kaspersky

Kaspersky Endpoint Security для Windows

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 12.3.0.493

Уважаемый пользователь!

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

Дата редакции документа: 30.11.2023

Обозначение документа: 643.46856491.00100-08 90 01

https://www.kaspersky.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 ... 18
Активация программы с помощью мастера активации программы ... 23
Удаление приложения ... 25
Процедура приемки ... 26
Безопасное состояние ... 26
Проверка работоспособности. Тестовый файл EICAR ... 26
Разделение доступа к функциям программы по пользовательским ролям ... 27
Управление приложением через Консоль администрирования Kaspersky Security Center ... 29
О плагине управления Kaspersky Endpoint Security для Windows ... 29
Особенности использования защищенных протоколов для взаимодействия с внешними службами ... 30
Настройка локальных параметров приложения ... 31
Управление задачами ... 32
Управление политиками ... 34
Интерфейс приложения ... 38
Значок приложения в области уведомлений ... 40
Упрощенный интерфейс приложения ... 42
Настройка отображения интерфейса приложения ... 43
Запуск и остановка Kaspersky Endpoint Security ... 44
Приостановка и возобновление защиты и контроля компьютера ... 47
Поиск вредоносного ПО ... 49
Проверка компьютера ... 50
Проверка съемных дисков при подключении к компьютеру ... 56
Фоновая проверка ... 58
Проверка из контекстного меню ... 59
Проверка целостности приложения ... 63
Формирование области проверки ... 65
Запуск проверки по расписанию ... 66
Запуск проверки с правами другого пользователя ... 69
Оптимизация проверки ... 69
Обновление баз и модулей программы ... 72
Схема обновления с серверного хранилища ... 73
Запуск и остановка задачи обновления ... 76

Запуск задачи обновления с правами другого пользователя 77
Выбор режима запуска для задачи обновления 78
Добавление источника обновлений 79
Обновление модулей приложения 82
Использование прокси-сервера при обновлении 83
Откат последнего обновления 87
Обновление антивирусных баз в ручном режиме 89
Устранение уязвимостей и установка критических обновлений в приложении 90
Работа с активными угрозами 91
Лечение активных угроз на рабочих станциях 92
Лечение активных угроз на серверах 93
Включение и выключение технологии лечения активного заражения 93
Обработка активных угроз 94
Kaspersky Security Network 97
Включение и выключение использования Kaspersky Security Network 98
Ограничения работы с Локальным KSN 99
Включение и выключение облачного режима для компонентов защиты 100
Настройка KSN Proxy 100
Проверка репутации файла в Kaspersky Security Network 102
Анализ поведения 104
Включение и выключение Анализа поведения 105
Выбор действия при обнаружении вредоносной активности приложения 106
Защита папок общего доступа от внешнего шифрования 107
Включение и выключение защиты папок общего доступа от внешнего шифрования 107
Выбор действия при обнаружении внешнего шифрования папок общего доступа 110
Создание исключения для защиты папок общего доступа от внешнего шифрования 111
Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования 112
Защита от эксплойтов 114
Включение и выключение Защиты от эксплойтов 114
Защита памяти системных процессов 115
Предотвращение вторжений 117
Включение и выключение Предотвращения вторжений 118
Работа с группами доверия приложений 119
Изменение группы доверия для приложения 119
Настройка прав группы доверия 120
Выбор группы доверия для приложений, запускаемых до Kaspersky Endpoint Security 121
Выбор группы доверия для неизвестных приложений 121
Выбор группы доверия для приложений с цифровой подписью 122
Работа с правами приложений 122
Защита ресурсов ОС и персональных данных 124

Удаление информации о неиспользуемых приложениях 125
Мониторинг работы Предотвращения вторжений 126
Защита доступа к аудио и видео 126
Откат вредоносных действий 129
Защита от файловых угроз 131
Включение и выключение Защиты от файловых угроз 131
Автоматическая приостановка Защиты от файловых угроз 134
Изменение действия компонента Защита от файловых угроз над зараженными файлами 135
Формирование области защиты компонента Защита от файловых угроз 135
Использование методов проверки 137
Использование технологий проверки в работе компонента Защита от файловых угроз 137
Оптимизация проверки файлов 138
Проверка составных файлов 138
Изменение режима проверки файлов 139
Защита от веб-угроз 141
Включение и выключение Защиты от веб-угроз 142
Настройка методов обнаружения вредоносных веб-адресов 144
Анти-Фишинг 146
Формирование списка доверенных веб-адресов 147
Защита от почтовых угроз 149
Включение и выключение Защиты от почтовых угроз 150
Изменение действия над зараженными сообщениями электронной почты 153
Формирование области защиты компонента Защита от почтовых угроз 154
Проверка составных файлов, вложенных в сообщения электронной почты 155
Фильтрация вложений в сообщениях электронной почты 156
Защита от сетевых угроз 158
Включение и выключение Защиты от сетевых угроз 159
Блокирование атакующего компьютера 160
Настройка адресов исключений из блокирования 162
Настройка защиты от сетевых атак по типам 164
Защита от атак BadUSB 166
Включение и выключение Защиты от атак BadUSB 168
Использовании экранной клавиатуры при авторизации USB-устройств 168
AMSI-защита 169
Включение и выключение AMSI-защиты 170
Проверка составных файлов AMSI-защитой 170
Проверка защищенных соединений 173
Включение проверки защищенных соединений 174
Установка доверенных корневых сертификатов 177
Проверка защищенных соединений в Firefox и Thunderbird 178

