флажок **Включить самозащиту**, чтобы включить или выключить механизм самозащиты.
4. Сохраните внесенные изменения.

Включение и выключение поддержки AM-PPL

Kaspersky Endpoint Security поддерживает технологию Antimalware Protected Process Light (далее "AM-PPL") от Microsoft. AM-PPL защищает процессы Kaspersky Endpoint Security от вредоносных действий (например, завершение работы приложения). AM-PPL разрешает запуск только доверенных процессов. Процессы Kaspersky Endpoint Security подписаны в соответствии с требованиями безопасности Windows, поэтому являются доверенными. Подробнее о технологии AM-PPL см. на сайте Microsoft (https://learn.microsoft.com/ru-ru/windows/win32/services/protecting-anti-malware-services-/). По умолчанию технология AM-PPL включена.

Kaspersky Endpoint Security также имеет встроенные механизмы защиты процессов приложения. Поддержка AM-PPL позволяет делегировать функции защиты процессов операционной системе. Таким образом, вы увеличиваете быстродействие приложения и уменьшаете потребление ресурсов компьютера.

Используйте технологию AM-PPL постоянно. AM-PPL является важным компонентом защиты операционной системы. Выключение поддержки технологии AM-PPL может привести к сбоям в работе некоторых функций Kaspersky Endpoint Security (например, интеграция приложения с Windows Security Center). Разрешается выключать поддержку технологии AM-PPL только в отдельной тестовой среде для диагностики неисправностей в работе приложения.

Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

► *Чтобы включить или выключить поддержку технологии AM-PPL, выполните следующие действия:*

1. Выключите механизм самозащиты приложения (см. раздел "Включение и выключение механизма самозащиты" на стр. 348).

   Механизм самозащиты предотвращает изменение и удаление процессов приложения в памяти компьютера, в том числе изменение статуса AM-PPL.
2. Запустите интерпретатор командной строки cmd от имени администратора.
3. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

   Вы можете добавить в системную переменную %PATH% путь к исполняемому файлу при установке приложения.
4. В командной строке введите:
   - `klpsm.exe enable` – включение поддержки технологии AM-PPL (см. рис. ниже).
   - `klpsm.exe disable` – выключение поддержки технологии AM-PPL.
5. Перезапустите Kaspersky Endpoint Security.
6. Возобновите работу механизма самозащиты приложения (см. раздел "Включение и выключение механизма самозащиты" на стр. 348).

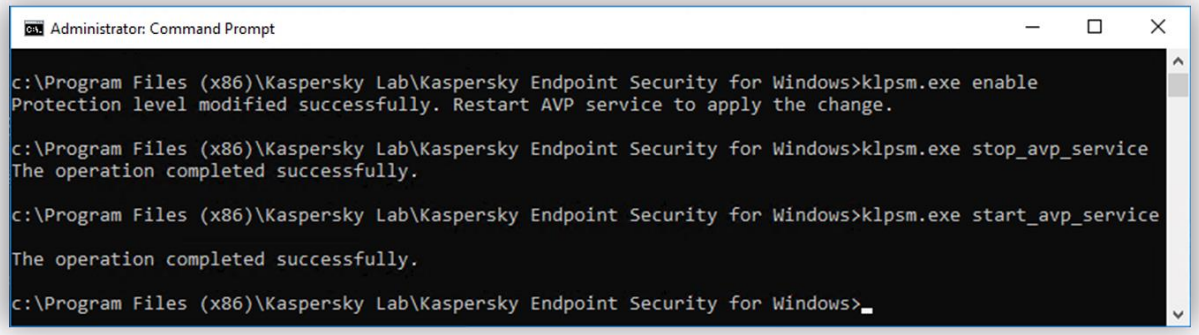


Рисунок 72. Включение поддержки технологии AM-PPL

Защита служб приложения от внешнего управления

Защита служб приложения от внешнего управления блокирует попытки пользователей и других приложений остановить работу служб Kaspersky Endpoint Security. Защита обеспечивает работу следующих служб:

- служба Kaspersky Endpoint Security (AVP.KES.12.12);
- служба Kaspersky Seamless Update Service (AVPSUS.KES.12.12).

Для завершения работы приложения из командной строки необходимо, чтобы защита от внешнего управления службами Kaspersky Endpoint Security была выключена.
Вы можете предоставить возможность внешнего управления службами приложения только на компьютерах без поддержки технологии AM-PPL или с выключенной технологией (см. раздел "Включение и выключение поддержки AM-PPL" на стр. 349).

Как включить или выключить защиту служб приложения от внешнего управления в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

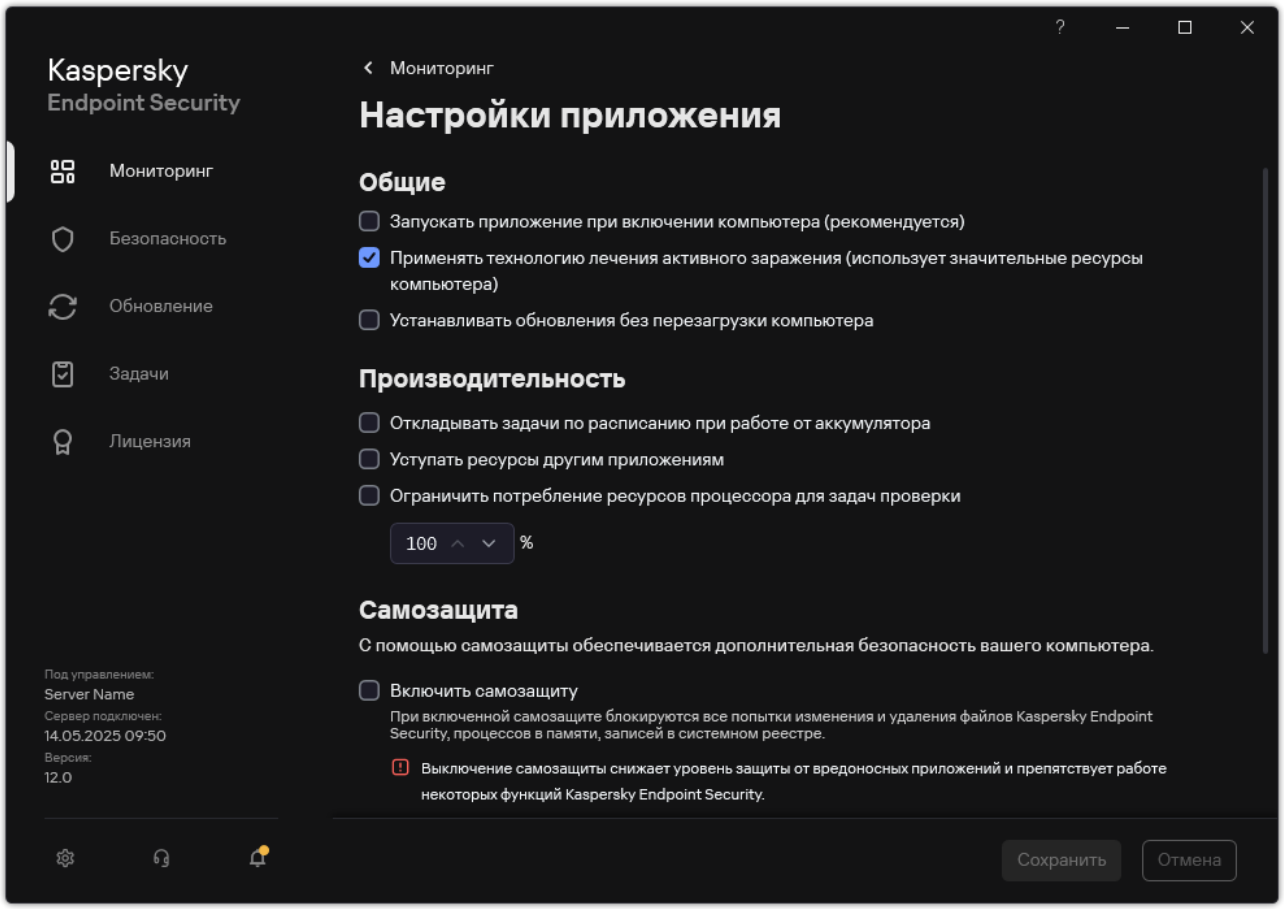
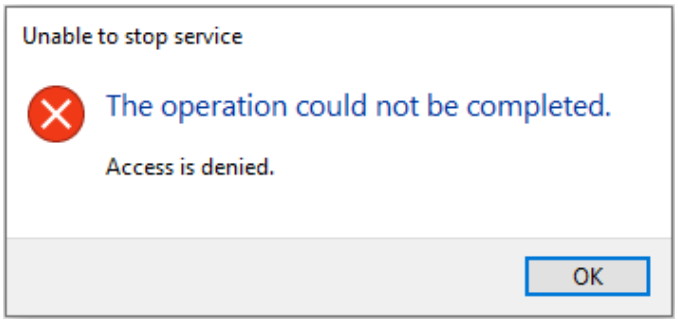


Рисунок 73. Параметры приложения Kaspersky Endpoint Security для Windows

3. Используйте флажок **Блокировать внешнее управление службами приложения**, чтобы включить или выключить защиту служб Kaspersky Endpoint Security от внешнего управления.
4. Сохраните внесенные изменения.

В результате при попытке пользователя остановить работу служб приложения отображается системное окно с ошибкой. Пользователь может управлять службами приложения только из интерфейса Kaspersky Endpoint Security.



Обеспечение работы приложений удаленного администрирования

Нередко возникают ситуации, когда при использовании механизма защиты от внешнего управления возникает необходимость применить приложения удаленного администрирования.

► *Чтобы обеспечить работу приложений удаленного администрирования, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные приложения**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Выберите исполняемый файл приложения удаленного администрирования.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.
6. Установите флажок **Разрешить взаимодействие с интерфейсом <PRODUCT>**.
7. Сохраните внесенные изменения.

Защита паролем

Компьютер могут использовать несколько пользователей с разным уровнем компьютерной грамотности. Неограниченный доступ пользователей к Kaspersky Endpoint Security и его параметрам может привести к снижению уровня безопасности компьютера в целом. Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы приложения).

Если пользователь, который запустил сессию Windows, (*сессионный пользователь*) имеет разрешение на выполнение действия, Kaspersky Endpoint Security не запрашивает имя пользователя и пароль или временный пароль. Пользователь получает доступ к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями.

Если у сессионного пользователя отсутствует разрешение на выполнение действия, пользователь может получить доступ к приложению следующими способами:

- Ввод имени пользователя и пароля.

  Этот способ удобен для повседневной работы. Для выполнения действия, защищенного паролем, требуется ввести данные доменной учетной записи пользователя с необходимым разрешением. При этом компьютер должен быть в домене. Если компьютер не в домене, вы можете использовать учетную запись KLAdmin или учетную запись, добавленную вручную.

- Ввод временного пароля.

  Этот способ удобен, если пользователь находится вне корпоративной сети и необходимо предоставить ему временное разрешение на выполнение запрещенного действия (например, завершить работу приложения). По истечении срока действия временного пароля или истечении сессии приложение возвращает параметры Kaspersky Endpoint Security в прежнее состояние.

При попытке пользователя выполнить действие, защищенное паролем, Kaspersky Endpoint Security предложит пользователю ввести имя пользователя и пароль или временный пароль (см. рис. ниже).

В окне ввода пароля язык ввода можно поменять только с помощью одновременного нажатия клавиш **ALT+SHIFT**. При использовании других комбинаций клавиш, даже если они установлены в операционной системе, смена языка ввода не происходит.

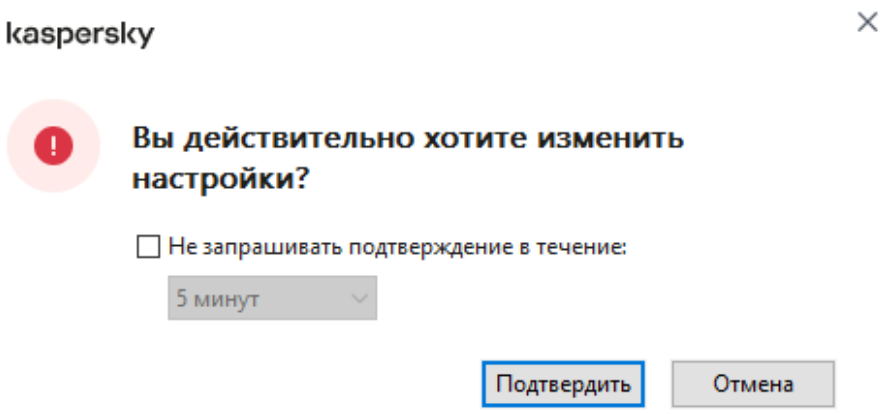


Рисунок 74. Запрос пароля для доступа к Kaspersky Endpoint Security

Имя пользователя и пароль

Для доступа к Kaspersky Endpoint Security необходимо ввести данные учетной записи. Защита паролем поддерживает работу со следующими учетными записями:

- **KLAdmin**. Учетная запись администратора без ограничений доступа к Kaspersky Endpoint Security. Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем. Отменить разрешение для учетной записи KLAdmin невозможно. Kaspersky Endpoint Security требует задать пароль для учетной записи KLAdmin во время включения Защиты паролем.

- **Учетная запись, добавленная вручную**. Учетная запись вне домена Active Directory. Это сервисная учетная запись, которую вы можете использовать вместо KLAdmin, чтобы не делиться паролем от учетной записи администратора. Вы можете задать любые имя пользователя и пароль, а также настроить отдельные разрешения.
- **Группа "Все"**. Стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети. Пользователи из группы "Все" могут получить доступ к приложению в соответствии с предоставленными разрешениями.
- **Отдельные пользователи или группы**. Учетные записи пользователей, для которых вы можете настроить отдельные разрешения. Например, если для группы "Все" выполнение действия запрещено, то вы можете разрешить выполнение действия для отдельного пользователя или группы.
- **Сессионный пользователь**. Учетная запись пользователя, который запустил сессию Windows. Вы можете сменить сессионного пользователя во время ввода пароля (флажок **Запомнить пароль на текущую сессию**). В этом случае Kaspersky Endpoint Security назначает сессионным пользователем, учетные данные которого вы ввели, вместо пользователя, который запустил сессию Windows.

Временный пароль

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для отдельного компьютера вне корпоративной сети. Администратор создает временный пароль для отдельного компьютера в Kaspersky Security Center в свойствах компьютера пользователя. Администратор выбирает действия, на которые будет распространяться временный пароль, и срок действия временного пароля.

Алгоритм работы Защиты паролем

Kaspersky Endpoint Security принимает решение о выполнении действия, защищенного паролем, по следующему алгоритму (см. рис. ниже).

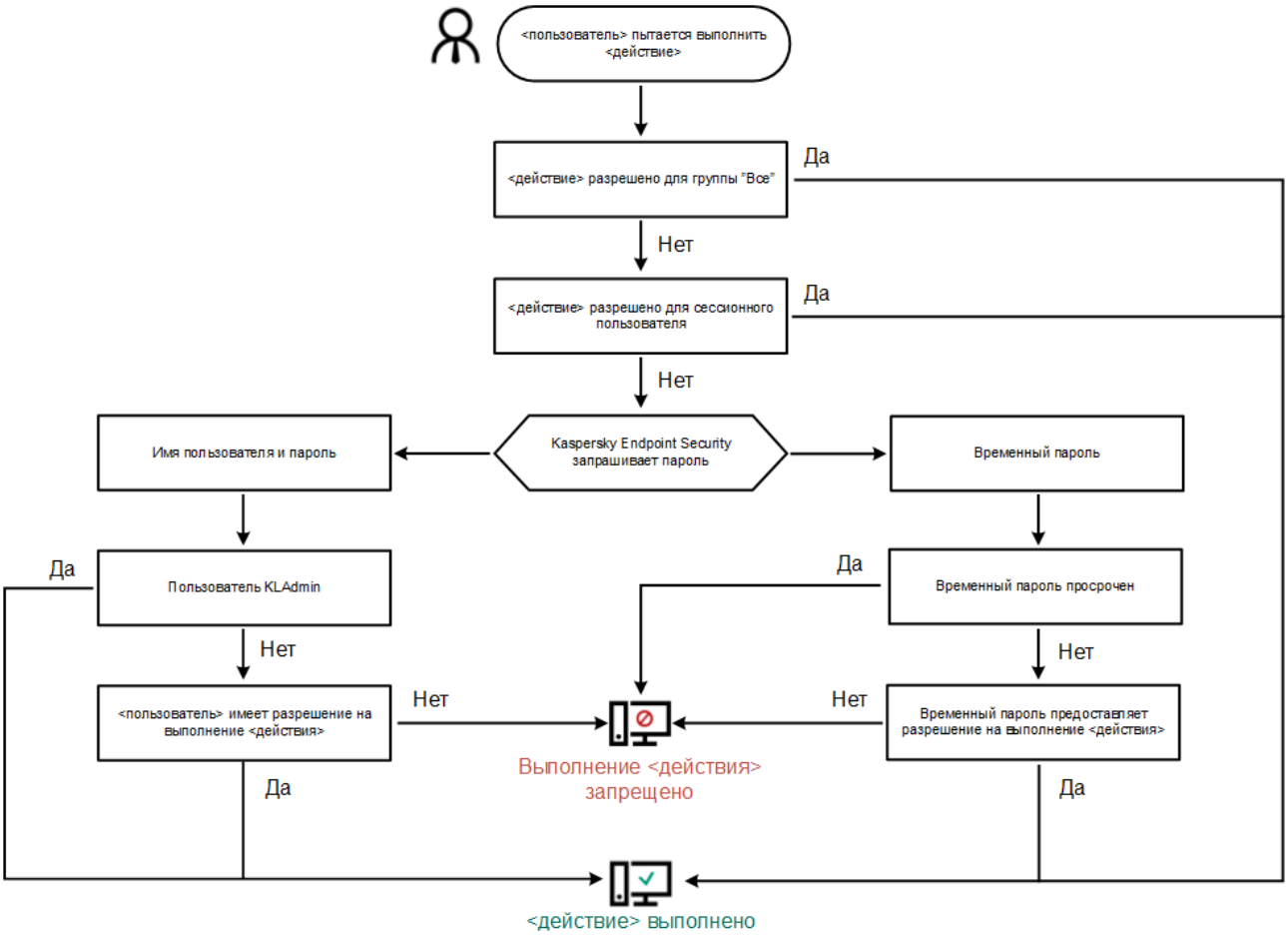


Рисунок 75. Алгоритм работы Защиты паролем

В этом разделе

Включение Защиты паролем 355
Предоставление разрешений для отдельных пользователей или групп 357
Использование временного пароля для предоставления разрешений 358
Отзыв временного пароля 359
Особенности разрешений Защиты паролем 361
Сброс пароля KLAdmin 363

kaspersky

Включение Защиты паролем

Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы приложения).

► *Как включить Защиту паролем в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. Используйте переключатель **Защита паролем**, чтобы включить или выключить компонент.
4. Задайте пароль для учетной записи KLAdmin и подтвердите его.

   Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем.

   Если компьютер работает под управлением политики, администратор может сбросить пароль для учетной записи KLAdmin в свойствах политики (см. раздел "Сброс пароля KLAdmin" на стр. 363). Если компьютер не подключен к Kaspersky Security Center, и вы забыли пароль для учетной записи KLAdmin, восстановить пароль невозможно.

5. Настройте разрешения для всех пользователей внутри корпоративной сети:
   a. В таблице учетных записей откройте список разрешений для группы "Все" по кнопке **Изменить**.

      Группа "Все" – стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети.

   b. Установите флажки напротив тех действий, которые будут доступны пользователям без ввода пароля.

      Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы приложения** снят, вы можете завершить работу приложения только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 358).

      Разрешения Защиты паролем имеют ряд особенностей (см. раздел "Особенности разрешений Защиты паролем" на стр. 361). Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

6. Сохраните внесенные изменения.

После включения Защиты паролем приложение ограничит доступ пользователей к Kaspersky Endpoint Security в соответствии с разрешениями для группы "Все". Вы можете выполнить запрещенные для группы "Все" действия только с помощью учетной записи KLAdmin, отдельной учетной записи с нужными разрешениями (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 358).

Вы можете выключить Защиту паролем только с помощью учетной записи KLAdmin. Выключить защиту паролем с помощью другой учетной записи или с помощью временного пароля невозможно.

Во время проверки пароля вы можете установить флажок **Запомнить пароль на текущую сессию**. В этом случае Kaspersky Endpoint Security не будет требовать ввода пароля при попытке пользователя выполнить другое разрешенное действие, защищенное паролем, в течение сессии.

Предоставление разрешений для отдельных пользователей или групп

Защита паролем позволяет предоставить доступ к Kaspersky Endpoint Security для отдельных учетных записей Active Directory, а также учетных записей, добавленных вручную.

Учетные записи Active Directory

Вы можете предоставить доступ к Kaspersky Endpoint Security для отдельных пользователей или групп внутри домена Active Directory. Например, если группе "Все" запрещено завершать работу приложения, вы можете предоставить отдельному пользователю разрешение **Завершение работы приложения**. В результате вы можете завершить работу приложения только с помощью учетной записи этого пользователя или учетной записи KLAdmin.

Вы можете использовать данные учетной записи для доступа к приложению, только если компьютер в домене. Если компьютер не в домене, вы можете использовать учетную запись KLAdmin или временный пароль (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 358).

Учетные записи, добавленные вручную

Вы можете создать учетную запись, которой нет в Active Directory, и назначить этой учетной записи отдельные разрешения. То есть вы можете создать *сервисную учетную запись* и использовать эту учетную запись вместо KLAdmin. Таким образом, вам не нужно делиться паролем от KLAdmin с другими пользователями или создавать новые учетные записи Active Directory. Вы можете задать любые имя пользователя и пароль. Например, вы можете предоставить пользователю сервисной учетной записи разрешение **Просмотр отчетов**. В результате, если для группы "Все" просмотр отчетов запрещен, вы можете открыть отчеты приложения с помощью сервисной учетной записи или учетной записи KLAdmin.

Предоставление разрешений для отдельных пользователей или групп

► *Как предоставить разрешение для отдельных пользователей или групп в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. В таблице учетных записей нажмите на кнопку **Добавить**.

4. Выберите тип учетной записи, которую вы хотите добавить:

   - **Выбрать пользователя / группу из Active Directory** – учетные записи Active Directory.

     Для выбора учетной записи нажмите на кнопку **Выбрать пользователя или группу**. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.

   - **Добавить пользователя вручную** – сервисная учетная запись, заданная вручную.

     Для добавления сервисной учетной записи введите имя пользователя и пароль (например, SecureAdmin).

     > Вы можете сбросить пароль сервисной учетной записи в свойствах политики. Действия по сбросу пароля сервисной учетной записи не отличаются от действий по сбросу пароля KLAdmin (см. раздел "Сброс пароля KLAdmin" на стр. 363). Если изменение параметров Защиты паролем разрешено ("замок" открыт) или политика на компьютере отсутствует, вы можете сбросить пароль сервисной учетной записи в интерфейсе приложения. Для этого нужно подтвердить изменение данных сервисной учетной записи с помощью пароля KLAdmin.

5. В списке **Разрешения** установите флажки напротив тех действий, которые будут доступны добавленному пользователю или группе без ввода пароля.

   Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы приложения** снят, вы можете завершить работу приложения только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 358).

   > Разрешения Защиты паролем имеют ряд особенностей (см. раздел "Особенности разрешений Защиты паролем" на стр. 361). Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

6. Сохраните внесенные изменения.

В результате, если для группы "Все" доступ к приложению ограничен, пользователи получат доступ к Kaspersky Endpoint Security в соответствии с разрешениями для этих пользователей.

Использование временного пароля для предоставления разрешений

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для отдельного компьютера вне корпоративной сети. Это нужно, чтобы разрешить выполнение запрещенного действия без передачи пользователю учетных данных KLAdmin. Для использования временного пароля компьютер должен быть добавлен в Kaspersky Security Center.

► *Как предоставить пользователю разрешение на выполнение запрещенного действия с помощью временного пароля через Консоль администрирования (MMC)*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Приложения**.
6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (12.12)** и откройте свойства приложения двойным щелчком мыши.
7. В окне параметров приложения выберите раздел **Общие настройки** → **Интерфейс**.
8. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
9. В открывшемся окне в блоке **Временный пароль** нажмите на кнопку **Список временных паролей**.

   Откроется окно Мониторинга временных паролей.
10. Нажмите на кнопку **Добавить**.
11. В поле **Дата истечения** установите срок действия временного пароля.
12. В таблице **Область действия временного пароля** установите флажки напротив тех действий, которые будут доступны пользователю после ввода временного пароля.
13. Нажмите на кнопку **Создать**.

    Откроется окно с временным паролем (см. рис. ниже).
14. Скопируйте и передайте пользователю пароль.

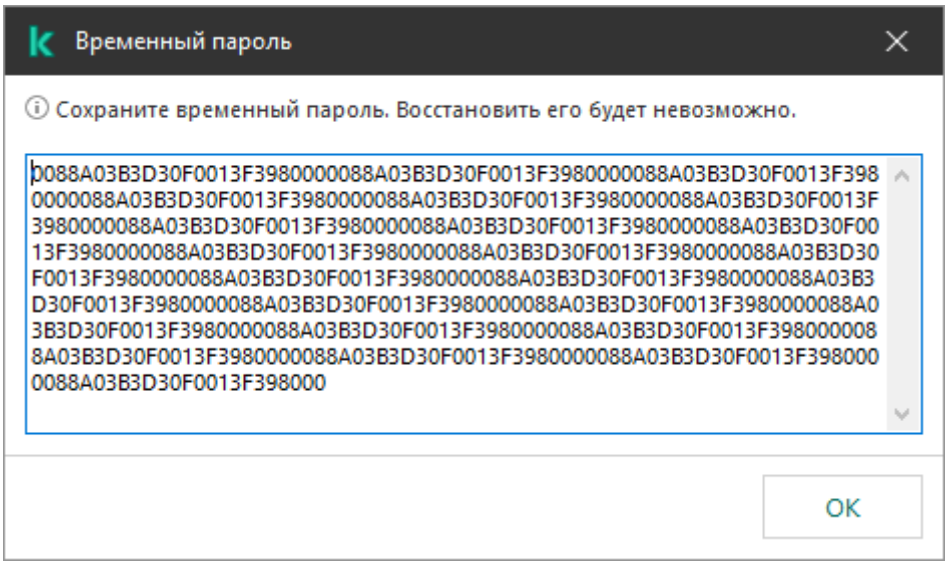
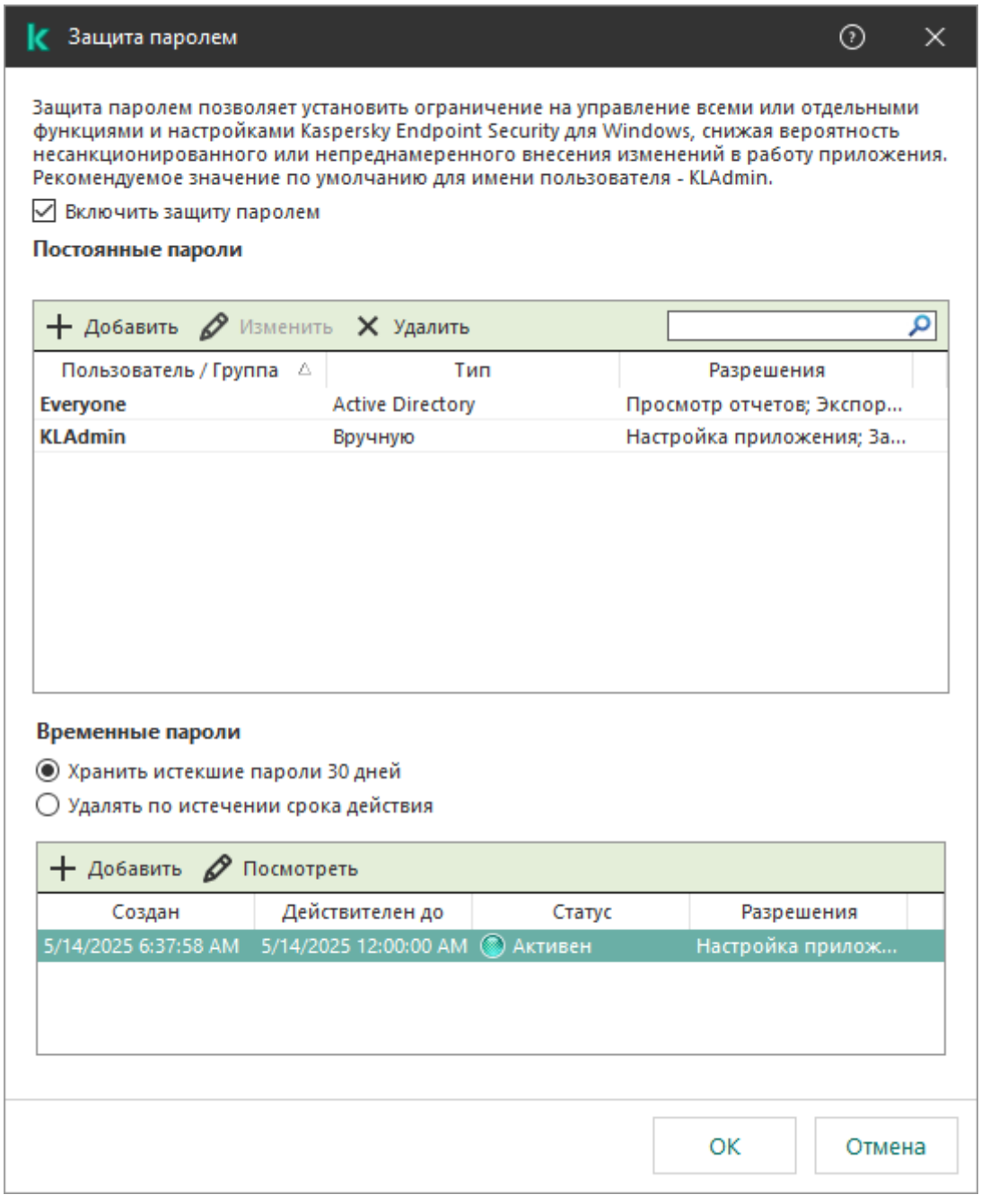


Рисунок 76. Временный пароль

Отзыв временного пароля

Начиная с версии Kaspersky Endpoint Security для Windows 12.9 добавлен инструмент *Мониторинг временных паролей*. Мониторинг временных паролей позволяет выполнять следующие действия:

- сохранять историю паролей (до 30 дней);
- контролировать статус временного пароля: *Активен*, *Истек*, *Отозван*;
- отзывать временные пароли.



Мониторинг временных паролей обновляет статус пароля и отзывает пароль только после синхронизации компьютера с Kaspersky Security Center.

► *Как отозвать временный пароль через Консоль администрирования (MMC)*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Приложения**.
6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (12.12)** и откройте свойства приложения двойным щелчком мыши.
7. В окне параметров приложения выберите раздел **Общие настройки** → **Интерфейс**.
8. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
9. В открывшемся окне в блоке **Временный пароль** настройте параметры хранения истекших паролей.
10. Нажмите на кнопку **Список временных паролей**.

    Откроется окно Мониторинга временных паролей. Мониторинг временных паролей отображает срок действия пароля, статус пароля и список разрешений.
11. Выберите активный временный пароль, который вы хотите отозвать, и откройте свойства пароля двойным щелчком мыши.
12. В открывшемся окне нажмите на кнопку **Отозвать**.
13. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки  .

В результате Мониторинг временных паролей установит статус пароля *Отзывается (синхронизация с хостом)*. После синхронизации компьютера с Kaspersky Security Center приложение отзывает временный пароль и блокирует предоставленные разрешения немедленно.

Особенности разрешений Защиты паролем

Разрешения Защиты паролем имеют ряд особенностей и ограничений.

Настройка приложения

Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты  открыты).

Завершение работы приложения

Особенностей и ограничений нет.

Выключение компонентов защиты

- Предоставить разрешение на выключение компонентов защиты для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357) с разрешением **Выключение компонентов защиты** в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты  открыты).
- Для выключения компонентов защиты в параметрах приложения пользователь должен иметь разрешение **Настройка приложения**.
- Для выключения компонентов защиты из контекстного меню (пункт **Приостановить защиту**) пользователь, кроме разрешения **Выключение компонентов защиты**, должен иметь разрешение **Выключение компонентов контроля**.

Выключение компонентов контроля

- Предоставить разрешение на выключение компонентов контроля для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357) с разрешением **Выключение компонентов контроля** в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты  открыты).
- Для выключения компонентов контроля в параметрах приложения пользователь должен иметь разрешение **Настройка приложения**.
- Для выключения компонентов контроля из контекстного меню (пункт **Приостановить защиту**) пользователь, кроме разрешения **Выключение компонентов контроля**, должен обладать разрешением **Выключение компонентов защиты**.

Выключение политики Kaspersky Security Center

Предоставить разрешение на выключение политики Kaspersky Security Center для группы "Все" невозможно. Чтобы разрешить выключение политики не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357) с разрешением **Выключение политики Kaspersky Security Center** в параметрах Защиты паролем.

Удаление ключа

Особенностей и ограничений нет.

Удаление / изменение / восстановление приложения

Если вы предоставили разрешение на удаление, изменение и восстановление приложения для группы "Все", Kaspersky Endpoint Security не будет требовать ввода пароля при попытке пользователя выполнить эти операции. Таким образом, любой пользователь, включая пользователей вне домена, может установить, изменить или восстановить приложение.

Восстановление доступа к данным на зашифрованном устройстве

Вы можете восстановить доступ к данным на зашифрованных устройствах только с помощью учетной записи KLAdmin. Разрешить это действие другому пользователю невозможно.

Просмотр отчетов

Особенностей и ограничений нет.

Восстановление из резервного хранилища

Особенностей и ограничений нет.

Экспорт настроек

По умолчанию экспорт настроек приложения запрещен для группы "Все". Вы можете экспортировать настойки приложения с помощью учетной записи KLAdmin. Экспорт настроек приложения включает в себя только создание конфигурационного файла с параметрами Kaspersky Endpoint Security в интерфейсе приложения (см. раздел "Создание и использование конфигурационного файла" на стр. 373). Разрешение не ограничивает экспорт списков исключений из проверки, доверенных веб-адресов, доверенных устройств или других списков компонентов приложения.

Сброс пароля KLAdmin

Если вы забыли пароль для учетной записи KLAdmin, вы можете сбросить пароль в свойствах политики. Сбросить пароль в интерфейсе приложения невозможно.

Вы можете выполнять действия, защищенные паролем, с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 358). В этом случае вводить данные учетной записи KLAdmin не нужно.

Если компьютер не подключен к Kaspersky Security Center и вы забыли пароль для учетной записи KLAdmin, восстановить пароль невозможно.

► *Как сбросить пароль для учетной записи KLAdmin в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Интерфейс**.
4. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
5. В открывшемся окне снимите флажок **Включить защиту паролем**.
6. Сохраните внесенные изменения.
7. Повторно установите флажок **Включить защиту паролем**.
8. Нажмите на кнопку **ОК**.

   Откроется окно для ввода пароля администратора.
9. Задайте новый пароль для учетной записи KLAdmin и подтвердите его.
10. Сохраните внесенные изменения.

В результате пароль для учетной записи KLAdmin будет обновлен после применения политики.

kaspersky

Защита подключения к Серверу администрирования

Для подключения компьютера к Серверу администрирования предназначен компонент Kaspersky Security Center – *Агент администрирования*. Если злоумышленник обладает достаточными правами для изменения параметров подключения к серверу, есть риск переподключения компьютера к недоверенному серверу. Таким образом, злоумышленник может применить собственные групповые политики и, например, выключить самозащиту приложения. Kaspersky Endpoint Security позволяет предотвратить несанкционированное переподключение компьютера к другому серверу. Для защиты подключения к серверу приложение предлагает задать пароль и использовать стандарт формирования ключа на основе пароля (англ. Password-Based key Derivation Function, PBKDF2). В результате получить доступ к приложению без пароля невозможно.

Для комплексной защиты Kaspersky Endpoint Security и Агента администрирования от несанкционированного доступа рекомендуется включить дополнительную защиту. Для Kaspersky Endpoint Security рекомендуется включить Защиту паролем (см. раздел "Защита паролем" на стр. 352). Для защиты Агента администрирования рекомендуется установить пароль деинсталляции. Подробнее о защите Агента администрирования от удаления см. в справке Kaspersky Security Center https://support.kaspersky.com/KSC/15.1/ru-ru/158030.htm.

Для управления подключением компьютера к Серверу администрирования предназначена задача *Защита подключения к Серверу администрирования*. Задача позволяет выполнять следующие действия:

- Задать пароль для защиты подключения к серверу.
- Сменить пароль.
- Переподключить компьютер к другому серверу.
- Выключить защиту подключения к серверу.

Аутентификация компьютера при подключении к Серверу администрирования

После установки пароля приложение создает массив данных с помощью PBKDF2-преобразования пароля. Далее приложение зашифровывает этот массив данных с помощью ключа Агента администрирования. На основании зашифрованного массива данных приложение осуществляет проверку прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем при попытке переподключить компьютер к Серверу администрирования приложение расшифровывает массив данных с помощью ключа Агента администрирования и сравнивает его с локальной копией. Если они не совпадают, доступ к приложению ограничен.

Защита подключения к Серверу администрирования

► *Как установить пароль для защиты подключения компьютера к серверу в Консоли администрирования (MMC)*

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (12.12) → Защита подключения к Серверу администрирования**.

Шаг 2. Защита подключения к Серверу администрирования

Установите пароль для защиты подключения к Серверу администрирования:

1. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать паролем**.
2. В раскрывающемся списке **Сервер администрирования** выберите **Новый сервер**.
3. В поле **Пароль для подключения к Серверу администрирования** задайте пароль для подключения к Серверу администрирования и подтвердите его.

   Если вы забудете пароль, вы сможете сменить его с помощью задачи.
4. Если у вас развернуто приложение Kaspersky Endpoint Security версии 12.7 или более ранние версии приложения, установите флажок **Включить совместимость шифрования пароля для более ранних версий приложения (12.7 и ниже)**.

   Начиная с версии Kaspersky Endpoint Security для Windows 12.8 в приложении используется более сильное шифрование пароля. Если в вашей организации развернуто приложение Kaspersky Endpoint Security 12.8 и выше, рекомендуется снять флажок и использовать более сильное шифрование пароля. Более ранние версии приложения не поддерживает сильное шифрование пароля. Для выполнения задачи необходимо установить флажок.

Шаг 3. Выбор учетной записи для запуска задачи

Выберите **Учетная запись по умолчанию**. По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

Шаг 4. Настройка расписания запуска задачи

В блоке **Запуск по расписанию** выберите **Вручную**.

Шаг 5. Определение названия задачи

Введите название задачи, например, *Пароль для подключения к главному серверу*.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Установите флажок **Запустить задачу после завершения работы мастера** или запустите задачу вручную. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Переподключение компьютера к другому Серверу администрирования

Переподключение компьютера к другому Серверу администрирования состоит из следующих этапов:

1. В консоли текущего сервера `[KSC1]` нужно запустить задачу *Смена Сервера администрирования* для Агента администрирования.

   После выполнения задачи компьютер будет переподключен к новому серверу `[KSC2]`.

   Компьютер будет отображаться в консоли сервера `[KSC1]` со статусом *Критический*  . Настроить параметры приложения с помощью политик или дистанционно запустить задачи на компьютере будет невозможно.
2. В консоли нового сервера `[KSC2]` нужно создать новую задачу *Защита подключения к Серверу администрирования* для Kaspersky Endpoint Security. В свойствах задачи вам нужно ввести пароль от прежнего сервера и задать пароль для нового сервера.

Как установить новый пароль для переподключения к новому серверу в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (12.12) → Защита подключения к Серверу администрирования**.

Шаг 2. Защита подключения к Серверу администрирования

Установите пароль для защиты подключения к новому Серверу администрирования:

1. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать паролем**.
2. В раскрывающемся списке **Сервер администрирования** выберите **Переподключиться от другого сервера**.
3. В поле **Текущий пароль** введите пароль, установленный для подключения к прежнему доверенному серверу.
4. В поле **Новый пароль** задайте пароль для подключения к новому Серверу администрирования и подтвердите его.

   Если вы забудете пароль, вы сможете сменить его с помощью задачи.

5. Если у вас развернуто приложение Kaspersky Endpoint Security версии 12.7 или более ранние версии приложения, установите флажок **Включить совместимость шифрования пароля для более ранних версий приложения (12.7 и ниже)**.

   Начиная с версии Kaspersky Endpoint Security для Windows 12.8 в приложении используется более сильное шифрование пароля. Если в вашей организации развернуто приложение Kaspersky Endpoint Security 12.8 и выше, рекомендуется снять флажок и использовать более сильное шифрование пароля. Более ранние версии приложения не поддерживает сильное шифрование пароля. Для выполнения задачи необходимо установить флажок.

Шаг 3. Выбор учетной записи для запуска задачи

Выберите **Учетная запись по умолчанию**. По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

Шаг 4. Настройка расписания запуска задачи

В блоке **Запуск по расписанию** выберите **Вручную**.

Шаг 5. Определение названия задачи

Введите название задачи, например, *Пароль для подключения к главному серверу*.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Установите флажок **Запустить задачу после завершения работы мастера** или запустите задачу вручную. Вы можете следить за ходом выполнения задачи в свойствах задачи.

После выполнения задачи убедитесь, что компьютер в консоли нового сервера `[KSC2]` имеет

статус *OK*  . Проверьте дистанционный запуск задач и настройку параметров приложения с помощью политик.

Сброс пароля для подключения к Серверу администрирования

Если вы забыли пароль для подключения к Серверу администрирования или пароль раскрыт, вы можете сбросить пароль в свойствах задачи. Также вы можете сбросить пароль и задать новый пароль для группы компьютеров с разным статусом защиты подключения к Серверу администрирования. То есть, если для некоторых компьютеров защита включена, а для некоторых нет, после выполнения задачи пароль будет установлен для всех компьютеров.

Вы можете сбросить пароль для подключения к Серверу администрирования только в консоли доверенного сервера, к которому подключен компьютер.

► *Как сбросить пароль для подключения к Серверу администрирования в Консоли администрирования (MMC)*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.
3. Выберите задачу **Защита подключения к Серверу администрирования** и откройте свойства задачи двойным щелчком мыши.
4. В окне свойств задачи выберите раздел **Настройки**.
5. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать и сменить пароль**.
6. В поле **Пароль для подключения к Серверу администрирования** задайте новый пароль для подключения к текущему доверенному серверу и подтвердите его.
7. Сохраните внесенные изменения.
8. Запустите задачу.

В результате пароль для подключения к Серверу администрирования будет обновлен после выполнения задачи.

Выключение защиты подключения к Серверу администрирования

Вы можете дистанционно выключить защиту подключения к Серверу администрирования только в консоли доверенного сервера, к которому подключен компьютер. Также вы можете выключить защиту локально через командную строку.

► *Как выключить защиту подключения компьютера к серверу в Консоли администрирования (MMC)*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.

3. Выберите задачу **Защита подключения к Серверу администрирования** и откройте свойства задачи двойным щелчком мыши.
4. В окне свойств задачи выберите раздел **Настройки**.
5. В блоке **Защита подключения к Серверу администрирования** выберите **Не защищать**.
6. Сохраните внесенные изменения.
7. Запустите задачу.

   Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой.

kaspersky

Производительность Kaspersky Endpoint Security и совместимость с другими приложениями

Под производительностью Kaspersky Endpoint Security подразумевается количество обнаруживаемых типов объектов, которые могут нанести вред компьютеру, а также потребление энергии и ресурсов компьютера.

Выбор типов обнаруживаемых объектов

Kaspersky Endpoint Security позволяет гибко настраивать защиту компьютера и выбирать типы объектов (см. раздел "Создание исключения по типу обнаруживаемых объектов" на стр. 326), которые приложение обнаруживает в ходе работы. Kaspersky Endpoint Security всегда проверяет операционную систему на наличие вирусов, червей и троянских приложений. Вы не можете выключить проверку этих типов объектов. Такие приложения могут нанести значительный вред компьютеру пользователя. Чтобы обеспечить большую безопасность компьютера, вы можете расширить список обнаруживаемых типов объектов, включив контроль действий легальных приложений, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Использование режима энергосбережения

Во время работы на портативных компьютерах потребление приложениями энергоресурсов имеет особое значение. Зачастую задачи, которые Kaspersky Endpoint Security выполняет по расписанию, требуют значительного количества ресурсов. При питании компьютера от аккумулятора для экономии его заряда вы можете использовать режим энергосбережения.

Режим энергосбережения позволяет автоматически откладывать выполнение задач, для которых установлен запуск по расписанию:

- задача обновления;
- задача полной проверки;
- задача проверки важных областей;
- задача выборочной проверки;
- задача проверки целостности.

Независимо от того, включен режим энергосбережения или нет, Kaspersky Endpoint Security приостанавливает выполнение задач шифрования при переходе портативного компьютера в режим работы от аккумулятора. При выходе портативного компьютера из режима работы от аккумулятора в режим работы от сети приложение возобновляет выполнение задач шифрования.

Передача ресурсов компьютера другим приложениям

Потребление ресурсов компьютера при проверке компьютера может увеличить нагрузку на центральный процессор и дисковые подсистемы. Чтобы решить проблему совместной работы при увеличении нагрузки на процессор и дисковые подсистемы, Kaspersky Endpoint Security может уступать ресурсы другим приложениям.

Применение технологии лечения активного заражения

Современные вредоносные приложения могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. Обнаружив вредоносную активность в операционной системе, Kaspersky Endpoint Security выполняет расширенную процедуру лечения, применяя

специальную технологию лечения активного заражения. *Технология лечения активного заражения* направлена на лечение операционной системы от вредоносных приложений, которые уже запустили свои процессы в оперативной памяти и мешают Kaspersky Endpoint Security удалить их с помощью других методов. В результате угроза нейтрализуется. В процессе процедуры лечения активного заражения не рекомендуется запускать новые процессы или редактировать реестр операционной системы. Технология лечения активного заражения требует значительных ресурсов операционной системы, что может замедлить работу других приложений.

После окончания процедуры лечения активного заражения на компьютере под управлением операционной системы Microsoft Windows для рабочих станций Kaspersky Endpoint Security запрашивает у пользователя разрешение на перезагрузку компьютера. После перезагрузки компьютера Kaspersky Endpoint Security удаляет файлы вредоносного программного обеспечения и запускает облегченную полную проверку компьютера.