Проверка защищенных соединений в Firefox и Thunderbird 179
Исключение защищенных соединений из проверки 180
Контроль приложений 183
Ограничения функциональности Контроля приложений 187
Включение и выключение Контроля приложений 188
Выбор режима Контроля приложений 189
Действия с правилами Контроля приложений в интерфейсе приложения 190
Добавление условия срабатывания в правило Контроля приложений 192
Добавление правила Контроля приложений 193
Изменение статуса правила Контроля приложений 194
Тестирование правил Контроля приложений 194
Мониторинг активности приложений 195
Правила формирования масок имен файлов или папок 196
Изменение шаблонов сообщений Контроля приложений 196
Контроль устройств 198
Включение и выключение Контроля устройств 201
О правилах доступа 202
Изменение правила доступа к устройствам 203
Изменение правила доступа к шине подключения 206
Контроль доступа к мобильным устройствам 207
Контроль доступа к Bluetooth-устройствам 212
Контроль печати 214
Контроль подключения к Wi-Fi 218
Мониторинг использования съемных дисков 221
Изменение периода кеширования 224
Действия с доверенными устройствами 225
Добавление устройства в список доверенных из интерфейса приложения 226
Добавление устройства в список доверенных из Kaspersky Security Center 226
Экспорт и импорт списка доверенных устройств 228
Получение доступа к заблокированному устройству 229
Онлайн-режим предоставления доступа 231
Офлайн-режим предоставления доступа 232
Изменение шаблонов сообщений Контроля устройств 234
Анти-Бриджинг 234
Включение Анти-Бриджинга 235
Изменение статуса правила установки соединений 235
Изменение приоритета правила установки соединений 236
Адаптивный контроль аномалий 237
Включение и выключение Адаптивного контроля аномалий 240
Включение и выключение правила Адаптивного контроля аномалий 241

Изменение действия при срабатывании правила Адаптивного контроля аномалий 241
Создание исключения для правила Адаптивного контроля аномалий 242
Экспорт и импорт исключений для правил Адаптивного контроля аномалий 243
Применение обновлений для правил Адаптивного контроля аномалий 244
Изменение шаблонов сообщений Адаптивного контроля аномалий 245
Просмотр отчетов Адаптивного контроля аномалий 246
Веб-Контроль 247
Включение и выключение Веб-Контроля 249
Действия с правилами доступа к веб-ресурсам 250
Добавление правила доступа к веб-ресурсам 251
Назначение приоритета правилам доступа к веб-ресурсам 253
Включение и выключение правила доступа к веб-ресурсам 253
Проверка работы правил доступа к веб-ресурсам 253
Экспорт и импорт списка адресов веб-ресурсов 254
Мониторинг активности пользователей в интернете 255
Изменение шаблонов сообщений Веб-Контроля 258
Правила формирования масок адресов веб-ресурсов 259
Контроль сетевых портов 262
Включение контроля всех сетевых портов 263
Формирование списка контролируемых сетевых портов 264
Формирование списка приложений, для которых контролируются все сетевые порты 264
Анализ журналов 266
Настройка предустановленных правил 267
Добавление пользовательских правил 268
Мониторинг файловых операций 270
Формирование области мониторинга 270
Просмотр информации о целостности системы 272
Защита паролем 273
Включение Защиты паролем 276
Предоставление разрешений для отдельных пользователей или групп 277
Использование временного пароля для предоставления разрешений 278
Особенности разрешений Защиты паролем 279
Сброс пароля KLAdmin 280
Доверенная зона 282
Создание исключения из проверки 282
Выбор типов обнаруживаемых объектов 286
Формирование списка доверенных приложений 288
Создание локальной доверенной зоны 291
Использование доверенного системного хранилища сертификатов 295

Работа с резервным хранилищем 296
Настройка максимального срока хранения файлов в резервном хранилище 296
Настройка максимального размера резервного хранилища 297
Восстановление файлов из резервного хранилища 298
Удаление резервных копий файлов из резервного хранилища 299
Служба уведомлений 300
Настройка параметров журналов событий 300
Настройка отображения и доставки уведомлений 301
Настройка отображения предупреждений о состоянии приложения в области уведомлений 302
Работа с отчетами 303
Просмотр отчетов 304
Настройка максимального срока хранения отчетов 305
Настройка максимального размера файла отчета 306
Сохранение отчета в файл 307
Удаление информации из отчетов 309
Самозащита Kaspersky Endpoint Security 310
Включение и выключение механизма самозащиты 311
Включение и выключение поддержки AM-PPL 312
Защита служб приложения от внешнего управления 313
Обеспечение работы приложений удаленного администрирования 314
Производительность Kaspersky Endpoint Security и совместимость с другими приложениями 316
Включение и выключение режима энергосбережения 318
Включение и выключение режима передачи ресурсов другим приложениям 319
Создание и использование конфигурационного файла 321
Восстановление параметров приложения по умолчанию 323
Kaspersky Anti Targeted Attack Platform (EDR) 324
Интеграция встроенного агента с EDR (KATA) 325
Настройка отправки телеметрии 327
Работа с приложением из командной строки 329
Установка приложения 329
Активация приложения 337
Удаление приложения 337
Команды AVP 338
SCAN. Поиск вредоносного ПО 339
UPDATE. Обновление баз и модулей приложения 344
ROLLBACK. Откат последнего обновления 345
TRACES. Трассировка 346
START. Запуск профиля 347
STOP. Остановка профиля 348
STATUS. Статус профиля 349