Запрос перезагрузки на компьютере под управлением операционной системы Microsoft Windows для серверов невозможен из-за особенностей приложения Kaspersky Endpoint Security. Незапланированная перезагрузка файлового сервера может повлечь за собой проблемы, связанные с временным отказом доступа к данным файлового сервера или потерей несохраненных данных. Перезагрузку файлового сервера рекомендуется выполнять строго по расписанию. Поэтому по умолчанию технология лечения активного заражения для файловых серверов выключена (см. раздел "Технология лечения активного заражения" на стр. 102).

В случае обнаружения активного заражения на файловом сервере, на Kaspersky Security Center передается событие о необходимости лечения активного заражения. Для лечения активного заражения на сервере требуется включить технологию лечения активного заражения для серверов и запустить групповую задачу *Поиск вредоносного ПО* в удобное для пользователей сервера время.

В этом разделе

Включение и выключение режима энергосбережения 370

Включение и выключение режима передачи ресурсов другим приложениям 371

Включение и выключение режима энергосбережения

► *Чтобы включить или выключить режим энергосбережения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

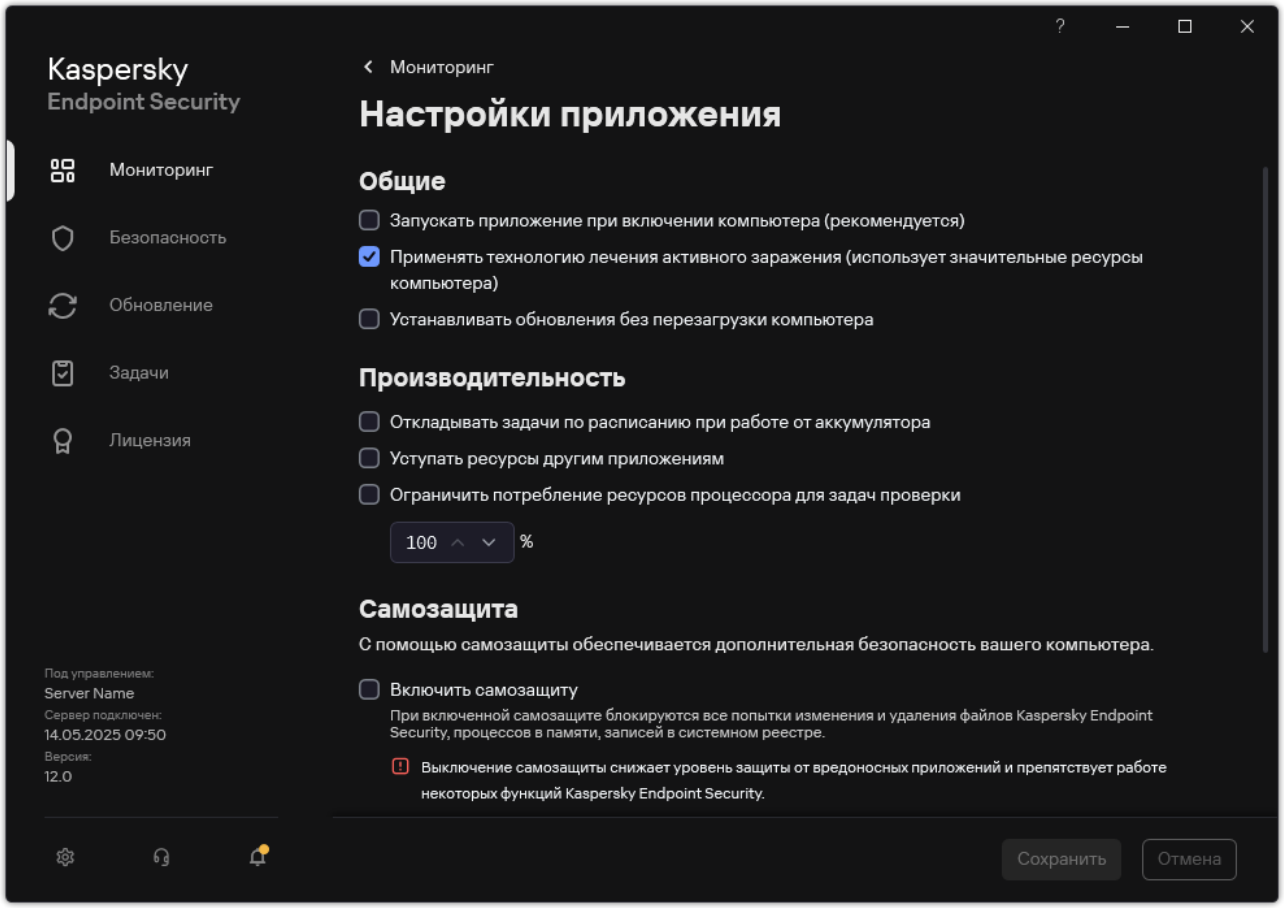


Рисунок 77. Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Производительность** используйте флажок **Откладывать задачи по расписанию при работе от аккумулятора**, чтобы включить или выключить режим энергосбережения.

   Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию:

   - *Обновление баз и модулей приложения*;
   - *Полная проверка*;
   - *Проверка важных областей*;
   - *Выборочная проверка*;
   - *Проверка целостности приложения*;
   - *Поиск IOC*.

4. Сохраните внесенные изменения.

kaspersky

Включение и выключение режима передачи ресурсов другим приложениям

Потребление ресурсов компьютера Kaspersky Endpoint Security при проверке компьютера может увеличить нагрузку на центральный процессор и дисковые подсистемы. Это может замедлить работу других приложений. Для оптимизации производительности в Kaspersky Endpoint Security предусмотрен *режим передачи ресурсов другим приложениям*. В этом режиме операционная система может понизить приоритет потоков задач проверки Kaspersky Endpoint Security при высокой нагрузке на центральный процессор. Это позволит перераспределить ресурсы операционной системы для других приложений. То есть задачи проверки получат меньше процессорного времени. В результате Kaspersky Endpoint Security будет проверять компьютер дольше. По умолчанию режим передачи ресурсов другим приложениям включен.

► *Как включить или выключить режим передачи ресурсов другим приложениям в интерфейсе приложения*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.
3. В блоке **Производительность** используйте флажок **Уступать ресурсы другим приложениям**, чтобы включить или выключить режим передачи ресурсов другим приложениям.
4. Сохраните внесенные изменения.

kaspersky

Создание и использование конфигурационного файла

Конфигурационный файл с параметрами работы Kaspersky Endpoint Security позволяет решить следующие задачи:

- Выполнить локальную установку Kaspersky Endpoint Security через командную строку с заранее заданными параметрами (см. раздел "Setup. Установка приложения" на стр. 376).
- Выполнить удаленную установку Kaspersky Endpoint Security через Kaspersky Security Center с заранее заданными параметрами.
- Перенести параметры работы Kaspersky Endpoint Security с одного компьютера на другой (см. инструкцию ниже).

Экспорт конфигурационного файла

► *Чтобы создать конфигурационный файл, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Управление настройками**.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне укажите путь, по которому вы хотите сохранить конфигурационный файл, и введите его имя.

   Чтобы использовать конфигурационный файл для локальной или удаленной установки Kaspersky Endpoint Security, необходимо назвать его install.cfg.

5. Если требуется, введите пароль для экспорта конфигурации приложения в файл.

   Для сохранения конфигурационного файла должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешение **Экспорт настроек**.

6. Сохраните файл.

В результате приложение создаст конфигурационный файл. Так как конфигурационный файл может содержать параметры учетных записей, Kaspersky Endpoint Security шифрует файл. Внести изменения в конфигурационный файл невозможно. Любые попытки внести изменения в файл приведут к его повреждению.

Импорт конфигурационного файла

Конфигурационный файл может содержать параметры учетных записей, добавленных в приложение. Если вы импортируете файл на том же компьютере, на котором файл был создан, то Kaspersky Endpoint Security импортирует пароли учетных записей. Если вы импортируете файл на другом компьютере, вам необходимо ввести пароли вручную.

► *Чтобы импортировать параметры работы Kaspersky Endpoint Security из конфигурационного файла, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Управление настройками**.
3. Нажмите на кнопку **Импортировать**.
4. В открывшемся окне укажите путь к конфигурационному файлу.
5. Откройте файл.

Все значения параметров Kaspersky Endpoint Security будут установлены в соответствии с выбранным конфигурационным файлом.

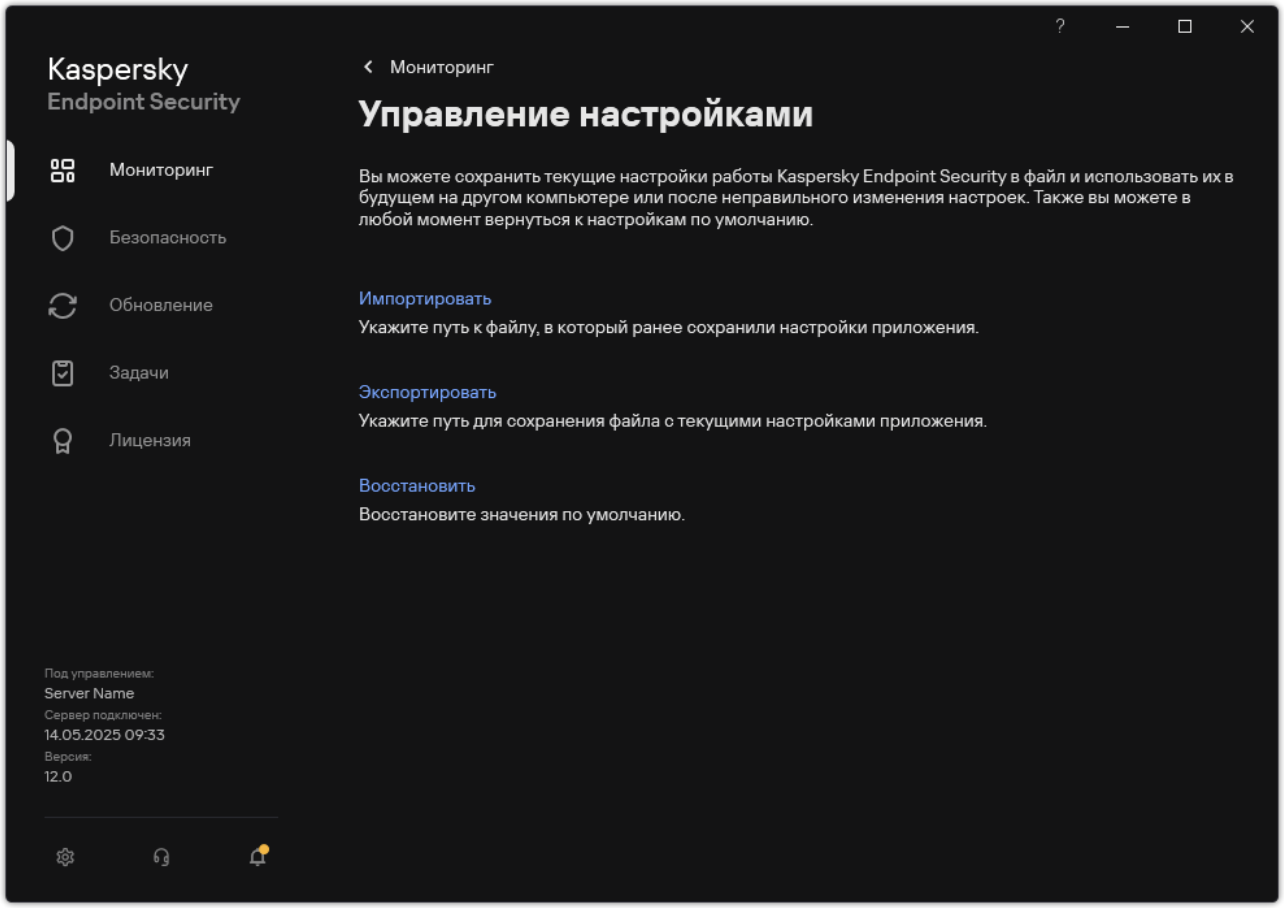


Рисунок 78. Управление настройками приложения

См. также:

Setup. Установка приложения 376
EXPORT. Экспорт параметров приложения 401
IMPORT. Импорт параметров приложения 402

kaspersky

Восстановление параметров приложения по умолчанию

Вы в любое время можете восстановить настройки приложения, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

► *Чтобы восстановить параметры приложения по умолчанию, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Управление настройками**.
3. Нажмите на кнопку **Восстановить**.
4. Сохраните внесенные изменения.

kaspersky

Работа с приложением из командной строки

Этот раздел содержит описание работы с Kaspersky Endpoint Security из командной строки.

В этом разделе

Setup. Установка приложения 376
Setup /x. Удаление приложения 385
msiexec /i. Восстановление приложения 386
Команды AVP 387
Команды KESCLI 409
Команды управления Detection and Response 417
Сообщения об ошибках 427
Коды возврата 431
Коды ошибок 437
Использование профилей задач 443
Профили приложения 444

Setup. Установка приложения

Установку Kaspersky Endpoint Security из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки приложения.
- В тихом режиме. После запуска установки в тихом режиме ваше участие в процессе установки не требуется (тихая установка). Для установки приложения в тихом режиме используйте ключи `/s` и `/qn`.

  Перед установкой приложения в тихом режиме откройте и прочитайте Лицензионное соглашение и текст Политики конфиденциальности. Лицензионное соглашение и текст Политики конфиденциальности входят в комплект поставки Kaspersky Endpoint Security. Приступайте к установке приложения, только если вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения, если вы понимаете и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности, если вы полностью прочитали и понимаете Политику конфиденциальности. Если вы не принимаете положения и условия Лицензионного соглашения и Политику конфиденциальности, не устанавливайте и не используйте Kaspersky Endpoint Security.

Вы можете просмотреть список команд для установки приложения с помощью команды `/h`. Чтобы получить справку по синтаксису команды установки, введите `setup_kes.exe /h`. В результате инсталлятор покажет окно с описанием параметров команды (см. рис. ниже).

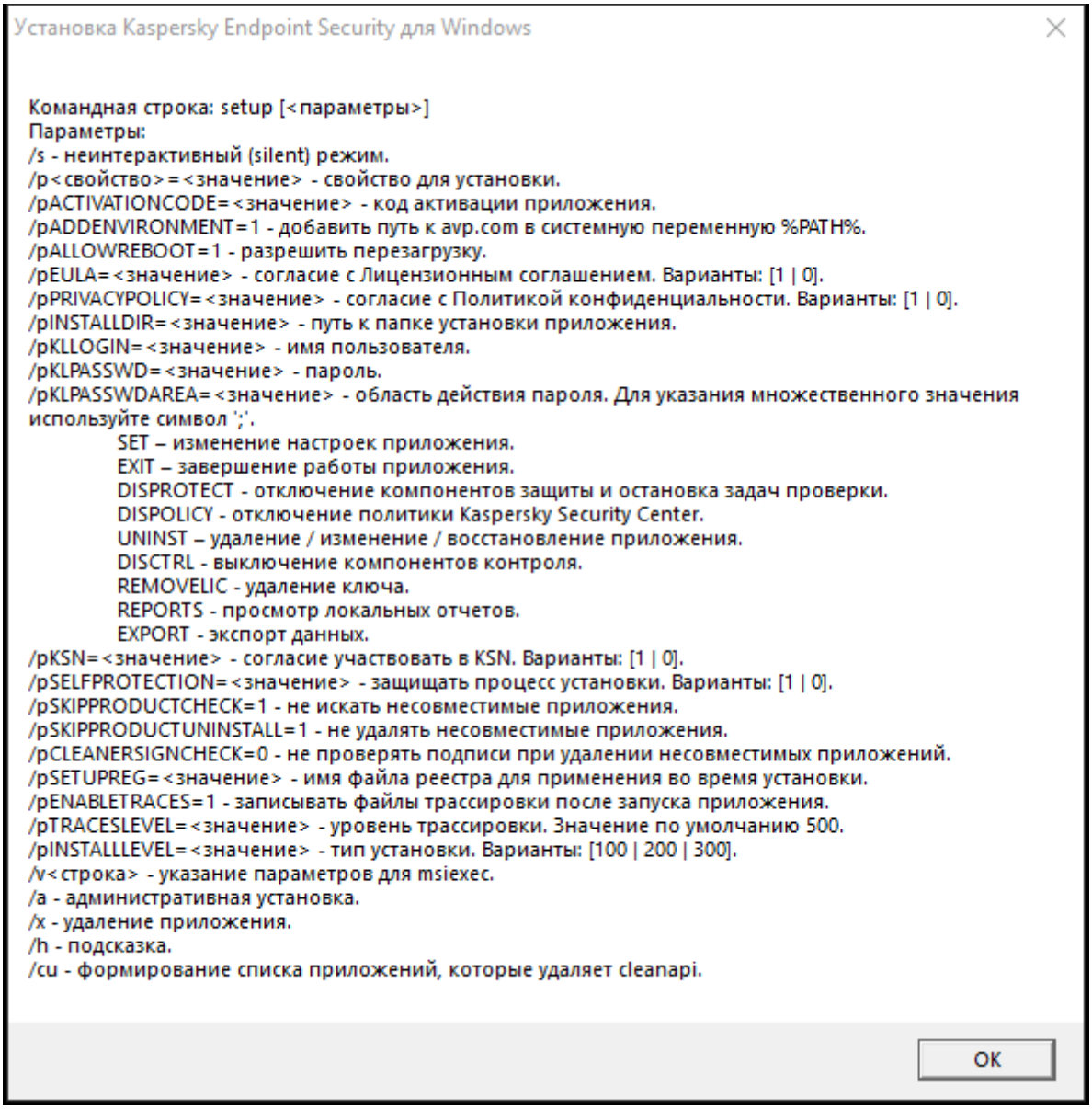


Рисунок 79. Описание параметров команды установки

► *Чтобы установить приложение или обновить предыдущую версию приложения, выполните следующие действия:*