STATISTICS. Статистика выполнения профиля 349
RESTORE. Восстановление файлов из резервного хранилища 349
EXPORT. Экспорт параметров приложения 350
IMPORT. Импорт параметров приложения 351
ADDKEY. Применение файла ключа 352
LICENSE. Лицензирование 353
RENEW. Приобретение лицензии 354
PBATESTRESET. Сбросить результаты проверки перед шифрованием диска 354
EXIT. Завершение работы приложения 354
EXITPOLICY. Выключение политики 355
STARTPOLICY. Включение политики 355
DISABLE. Выключение защиты 355
SPYWARE. Обнаружение шпионского ПО 355
KSN. Переключение KSN / KPSN 355
KATAEDR. Интеграция с EDR (KATA) 356
Команды KESCLI 357
Scan. Поиск вредоносного ПО 358
GetScanState. Статус выполнения проверки 359
GetLastScanTime. Определения времени выполнения проверки 360
GetThreats. Получение данных об обнаруженных угрозах 360
UpdateDefinitions. Обновление баз и модулей приложения 362
GetDefinitionState. Определение времени выполнения обновления 363
EnableRTP. Включение защиты 363
GetRealTimeProtectionState. Статус Защиты от файловых угроз 363
Version. Определение версии приложения 363
Сообщения об ошибках 364
Коды возврата 367
Коды ошибок 373
Использование профилей задач 379
Профили приложения 381
Действия после сбоя или неустранимой ошибки в работе приложения 382
Способы получения технической поддержки 383
Техническая поддержка через Kaspersky CompanyAccount 383
Обращение в Службу технической поддержки 385
О составе и хранении файлов трассировки 386
Трассировка работы приложения 389
Трассировка производительности приложения 390
Запись дампов 391
Защита файлов дампов и трассировок 391

Глоссарий 393
Информация о стороннем коде 399
Соответствие терминов 400
Приложение 1. Значения параметров программы в сертифицированной конфигурации 401
Приложение 2. Группы доверия приложений 404
Приложение 3. Расширения файлов для быстрой проверки съемных дисков 405
Приложение 4. Типы файлов для фильтра вложений Защиты от почтовых угроз 407
Приложение 5. Сетевые параметры для взаимодействия с внешними службами 410

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.

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/kes-for-windows/12.3?page=kb) 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.

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 (ОО) 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 16

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.
- оперативная память:
  - рабочая станция (x86) – 1 ГБ;
  - рабочая станция (x64) – 2 ГБ;
  - сервер – 2 ГБ.

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.

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. Core Mode) (см. известные ограничения).

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 Core Mode);
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (включая Core Mode);
- Windows Server 2016 Essentials / Standard / Datacenter (включая Core Mode);
- Windows Server 2019 Essentials / Standard / Datacenter (включая Core Mode);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая Core Mode).

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:

- VMware Workstation 17.0.2 Pro;
- VMware ESXi 8.0 Update 1c;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7 2305;
- Citrix Provisioning 2305;
- Citrix Hypervisor 8.2 (Cumulative Update 1).

Поддержка Kaspersky Security Center

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

- Kaspersky Security Center 12;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2;
- Kaspersky Security Center 13.2.2;
- 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.

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.
17. Должен быть обеспечен надежный источники меток времени.
18. Должна быть обеспечена синхронизация по времени с другими компонентами Kaspersky Endpoint Detection and Response, а также программы и ее средой функционирования.

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

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

- наличие несовместимого программного обеспечения (список несовместимого ПО приведен в файле incompatible.txt в комплекте поставки);
- выполнение аппаратных и программных требований;
- 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).

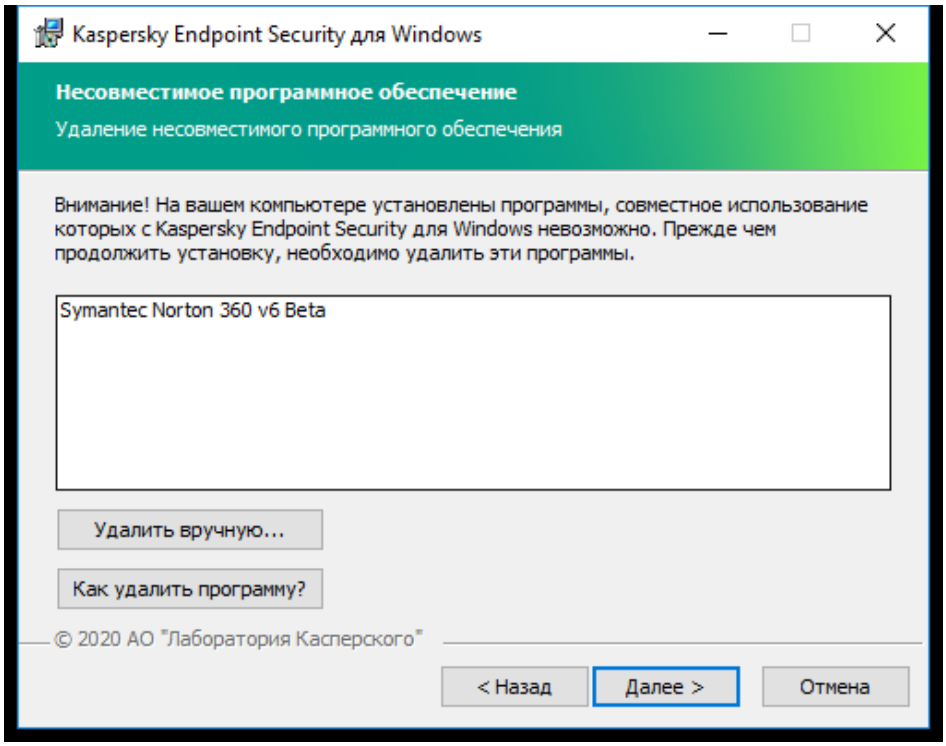


Рисунок 1. Удаление несовместимого обеспечения

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 12.3 для Windows, а предыдущая версия приложения автоматически удаляется. Это относится к следующим версиям приложения:

- Kaspersky Endpoint Security для Windows 11.7.0 (сборка 11.7.0.669).
- Kaspersky Endpoint Security для Windows 11.8.0 (сборка 11.8.0.384).
- Kaspersky Endpoint Security для Windows 11.9.0 (сборка 11.9.0.351).
- 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).