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.
3. Выполните команду:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path
to the configuration file>] [/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1]
[/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=<password>
/pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0
/pTRACESLEVEL=<tracing level>] [/pSKIPKB5007186CHECK=1] [/s]
```

или

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[CONFIGPATH=<path to the configuration file>]
[ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name>
KLPASSWD=<password> KLPASSWDAREA=<password scope>] [ENABLETRACES=1|0
TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

В результате приложение будет установлено на компьютер. Вы можете убедиться, что приложение установлено, и проверить параметры приложения с помощью команды `status` (см. раздел "`STATUS. Статус профиля`" на стр. 399).

Таблица 22. Параметры установки приложения

`EULA=1`	Согласие с положениями Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки Kaspersky Endpoint Security. Согласие с положениями Лицензионного соглашения является необходимым условием для установки приложения или обновления версии приложения.
`PRIVACYPOLICY=1`	Согласие с Политикой конфиденциальности. Текст Политики конфиденциальности входит в комплект поставки Kaspersky Endpoint Security. Согласие с Политикой конфиденциальности является необходимым условием для установки приложения или обновления версии приложения.
`KSN`	Согласие или отказ участвовать в Kaspersky Security Network (KSN). Если параметр не указан, Kaspersky Endpoint Security запросит подтверждения участия в KSN при первом запуске приложения. Возможные значения: • `1` – согласие участвовать в KSN. • `0` – отказ участвовать в KSN (значение по умолчанию). Дистрибутив Kaspersky Endpoint Security оптимизирован для использования Kaspersky Security Network. Если вы отказались от участия в Kaspersky Security Network, то сразу после завершения установки обновите Kaspersky Endpoint Security.
`CONFIGPATH=<path to the configuration file>`	Установка приложение с заранее заданными параметрами. Для этого вам нужно загрузить файл, который задает параметры работы Kaspersky Endpoint Security. Вы можете создать конфигурационный файл в локальном интерфейсе приложения (см. раздел "Создание и использование конфигурационного файла" на стр. 373).

ALLOWREBOOT=1	Автоматическая перезагрузка компьютера после установки или обновления приложения, если требуется. Если параметр не задан, автоматическая перезагрузка компьютера запрещена. При установке Kaspersky Endpoint Security перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые приложения. Также перезагрузка может потребоваться при обновлении версии приложения.
SKIPPRODUCTCHECK=1	Выключение проверки установленного ПО. Список ПО, с которым могут быть проблемы совместимости, приведен в файле incompatible.txt в комплекте поставки. Если параметр не задан, при обнаружении приложения из списка установка Kaspersky Endpoint Security будет прекращена.
SKIPPRODUCTUNINSTALL=1	Запрет на автоматическое удаление найденных приложений из списка incompatible.txt. Если параметр не задан, Kaspersky Endpoint Security пытается удалить приложения, с которыми могут быть проблемы совместимости. Включить автоматическое удаление ПО при установке Kaspersky Endpoint Security с помощью установщика msiexec невозможно. Для автоматического удаления ПО, с которым могут быть проблемы совместимости, используйте файл setup_kes.exe.
CLEANERSIGNCHECK=0|1	Проверка цифровых подписей файлов найденного ПО из файла incompatible.txt. Для удаления ПО приложение Kaspersky Endpoint Security запускает файл инсталлятора программного обеспечения. Если у файла инсталлятора нет цифровой подписи, Kaspersky Endpoint Security считает такой файл недоверенным, и для предотвращения исполнения вредоносного кода приложение прекращает удаление ПО. Если приложение не может проверить цифровую подпись файла найденного ПО, установка Kaspersky Endpoint Security будет остановлена с ошибкой. Значение по умолчанию отличается в зависимости от способа установки приложения: • 0 – проверка цифровой подписи выключена (значение по умолчанию при развертывании через Kaspersky Security Center). • 1 – проверка цифровой подписи включена (значение по умолчанию при локальной установке приложения).

STANDALONEMODE=1	Установка приложения в конфигурации Endpoint Detection and Response агента (EDR-агент) для интеграции с решениями Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Endpoint Detection and Response Expert (on-premise). Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение класса Endpoint Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.
KLLOGIN	Установка имени пользователя для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (компонент Защита паролем (на стр. 352)). Имя пользователя устанавливается вместе с параметрами KLPASSWD и KLPASSWDAREA. По умолчанию используется имя пользователя KLAdmin.
KLPASSWD	Установка пароля для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (пароль устанавливается вместе с параметрами KLLOGIN и KLPASSWDAREA). Если вы указали пароль, но не задали имя пользователя с помощью параметра KLLOGIN, то по умолчанию используется имя пользователя KLAdmin.

KLPASSWDAREA

Определение области действия пароля для доступа к Kaspersky Endpoint Security. При попытке пользователя выполнить действие из этой области Kaspersky Endpoint Security запрашивает учетные данные пользователя (параметры KLLOGIN и KLPASSWD). Для указания множественного значения используйте символ ;.

Возможные значения:

- SET – изменение параметров приложения.
- EXIT – завершение работы приложения.
- DISPROTECT – выключение компонентов защиты и остановка задач проверки.
- DISPOLICY – выключение политики Kaspersky Security Center.
- UNINST – удаление приложения с компьютера.
- DISCTRL – выключение компонентов контроля.
- REMOVELIC – удаление ключа.
- REPORTS – просмотр отчетов.
- EXPORT – экспорт параметров приложения.

Например,
KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT.

Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем. Поэтому настроить область действия пароля для учетной записи KLAdmin невозможно. Если вы попытаетесь настроить область действия пароля для учетной записи KLAdmin, приложение запретит перечисленные действия для группы "Все".

PROTECTOSSERVICES

Функция Защита сервисов операционной системы. Защита сервисов операционной системы предотвращает вмешательство сторонних приложений в работу сервисов операционной системы. К таким сервисам относится, например, сервис автозапуска приложений.

- 1 – Защита сервисов операционной системы включена (значение по умолчанию).
- 0 – Защита сервисов операционной системы выключена.

ENABLETRACES

Включение или выключение трассировки приложения. После запуска Kaspersky Endpoint Security приложение сохраняет файлы трассировки в папке %ProgramData%\Kaspersky Lab\KES.12.12\Traces. Возможные значения:

- 1 – трассировка включена.
- 0 – трассировка выключена (значение по умолчанию).

TRACESLEVEL	Уровень детализации трассировки. Возможные значения: • 100 (критический). Только сообщения о неустранимых ошибках. • 200 (высокий). Сообщения обо всех ошибках, включая неустранимые. • 300 (диагностический). Сообщения обо всех ошибках, а также предупреждения. • 400 (важный). Сообщения обо всех ошибках, предупреждения, а также дополнительная информация. • 500 (обычный). Сообщения обо всех ошибках, предупреждениях, а также подробная информация о работе приложения в нормальном режиме (значение по умолчанию). • 600 (низкий). Все сообщения.
ENABLEAZURESUPPORT	Включение или выключение режима совместимости с Azure WVD. Возможные значения: • 1 – режим совместимости с Azure WVD включен. • 0 – режим совместимости с Azure WVD выключен (значение по умолчанию). Функция позволяет корректно показывать состояние виртуальной машины Azure в консоли Kaspersky Anti Targeted Attack Platform. Для контроля за состоянием компьютера Kaspersky Endpoint Security отправляет на серверы KATA телеметрию. Телеметрия включает в себя идентификатор компьютера (Sensor ID). Режим совместимости с Azure WVD позволяет назначать постоянный уникальный Sensor ID для этих виртуальных машин. Если режим совместимости выключен, то из-за особенностей работы виртуальных машин Azure Sensor ID может изменяться после перезагрузки компьютера. Из-за этого возможно дублирование виртуальных машин в консоли.
AMPPL	Включение или выключение защиты процессов Kaspersky Endpoint Security с использованием технологии AM-PPL (Antimalware Protected Process Light). Подробнее о технологии AM-PPL см. на сайте Microsoft (https://learn.microsoft.com/ru-ru/windows/win32/services/protecting-anti-malware-services-/). Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019. Возможные значения: • 1 – защита процессов Kaspersky Endpoint Security с использованием технологии AM-PPL включена (значение по умолчанию). • 0 – защита процессов Kaspersky Endpoint Security с использованием технологии AM-PPL выключена.

UPGRADEMODE	Режим обновления приложения: • Seamless – обновление приложения с перезагрузкой компьютера (значение по умолчанию). • Force – обновление приложения без перезагрузки. Вы можете обновлять версию приложения без перезагрузки начиная с версии 11.10.0. Для обновление более ранних версий приложения необходимо выполнять перезагрузку компьютера. Также вы можете устанавливать патчи без перезагрузки начиная с версии 11.11.0. При установке Kaspersky Endpoint Security перезагрузка не требуется. Таким образом, режим обновления приложения будет установлен в параметрах приложения. Вы можете изменить этот параметр в настройках приложения или в политике. Если приложение уже установлено, при установке обновления приоритет параметра из командной строки ниже, чем параметр, заданный в настройках приложения или в файле setup.ini. То есть, если в командной строке задан режим Force, а в параметрах приложения задан режим Seamless, инсталлятор установит обновление с перезагрузкой (Seamless).
RESTAPI	Управление приложением через REST API. Для управления приложением через REST API обязательно нужно задать имя пользователя (параметр RESTAPI_User). Возможные значения: • 1 – управление через REST API разрешено. • 0 – управление через REST API запрещено (значение по умолчанию). Для управления приложением через REST API должно быть разрешено управление с помощью систем администрирования. Для этого задайте параметр AdminKitConnector=1. Если вы управляете приложением через REST API, управлять приложением с помощью систем администрирования "Лаборатории Касперского" невозможно.
RESTAPI_User	Имя пользователя доменной учетной записи Windows для управления приложением через REST API. Управление приложением через REST API доступно только этому пользователю. Введите имя пользователя в формате <DOMAIN>\<UserName> (например, RESTAPI_User=COMPANY\Administrator). Для работы с REST API вы можете выбрать только одного пользователя. Добавление имени пользователя является необходимым условием для управления приложением через REST API.
RESTAPI_Port	Порт для управления приложением через REST API. По умолчанию используется порт 6782. Убедитесь, что порт свободен.

`RESTAPI_Certificate`	Сертификат для идентификации запросов (например, `RESTAPI_Certificate=C:\cert.pem`). Для безопасной работы Kaspersky Endpoint Security с REST-клиентом вам нужно настроить идентификацию запросов. Для этого вам нужно установить сертификат и в дальнейшем подписывать полезные данные каждого запроса.
`ADMINKITCONNECTOR`	Управление приложением с помощью систем администрирования. К системам администрирования относится, например, Kaspersky Security Center. Кроме систем администрирования "Лаборатории Касперского" вы можете использовать сторонние решения. Для этого Kaspersky Endpoint Security предоставляет API. Возможные значения: • `1` – управление приложением с помощью систем администрирования разрешено (значение по умолчанию). • `0` – разрешено управление приложением только через локальный интерфейс.
`EnableUniqueSensorID`	Создание уникального идентификатора компьютера (Sensor ID) при установке или обновлении приложения. Sensor ID используется в решении Kaspersky Anti Targeted Attack Platform для идентификации компьютеров, которые отправляют телеметрию на сервер. При создании Sensor ID приложение использует алгоритм, который учитывает конфигурацию компьютера, например, серийный номер материнской платы. В некоторых случаях, например, при использовании приложения в виртуальной среде, Sensor ID может повторяться. Таким образом, Kaspersky Anti Targeted Attack Platform не может идентифицировать компьютер, с которого отправлена телеметрия. Для создания уникального Sensor ID вам нужно задать параметр `EnableUniqueSensorID=1`. В результате приложение будет использовать другой алгоритм для создания Sensor ID, который учитывает другие данные о компьютере. Это обеспечивает уникальный Sensor ID. По умолчанию параметр не задан. Приложение наследует Sensor ID в следующих случаях: • обновление версии приложения; • миграция конфигурации [KES+KEA] на [KES+встроенный агент]. При восстановлении приложения установщик пытается наследовать Sensor ID. Если восстановить Sensor ID не удалось, приложение создает новый Sensor ID.
`SKIPKB5007186CHECK=1`	Выключение проверки установленного обновления операционной системы KB5007186. Перед установкой приложения установщик проверяет наличие обновлений операционной системы. Обновление KB5007186 входит в список обновлений операционной системы, которые могут привести к проблемам в работе приложения. Подробнее см. в базе знаний Службы технической поддержки https://support.kaspersky.ru/kes-for-windows/12.4/troubleshooting/compatibility/15819. Поэтому установщик, обнаружив это обновление, останавливает установку приложения. Для продолжения установки приложения задайте параметр `SKIPKB5007186CHECK=1`.

Пример:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Passwo
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=
```

После установки приложения Kaspersky Endpoint Security происходит активация по пробной лицензии, если вы не указали код активации в файле setup.ini. Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно активировать приложение по коммерческой лицензии с помощью мастера активации приложения или специальной команды.

Во время установки приложения или обновления версии приложения в тихом режиме поддерживается использование следующих файлов:

- setup.ini – общие параметры установки приложения.

  Чтобы применить параметры из файла setup.ini, разместите файл в папке с дистрибутивом Kaspersky Endpoint Security.

- install.cfg (см. раздел "Создание и использование конфигурационного файла" на стр. 373) – параметры работы Kaspersky Endpoint Security.

  Чтобы применить параметры из конфигурационного файла install.cfg вам нужно указать путь к файлу в команде установки приложения: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – ключи реестра.

  Запись ключей реестра из файла setup.reg в реестр осуществляется, только если в файле setup.ini указано значение `setup.reg` для параметра `SetupReg`. Файл setup.reg формируется специалистами "Лаборатории Касперского". Не рекомендуется изменять содержимое этого файла. Чтобы применить параметры из файла setup.reg, разместите файл в папке с дистрибутивом Kaspersky Endpoint Security. Также вы можете разместить файл setup.reg в другой папке. В этом случае вам нужно указать путь к файлу в команде установки приложения: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Удаление приложения

Удаление Kaspersky Endpoint Security из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки приложения.
- В тихом режиме. После запуска удаления в тихом режиме ваше участие в процессе удаления не требуется (тихое удаление). Для удаления приложения в тихом режиме используйте ключи `/s` и `/qn`.

► *Чтобы удалить приложение в тихом режиме, выполните следующие действия:*

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.
3. Выполните команду:
   - Если операция удаления не защищена паролем (см. раздел "Защита паролем" на стр. 352):

     ```
     setup_kes.exe /s /x
     ```
     или
     ```
     msiexec.exe /x <GUID> /qn
     ```

     где `<GUID>` – уникальный идентификатор приложения. Вы можете узнать GUID приложения с помощью команды:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```
   - Если операция удаления защищена паролем (см. раздел "Защита паролем" на стр. 352):

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```
     или
     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

   Также вы можете использовать параметр `SAVEQB` для сохранения файлов, проверенных приложением и помещенных в резервное хранилище. Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.12.12\QB`. По умолчанию сохранение файлов в резервном хранилище выключено (`SAVEQB=0`).

Пример:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin
KLPASSWD=samplePassword /qn
```

msiexec /i. Восстановление приложения

При восстановлении приложение проверяет и восстанавливает целостность всех поврежденных модулей приложения и ключей системного реестра, созданных при установке приложения.

Восстановление Kaspersky Endpoint Security из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки приложения.
- В тихом режиме. После запуска восстановления в тихом режиме ваше участие в процессе восстановления не требуется.

Если инсталлятор Kaspersky Endpoint Security запущен в режиме восстановления, а приложение не требует восстановления, то инсталлятор не выполняет никаких изменений.
Если инсталлятор Kaspersky Endpoint Security запущен в режиме восстановления, а приложение не установлено, то инсталлятор запустит установку приложения.

► *Чтобы восстановить приложение в тихом режиме, выполните следующие действия:*

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.
3. Выполните команду:
   - Если операция восстановления не защищена паролем (см. раздел "Защита паролем" на стр. 352):

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     где <GUID> – уникальный идентификатор приложения. Вы можете узнать GUID приложения с помощью команды:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Если операция восстановления защищена паролем (см. раздел "Защита паролем" на стр. 352):

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Пример:

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Команды AVP

► *Чтобы управлять Kaspersky Endpoint Security из командной строки, выполните следующие действия:*

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

   Вы можете добавить в системную переменную %PATH% путь к исполняемому файлу при установке приложения.
3. Используйте следующий шаблон для выполнения команды:

```
avp.com <command> [options]
```

В результате Kaspersky Endpoint Security выполнит команду (см. рис. ниже).

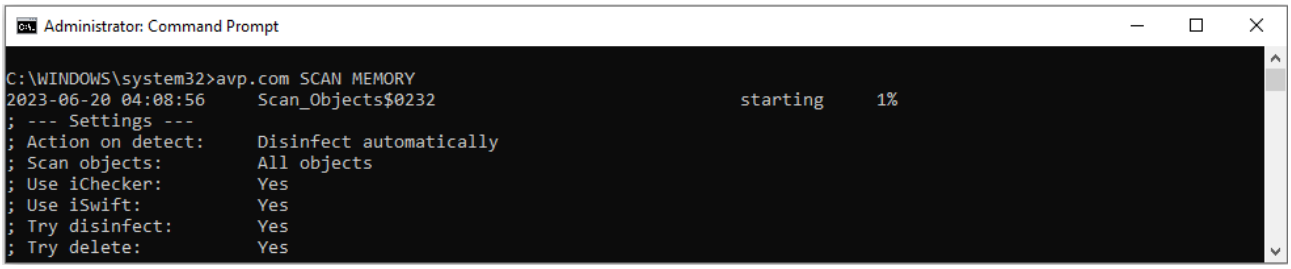


Рисунок 80. Управление программой из командной строки

В этом разделе

SCAN. Поиск вредоносного ПО 388
UPDATE. Обновление баз и модулей приложения 393
ROLLBACK. Откат последнего обновления 395
TRACES. Трассировка 396
START. Запуск профиля 397
STOP. Остановка профиля 398
STATUS. Статус профиля 399
STATISTICS. Статистика выполнения профиля 399
RESTORE. Восстановление файлов из резервного хранилища 400
EXPORT. Экспорт параметров приложения 401
IMPORT. Импорт параметров приложения 402
ADDKEY. Применение файла ключа 403
LICENSE. Лицензирование 404
RENEW. Приобретение лицензии 406
EXIT. Завершение работы приложения 406
EXITPOLICY. Выключение политики 407
STARTPOLICY. Включение политики 407
DISABLE. Выключение защиты 407
SPYWARE. Обнаружение шпионского ПО 407
KSN. Переключение KSN / KPSN 408
SERVERBINDINGDISABLE. Выключение защиты подключения к серверу 409

kaspersky

SCAN. Поиск вредоносного ПО

Запуск задачи *Поиск вредоносного ПО*.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>]
[<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with
scan settings>]
```

Область проверки

`<files to scan>`

Список файлов и папок через пробел. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например:

- `"C:\Program Files (x86)\Example Folder"` – длинный путь.
- `C:\PROGRA~2\EXAMPL~1` – короткий путь.

`/ALL`

Запустить задачу *Поиск вредоносного ПО*. Kaspersky Endpoint Security проверяет следующие объекты:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- загрузочные секторы;
- резервное хранилище операционной системы;
- все жесткие и съемные диски.

В Kaspersky Endpoint Security для Windows версии 12.12 почта исключена из области проверки приложения. Проверку входящих и исходящих сообщений выполняет компонент Защита от почтовых угроз (см. раздел "Формирование области защиты компонента Защита от почтовых угроз" на стр. 163). Если вы используете плагин управления более ранней версии, то приложение исключает почту из области проверки, даже если эта область включена в политике.

/MEMORY	Проверить память ядра.
/STARTUP	Проверить объекты, загрузка которых осуществляется при запуске операционной системы.
/REMDRIVES	Проверить съемные диски.
/FIXDRIVES	Проверить жесткие диски.
/NETDRIVES	Проверить сетевые диски.
/QUARANTINE	Проверить файлы в резервном хранилище Kaspersky Endpoint Security.
/@:<file list.lst>	Проверить файлы и папки, перечисленные в списке. Каждый файл из списка нужно вводить с новой строки. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например: • "C:\Program Files (x86)\Example Folder" – длинный путь. • C:\PROGRA~2\EXAMPL~1 – короткий путь.

Действие при обнаружении угрозы

/i0	**Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.
/i1	**Лечить. Информировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз.
/i2	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. Этот вариант действия выбран по умолчанию.
/i3	**Удалять, если лечение невозможно**. Также удалять составные файлы (например, архивы), если вылечить или удалить зараженный файл невозможно.

`/i4`	**Удалять**. Также удалять составные файлы (например, архивы), если удалить зараженный файл невозможно.

Типы файлов

`/fe`	**Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Формат файла определяется на основании его расширения.
`/fi`	**Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы (см. раздел "Потенциально заражаемый файл" на стр. 460). Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.
`/fa`	**Все файлы**. Если выбран этот параметр, приложение проверяет все файлы без исключения (любых форматов и расширений). Параметр выбран по умолчанию.

Исключения из проверки

`-e:a`	Исключение из проверки архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
`-e:<file mask>`	Исключение из проверки файлов по маске. Например: • Маска `*.exe` будет включать все пути к файлам с расширением exe. • Маска `example*` будет включать все пути к файлам с именем EXAMPLE.
`-e:<seconds>`	Исключение из проверки файлов, длительность проверки которых превышает установленное значение в секундах.
`-es:<megabytes>`	Исключение из проверки файлов, размер которых превышает установленное значение в мегабайтах.

Режим сохранения событий в файл отчета (только для профилей Scan, Updater, Rollback)

`/R:<report file>`	Сохранять только критические события в файл отчета.
`/RA:<report file>`	Сохранять все события в файл отчета.

Технологии проверки

`/iChecker=on|off`	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
`/iSwift=on|off`	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

Дополнительные параметры

`/C:<file with scan settings>`	Файл с параметрами задачи *Поиск вредоносного ПО*. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Пример:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

kaspersky

См. также:

Проверка компьютера ... 63
Формирование области проверки ... 78
Scan. Поиск вредоносного ПО ... 411
Устранение необработанных угроз ... 106

UPDATE. Обновление баз и модулей приложения

Запуск задачи *Обновление баз и модулей приложения*.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file
with update settings>]
```

Параметры задачи обновления

`local`

Запуск задачи *Обновление баз и модулей приложения*, созданной автоматически после установки приложения. Вы можете изменить параметры задачи *Обновление баз и модулей приложения* в локальном интерфейсе приложения или в консоли Kaspersky Security Center. Если этот параметр не установлен, Kaspersky Endpoint Security запускает задачу *Обновление баз и модулей приложения* с параметрами по умолчанию или с параметрами, заданными в команде. Таким образом, вы можете настроить параметры задачи *Обновление баз и модулей приложения*, следующим образом:

- `UPDATE` – запуск задачи *Обновление баз и модулей приложения* с параметрами по умолчанию: источник обновлений – серверы обновлений "Лаборатории Касперского", учетная запись – System, и другие.
- `UPDATE local` – запуск задачи *Обновление баз и модулей приложения*, созданной автоматически после установки (предустановленная задача).
- `UPDATE <update settings>` – запуск задача *Обновление баз и модулей приложения* с параметрами, заданными вручную (см. ниже).

Источник обновлений

`"<update source>"`

Адрес HTTP-, FTP-сервера или папки общего доступа с пакетом обновлений. Вы можете указать только один источник обновлений. Если источник обновлений не указан, Kaspersky Endpoint Security использует источник по умолчанию – серверы обновлений "Лаборатории Касперского".

Режим сохранения событий в файл отчета (только для профилей Scan, Updater, Rollback)

`/R:<report file>`

Сохранять только критические события в файл отчета.

`/RA:<report file>`

Сохранять все события в файл отчета.

Дополнительные параметры

`/C:<file with update settings>`	Файл с параметрами задачи *Обновление баз и модулей приложения*. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `["<update source>"] [/R[A]:<report file>]`.

Пример:

```
avp.com UPDATE local
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

См. также:

Запуск и остановка задачи обновления 90

ROLLBACK. Откат последнего обновления

Откат последнего обновления антивирусных баз. Это позволяет вернуться к использованию предыдущей версии баз и модулей приложения при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасное приложение.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Режим сохранения событий в файл отчета (только для профилей Scan, Updater, Rollback)

`/R:<report file>`	Сохранять только критические события в файл отчета.
`/RA:<report file>`	Сохранять все события в файл отчета.

Пример:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Трассировка

Файлы трассировки (см. раздел "О составе и хранении файлов трассировки" на стр. 449) хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения. Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке `%ProgramData%\Kaspersky Lab\KES.12.12\Traces`. По умолчанию трассировка выключена.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Уровень трассировки

`<tracing level>`	Уровень детализации трассировки. Возможные значения: • `100` (критический). Только сообщения о неустранимых ошибках. • `200` (высокий). Сообщения обо всех ошибках, включая неустранимые. • `300` (диагностический). Сообщения обо всех ошибках, а также предупреждения. • `400` (важный). Сообщения обо всех ошибках, предупреждения, а также дополнительная информация. • `500` (обычный). Сообщения обо всех ошибках, предупреждениях, а также подробная информация о работе приложения в нормальном режиме (значение по умолчанию). • `600` (низкий). Все сообщения.

Дополнительные параметры

`all`	Выполнить команду с параметрами `file` и `mem`.
`file`	Сохранить один файл трассировки (без ограничений по размеру).
`rot`	Сохранить результаты трассировки в ограниченное число комплектов файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера.
`mem`	Записывать результаты трассировки в файлы дампов.

Примеры:

```
avp.com TRACES on 500
avp.com TRACES off
avp.com TRACES on 500 mem
avp.com TRACES off file
```

См. также:

Трассировка работы приложения ... 452
Трассировка производительности приложения ... 453
О составе и хранении файлов трассировки ... 449
Запись дампов ... 454
Защита файлов дампов и трассировок ... 455

START. Запуск профиля

Запуск профиля (например, запуск обновления баз или включение компонента защиты).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com START <profile> [/R[A]:<report file>]
```

Профиль

`<profile>`	Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Профили приложения" на стр. 444) вы можете узнать по команде `HELP START`.

Режим сохранения событий в файл отчета (только для профилей Scan, Updater, Rollback)

`/R:<report file>`	Сохранять только критические события в файл отчета.
`/RA:<report file>`	Сохранять все события в файл отчета.

Пример:

```
avp.com START Scan_Objects
```

STOP. Остановка профиля

Остановка выполнения профиля (например, остановка проверки съемных дисков или выключение компонента защиты).

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешения **Выключение компонентов защиты**, **Выключение компонентов контроля**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Профиль

`<profile>`

Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Профили приложения" на стр. 444) вы можете узнать по команде `HELP STOP`.

Авторизация

`/login=<user name>`
`/password=<password>`

Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357).

STATUS. Статус профиля

Отображение информации о состоянии профилей приложения (см. раздел "Профили приложения" на стр. 444) (например, `running` или `completed`). Список доступных профилей вы можете узнать по команде `HELP STATUS`.

Также Kaspersky Endpoint Security показывает информацию о состоянии служебных профилей. Информация о состоянии служебных профилей может понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com STATUS [<profile>]
```

Если вы введете команду без профиля, Kaspersky Endpoint Security покажет состояние всех профилей приложения.

STATISTICS. Статистика выполнения профиля

Отображение статистической информации о профиле приложения (см. раздел "Профили приложения" на стр. 444) (например, время проверки или количество обнаруженных угроз). Список доступных профилей вы можете узнать по команде `HELP STATISTICS`.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com STATISTICS <profile>
```

kaspersky

RESTORE. Восстановление файлов из резервного хранилища

Восстановление файла из резервного хранилища в папку его исходного размещения. Если по указанному пути уже существует файл с таким же именем, приложение запросит подтверждение для замены файла. Восстанавливаемый файл копируется с исходным именем.

> Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешение **Восстановление из резервного хранилища**.

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.12.12\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

> В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Дополнительные параметры

`/REPLACE`	Переписать существующий файл.
`<file name>`	Имя восстанавливаемого файла.

Авторизация

`/login=<user name>` `/password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357).

Пример:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin
/password=samplePassword
```

EXPORT. Экспорт параметров приложения

Экспорт параметров Kaspersky Endpoint Security в файл. Если в команде указано только имя файла, в который нужно экспортировать параметры, приложение размещает файл следующим образом:

- Если путь к avp.com добавлен в системную переменную %PATH%, приложение помещает файл в папку `C:\Windows\SysWOW64`.
- Если вы выполняете команду из папки установки приложения, экспорт завершится с ошибкой, так как самозащита приложения заблокирует создание нового файла в папке приложения. Для экспорта параметров приложения в файл введите путь к файлу.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешение **Экспорт настроек**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Профиль

`<profile>`

Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Профили приложения" на стр. 444) вы можете узнать по команде `HELP EXPORT`.

Файл для экспорта

`<file name>`

Имя файла, в который должны быть экспортированы параметры профиля. Также вы можете ввести путь к файлу. Вы можете экспортировать параметры профиля в конфигурационный файл в формате DAT или CFG, в текстовый файл в формате TXT или в документ в формате XML.

Авторизация

`/login=<user name>`
`/password=<password>`

Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357).

Примеры:

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
avp.com EXPORT fm fm_config.txt
```

См. также:

Создание и использование конфигурационного файла 373

IMPORT. Импорт параметров приложения

Импорт параметров Kaspersky Endpoint Security из файла, который был создан с помощью команды `EXPORT`.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешение **Настройка приложения**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Файл для импорта

`<file name>`

Имя файла, из которого должны быть импортированы параметры приложения. Вы можете импортировать параметры Kaspersky Endpoint Security из конфигурационного файла в формате DAT или CFG, текстового файла в формате TXT или документа в формате XML.

Авторизация

`/login=<user name>` `/password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357).

Пример:

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

См. также:

Создание и использование конфигурационного файла 373

ADDKEY. Применение файла ключа

Активация Kaspersky Endpoint Security с помощью файла ключа. Если приложение уже активировано, ключ будет добавлен в качестве резервного.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Файл ключа

`<file name>`	Имя файла ключа.

Авторизация

`/login=<user name> /password=<password>`	Данные учетной записи пользователя. Данные учетные записи нужно вводить, только если включена Защита паролем (на стр. 352).

Пример:

```
avp.com ADDKEY file.key
```

LICENSE. Лицензирование

Управление лицензионными ключами приложения Kaspersky Endpoint Security, а также ключами решений EDR Optimum или EDR Expert (Kaspersky Endpoint Detection and Response Add-on).

Для выполнения команды удаления лицензионного ключа должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешение **Удаление ключа**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Операция	
`/ADD <file name>`	Активация Kaspersky Endpoint Security с помощью файла ключа. Если приложение уже активировано, ключ будет добавлен в качестве резервного.
`/ADD <activation code>`	Активировать Kaspersky Endpoint Security с помощью кода активации. Если приложение уже активировано, ключ будет добавлен в качестве резервного.
`/REFRESH`	Обновить статус лицензии Kaspersky Endpoint Security. В результате приложение получает актуальную информацию о статусе лицензии с серверов активации "Лаборатории Касперского".

`/REFRESH <license ID>`	Обновить статус лицензий по лицензионному идентификатору. С помощью этой команды вы можете обновить статус лицензий EDR Add-on, MDR Add-on, KUMA Add-on или другой лицензии. Вы можете узнать лицензионный идентификатор в лицензионном сертификате. В результате приложение получает актуальную информацию о статусе лицензии с серверов активации "Лаборатории Касперского".
`/CHECK`	Получить информацию о лицензии. Kaspersky Endpoint Security показывает информацию обо всех добавленных лицензионных ключах, включая резервные ключи и ключи EDR Add-on, MDR Add-on, KUMA Add-on и другие ключи. Kaspersky Endpoint Security показывает следующую информацию о лицензии: • название лицензии; • идентификатор лицензии; • адрес Сервера защиты (SVM), к которому подключена виртуальная машина с приложением, установленным в режиме Легкого агента; • тип лицензии: пробная, коммерческая, beta, подписка; • дата и время активации приложения; • дата и время истечения срока действия лицензии; • количество дней до истечения срока действия лицензии.
`/CHECK <license ID>`	Получить информацию о лицензии по идентификатору. С помощью этой команды вы можете получить информацию о лицензии. Вы можете узнать лицензионный идентификатор в лицензионном сертификате.
`/DEL /login=<user name> /password=<password>`	Удалить лицензионный ключ приложения. Также будет удален резервный ключ.
`/DEL <license ID> /login=<user name> /password=<password>`	Удалить ключ по лицензионному идентификатору. С помощью этой команды вы можете удалить ключ от лицензий EDR Add-on, MDR Add-on, KUMA Add-on или другой ключ. Вы можете узнать лицензионный идентификатор в лицензионном сертификате.

Авторизация

`/login=<user name>` `/password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357).

Пример:

```
avp.com LICENSE /ADD file.key

avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD

avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin
/password=samplePassword
```

RENEW. Приобретение лицензии

Переход на веб-сайт "Лаборатории Касперского" для приобретения лицензии или продления ее срока действия.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

EXIT. Завершение работы приложения

Завершение работы Kaspersky Endpoint Security. Приложение будет выгружено из оперативной памяти компьютера.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешение **Завершение работы приложения**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Выключение политики

Выключение политики Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком ().

> Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешение **Выключение политики Kaspersky Security Center**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Включение политики

Включение политики Kaspersky Security Center на компьютере. Параметры приложения будут настроены в соответствии с политикой.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

DISABLE. Выключение защиты

Выключение Защиты от файловых угроз на компьютере с истекшей лицензией на Kaspersky Endpoint Security. Выполнить команду на компьютере с неактивированным приложением или с действующей лицензией невозможно.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

SPYWARE. Обнаружение шпионского ПО

Управление обнаружением шпионского ПО. По умолчанию обнаружение шпионского ПО включено.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com SPYWARE on|off
```

kaspersky

KSN. Переключение KSN / KPSN

Выбор решения "Лаборатории Касперского" для определения репутации файлов или сайтов. Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от "Лаборатории Касперского", а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.
- *Kaspersky Private Security Network (KPSN)* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:
  - отсутствие подключения локальных рабочих мест к сети Интернет;
  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com KSN /global | /private <file name>
```

Конфигурационный файл Kaspersky Security Network

`<file name>` Имя
PK

Пример:

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

См. также:

Включение и выключение использования Kaspersky Security Network 110
Включение и выключение облачного режима для компонентов защиты 111
Проверка репутации файла в Kaspersky Security Network 112

SERVERBINDINGDISABLE. Выключение защиты подключения к серверу

Запуск задачи *Защита подключения к Серверу администрирования* (см. раздел "*Защита подключения к Серверу администрирования*" на стр. 364), которая удаляет пароль для подключения компьютера к Серверу администрирования. Таким образом, задача выключает защиту подключения к Серверу администрирования.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Пароль

`/password=<password>`

Пароль учетной записи KLAdmin (см. раздел "Защита паролем" на стр. 352) или пароль из задачи *Защита подключения к Серверу администрирования*.

Если параметр не задан, Kaspersky Endpoint Security предложит ввести пароль в следующей строке.

kaspersky

Команды KESCLI

Команды KESCLI позволяют получать информацию о состоянии защиты компьютера с помощью компонента OPSWAT, а также выполнять стандартные задачи (например, *Поиск вредоносного ПО*, *Обновление баз и модулей приложения*).

Вы можете просмотреть список команд KESCLI с помощью команды `kescli --help` или сокращенной команды `kescli -h`.

► *Чтобы управлять Kaspersky Endpoint Security из командной строки, выполните следующие действия:*

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

   Вы можете добавить в системную переменную %PATH% путь к исполняемому файлу при установке приложения.
3. Используйте следующий шаблон для выполнения команды:

```
kescli <command> [options]
```

В результате Kaspersky Endpoint Security выполнит команду (см. рис. ниже).

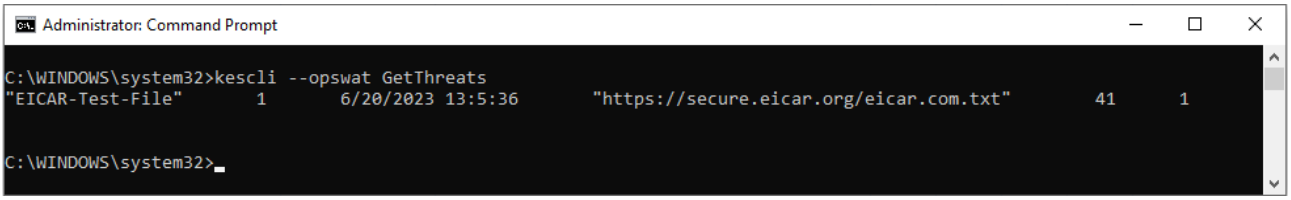


Рисунок 81. Управление приложением из командной строки

В этом разделе

Scan. Поиск вредоносного ПО 411
GetScanState. Статус выполнения проверки 412
GetLastScanTime. Определения времени выполнения проверки 412
GetThreats. Получение данных об обнаруженных угрозах 412
UpdateDefinitions. Обновление баз и модулей приложения 416
GetDefinitionState. Определение даты и времени последнего обновления баз 416
EnableRTP. Включение защиты 416
GetRealTimeProtectionState. Статус Защиты от файловых угроз 417
Version. Определение версии приложения 417

kaspersky

Scan. Поиск вредоносного ПО

Запуск задачи *Поиск вредоносного ПО* (Полная проверка).

> Для запуска задачи администратору нужно разрешить использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Вы можете проверить статус выполнения задачи *Поиск вредоносного ПО* с помощью команды `GetScanState` (см. раздел "`GetScanState. Статус выполнения проверки`" на стр. 412) и посмотреть дату и время последнего выполнения проверки с помощью команды `GetLastScanTime` (см. раздел "`GetLastScanTime. Определения времени выполнения проверки`" на стр. 412).

Область проверки

`<scan scope>`	Список файлов и папок через символ `;`. Например, `"C:\Program Files (x86)\Example Folder"`.

Действие при обнаружении угрозы

`0`	**Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.
`1`	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. Этот вариант действия выбран по умолчанию.

Пример:

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My
Documents;C:\Program Files" 1
```

См. также:

Проверка компьютера ... 63
Формирование области проверки ... 78
SCAN. Поиск вредоносного ПО ... 388
Устранение необработанных угроз ... 106

GetScanState. Статус выполнения проверки

Отображение информации о статусе выполнения задачи *Поиск вредоносного ПО* (Полная проверка):

- `1` – проверка выполняется.
- `0` – проверка не запущена.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetScanState
```

GetLastScanTime. Определения времени выполнения проверки

Отображение информации о дате и времени последнего выполнения задачи *Поиск вредоносного ПО* (Полная проверка).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetLastScanTime
```

GetThreats. Получение данных об обнаруженных угрозах

Отображение списка обнаруженных угроз (*Отчет об угрозах*). Отчет содержит информацию об угрозах и вирусной активности за 30 дней до момента создания отчета.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetThreats
```

В результате выполнение команды Kaspersky Endpoint Security отправит ответ в следующем формате:

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```

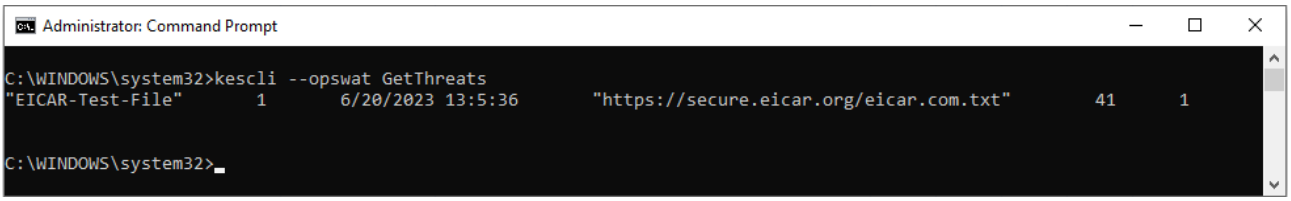


Рисунок 82. Управление приложением из командной строки

Тип объекта

0	Неизвестно (Unknown).
1	Вирусы (Virware).
2	Троянские приложения (Trojware).
3	Вредоносные приложения (Malware).
4	Рекламные приложения (Adware).
5	Приложения автодозвона (Pornware).
6	Приложения, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя (Riskware).
7	Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода (Packed).
20	Неизвестные объекты (Xfiles).
21	Известные приложения (Software).
22	Скрытые файлы (Hidden).
23	Приложения, требующие вашего внимания (Pupware).
24	Аномальное поведение (Anomaly).
30	Не определено (Undetect).
40	Рекламные баннеры (Banner).
50	Сетевая атака (Attack).
51	Доступ к реестру (Registry).
52	Подозрительные действия (Suspicion).
60	Уязвимости (Vulnerability).
70	Фишинг (Phishing).
80	Нежелательные почтовые вложения (Attachment).

90	Вредоносное приложение, обнаруженная с помощью Kaspersky Security Network (`Urgent`).
100	Неизвестная ссылка (`Suspic URL`).
110	Другое вредоносное приложение (`Behavioral`).

Действие при обнаружении угрозы

0	Неизвестно (unknown).
1	Угроза устранена (ok).
2	Объект заражен и не вылечен (infected).
5	Объект в архиве и не вылечен (archive).
9	Объект вылечен (disinfected).
10	Объект не вылечен (not disinfected).
11	Объект удален (deleted).
13	Создана резервная копия объекта (backupped).
15	Объект помещен в резервное хранилище (quarantined).
23	Объект удален при перезагрузке компьютера (delete on reboot).
25	Объект вылечен при перезагрузке компьютера (disinfect on reboot).
29	Объект помещен в резервное хранилище пользователем (added by user).
30	Объект добавлен в исключения (added to exclude).
31	Объект помещен в резервное хранилище при перезагрузке компьютера (quarantine on reboot).
36	Ложное срабатывание (false alarm).
38	Процесс завершен (terminated).
40	Объект не обнаружен (not found).
41	Невозможно устранить угрозу (untreatable).
42	Объект восстановлен (rolled back).
43	Объект создан в результате активности угрозы (produced by threat).
44	Объект восстановлен при перезагрузке компьютера (roll back on reboot).
0xffffffff	Объект не обработан (discarded).

Уровень опасности угрозы

0	Неизвестно
1	Высокий

2	Средний
4	Низкий
8	Информационный (ниже уровня *Низкий*)

UpdateDefinitions. Обновление баз и модулей приложения

Запуск задачи *Обновление баз и модулей приложения*. Kaspersky Endpoint Security использует источник по умолчанию – серверы обновлений "Лаборатории Касперского".

> Для запуска задачи администратору нужно разрешить использование локальных задач в политике (см. раздел "Управление задачами" на стр. 41).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

> Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
kescli --opswat UpdateDefinitions
```

Вы можете просмотреть дату и время выпуска используемых антивирусных баз с помощью команды `GetDefinitionsetState` (см. раздел "`GetDefinitionState. Определение даты и времени последнего обновления баз`" на стр. 416).

GetDefinitionState. Определение даты и времени последнего обновления баз

Отображение информации о дате и времени последнего обновления антивирусных баз.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetDefinitionState
```

EnableRTP. Включение защиты

Включение компонентов защиты Kaspersky Endpoint Security на компьютере: Защита от файловых угроз, Защита от веб-угроз, Защита от почтовых угроз, Защита от сетевых угроз, Предотвращение вторжений.

Для включения компонентов защиты администратору нужно убедиться, что необходимые параметры в политике доступны для изменения (атрибуты  открыты).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat EnableRTP
```

В результате компоненты защиты будут включены, даже если вы запретили изменение параметров приложения с помощью Защиты паролем (см. раздел "Включение Защиты паролем" на стр. 355).

Вы можете проверить статус работы Защиты от файловых угроз с помощью команды `GetRealTimeProtectionState` (см. раздел "`GetRealTimeProtectionState. Статус Защиты от файловых угроз`" на стр. 417).

GetRealTimeProtectionState. Статус Защиты от файловых угроз

Отображение информации о статусе работы компонента Защита от файловых угроз:

- `1` – компонент включен.
- `0` – компонент выключен.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetRealTimeProtectionState
```

Version. Определение версии приложения

Отображение версии приложения Kaspersky Endpoint Security для Windows.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --Version
```

Вы также можете использовать сокращенную команду `-v`.

Команды управления Detection and Response

Вы можете управлять встроенными функциями решений Detection and Response из командной строки (например, Kaspersky Sandbox или Kaspersky Endpoint Detection and Response Optimum). Вы можете управлять решениями Detection and Response, если управление через консоль Kaspersky Security Center невозможно. Вы можете просмотреть список команд для управления приложением с помощью команды `HELP`. Чтобы получить справку по синтаксису конкретной команды, введите `HELP <command>`.

► *Чтобы управлять встроенными функциями решений Detection and Response из командной строки, выполните следующие действия:*

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Используйте следующий шаблон для выполнения команды:

```
avp.com <command> [options]
```

В результате Kaspersky Endpoint Security выполнит команду.

В этом разделе

PREVENTION. Управление Запретом запуска объектов 418
ISOLATION. Управление Сетевой изоляцией 419
RESTORE. Восстановление файлов из карантина 419
IOCSCAN. Поиск индикаторов компрометации (IOC) 420

PREVENTION. Управление Запретом запуска объектов

Выключение компонента Запрет запуска объектов или отображение текущих параметров работы компонента, включая список правил запрета запуска объектов.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com prevention disable
avp.com prevention /show
```

В результате выполнения команды `prevention /show` вы получите следующий ответ:

```
prevention.enable=true|false
prevention.mode=audit|prevent
prevention.rules
    id: <rule ID>
    target: script|process|document
    md5: <MD5 hash of the file>
    sha256: <SHA256 hash of the file>
    pattern: <path to the object>
    case-sensitive: true|false
```

Коды возврата команды:

- `-1` – команда не поддерживается версией приложения, которое установлено на компьютере.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.
- `9` – неверная операция (например, попытка выключить компонент, если компонент уже выключен).

ISOLATION. Управление Сетевой изоляцией

Выключение Сетевой изоляции компьютера или отображение текущих параметров работы компонента. Параметры работы компонента также включают в себя список сетевых соединений, которые добавлены в исключения.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команд

```
avp.com isolation /OFF /login=<user name> /password=<password>
avp.com isolation /STAT
```

В результате выполнения команды `stat` вы получите следующий ответ: `Network isolation on|off`.

RESTORE. Восстановление файлов из карантина

Восстановить файл из карантина в папку его исходного размещения. *Карантин* – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Endpoint Security использует карантин при работе с решениями Kaspersky Endpoint Detection and Response Optimum. В остальных случаях Kaspersky Endpoint Security помещает файл в резервное хранилище (см. раздел "Работа с резервным хранилищем" на стр. 332). Подробнее о работе с карантином в составе решения см. в Kaspersky Endpoint Detection and Response Optimum (https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/index.htm).

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 355). Пользователь должен иметь разрешение **Восстановление из резервного хранилища**.
Объект помещается на карантин под системной учетной записью (SYSTEM).

Восстановление файлов из карантина имеет следующие особенности:

- Если папка назначения удалена или у пользователя нет прав доступа к этой папке, приложение помещает файл в папку `%DataRoot%\QB\Restored`. Далее вам нужно вручную переместить файл в папку назначения.

- Приложение учитывает регистр имени восстанавливаемого файла. Если вы введите имя файла в неверном регистре, приложение не восстановит файл.
- Если в папке восстановления уже есть файл с таким же именем, приложение отменит восстановление файла.
- Приложение удаляет файл из карантина после восстановления.

Синтаксис команды

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Дополнительные параметры

`/REPLACE`	Переписать существующий файл.
`<file name>`	Имя восстанавливаемого файла.

Авторизация

`/login=<user name>` `/password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 357).

Пример:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin
/password=samplePassword
```

Коды возврата команды:

- `-1` – команда не поддерживается версией приложения, которое установлено на компьютере.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.

IOCSCAN. Поиск индикаторов компрометации (IOC)

Запуск задачи *Поиск IOC*. *Индикатор компрометации (Indicator of Compromise, IOC)* – набор данных об объекте или активности, который указывает на несанкционированный доступ к компьютеру (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача *Поиск IOC* позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Поиск IOC прерывается при обнаружении 128 совпадений с индикаторами компрометации, описанными в IOC-файлах. Это необходимо для ограничения количества записей в отчете задачи Поиск IOC для удобства его анализа и защиты отчета от переполнения из-за неточно сформулированных индикаторов компрометации, для которых совпадений может быть очень много.