Конфигурация Kaspersky Endpoint Security

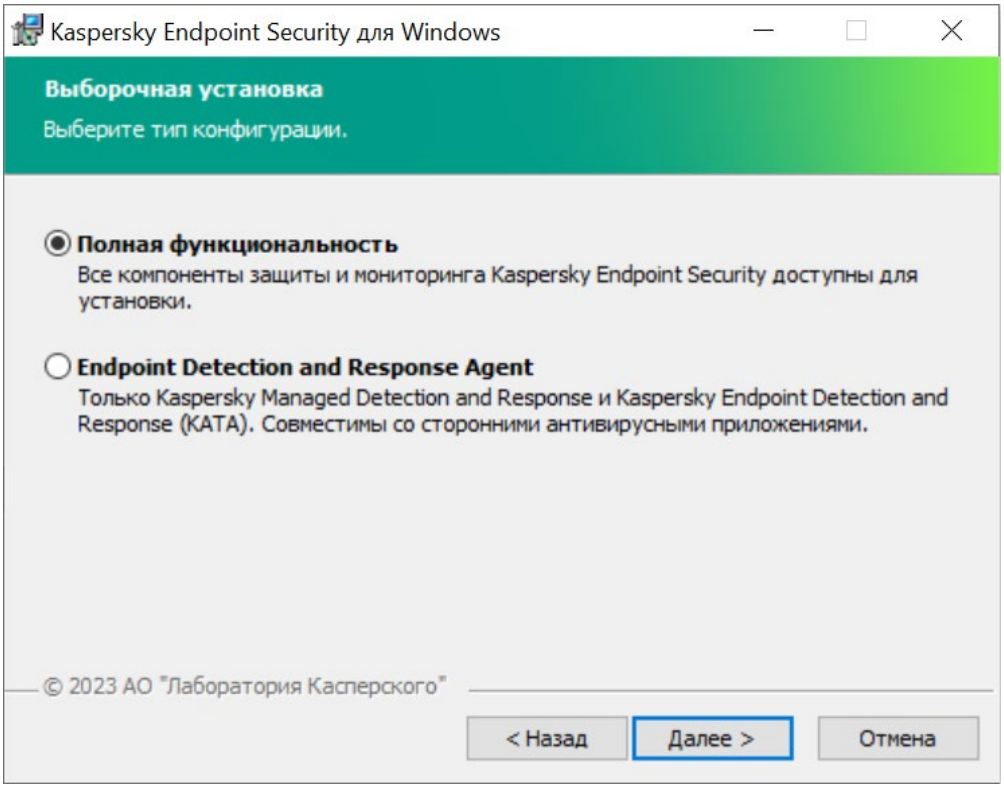


Рисунок 2. Выбор компонентов для установки приложения

Полная функциональность. 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. Вы можете выбрать компоненты, которые необходимо установить, на следующем шаге мастера установки приложения.

Endpoint Detection and Response Agent. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: Endpoint Detection and Response (KATA) (см. раздел "Kaspersky Anti Targeted Attack Platform (EDR)" на стр. 324) или Managed Detection and Response. 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 Agent может быть совместим со сторонними EPP-приложениями.

Выберите конфигурацию **Полная функциональность**.

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, включая задачи проверки;
- 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);
  - Мониторинг файловых операций (только для серверов).

- Detection and Response:
  - Endpoint Detection and Response (KATA).
- Коннектор к Агенту администрирования.