Синтаксис команды

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder>
[/process=on|off] [/hint=<full path to executable file of a process|full file
path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off]
[/volumes=on|off] [/eventlog=on|off] [/datetime=<event publication date>]
[/channels=<list of channels>] [/files=on|off]
[/drives=<all|system|critical|custom>] [/excludes=<list of
exclusions>][/scope=<list of folders to scan>]
```

IOC-файлы

`<full path to the IOC file>`

Полный путь к IOC-файлу, по которому требуется выполнить поиск. Вы можете указать несколько IOC-файлов через пробел. Полный путь к IOC-файлу следует ввести без аргумента `/path`.

Например, `C:\Users\Admin\Desktop\IOC\file1.ioc`

`/path=<path to the folder with IOC files>`

Путь к папке с IOC-файлами, по которым требуется выполнять поиск. *IOC-файлы* – файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. IOC-файлы должны соответствовать стандарту описания OpenIOC.

Например, `C:\Users\Admin\Desktop\IOC`

Тип данных для поиска IOC

`/process=on|off`

Анализ данных о процессах при поиске IOC (термин ProcessItem).

Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет запущенные на компьютере процессы при выполнении проверки. Если в IOC-файле указаны IOC-термины IOC-документа ProcessItem, они игнорируются (определяются как отсутствие совпадения).

Если параметр не установлен, Kaspersky Endpoint Security проверяет данные о процессах, только если IOC-документ ProcessItem описан в переданном на проверку IOC-файле.

`/hint=<full path to the executable file of the process|full path to the file>`

Анализ данных о файле при поиске IOC (термины ProcessItem и FileItem).

Вы можете выбрать файл следующими способами:

- `<full path to the executable file of the process>` – термин ProcessItem;
- `<full path to the file>` – термин FileItem.

`/registry=on|off`

Анализ данных о реестре Windows при поиске IOC (термин RegistryItem).

Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет реестр Windows. Если в IOC-файле указаны термины IOC-документа RegistryItem, они игнорируются (определяются как отсутствие совпадения).

Если параметр не установлен, Kaspersky Endpoint Security проверяет реестр Windows, только если IOC-документ RegistryItem описан в переданном на проверку IOC-файле.

Для типа данных RegistryItem Kaspersky Endpoint Security анализирует определенный набор разделов реестра (см. раздел "Приложение 9. Область поиска IOC в реестре (RegistryItem)" на стр. 485).

`/dnsentry=on|off`

Анализ данных о записях в локальном кеше DNS при поиске IOC (термин DnsEntryItem).

Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет локальный кеш DNS. Если в IOC-файле указаны термины IOC-документа DnsEntryItem, они игнорируются (определяются как отсутствие совпадения).

Если параметр не установлен, Kaspersky Endpoint Security проверяет локальный кеш DNS, только если IOC-документ DnsEntryItem описан в переданном на проверку IOC-файле.

`/arpentry=on|off`

Анализ данных о записях в ARP-таблице при поиске IOC (термин ArpEntryItem).

Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет таблицу ARP. Если в IOC-файле указаны термины IOC-документа ArpEntryItem, они игнорируются (определяются как отсутствие совпадения).

Если параметр не установлен, Kaspersky Endpoint Security проверяет ARP-таблицу, только если IOC-документ ArpEntryItem описан в переданном на проверку IOC-файле.

`/ports=on|off`

Анализ данных о портах, открытых на прослушивание, при поиске IOC (термин PortItem).

Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет таблицу активных соединений на устройстве. Если в IOC-файле указаны термины IOC-документа PortItem, они игнорируются (определяются как отсутствие совпадения).

Если параметр не установлен, Kaspersky Endpoint Security проверяет таблицу активных соединений, только если IOC-документ PortItem описан в переданном на проверку IOC-файле.

`/services=on|off`

Анализ данных о службах, установленных на устройстве, при поиске IOC (термин ServiceItem).

Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет данные о службах, установленных на устройстве. Если в IOC-файле указаны термины IOC-документа ServiceItem, они игнорируются (определяются как отсутствие совпадения).

Если параметр не установлен, Kaspersky Endpoint Security проверяет данные о службах, только если IOC-документ ServiceItem описан в переданном на проверку IOC-файле.

`/system=on|off`

Анализ данных об окружении при поиске IOC (термин SystemInfoItem).

Если параметр установлен со значением `off`, Kaspersky Endpoint Security не анализирует данные об окружении. Если в IOC-файле указаны термины IOC-документа SystemInfoItem, они игнорируются (определяются как отсутствие совпадения).

Если параметр не установлен, Kaspersky Endpoint Security анализирует данные об окружении, только если IOC-документ SystemInfoItem описан в переданном на проверку IOC-файле.

`/users=on|off`	Анализ данных о пользователях при поиске IOC (термин UserItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не анализирует данные о пользователях, созданных в системе. Если в IOC-файле указаны термины IOC-документа UserItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные о пользователях, созданных в системе, только если IOC-документ UserItem описан в переданном на проверку IOC-файле.
`/volumes=on|off`	Анализ данных о томах при поиске IOC (термин VolumeItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет данные о томах на устройстве. Если в IOC-файле указаны термины IOC-документа VolumeItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные о томах, только если IOC-документ VolumeItem описан в переданном на проверку IOC-файле.
`/eventlog=on|off`	Анализ данных о записях в журнале событий Windows при поиске IOC (термин EventLogItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет записи в журнале событий Windows. Если в IOC-файле указаны термины IOC-документа EventLogItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет записи в журнале событий Windows, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.

`/datetime=<event publication date>`	Учет даты публикации события в журнале событий Windows при определении области поиска IOC для соответствующего IOC-документа. При поиске IOC Kaspersky Endpoint Security проверяет записи в журнале событий Windows, опубликованные в период с указанного времени и даты и до момента выполнения задачи. В качестве значения параметра Kaspersky Endpoint Security позволяет задать дату публикации события. Проверка будет выполняться только для событий, опубликованных в журнале событий Windows после указанной даты и до момента выполнения проверки. Если параметр не указан, Kaspersky Endpoint Security проверяет события с любой датой публикации. Параметр `TaskSettings::BaseSettings::EventLogItem::datetime` недоступен для редактирования. Параметр используется, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.
`/channel=<list of channels>`	Список имен каналов (журналов), для которых требуется выполнить поиск IOC. Если параметр указан, Kaspersky Endpoint Security проверяет записи, опубликованные в указанных журналах. При этом в IOC-документе должен быть описан термин EventLogItem. Имя журнала задается в формате строки, в соответствии с именем журнала (канала), указанного в свойствах этого журнала (параметр Full Name) или в свойствах события (параметр `<Channel></Channel>` в xml-схеме события). Вы можете указать несколько каналов через пробел. Если параметр не указан, Kaspersky Endpoint Security проверяет записи для каналов `Application`, `System`, `Security`.
`/files=on|off`	Анализ данных о файлах при поиске IOC (термин FileItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не анализирует данные о файлах. Если в IOC-файле указаны термины IOC-документа FileItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные о файлах, только если IOC-документ FileItem описан в переданном на проверку IOC-файле.

/drives=<all|system|critical|custom>	Область поиска IOC при анализе данных для IOC-документа FileItem. Доступны следующие значения области поиска: • <all> – все доступные файловые области. • <system> – файлы, расположенные в папках, в которых установлена ОС. • <critical> – временные файлы в пользовательских и системных папках. • <custom> – файлы в указанных пользователем областях (/scope=<list of folders to scan>). Если параметр не установлен, проверка выполняется в критических областях.
/excludes=<list of exclusions>	Область исключений при анализе данных для IOC-документа FileItem. Вы можете указать несколько путей через пробел.
/scope=<list of folders to scan>	Пользовательская область поиска IOC при анализе данных для IOC-документа FileItem (/drives=custom). Вы можете указать несколько путей через пробел.
/retro /<number of days>	*Ретроспективный поиск IOC* – это режим работы задачи *Поиск IOC*, при котором Kaspersky Endpoint Security выполняет поиск индикаторов компрометации по данным, полученным за определенный интервал времени. Режим предназначен для поиска индикаторов компрометации по данным сетевой активности компьютера. Вы можете указать интервал времени в диапазоне 1 - 14 дней. По умолчанию приложение выполняет поиск индикаторов компрометации за один день.
/network=on|off	Анализ сетевых данных (термин NetworkItem).
/url=on|off	Анализ данных в журналах браузеров (термин UrlHistoryItem). Ретроспективный поиск IOC анализирует журналы следующих браузеров: Google Chrome, Mozilla Firefox, Microsoft Edge (версии 79 и выше).
/email	Анализ почтовых объектов (термин EmailItem).
/route	Анализ таблиц маршрутизации (термин RouteEntryItem).

Коды возврата команды:

- -1 – команда не поддерживается версией приложения, которое установлено на компьютере.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.

- `4` – синтаксическая ошибка.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Security выводит в командную строку следующие данные о результатах выполнения задачи:

`Uuid`	Идентификатор IOC-файла из заголовка структуры IOC-файла (тег `<ioc id="">`)
`Name`	Описание IOC-файла из заголовка структуры IOC-файла (тег `<description></description>`)
`Matched Indicator Items`	Перечень идентификаторов всех сработавших индикаторов.
`Matched objects`	Данные по каждому документу IOC, по которому было найдено совпадение.

kaspersky

Сообщения об ошибках

При работе с программой возможно появление следующих сообщений об ошибках:

Таблица 23. Сообщения об ошибках и коды возврата

Сообщение об ошибке в командной строке	Код возврата в Shell
Error %d getting thread's context	
Error %d loading QueryInformationThread function	
Error %d opening thread	
Error %d querying thread information	
Error %d suspending thread	
Error in UpdateKSNConfig	
Error in thread safety code: could not acquire a lock	
Error: %S (err 0x%x)	
Error: %S: %s (err 0x%x)	
Error: '%S' has not been completed due to execution timeout	_Shell::_E_TIMEOUT
Error: '%S' is disabled	
Error: Cannot change state for '%S' (%S), task already in state?	SHELL_RET_FAILED
Error: Cannot change state for '%S' (%S), task disabled?	SHELL_RET_FAILED
Error: Cannot create message receiver	
Error: Cannot create task, err=%08X	SHELL_RET_FAILED
Error: Cannot find task '%S'	SHELL_RET_FAILED /SHELL_RET_PARAMETER_INVALID
Error: Cannot get product settings	
Error: Cannot get tasks list	SHELL_RET_FAILED
Error: Cannot initialize task parameters block	SHELL_RET_PARAMETER_INVALID
Error: Cannot open configuration file '%S'	
Error: Cannot open list file '%S'	
Error: Cannot set report handler	

Сообщение об ошибке в командной строке	Код возврата в Shell
Error: Cannot start task '%S', error=%08X	SHELL_RET_NO_LICENCE
Error: Cannot start task '%S', no licence	_Shell::_S_NO_LICENSE
Error: Cannot start task '%S', parameters invalid	SHELL_RET_PARAMETER_INVALID
Error: Cannot verify task parameters block	
Error: Change state failed for task '%S' (%S), error=%08X	SHELL_RET_FAILED
Error: Command unavailable due to password protection disabled	
Error: Configuration file not specified (/C)	
Error: Credential is not obtained, access denied	
Error: Duplicate taskid '%S'	
Error: Failed to flush cached data	
Error: File list not specified	
Error: File list not specified (/@)	
Error: Internal error %08X	SHELL_RET_FAILED
Error: Invalid command '%S'	
Error: Invalid parameter '%S'	
Error: Local task control is denied by policy	
Error: NOT IMLEMENTED	SHELL_RET_FAILED
Error: Not enough memory	
Error: Nothing to scan	
Error: Parameter '%S' must contain exclusion specification	
Error: Parameter '%S' must specify size in megabytes	
Error: Parameter not supported by task '%S'	
Error: Password or login is invalid, access denied	
Error: Profile name must be specified	SHELL_RET_PARAMETER_INVALID

Сообщение об ошибке в командной строке	Код возврата в Shell
Error: Task '%S' not found	SHELL_RET_TASK_FAILED
Error: Unknown parameter '%S'	
Error: Usage parameter /APP=<on|off>	
Error: Usage parameter /iChecker=<on|off>	
Error: Usage parameter /iSwift=<on|off>	
Error: cannot open report file %S, error=%d %s	
Error: control of this task is not allowed	
Error: failed to register message handlers	
Error: failed to set INetSwift state	
Error: failed to unregister message handlers	
Error: Local task control is denied by policy	
Scan_Quarantine failed: %	SHELL_RET_FAILED
Scan_Quarantine completed successfully	SHELL_RET_OK
Failed to get AVP_SERVICE_PRODUCT. Error	SHELL_RET_FAILED
Disable command cannot be elevated. Error	SHELL_RET_FAILED
Failed to disable product from command line. Error	SHELL_RET_FAILED
Failed to get AVP_SERVICE_PRODUCT. Error	
Failed to get TaskManager service. Error	
Failed to get service locator. Error	
Invalid parameters	SHELL_RET_PARAMETER_INVALID
Failed while activating Global KSN	SHELL_RET_FAILED
Failed to execute command set silent detect. Error	_Shell::_E_FAIL
Failed to execute command silent detect check. Error	_Shell::_E_FAIL
Path not exist	
Cannot write to file, no permission	

Сообщение об ошибке в командной строке	Код возврата в Shell
Cannot add key file	SHELL_RET_TASK_FAILED
INetSwift state set to	SHELL_RET_OK
Internal error	SHELL_RET_FAILED
Fail to terminate command on user's request	_Shell::_E_BREAK_FAIL
Command is terminated on user's request	_Shell::_E_BREAK_OK

Коды возврата

Любая команда, выполняемая администратором в командной строке, может возвращать код возврата. Коды возврата бывают general или специфичные для отдельных задач.

Доступны следующие коды возврата:

- General коды возврата:
  - 0 - задача выполнена успешно;
  - 1 - некорректное значение параметра;
  - 2 - неизвестная ошибка;
  - 3 - ошибка во время выполнения задачи;
  - 4 - выполнение задачи прервано.
- Коды возврата задач антивирусной проверки:
  - 101 - все опасные объекты обработаны;
  - 102 - обнаружены опасные объекты.
- Коды возврата других задач:
  - -14 - истекло время ожидания.
  - 239 - ошибка во время приостановки задачи.
  - 240 - задача отменена пользователем.
  - -15 - файл заблокирован другим процессом и недоступен для обработки программой.
  - -10 - указан неверный путь к объекту.
  - -8 - ключ недействителен.
  - -7 - ключ находится в черном списке.
  - -13 - ключ предназначен для другого продукта.
  - [1-127] - дни до истечения срока действия лицензии.

    Если до истечения срока действия лицензии осталось более 127 дней, код возврата 127. Если

до истечения срока действия лицензии осталось менее 127 дней, код возврата соответствует реальному количеству дней. Если лицензия уже истекла, код возврата 1.

- 8000045 - недостаточно прав.
- 102 - есть необработанные угрозы.

Таблица 24. Символьные и числовые значения кодов возврата

Символьные значения	Числовые значения	Доступно для команд
_Shell::_E_TIMEOUT	-14	START UPDATE ROLLBACK SCAN
_Shell::_E_BREAK_FAIL	239	UPDATE ROLLBACK SCAN
_Shell::_E_BREAK_OK	240	UPDATE ROLLBACK SCAN
_Shell::_E_FAIL	-3	MESSAGES LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket /DeleteKey /Refresh
_Shell::_E_FILE_BLOCKED	-15	UPDATE ROLLBACK SCAN
_Shell::_E_INVALID_PATH	-10	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_INVALID_SYNTAX	-2	UPDATE ROLLBACK MESSAGES SCAN
_Shell::_E_KEY_CORRUPTED	-8	LICENSE: /Add (ActivateByKeyEx) /AddTicket

Символьные значения	Числовые значения	Доступно для команд
_Shell::_E_KEY_IN_BLST	-7	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_KEY_NOT_MATCH	-13	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_S_ALL_DETECTION	2	UPDATE ROLLBACK SCAN
_Shell::_S_NO_LICENSE	0	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket /DeleteKey
_Shell::_S_OK	0	UPDATE ROLLBACK SCAN LICENSE: /Add (ActivateByKeyEx) /AddTicket /Refresh
_Shell::_S_PARTIAL_DETECTION	3	UPDATE ROLLBACK SCAN
[1-127]	[1-127]	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket
errACCESS_DENIED	8000045	STOP EXITPOLICY

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_FAILED	2	START STOP STATUS STATISTICS MODE HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SPYWARE MESSAGES RESTORE PBATESTRESET PATCHCOMPATIBILITYRESET SCAN
-SHELL_RET_FAILED	-2	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_NO_LICENCE	2	START UPDATE ROLLBACK SCAN

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_OK	0	START STOP STATUS STATISTICS HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SLC SPYWARE LETSDUMP MESSAGES RESTORE PBATESTRESET PATCHCOMPATIBILITYRESET SCAN LICENSE: /Add (ActivateByCode)

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_PARAMETER_INVALID	1	START STOP STATUS STATISTICS EXPORT IMPORT ADDKEY INETSWIFT UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SPYWARE RESTORE PATCHCOMPATIBILITYRESET SCAN
-SHELL_RET_PARAMETER_INVALID	-1	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_SCAN_ALL_THREATED	101	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_NO_THREATS	0	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_SUSPICIOUS_UNTREATED	0	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_THREATS	102	UPDATE ROLLBACK SCAN

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_TASK_FAILED	3	STOP EXPORT IMPORT ADDKEY UPDATE ROLLBACK RESTORE SCAN
-SHELL_RET_TASK_FAILED	-3	LICENSE: /Add (ActivateByKey) /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_TASK_STOPPED	4	UPDATE ROLLBACK SCAN

Коды ошибок

При работе с приложением через командную строку возможно появление ошибок. При появлении ошибки Kaspersky Endpoint Security показывает сообщение об ошибке, например, `Error: Cannot start task 'EntAppControl'`. Также Kaspersky Endpoint Security может показать дополнительные сведения в виде кода, например, `error=8947906D` (см. таблицу ниже).

Таблица 25. Коды ошибок

Код ошибки	Описание
09479001	Этот ключ уже используется
0947901D	Истек срок действия лицензии. Обновление баз недоступно
89479002	Ключ не найден
89479003	Цифровая подпись повреждена или не найдена
89479004	Данные повреждены
89479005	Файл ключа поврежден
89479006	Истек срок действия лицензии
89479007	Файл ключа не указан
89479008	Неверный файл ключа

Код ошибки	Описание
89479009	Не удалось сохранить данные
8947900A	Не удалось прочитать данные
8947900B	Ошибка ввода / вывода
8947900C	Базы не найдены
8947900E	Библиотека лицензирования не загружена
8947900F	Базы повреждены или обновлены вручную
89479010	Базы повреждены
89479011	Невозможно применить недействительный файл ключа для добавления резервного ключа
89479012	Системная ошибка
89479013	Список запрещенных ключей поврежден
89479014	Подпись файла не соответствует цифровой подписи "Лаборатории Касперского"
89479015	Невозможно использовать ключ для пробной лицензии в качестве ключа для коммерческой лицензии
89479016	Чтобы использовать бета-версию приложения, требуется лицензия для бета-тестирования
89479017	Файл ключа не подходит для данного приложения. Невозможно активировать Kaspersky Endpoint Security для Windows с помощью файла ключа для другого приложения. Пожалуйста, проверьте установленное приложение
89479018	Лицензионный ключ заблокирован "Лабораторией Касперского"
89479019	Приложение уже использовалось по пробной лицензии. Невозможно снова добавить ключ для пробной лицензии
8947901A	Файл ключа поврежден
8947901B	Цифровая подпись не найдена, повреждена или не соответствует подписи "Лаборатории Касперского"
8947901C	Невозможно добавить ключ, если срок действия соответствующей ему некоммерческой лицензии истек
8947901E	Дата создания файла ключа или его применения некорректна. Проверьте системную дату
8947901F	Невозможно добавить ключ для пробной лицензии, пока действует другая аналогичная лицензия
89479020	Список запрещенных ключей поврежден или не найден
89479021	Описание обновлений повреждено или не найдено
89479022	Ключ не подходит для этого приложения
89479023	Невозможно применить недействительный файл ключа для добавления резервного ключа

Код ошибки	Описание
89479025	Возникла ошибка при отправке запроса на сервер активации. Возможные причины: ошибка соединения с интернетом или временные проблемы на сервере активации. Попробуйте активировать приложение с помощью кода активации позже (через 1-2 часа). В случае повторения ошибки обратитесь к вашему интернет-провайдеру
89479026	В запросе указан неверный код активации
89479027	Невозможно получить статус ответа
89479028	Ошибка при сохранении временного файла
89479029	Введен неверный код активации или на компьютере установлена некорректная системная дата. Проверьте системную дату на компьютере
8947902A	Ключ не подходит для данного приложения или истек срок действия лицензии
8947902B	Не удалось получить файл ключа. Введен неверный код активации
8947902C	Сервер активации возвратил ошибку 400
8947902D	Сервер активации возвратил ошибку 401
8947902E	Сервер активации возвратил ошибку 403
8947902F	Недоступен необходимый ресурс на сервере активации. Сервер активации возвратил ошибку 404. Пожалуйста, проверьте настройки подключения к интернету
89479030	Сервер активации возвратил ошибку 405
89479031	Сервер активации возвратил ошибку 406
89479032	Требуется аутентификация на прокси-сервере. Пожалуйста, проверьте настройки сети
89479033	Истек тайм-аут ожидания запроса
89479034	Сервер активации возвратил ошибку 409
89479035	Недоступен необходимый ресурс на сервере активации. Сервер активации возвратил ошибку 410. Пожалуйста, проверьте настройки подключения к интернету
89479036	Сервер активации возвратил ошибку 411
89479037	Сервер активации возвратил ошибку 412
89479038	Сервер активации возвратил ошибку 413
89479039	Сервер активации возвратил ошибку 414
8947903A	Сервер активации возвратил ошибку 415
8947903C	Внутренняя ошибка сервера
8947903D	Функциональность не поддерживается
8947903E	Некорректный ответ от шлюза. Пожалуйста, проверьте настройки сети
8947903F	Ресурс временно недоступен
89479040	Истек тайм-аут ожидания ответа от шлюза. Пожалуйста, проверьте настройки сети

Код ошибки	Описание
89479041	Протокол не поддерживается сервером
89479043	Неизвестная ошибка HTTP
89479044	Некорректный идентификатор ресурса
89479046	Некорректный адрес (URL)
89479047	Некорректная целевая папка
89479048	Ошибка выделения памяти
89479049	Ошибка конвертации параметров в ANSI-строку (url, folder, agent)
8947904A	Ошибка создания рабочего потока
8947904B	Рабочий поток уже запущен
8947904C	Рабочий поток не запущен
8947904D	Файл ключа не найден на сервере активации
8947904E	Ключ заблокирован
8947904F	Внутренняя ошибка сервера активации
89479050	Недостаточно данных в запросе на активацию
89479053	Срок действия лицензии, соответствующей добавляемому ключу, уже истек
89479054	На компьютере установлена некорректная системная дата. Пожалуйста, проверьте системную дату на компьютере
89479055	Срок действия пробной лицензии истек
89479056	Период активации приложения истек
89479057	Превышено допустимое количество активаций приложения с помощью указанного кода
89479058	Процедура активации завершилась с системной ошибкой
89479059	Невозможно использовать ключ для пробной лицензии в качестве ключа для коммерческой лицензии
8947905C	Требуется код активации
89479062	Невозможно подключиться к серверу активации
89479064	Сервер активации недоступен. Пожалуйста, проверьте настройки подключения к интернету и попробуйте активировать приложение снова
89479065	Срок действия лицензии истек
89479066	Невозможно заменить активный ключ на ключ с истекшим сроком годности
89479067	Невозможно добавить резервный ключ, если срок действия соответствующей лицензии истекает раньше по сравнению с действующей лицензией
89479068	Отсутствует обновленный ключ по подписке
8947906A	Неподходящий код активации

Код ошибки	Описание
8947906B	Ключ уже активен
8947906C	Типы лицензий, которые соответствуют активному и резервному ключам, не совпадают
8947906D	Лицензия не допускает работу компонента
8947906E	Невозможно добавить ключ по подписке в качестве резервного
89479213	Общая ошибка транспортного уровня
89479214	Не удалось связаться с сервером активации
89479215	Неверный формат веб-адреса
89479216	Не удалось преобразовать адрес прокси-сервера
89479217	Не удалось преобразовать адрес сервера. Пожалуйста, проверьте настройки подключения к интернету
89479218	Попытка соединения с сервером завершилась с ошибкой
89479219	Удаленный отказ в доступе
8947921A	Тайм-аут операции истек
8947921B	Ошибка отправки HTTP-запроса
8947921C	Ошибка SSL-соединения
8947921D	Операция прервана в результате обратного вызова
8947921E	Слишком много перенаправлений
8947921F	Проверка адресата завершилась с ошибкой
89479220	Пустой ответ от сервера
89479221	Ошибка отправки данных
89479222	Ошибка приема данных
89479223	Проблема, связанная с SSL-сертификатом
89479224	Проблема, связанная с шифрованием SSL
89479225	Проблема, связанная с центром SSL-сертификации
89479226	Некорректное содержимое сетевого пакета
89479227	Учетной записи отказано в доступе
89479228	Некорректный файл SSL-сертификата
89479229	Не удалось завершить SSL-соединение
8947922A	Повторная ошибка
8947922B	Некорректный файл с отозванными сертификатами
8947922C	Ошибка запроса SSL-сертификата
89479401	Неизвестная ошибка сервера

Код ошибки	Описание
89479402	Внутренняя ошибка сервера
89479403	Ключ для введенного кода активации отсутствует
89479404	Активный ключ заблокирован
89479405	Отсутствуют обязательные параметры запроса для активации
89479406	Неверный номер или пароль клиента
89479407	Неверный код активации
89479408	Код активации не подходит для данного приложения. Невозможно активировать Kaspersky Endpoint Security для Windows с помощью кода активации для другого приложения. Пожалуйста, проверьте установленное приложение
89479409	Требуется код активации
8947940B	Истек период активации
8947940C	Превышено число активаций приложения с помощью этого кода активации
8947940D	Неверный формат идентификатора запроса
8947940E	Код активации уже используется
8947940F	Невозможно обновить код активации
89479410	Код активации не подходит для этого региона
89479411	Данный код активации не предназначен для используемой языковой версии приложения
89479412	Код активации предназначен для новой версии данного приложения. Для активации установленной версии приложения необходимо получить другой код активации
89479413	Сервер активации вернул ошибку 643
89479414	Сервер активации вернул ошибку 644
89479415	Сервер активации вернул ошибку 645
89479416	Сервер активации вернул ошибку 646
89479417	Требуется сервер активации версии 1.0
89479418	Неверный формат кода активации
89479419	Время на компьютере не синхронизировано со временем на сервере активации
8947941A	Неверная версия приложения
8947941B	Срок действия подписки истек
8947941C	Превышено допустимое количество активаций
8947941D	Неверная подпись тикета
8947941E	Требуются дополнительные данные пользователя
8947941F	Проверка данных пользователя завершилась с ошибкой

Код ошибки	Описание
89479420	Подписка неактивна
89479421	В данный момент производятся технические работы с сервером активации
89479501	Непредвиденная ошибка
89479502	Передан недопустимый параметр. Например, пустой список адресов серверов активации
89479503	Код активации недействителен (неправильная контрольная сумма)
89479504	Неверный идентификатор пользователя
89479505	Неверный пароль пользователя
89479506	Сервер активации вернул неверный ответ
89479507	Исполнение запроса на активацию было прервано
89479509	Сервер активации вернул пустой список переадресации

Использование профилей задач

Профиль задачи (далее также "профиль") – это набор параметров в текстовом или бинарном виде для создания задачи Kaspersky Endpoint Security.

Профили определяются в реестре операционной системы Windows в ветке `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.12.12\profiles` или `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.12.12\profiles`.

Профили имеют иерархическую структуру. Изменения, внесенные в родительский профиль, отражаются и на профилях, входящих в его состав. Например, при удалении родительского профиля все профили, входящие в его состав, также будут удалены.

Профиль может содержать следующие параметры:

- `flags` – внутренний механизм, описывающий доступные операции с задачей;
- `enabled` – параметр, разрешающий или запрещающий запуск задачи;
- `installed` – внутренний механизм, определяющий, установлены ли модули для данного профиля;
- `level` – внутренний механизм, используемый для разделения параметров по уровням;
- `type` – текстовое описание типа задачи;
- `remote` – параметр, позволяющий запустить задачу в отдельном процессе;
- `admflags` - параметры управления задачей с помощью Kaspersky Security Center;
- `pid` – идентификатор бинарного модуля, который содержит реализацию задачи;
- `iid` – идентификатор интерфейса задачи, определяющий класс, который содержит исполняемый

код для работы задачи;

- `persistent` – параметр, определяющий количество задач одного типа, которые можно создать в программе Kaspersky Endpoint Security;
- `idSettings` – идентификатор структуры параметров;
- `idStatistics` – идентификатор структуры статистики выполнения задачи;
- `schedule` – параметры расписания задачи;
- `runas` – параметры прав запуска задачи (используется только при значении параметра `persistent = 0`);
- `smode` – параметр, используемый для отложенного выполнения задачи;
- `settings` – дополнительные параметры задачи;
- `def` – параметры задачи, установленные по умолчанию.

Kaspersky Endpoint Security выполняет задачи на основе заданных параметров профиля. При создании задачи программа считывает все профили из реестра и для каждого профиля выполняет следующие действия:

1. Создает пустую структуру параметров с типом `idSettings`.
2. Десериализует значения параметра `settings` в подготовленную структуру.

   Если значения параметра `settings` не заданы, то программа использует значения параметра `def` и десериализует их в структуру. При отсутствии значений параметра `def` используются системные значения, заданные по умолчанию для пустой структуры параметров.
3. Создает пустую структуру с типом `idStatistics`, если этот параметр был указан в профиле для создаваемой задачи.
4. Находит бинарный модуль по идентификатору `pid`.
5. Создает экземпляр задачи по идентификатору `iid` из бинарного модуля.
6. Передает структуру параметров и статистики полученному экземпляру задачи.
7. Если указаны значения параметров `installed = 1` и `persistent = 1`, то программа запускает задачу.
8. Если указано значение параметра `persistent = 0`, то программа проверяет параметры `schedule` и `smode` и планирует запуск задачи в соответствии с заданными значениями.

Консоль администрирования Kaspersky Security Center позволяет создавать несколько групповых задач одного типа с различными параметрами. Для каждой такой задачи в реестре создается профиль с названием вида `<profile name>$<unique id>`, где `unique id` - уникальный идентификатор для задачи.

Профили приложения

Профиль – компонент, задача или функция Kaspersky Endpoint Security. Профили предназначены для управления приложением из командной строки. Вы можете использовать профили для выполнения команд

START, STOP, STATUS, STATISTICS и EXPORT. С помощью профилей вы можете настроить параметры приложения (например, STOP DeviceControl) или запустить задачу (например, START Scan_My_Computer).

Доступны следующие профили:

- AdaptiveAnomaliesControl – Адаптивный контроль аномалий.
- AMSI – AMSI-защита.
- AntiCryptor – Защита от шифрования.
- BehaviorDetection – Анализ поведения.
- DeviceControl – Контроль устройств.
- EntAppControl – Контроль приложений.
- File_Monitoring или FM – Защита от файловых угроз.
- Firewall или FW – Сетевой экран.
- HIPS – Предотвращение вторжений.
- IDS – Защита от сетевых угроз.
- IntegrityCheck – Проверка целостности.
- LogInspector – Анализ журналов.
- Mail_Monitoring или EM – Защита от почтовых угроз.
- Rollback – Откат обновления (профиль невозможно применить, если приложение установлено в режиме Легкого агента).
- Scan_ContextScan – Проверка из контекстного меню.
- Scan_IdleScan – Фоновая проверка.
- Scan_Memory – Проверка памяти ядра.
- Scan_My_Computer – Полная проверка.
- Scan_Objects – Выборочная проверка.
- Scan_Qscan – Проверка объектов, загрузка которых осуществляется при запуске операционной системы.
- Scan_Removable_Drive – Проверка съемных дисков.
- Scan_Startup или STARTUP – Проверка важных областей.
- Updater – Обновление (профиль невозможно применить, если приложение установлено в режиме Легкого агента).
- Web_Monitoring или WM – Защита от веб-угроз.
- WebControl – Веб-Контроль.

Также Kaspersky Endpoint Security поддерживает работу служебных профилей. Служебные профили могут понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Действия после сбоя или неустранимой ошибки в работе приложения

Приложение автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда приложение не может восстановить свою работу, вам требуется переустановить приложение или его компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 447).

kaspersky

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Endpoint Security, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Endpoint Security.

Kaspersky предоставляет поддержку Kaspersky Endpoint Security в течение жизненного цикла (см. страницу жизненного цикла приложений (https://support.kaspersky.ru/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules/ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки (https://support.kaspersky.ru/b2b) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

kaspersky

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Endpoint Security, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Endpoint Security.