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

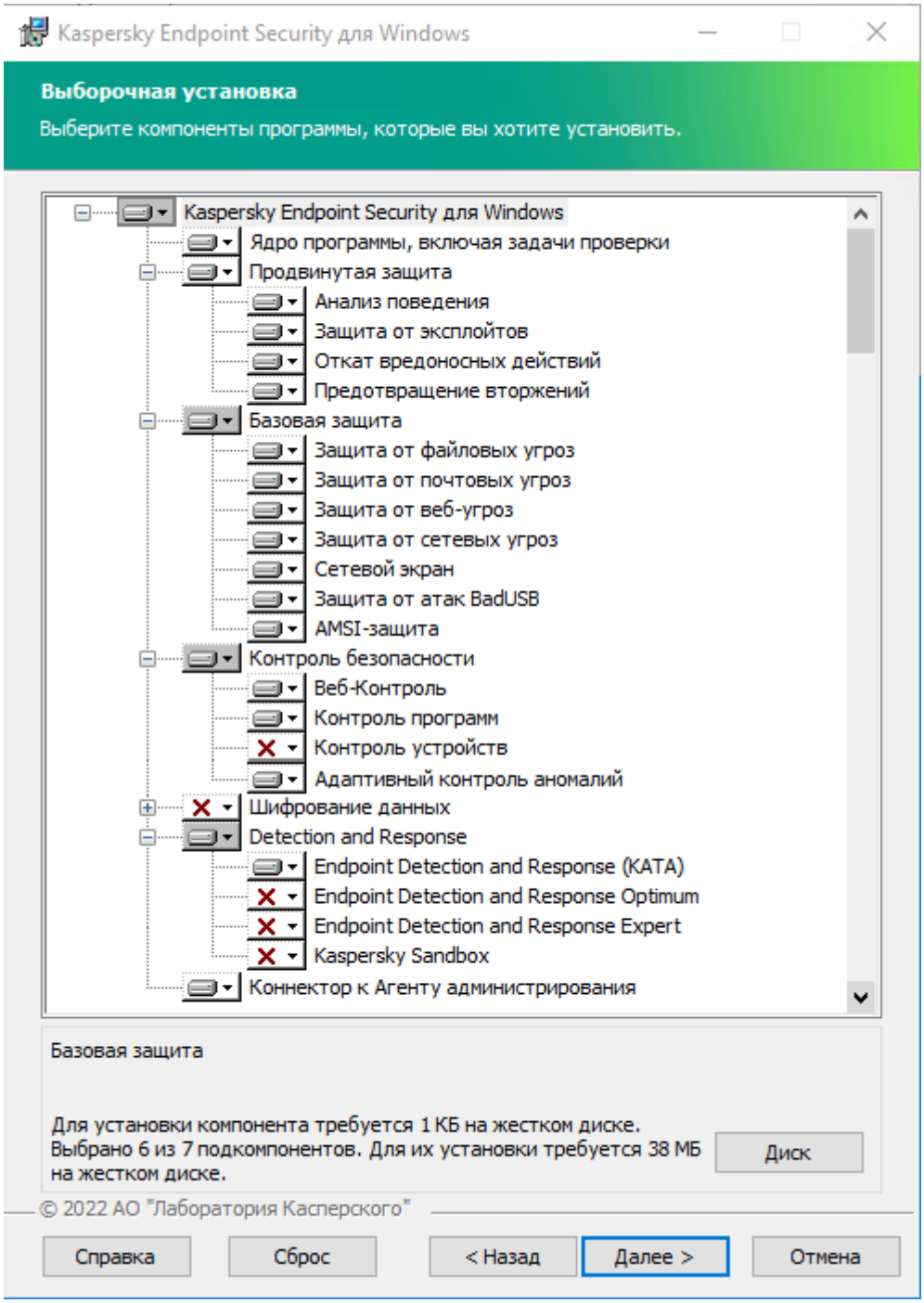


Рисунок 3. Сертификационная конфигурация программы для рабочей станции

Дополнительные параметры

Защитить процесс установки программы. 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 (необходимо использовать только при работе 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.

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.

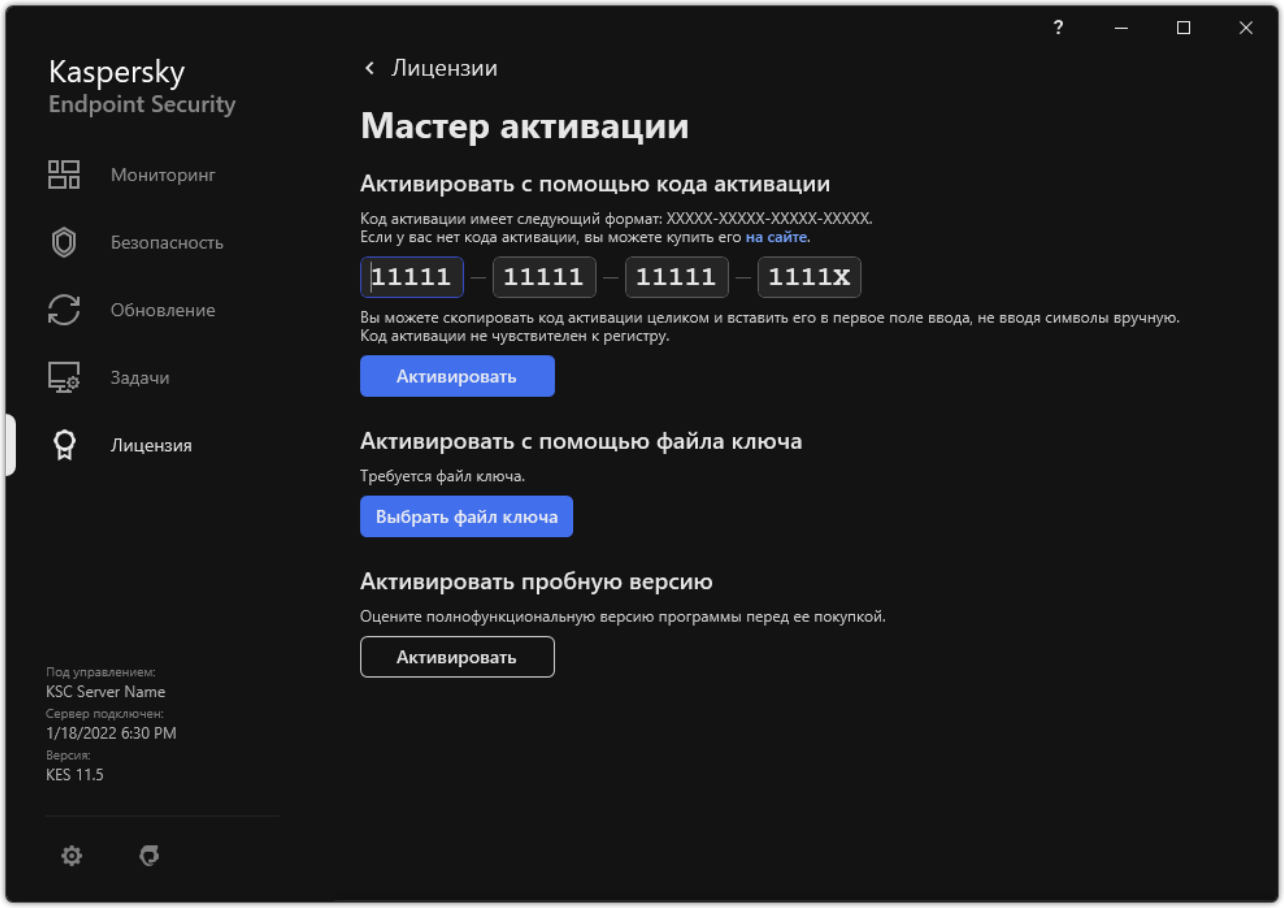


Рисунок 4. Активация приложения

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).

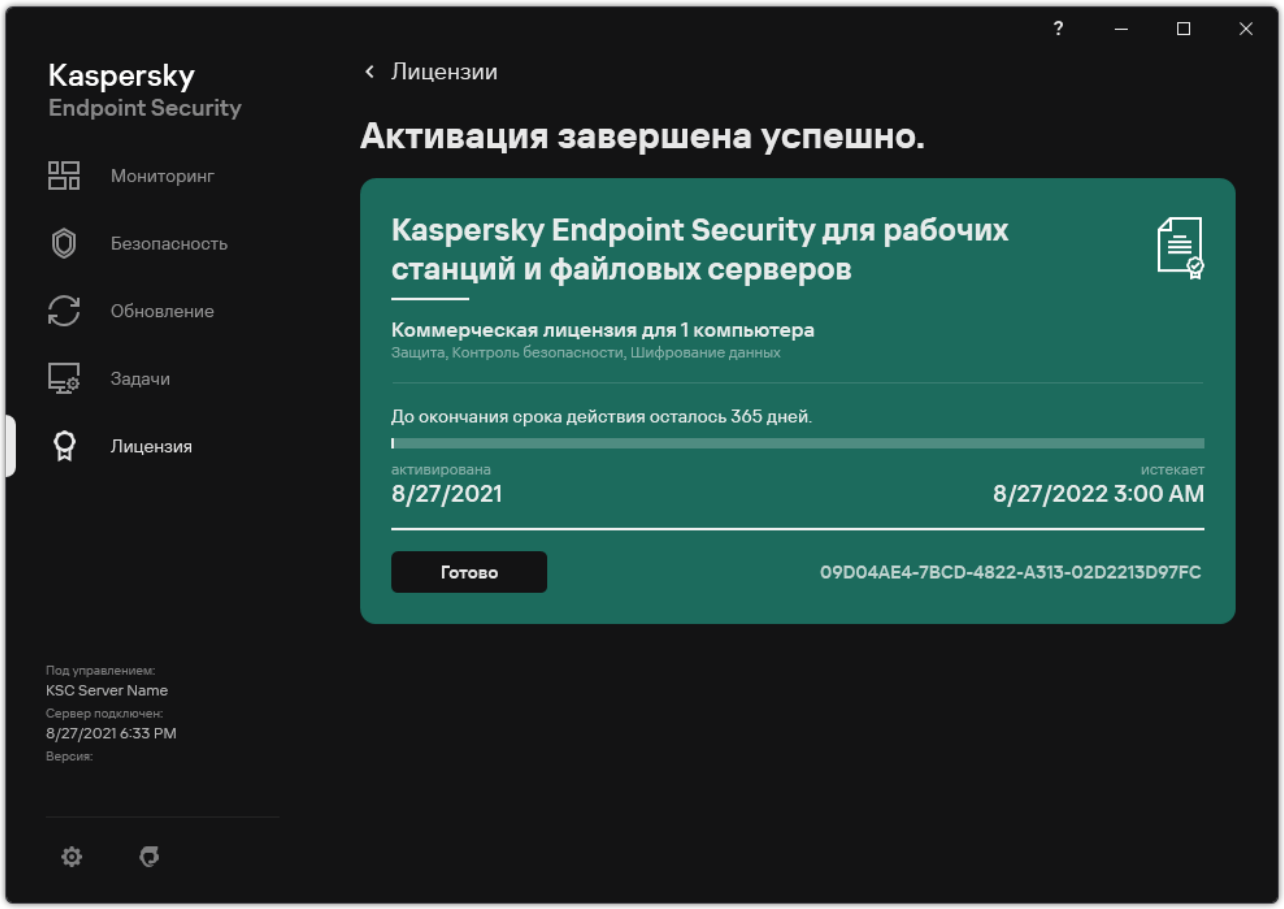


Рисунок 5. Информация о лицензионном ключе

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.

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 26
Проверка работоспособности. Тестовый файл EICAR 26

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. 401).

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.

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
Detection and Response	Endpoint 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/14.2/ru-RU/index.htm.

В этом разделе

О плагине управления Kaspersky Endpoint Security для Windows 29

Особенности использования защищенных протоколов для взаимодействия с внешними службами 30

Настройка локальных параметров приложения 31

Управление задачами 32

Управление политиками 34

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. 34), задачи (см. раздел "Управление задачами" на стр. 32), а также локальные параметры приложения (см. раздел "Настройка локальных параметров приложения" на стр. 31). 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. В отличие от плагина управления для Консоли администрирования Kaspersky Security Center, который устанавливается на рабочее место администратора, 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/14.2/ru-RU/index.htm.

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/14.2/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. 410).

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. 34).

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 входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security.
5. В контекстном меню клиентского компьютера выберите пункт **Свойства**.

   Откроется окно свойств клиентского компьютера.
6. В окне свойств клиентского компьютера выберите раздел **Программы**.

   Справа в окне свойств клиентского компьютера отобразится список приложений "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите приложение Kaspersky Endpoint Security.
8. Нажмите на кнопку **Свойства** под списком приложений "Лаборатории Касперского".

   Откроется окно **Параметры программы "Kaspersky Endpoint Security для Windows"**.
9. В разделе **Общие параметры** настройте параметры работы Kaspersky Endpoint Security, а также параметры отчетов и хранилищ.

   Остальные разделы окна **Параметры программы "Kaspersky Endpoint Security для Windows"** 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.

10. 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/14.2/ru-RU/index.htm.