Kaspersky предоставляет поддержку Kaspersky Endpoint Security в течение жизненного цикла (см. страницу жизненного цикла приложений (https://support.kaspersky.ru/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules/ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки (https://support.kaspersky.ru/b2b) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас создать *файл трассировки*. Файл трассировки позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на компьютере, подробные отчеты работы компонентов приложения.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры приложения:

- Активировать функциональность получения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов приложения, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения полученной диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав полученных в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

kaspersky

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в справке или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

О составе и хранении файлов трассировки 449

Трассировка работы приложения 452

Трассировка производительности приложения 453

Запись дампов 454

Защита файлов дампов и трассировок 455

О составе и хранении файлов трассировки

Вы сами несете ответственность за обеспечение безопасности полученной информации и, в частности, за контроль и ограничение доступа к полученной информации, хранимой на компьютере, до ее передачи в "Лабораторию Касперского".

Файлы трассировки хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения.

Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке `%ProgramData%\Kaspersky Lab\KES.12.12\Traces`.

Файлы трассировки называются следующим образом:
`KES<12.12_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Вы можете просмотреть данные, записанные в файлы трассировки.

Все файлы трассировки содержат следующие общие данные:

- Время события.
- Номер потока выполнения.

  Эту информацию не содержит файл трассировки Агента аутентификации.

- Компонент приложения, в результате работы которого произошло событие.
- Степень важности события (информационное, предупреждение, критическое, ошибка).
- Описание события выполнения команды компонента приложения и результата выполнения этой

команды.

Kaspersky Endpoint Security сохраняет пароли пользователя в файл трассировки только в зашифрованном виде.

Содержание файлов трассировки SRV.log, GUI.log и ALL.log

В файлы трассировки `SRV.log`, `GUI.log` и `ALL.log`, помимо общих данных, может записываться следующая информация:

- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на локальном компьютере.
- Данные об установленном на компьютере аппаратном обеспечении (например, данные о прошивке BIOS / UEFI). Эти данные записываются в файлы трассировки при выполнении полнодискового шифрования по технологии Шифрование диска Kaspersky.
- Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке интернет-трафика.
- Имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
- Имя учетной записи для входа в Microsoft Windows, если имя учетной записи является частью имени файла.
- Адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
- Веб-сайты, которые вы посещаете, а также ссылки с этих веб-сайтов. Эти данные записываются в файлы трассировки, когда приложение проверяет веб-сайты.
- Адрес прокси-сервера, имя компьютера, порт, IP-адрес, имя пользователя, используемое при авторизации на прокси-сервере. Эти данные записываются в файлы трассировки, если приложение использует прокси-сервер.
- Внешние IP-адреса, с которыми было установлено соединение с вашего компьютера.
- Тема сообщения, идентификатор, имя отправителя и адрес веб-страницы отправителя сообщения в социальной сети. Эти данные записываются в файлы трассировки, если включен компонент Веб-Контроль.
- Данные о сетевом трафике. Эти данные записываются в файлы трассировки, если включены компоненты мониторинга трафика (например, Веб-Контроль).
- Данные, полученные с серверов "Лаборатории Касперского" (например, версия антивирусных баз).
- Статусы компонентов Kaspersky Endpoint Security и сведения об их работе.
- Данные о действиях пользователя в приложении.
- События операционной системы.

Содержание файлов трассировки HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Файл трассировки `HST.log`, помимо общих данных, содержит информацию о выполнении задачи обновления баз и модулей приложения.

Файл трассировки `BL.log`, помимо общих данных, содержит информацию о событиях, возникающих во время работы приложения, а также данные, необходимые для устранения неполадок в работе приложения.

Этот файл создается, если приложение запускается с параметром avp.exe –bl.

Файл трассировки `Dumpwriter.log`, помимо общих данных, содержит служебную информацию, необходимую для устранения неполадок, возникающих при записи файла дампа приложения.

Файл трассировки `WD.log`, помимо общих данных, содержит информацию о событиях, возникающих в процессе работы службы avpsus, в том числе события обновления модулей приложения.

Файл трассировки `AVPCon.dll.log`, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файлов трассировки производительности

Файлы трассировки производительности называются следующим образом: `KES<12.12_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Файлы трассировки производительности, помимо общих данных, содержат информацию о нагрузке на процессор, о времени загрузки операционной системы и приложений, о запущенных процессах.

Содержание файла трассировки компонента AMSI-защита

Файл трассировки `AMSI.log`, помимо общих данных, содержит информацию о результатах проверок, запрошенных сторонними приложениями.

Содержание файла трассировки компонента Защита от почтовых угроз

Файл трассировки `mcou.OUTLOOK.EXE.log`, помимо общих данных, может содержать части сообщений электронной почты, в том числе адреса электронной почты.

Содержание файла трассировки компонента Проверка из контекстного меню

Файл трассировки `shellex.dll.log`, помимо общих данных, содержит информацию о выполнении задачи проверки и данные, необходимые для устранения неполадок в работе приложения.

Содержание файлов трассировки веб-плагина приложения

Файлы трассировки веб-плагина приложения хранятся на компьютере, на котором развернута Kaspersky Security Center Web Console, в папке `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Файлы трассировки веб-плагина приложения называются следующим образом: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. Web Console начинает записывать данные после установки и удаляет файлы трассировки после удаления Web Console.

Файлы трассировки веб-плагина приложения, помимо общих данных, содержат следующую информацию:

- Пароль пользователя KLAdmin для разблокировки интерфейса Kaspersky Endpoint Security (Защита паролем).
- Временный пароль для разблокировки интерфейса Kaspersky Endpoint Security (Защита паролем).
- Имя пользователя и пароль для почтового SMTP-сервера (Уведомления по электронной почте).
- Имя пользователя и пароль для прокси-сервера сети интернет (Прокси-сервер).
- Имя пользователя и пароль для задачи *Изменение состава компонентов приложения*.
- Учетные данные и пути, указанные в свойствах политики и в задачах Kaspersky Endpoint Security.

Содержание файла трассировки Агента аутентификации

Файл трассировки Агента аутентификации хранится в папке System Volume Information и называется следующим образом: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Файл трассировки Агента аутентификации, помимо общих данных, содержит информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации.

Трассировка работы приложения

Трассировка приложения – это подробная запись действий, выполняемых приложением, и сообщений о событиях, происходящих во время работы приложения. В процессе трассировки приложение создает комплект файлов с данными о работе разных компонентов приложения (см. раздел "О составе и хранении файлов трассировки" на стр. 449) (например, SRV.log, WD.log и другие).

Выполняйте трассировку приложения под руководством Службы технической поддержки "Лаборатории Касперского".

► *Чтобы создать файл трассировки приложения, выполните следующие действия:*

1. В главном окне приложения нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
3. Используйте переключатель **Включить трассировку приложения**, чтобы включить или выключить трассировку работы приложения.
4. В раскрывающемся списке **Трассировка** выберите режим трассировки работы приложения:
   - **С ограничением места**. Сохранить результаты трассировки в ограниченное число комплектов файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера. Если выбран этот режим, вы можете указать максимальное количество комплектов файлов для ротации и максимальный размер каждого комплекта файлов.

     По умолчанию приложение сохраняет пять комплектов файлов с трассировками. Размер каждого комплекта файлов составляет 3072 МБ. Таким образом, вам необходимо 15 ГБ свободного пространства на диске для сохранения файлов трассировки.
   - **Без ограничений**. Сохранить один файл трассировки (без ограничений по размеру).
5. В раскрывающемся списке **Уровень** выберите уровень трассировки.

   Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. Если указания Службы технической поддержки отсутствуют, рекомендуется устанавливать уровень трассировки **Обычный**.
6. Перезапустите Kaspersky Endpoint Security.
7. Чтобы остановить процесс трассировки, вернитесь в окно Мониторинга проблем и выключите трассировку.

Вы также можете создать файлы трассировки во время установки приложения из командной строки (см. раздел "Setup. Установка приложения" на стр. 376), в том числе с помощью файла setup.ini.

В результате в папке `%ProgramData%\Kaspersky Lab\KES.12.12\Traces` будут созданы файлы трассировки работы приложения. После создания файлов трассировки отправьте файлы в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Endpoint Security автоматически удаляет файлы трассировки при удалении приложения. Вы также можете вручную удалить файлы. Для этого трассировка должна быть выключена и приложение остановлено (см. раздел "Запуск и остановка Kaspersky Endpoint Security" на стр. 57).

Трассировка производительности приложения

Kaspersky Endpoint Security позволяет получить информацию о проблемах в работе компьютера при использовании приложения. Например, вы можете получить информацию о задержках при загрузке операционной системы после установки приложения. Для этого Kaspersky Endpoint Security создает файлы трассировки производительности (см. раздел "О составе и хранении файлов трассировки" на стр. 449). *Трассировка производительности* – это запись действий, выполняемых приложением, для диагностики проблем производительности Kaspersky Endpoint Security. Для получения информации Kaspersky Endpoint Security использует сервис трассировки событий Windows (англ. Event Tracing for Windows, ETW). Диагностику работы Kaspersky Endpoint Security и установление причин возникновения проблем выполняет Служба технической поддержки "Лаборатории Касперского".

Выполняйте трассировку приложения под руководством Службы технической поддержки "Лаборатории Касперского".

► *Чтобы создать файл трассировки производительности, выполните следующие действия:*

1. В главном окне приложения нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
3. Используйте переключатель **Включить трассировку производительности**, чтобы включить или выключить трассировку производительности приложения.
4. В раскрывающемся списке **Трассировка** выберите режим трассировки работы приложения:
   - **С ограничением места**. Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера. Если выбран этот режим, вы можете указать максимальный размер каждого файла.
   - **Без ограничений**. Сохранить один файл трассировки (без ограничений по размеру).
5. В раскрывающемся списке **Уровень** выберите уровень трассировки:
   - **Поверхностный**. Kaspersky Endpoint Security анализирует основные процессы операционной системы, связанные с производительностью.
   - **Детальный**. Kaspersky Endpoint Security анализирует все процессы операционной системы, связанные с производительностью.

6. В раскрывающемся списке **Тип трассировки** выберите тип трассировки:
   - **Базовая информация**. Kaspersky Endpoint Security анализирует процессы во время работы операционной системы. Используйте этот тип трассировки, если проблема воспроизводится после загрузки операционной системы, например, проблема доступа в интернет в браузере.
   - **При перезагрузке**. Kaspersky Endpoint Security анализирует процессы только на этапе загрузки операционной системы. После загрузки операционной системы Kaspersky Endpoint Security останавливает трассировку. Используйте этот тип трассировки, если проблема связана с задержкой загрузки операционной системы.
7. Перезагрузите компьютер и воспроизведите проблему.
8. Чтобы остановить процесс трассировки, вернитесь в окно Мониторинга проблем и выключите трассировку.

В результате в папке `%ProgramData%\Kaspersky Lab\KES.12.12\Traces` будет создан файл трассировки производительности. После создания файла трассировки отправьте файл в Службу технической поддержки "Лаборатории Касперского".

Запись дампов

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания этого файла дампа.

> Сохраненные дампы могут содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту файлов дампов.

Файлы дампов хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения. Файлы дампов хранятся в папке `%ProgramData%\Kaspersky Lab\KES.12.12\Traces`.

Как включить запись дампов в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

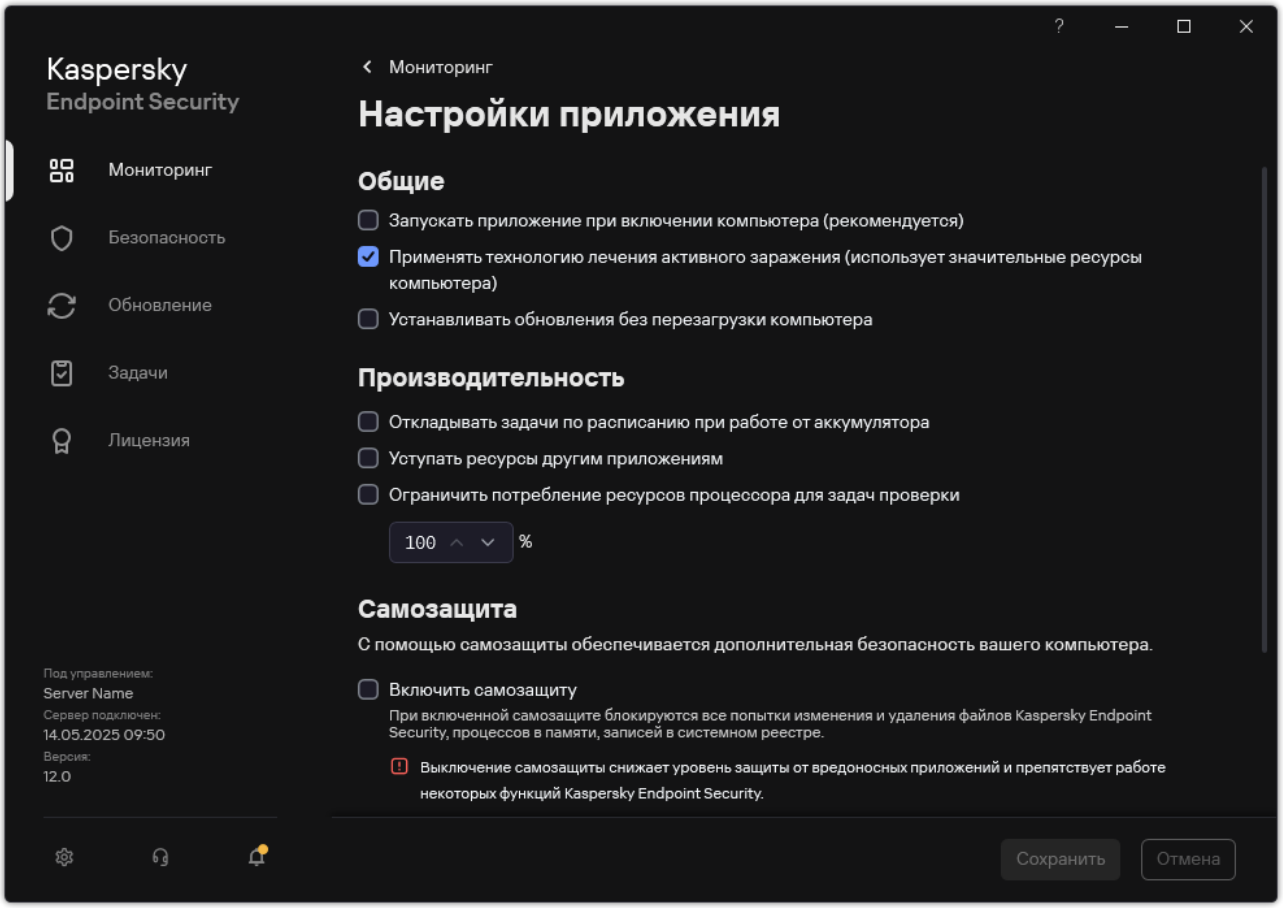


Рисунок 83. Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Отладочная информация** используйте флажок **Включить запись дампов**, чтобы включить или выключить запись дампов приложения.
4. Сохраните внесенные изменения.

Защита файлов дампов и трассировок

Файлы дампов и файлы трассировки содержат информацию об операционной системе, а также могут содержать данные пользователя (см. раздел "О составе и хранении файлов трассировки" на стр. 449). Чтобы предотвратить несанкционированный доступ к этим данным, вы можете включить защиту файлов дампов и файлов трассировки.

Если защита файлов дампов и файлов трассировки включена, доступ к файлам имеют следующие пользователи:

- К файлам дампов имеют доступ системный и локальный администраторы, а также пользователь, включивший запись файлов дампов и файлов трассировки.
- К файлам трассировки имеют доступ только системный и локальный администраторы.

Как включить защиту файлов дампов и файлов трассировки в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 51) нажмите на кнопку .
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.
3. В блоке **Отладочная информация** используйте флажок **Включить защиту файлов дампов и файлов трассировки**, чтобы включить или выключить защиту файлов.
4. Сохраните внесенные изменения.

Файлы дампов и файлы трассировки, записанные при включенной защите, остаются защищенными после отключения этой функции.

kaspersky

Глоссарий

О

OLE-объект

Файл, присоединенный или встроенный в другой файл. Приложения "Лаборатории Касперского" позволяют проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel® в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

А

Агент администрирования

Компонент приложения Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех приложений "Лаборатории Касперского", работающих в операционной системе Windows. Для приложений, работающих в других операционных системах, предназначены отдельные версии Агента администрирования.

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Активный ключ

Ключ, используемый в текущий момент для работы приложения.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

Б

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами "Лаборатории Касперского", регулярно обновляется и входит в поставку приложения "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку приложения "Лаборатории Касперского".

Г

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждого из установленных в группе приложений могут быть созданы групповые политики и сформированы групповые задачи.

Д

Доверенный платформенный модуль

Микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины.

Дополнительный ключ

Ключ, подтверждающий право на использование приложения, но не используемый в текущий момент.

З

Задача

Функции, выполняемые приложением "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной программы, представляющей угрозу). Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

И

Издатель сертификата

Центр сертификации, выдавший сертификат.

kaspersky

К

Коннектор к Агенту администрирования

Функциональность приложения, обеспечивающая связь приложения с Агентом администрирования. Агент администрирования предоставляет возможность удаленного управления приложением через Kaspersky Security Center.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Ложное срабатывание

Ситуация, когда незараженный файл определяется приложением "Лаборатории Касперского" как зараженный ввиду того, что его код напоминает код вируса.

М

Маска файла

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- ***** – символ, заменяющий нуль или более нуля любых символов;
- **?** – символ, заменяющий любой один символ.

Следует иметь в виду, что название и расширение файла всегда пишутся через точку.

Н

Настройки задачи

Настройки работы приложения, специфичные для каждого типа задач.

Нормализованная форма адреса веб-ресурса

Нормализованной формой адреса веб-ресурса называется текстовое представление адреса веб-ресурса, полученное в результате применения нормализации. *Нормализация* – процесс, в результате которого текстовое представление адреса веб-ресурса изменяется в соответствии с определенными правилами (например, исключение из текстового представления адреса веб-ресурса имени пользователя, пароля и

порта соединения, понижение верхнего регистра символов адреса веб-ресурса до нижнего регистра).

В контексте работы компонентов защиты цель нормализации адресов веб-ресурсов заключается в том, чтобы проверять синтаксически различные, но физически эквивалентные адреса веб-ресурсов один раз.

Пример:

Ненормализованная форма адреса: www.Example.com\.

Нормализованная форма адреса: www.example.com.

О

Область защиты

Объекты, которые компонент базовой защиты постоянно проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства.

Область проверки

Объекты, которые Kaspersky Endpoint Security проверяет во время выполнения задачи проверки.

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Отпечаток сертификата

Информация, по которой можно проверить подлинность сертификата сервера. Отпечаток создается путем применения криптографической хеш-функции к содержанию сертификата сервера.

П

Параметры приложения

Параметры работы приложения, общие для всех типов его задач и отвечающие за работу приложения в целом, например: параметры производительности приложения, параметры ведения отчетов, параметры резервного хранилища.

Портативный файловый менеджер

Приложение, предоставляющая интерфейс для работы с зашифрованными файлами на съемных дисках при недоступности функциональности шифрования на компьютере.

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это

исполняемые файлы, например, с расширением com, exe, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Программные модули

Файлы, входящие в состав дистрибутива приложения "Лаборатории Касперского" и отвечающие за реализацию его основных задач. Каждому типу задач, реализуемых приложением (Постоянная защита, Проверка по требованию, Обновление), соответствует свой исполняемый модуль. Запуская из главного окна полную проверку вашего компьютера, вы инициируете запуск модуля этой задачи.

P

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их лечением или удалением.

C

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Сертификат

Электронный документ, содержащий открытый ключ, информацию о владельце ключа и области применения ключа, а также подтверждающий принадлежность открытого ключа владельцу. Сертификат должен быть подписан выдавшим его центром сертификации.

Сетевая служба

Набор параметров, характеризующих сетевую активность. Для этой сетевой активности вы можете создать сетевое правило, регулирующее работу Сетевого экрана.

Сигнатурный анализ

Технология обнаружения угроз, которая использует базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

Субъект сертификата

Держатель закрытого ключа, связанного с сертификатом. Это может быть пользователь, приложение, любой виртуальный объект, компьютер или служба.

kaspersky

Ф

Фишинг

Вид интернет-мошенничества, заключающийся в рассылке сообщений электронной почты с целью кражи конфиденциальных данных, как правило, финансового характера.

Ч

Черный список адресов

Список адресов электронной почты, входящие сообщения с которых блокируются приложением "Лаборатории Касперского" независимо от их содержания.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

Эксплойт

Программный код, который использует какую-либо уязвимость в системе или программном обеспечении. Эксплойты часто используются для установки вредоносного программного обеспечения на компьютере без ведома пользователя.

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 26. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

Приложение 1. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированном конфигурации на другие значения, выводит программу из безопасного состояния.

В сертифицированной конфигурации Kaspersky Endpoint Security перед установкой программы вам нужно создать папку `%AllUsersProfile%\Application Data\Kaspersky Lab\Endpoint Agent\` (см. раздел "`Установка программы с помощью мастера`" на стр. 19). Далее вам необходимо предоставить доступ к новой папке только для учетной записи SYSTEM. Запретите удаление этой папки и изменение прав доступа. Перед установкой программы убедитесь, что права на чтение и запись в эту папку имеет только учетная запись SYSTEM.

Таблица 27. Параметры и их безопасные значения для программы в сертифицированной конфигурации

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Продвинутая защита		
Kaspersky Security Network	Kaspersky Security Network	Переключатель выключен. Допускается включить переключатель только при использовании Локального KSN (Kaspersky Private Security Network – KPSN).
Kaspersky Security Network	Включить облачный режим	Переключатель выключен.
Откат вредоносных действий	Откат вредоносных действий	Переключатель включен.
Базовая защита		
Защита от файловых угроз	Защита от файловых угроз	Переключатель включен.
Защита от файловых угроз	Уровень безопасности	Одно из следующих значений: • Рекомендуемый. • Высокий.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Защита от файловых угроз	Действие при обнаружении угрозы	Лечить; удалять, если лечение невозможно
Защита от файловых угроз → Расширенная настройка	Типы файлов	Все файлы
Защита от файловых угроз → Расширенная настройка	Область защиты	Все съемные диски, Все жесткие диски, Все сетевые диски.
Защита от файловых угроз → Расширенная настройка	Эвристический анализ	Флажок установлен.
Защита от файловых угроз → Расширенная настройка	Проверять архивы	Флажок установлен.
Защита от почтовых угроз	Защита от почтовых угроз	Переключатель включен.
Защита от почтовых угроз	Уровень безопасности	Одно из следующих значений: • Рекомендуемый. • Высокий.
Защита от почтовых угроз	Действие при обнаружении угрозы	Лечить; удалять, если лечение невозможно.
Защита от сетевых угроз	Защита от сетевых угроз	Переключатель включен.
Защита от сетевых угроз	Блокировать атакующие устройства на N мин	Флажок установлен. Время блокирования – 60 мин.
Защита от сетевых угроз	Исключения	Пустой список IP-адресов. Добавление некоторых исключений может вести к выходу из безопасного состояния. Администратору безопасности следует осторожно подходить к выбору исключений. Для минимизации риска рекомендуется оставить значения по умолчанию.
Контроль безопасности		
Контроль приложений	Контроль приложений	Переключатель включен.
Контроль устройств	Контроль устройств	Переключатель включен.
Задачи		

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Обновление	Загружать обновления модулей программы	Флажок снят.
Общие настройки		
Настройки приложения	Запускать Kaspersky Endpoint Security для Windows при включении компьютера	Флажок установлен.
Настройки приложения	Применять технологию лечения активного заражения	Флажок установлен.
Настройки приложения	Включить самозащиту	Флажок установлен.
Настройки приложения	Выключить внешнее управление системными службами	Флажок установлен.
Исключения и типы обнаруживаемых объектов	Типы обнаруживаемых объектов	Вирусы, черви; Троянские программы; Вредоносные утилиты; Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода; Множественно упакованные файлы
Исключения и типы обнаруживаемых объектов	Исключения	Список исключений пуст. Добавление некоторых исключений может вести к выходу из безопасного состояния. Администратору безопасности следует осторожно подходить к выбору исключений. Для минимизации риска рекомендуется оставить значения по умолчанию.
Исключения и типы обнаруживаемых объектов	Доверенные приложения	Список доверенных программ пуст. Добавление некоторых доверенных программ может вести к выходу из безопасного состояния. Администратору безопасности следует осторожно подходить к выбору доверенных программ. Для минимизации риска рекомендуется оставить значения по умолчанию.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Интерфейс	Защита паролем	Переключатель включен. Администратор безопасности должен установить надежный пароль и область действия (все опции).

kaspersky

Приложение 2. Группы доверия приложений

Все приложения, запускаемые на компьютере, Kaspersky Endpoint Security распределяет на группы доверия. Приложения распределяются на группы доверия в зависимости от степени угрозы, которую эти приложения могут представлять для операционной системы.

Существуют следующие группы доверия:

- **Доверенные**. В группу входят приложения, для которых выполняется одно или более следующих условий:
  - Приложения обладают цифровой подписью доверенных производителей.
  - О приложениях есть записи в базе доверенных приложений Kaspersky Security Network.
  - Пользователь поместил приложение в группу *Доверенные*.

  Запрещенных операций для таких приложений нет.
- **Слабые ограничения**. В группу входят приложения, для которых выполняются следующие условия:
  - Приложения не обладают цифровой подписью доверенных производителей.
  - О приложениях нет записей в базе доверенных приложений Kaspersky Security Network.
  - Пользователь поместил приложение в группу *Слабые ограничения*.

  Такие приложения имеют минимальные ограничения на работу с ресурсами операционной системы.
- **Сильные ограничения**. В группу входят приложения, для которых выполняются следующие условия:
  - Приложения не обладают цифровой подписью доверенных производителей.
  - О приложениях нет записей в базе доверенных приложений Kaspersky Security Network.
  - Пользователь поместил приложение в группу *Сильные ограничения*.

  Такие приложения имеют значительные ограничения на работу с ресурсами операционной системы.
- **Недоверенные**. В группу входят приложения, для которых выполняются следующие условия:
  - Приложения не обладают цифровой подписью доверенных производителей.
  - О приложениях нет записей в базе доверенных приложений Kaspersky Security Network.
  - Пользователь поместил приложение в группу *Недоверенные*.

  Для таких приложений запрещены все операции.

kaspersky

Приложение 3. Расширения файлов для быстрой проверки съемных дисков

com – исполняемый файл приложения размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст приложения dBase™, Clipper или Microsoft Visual FoxPro®, приложение пакета WAVmaker;

bin – бинарный файл;

bat – файл пакетного задания;

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – приложение, работающее в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о приложении;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых приложений;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовое приложение для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

msg – сообщение электронной почты Microsoft Mail;

plg – сообщение электронной почты;

mbx – сохраненное сообщение электронной почты Microsoft Office Outlook;

doc* – документы Microsoft Office Word, такие как: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Office Word, такие как: dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – приложение баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Windows Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave® Flash;

jpg, jpeg – файл графического формата хранения сжатых изображений;

emf – файл формата Enhanced Metafile;

ico – файл значка объекта;

ov? – исполняемые файлы Microsoft Office Word;

xl* – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft Office PowerPoint®, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint 2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Office Access®, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

kaspersky

Приложение 4. Типы файлов для фильтра вложений Защиты от почтовых угроз

Следует помнить, что фактический формат файла может не совпадать с форматом, указанным в расширении файла.

Если вы включили фильтрацию вложений в сообщениях электронной почты, то в результате фильтрации компонент Защита от почтовых угроз может переименовывать или удалять файлы следующих расширений:

com – исполняемый файл приложения размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст приложения dBase™, Clipper или Microsoft Visual FoxPro®, приложение пакета WAVmaker;

bin – бинарный файл;

bat – файл пакетного задания;

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – приложение, работающее в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о приложении;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых приложений;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовое приложение для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

msg – сообщение электронной почты Microsoft Mail;

plg – сообщение электронной почты;

mbx – сохраненное сообщение электронной почты Microsoft Office Outlook;

doc* – документы Microsoft Office Word, такие как: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Office Word, такие как: dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – приложение баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Windows Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave® Flash;

jpg, jpeg – файл графического формата хранения сжатых изображений;

emf – файл формата Enhanced Metafile;

ico – файл значка объекта;

ov? – исполняемые файлы Microsoft Office Word;

xl* – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft Office PowerPoint®, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint

2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Office Access®, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

Приложение 5. Сетевые параметры для взаимодействия с внешними службами

Kaspersky Endpoint Security и Kaspersky Security Center используют защищенный канал связи с TLS (Transport Layer Security) для работы с внешними службами "Лаборатории Касперского" (см. раздел "Особенности использования защищенных протоколов для взаимодействия с внешними службами" на стр. 39).

Приложение Kaspersky Endpoint Security использует следующие сетевые параметры для взаимодействия с внешними службами.

Таблица 28. Сетевые параметры

Адрес	Описание
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Протокол: `HTTPS` Порт: `443`	Активация приложения.

Адрес	Описание
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com s17.upd.kaspersky.com s18.upd.kaspersky.com s19.upd.kaspersky.com cm.k.kaspersky-labs.com Протокол: HTTPS Порт: 443	Обновление баз и модулей приложения.

Адрес	Описание
`downloads.upd.kaspersky.com` Протокол: HTTPS Порт: 443	• Обновление баз и модулей приложения. • Проверка доступа к серверам "Лаборатории Касперского". При сбоях доступа к серверам через системный DNS приложение будет использовать публичный DNS. Это нужно для обновления антивирусных баз и поддержки уровня безопасности компьютера. Приложение Kaspersky Endpoint Security будет использовать следующие публичные DNS в порядке их обхода: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Запросы приложения могут содержать адреса доменов и внешний IP-адрес пользователя, так как приложение устанавливает с DNS-сервером TCP/UDP-соединение. Эти данные нужны, например, для

Адрес	Описание
touch.kaspersky.com Протокол: HTTP	• Получение доверенного времени для проверки срока действия сертификата (TLS-соединение). • Предупреждение о запрете доступа к веб-ресурсу в браузере при работе Защиты от веб-угроз.
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com Протокол: HTTP Порт: 80	Обновление баз и модулей приложения.

Адрес	Описание
ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com Протокол: HTTPS Порт: 443	Использование Kaspersky Security Network.
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com Протокол: KSN Порт: 443, 1443	Использование Kaspersky Security Network.
click.kaspersky.com redirect.kaspersky.com Протокол: HTTPS Порт: 443	Переход по ссылкам из интерфейса.

Таблица 29. Параметры, использующиеся для шифрования

Адрес	Описание
crl.kaspersky.com ocsp.kaspersky.com Протокол: HTTP Порт: 80	Инфраструктура открытых ключей (англ. Public Key Infrastructure, PKI).

kaspersky

Приложение 7. Поддерживаемые расширения файлов для Запрета запуска объектов

Kaspersky Endpoint Security поддерживает запрет открытия файлов офисного формата через определенные приложения. Информация о поддерживаемых расширениях имен файлов и приложений приведена в следующей таблице.

Таблица 30. Поддерживаемые расширения файлов для Запрета запуска объектов

Имя приложения	Исполняемый файл	Расширение имени файла
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw

Имя приложения	Исполняемый файл	Расширение имени файла
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Яндекс.Браузер Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

kaspersky

Приложение 8. Поддерживаемые интерпретаторы скриптов для Запрета запуска объектов

Запрет запуска объектов поддерживает следующие интерпретаторы скриптов:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe

- wscript.exe
- wwahost.exe

Запрет запуска объектов поддерживает работу с Java-приложениями в среде выполнения Java (процессы java.exe и javaw.exe).

kaspersky

Приложение 9. Область поиска IOC в реестре (RegistryItem)

При добавлении типа данных **Реестр Windows - RegistryItem** в область поиска IOC, Kaspersky Endpoint Security по умолчанию анализирует следующие разделы реестра:

```
HKEY_CLASSES_ROOT\htafile
HKEY_CLASSES_ROOT\batfile
HKEY_CLASSES_ROOT\exefile
HKEY_CLASSES_ROOT\comfile
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
HKEY_LOCAL_MACHINE\Software\Classes\piffile
HKEY_LOCAL_MACHINE\Software\Classes\htafile
HKEY_LOCAL_MACHINE\Software\Classes\exefile
HKEY_LOCAL_MACHINE\Software\Classes\comfile
HKEY_LOCAL_MACHINE\Software\Classes\CLSID
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObje
ctDelayLoad
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explore
r
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

kaspersky

Приложение 10. Требования к IOC-файлам

При создании задач поиска IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Приложение поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- После загрузки IOC-файлов вы можете вручную изменять содержание файлов во встроенном редакторе прямо в свойствах задачи. Kaspersky Endpoint Security поддерживает изменение содержания IOC-файлов, которые соответствуют стандарту OpenIOC версии 1.1. Изменить содержание IOC-файлов, соответствующие стандарту OpenIOC версии 1.0, невозможно.
- Если при создании задачи *Поиск IOC* из командной строки (см. раздел "IOCSCAN. Поиск индикаторов компрометации (IOC)" на стр. 420) вы загрузите IOC-файлы, часть из которых не поддерживается, то при запуске задачи приложение будет использовать только поддерживаемые IOC-файлы. Если при создании задачи *Поиск IOC* из командной строки все загруженные вами IOC-файлы не поддерживаются, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации. Загрузить IOC-файлы, которые не поддерживаются, в Web Console или Cloud Console невозможно.
- Семантические ошибки и неподдерживаемые IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов приложение фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче поиска IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Размер одного IOC-файла не должен превышать 2 МБ. Использование файлов большего размера приводит к завершению задач поиска IOC с ошибкой. Суммарный размер всех добавляемых файлов в IOC-коллекции не должен превышать 10 МБ. Если размер всех файлов превышает 10 МБ, вам нужно разделить IOC-коллекцию и создать несколько задач *Поиск IOC*.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи *Поиск IOC*.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC.



ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX
https://support.kaspersky.com/Help/KESWin/12.12/IOC_Terms/IOC_TERMS.xlsx

Особенности и ограничения поддержки стандарта OpenIOC приложением приведены в следующей таблице.

Таблица 31. Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1.

Поддерживаемые условия	OpenIOC 1.0:
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	Для терминов Email/* поддерживаются только условия `contains` и `is`. Для корректной работы условия `is` адрес электронной почты в IOC-файле необходимо указывать в формате `"name@example.org" <SMTP:name@example.org>`.

Поддерживаемые атрибуты условий	OpenIOC 1.1:
	`preserve-case`
	`negate`

Поддерживаемые операторы	`AND` `OR`
Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is`, `greater-than`, `less-than`)

kaspersky

Особенности интерпретации типов данных

Типы данных "boolean string", "restricted string", "md5", "IP", "sha256", "base64Binary" интерпретируются как строка (string).

Приложение поддерживает интерпретацию параметра Content для типов данных int и date, заданного в виде промежутков:

OpenIOC 1.0:

С использованием оператора TO в поле Content:

```
<Content type="int">49600 TO 50700</Content>
<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>
<Content type="int">[154192 TO 154192]</Content>
```

OpenIOC 1.1:

С помощью условий greater-than и less-than

С использованием оператора TO в поле Content

Приложение поддерживает интерпретацию типов данных date и duration, если индикаторы заданы в формате ISO 8601, Zulu time zone, UTC.

kaspersky

Приложение 11. Учетные записи пользователей в правилах компонентов приложения

Для настройки работы некоторых компонентов приложения нужно добавить специальные правила. Например, для Веб-Контроля нужно добавить правило со списком веб-адресов, доступ к которым приложение будет блокировать. Также в правилах компонентов приложения вы можете настроить расписание работы компонента или выбрать пользователей, для которых приложение будет применять это правило.

Правила необходимо добавлять для настройки следующих компонентов приложения:

- Контроль приложений;
- Веб-Контроль (см. раздел "Добавление правила доступа к веб-ресурсам" на стр. 254);
- Контроль устройств (см. раздел "Контроль доступа к устройствам по типу" на стр. 213);
- Анализ журналов (см. раздел "Настройка предустановленных правил" на стр. 292);
- Адаптивный контроль аномалий (см. раздел "Создание исключения для правила Адаптивного контроля аномалий" на стр. 246);
- Контроль целостности системы (см. раздел "Контроль целостности системы в режиме реального времени" на стр. 280).

В Kaspersky Endpoint Security для Windows 12.5 добавлена возможность выбирать пользователей не только из Active Directory, но и из списка пользователей в Kaspersky Security Center или вы можете ввести данные локальной учетной записи вручную. Таким образом, вы можете добавить пользователей следующими способами:

- Active Directory (рекомендуется).
- Список пользователей в Kaspersky Security Center.
- Локальная учетная запись.

Для корректного добавления пользователей из всех источников необходимо обновить плагин управления и приложение Kaspersky Endpoint Security до версии 12.5 или выше.

Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Подробнее о рисках безопасности локальных учетных записей см. в Базе знаний Microsoft https://learn.microsoft.com/ru-ru/windows/security/identity-protection/access-control/local-accounts. Вы сами несете ответственность за обеспечение безопасности компьютера при использовании локальных учетных записей, в частности, за контроль и ограничение доступа к параметрам Kaspersky Endpoint Security.

Для идентификации пользователей приложение использует SID пользователя (Security Identifier). При использовании учетных записей из Active Directory или списка пользователей в Kaspersky Security Center приложение определяет SID на Сервере администрирования. Таким образом, приложение не оказывает дополнительную нагрузку на компьютер для идентификации пользователя. Если вы добавили в правило приложения более 1000 локальных учетных записей, то для идентификации пользователя приложение

обращается к контроллеру домена. Таким образом, возрастает нагрузка на компьютер. Для оптимизации нагрузки на компьютер рекомендуется использовать учетные записи из Active Directory или списка пользователей в Kaspersky Security Center.

Для идентификации учетных записей, добавленных вручную в формате `<username>` или `<hostname>\<username>`, приложение использует NetBIOS-имена. NetBIOS-имя имеет ограничение в 16 байт (15 символов). Если имя компьютера содержит более 15 символов, приложение не может идентифицировать пользователя. Далее приложение выключает правило и формирует ошибку, например, *Веб-Контроль: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)*. Для работы правила вам нужно вручную сократить длину имени компьютера. Вы можете добавлять учетные записи из Active Directory или Kaspersky Security Center. В этом случае приложение сокращает имя компьютера автоматически. Kaspersky Endpoint Security также поддерживает в правилах встроенные учетные записи пользователей и групп (например, группа "Все"). Из-за особенностей определения SID пользователя приложение позволяет использовать встроенные учетные записи, добавленные только из Active Directory или списка пользователей в Kaspersky Security Center. Правила, в которых встроенная учетная запись добавлена локально, не работают.

kaspersky

Приложение 12. Скрипт для создания папки Endpoint Agent

Перед установкой Kaspersky Endpoint Security необходимо выполнить скрипт, который автоматически создает папку Endpoint Agent и настраивает права доступа к папке только для учетной записи SYSTEM.

Для выполнения скрипта вам нужно скопировать текст ниже в текстовый редактор, например, Notepad. Далее измените расширение на BAT и запустите скрипт.

```
@setlocal
    @echo off
    set "folder_path=%ALLUSERSPROFILE%\Application Data\Kaspersky
Lab\Endpoint Agent"

    REM Check if folder already exists
    if exist "%folder_path%" (
        echo ERR: Folder %folder_path% already exists!
        exit /b 1
    )

    REM reset errorlevel
    cmd /c "exit /b 0"

    REM Create the folder
    mkdir "%folder_path%"
    if "%errorlevel%" neq "0" (
        echo ERR: Failed to create folder %folder_path%
        endlocal & echo on & exit /b 1
    )

    REM Set access permissions
    REM SYSTEM — full
    icacls "%folder_path%" /grant "SYSTEM:(OI)(CI)F"
    if "%errorlevel%" neq "0" (
        echo ERR: Failed to set access permissions SYSTEM: OI CI F for folder
%folder_path%
        endlocal & @echo on & @exit /b 1
    )

    REM Deny write rights
    icacls "%folder_path%" /deny "Users:(OI)(CI)W"
    if "%errorlevel%" neq "0" (
        echo ERR: Failed to set deny permissions Users: OI CI W for folder
%folder_path%
        endlocal & @echo on & @exit /b 1
    )
```

```
    icacls "%folder_path%" /deny "Authenticated Users:(OI)(CI)W"
    if "%errorlevel%" neq "0" (
         echo ERR: Failed to set deny permissions Authenticated Users: OI CI
W for folder %folder_path%
         endlocal & @echo on & @exit /b 1
    )

    @echo on
@endlocal
@echo INFO: Folder %folder_path% successfully created and configured
@exit /b 0
```