Kaspersky Endpoint Security поддерживает выполнение следующих задач:

- **Поиск вредоносного ПО** (см. раздел "**Поиск вредоносного ПО**" на стр. 49). 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. 66) 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**. Kaspersky Endpoint Security обновляет базы и модули приложения. Задача *Обновление* 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. 87). 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** (см. раздел "**Проверка целостности приложения**" на стр. 63). 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.

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. 44).

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/14.2/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. 303).

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/14.2/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. 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 **Локальные задачи** → **Управление задачами**.
5. Настройте режим работы с задачами (см. таблицу ниже).
6. Сохраните внесенные изменения.

Таблица 2. Параметры управления задачами

Параметр	Описание
Разрешить использование локальных задач	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.
Разрешить отображение 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.
Разрешить управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в 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 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.

Активная и неактивная политика

Политика предназначена для группы управляемых компьютеров и может быть активной или неактивной. 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.

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.

Политика для автономных пользователей

Политика для автономных пользователей активируется, когда компьютер покидает периметр сети организации.

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. 31). 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.

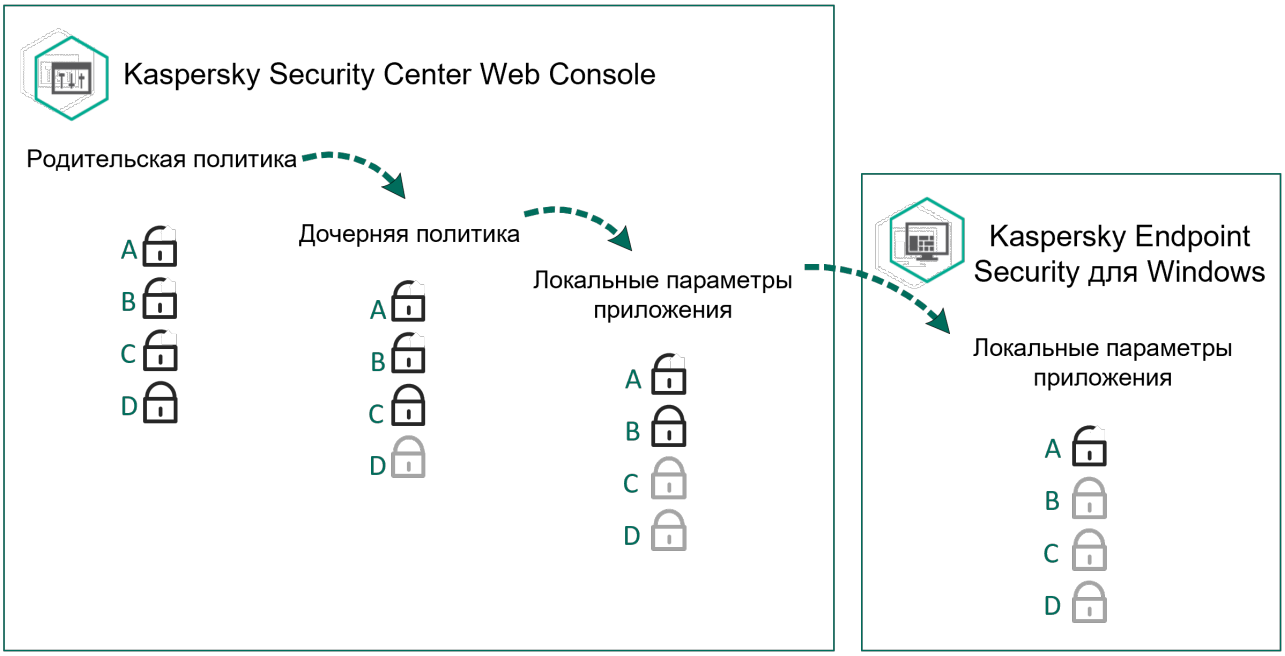


Рисунок 6. Наследование параметров

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.

Создание 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.

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/14.2/ru-RU/index.htm.

Индикатор уровня защиты

В верхней части окна **Свойства: <Название 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.
    - Анализ поведения.
    - Защита от эксплойтов.
    - Откат вредоносных действий.
  - **Важные**. Категория включает следующие компоненты:
    - Kaspersky Security Network.
    - Защита от веб-угроз.
    - Защита от почтовых угроз.
    - Предотвращение вторжений.
    - Защита паролем.
- **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 **Дополнительные настройки**. В этом окне вы можете включить любой из рекомендованных компонентов защиты.

Интерфейс приложения

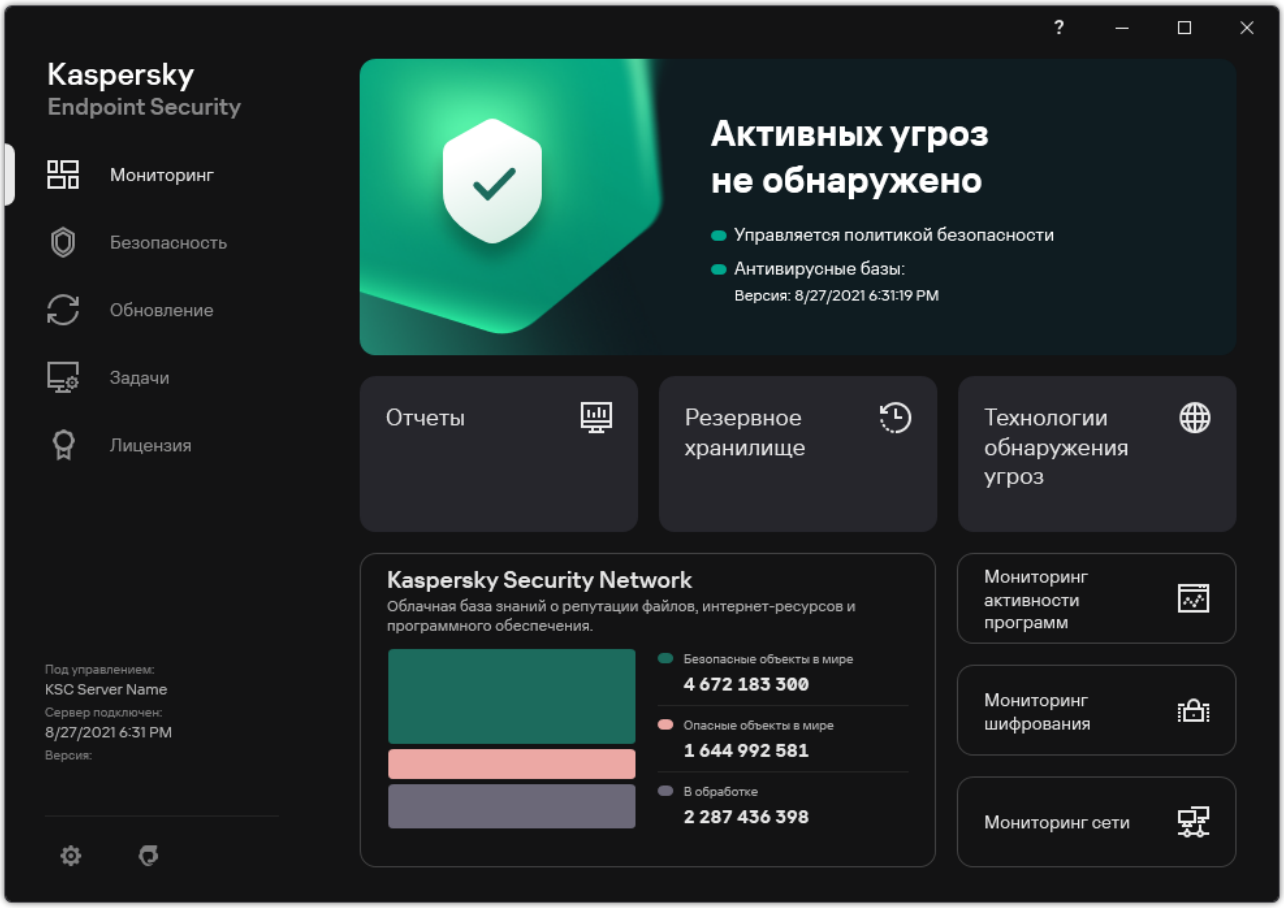


Рисунок 7. Главное окно программы

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 отслеживает файловые, реестровые и системные события в операционной системе, связанные с приложением.
- **Мониторинг сети**. Просмотр информации о сетевой активности компьютера в режиме реальном 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. 87). Администратор может скрыть раздел от пользователя (см. раздел "Управление задачами" на стр. 32) или ограничить управление задачами (см. раздел "Управление задачами" на стр. 32).

Задачи

Управление задачами проверки Kaspersky Endpoint Security. Вы можете выполнять поиск вредоносного ПО (на стр. 49) и проверку целостности приложения (см. раздел "Проверка целостности приложения" на стр. 63). Администратор может скрыть задачи от пользователя (см. раздел "Управление задачами" на стр. 32) или ограничить управление задачами (см. раздел "Управление задачами" на стр. 32).

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. 34).

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 40
Упрощенный интерфейс приложения 41
Настройка отображения интерфейса приложения 42

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. 42).

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. 273) (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. 276). 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**. Выключает политику 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. 273) (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 276). 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.

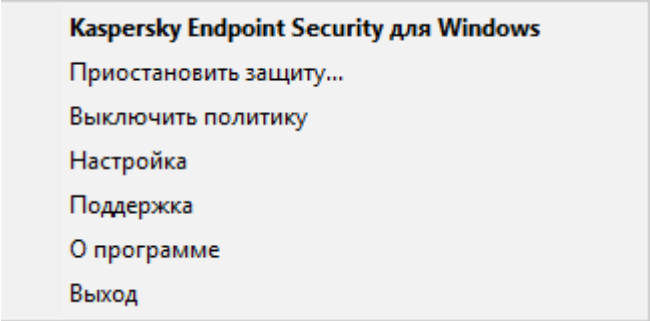


Рисунок 8. Контекстное меню значка программы

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. 42), 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**. Выключает политику 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. 273) (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 276). Для включения политики выберите пункт **Включить политику** в контекстном меню приложения.
- **Задачи**. Раскрывающийся список, содержащий следующие элементы:
  - **Проверка целостности**.
  - **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.

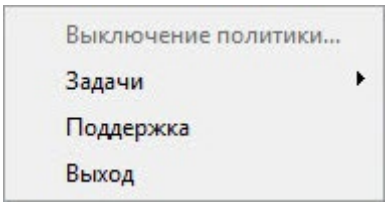


Рисунок 9. Контекстное меню значка программы при отображении упрощенного интерфейса программы

Настройка отображения интерфейса приложения

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

- **С упрощенным интерфейсом**. На клиентском компьютере недоступно главное окно приложения, а доступен только значок в области уведомлений Windows (см. раздел "Значок приложения в области уведомлений" на стр. 40). В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security (см. раздел "Упрощенный интерфейс приложения" на стр. 41). Также Kaspersky Endpoint Security показывает уведомления над значком приложения.
- **С полным интерфейсом**. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows (см. раздел "Значок приложения в области уведомлений" на стр. 40). В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком приложения.
- **Без интерфейса**. 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. 40) и уведомления.

Как настроить отображение интерфейса приложения 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 **Общие настройки** → **Интерфейс**.
5. 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. 40) 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.
6. 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. 41).

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

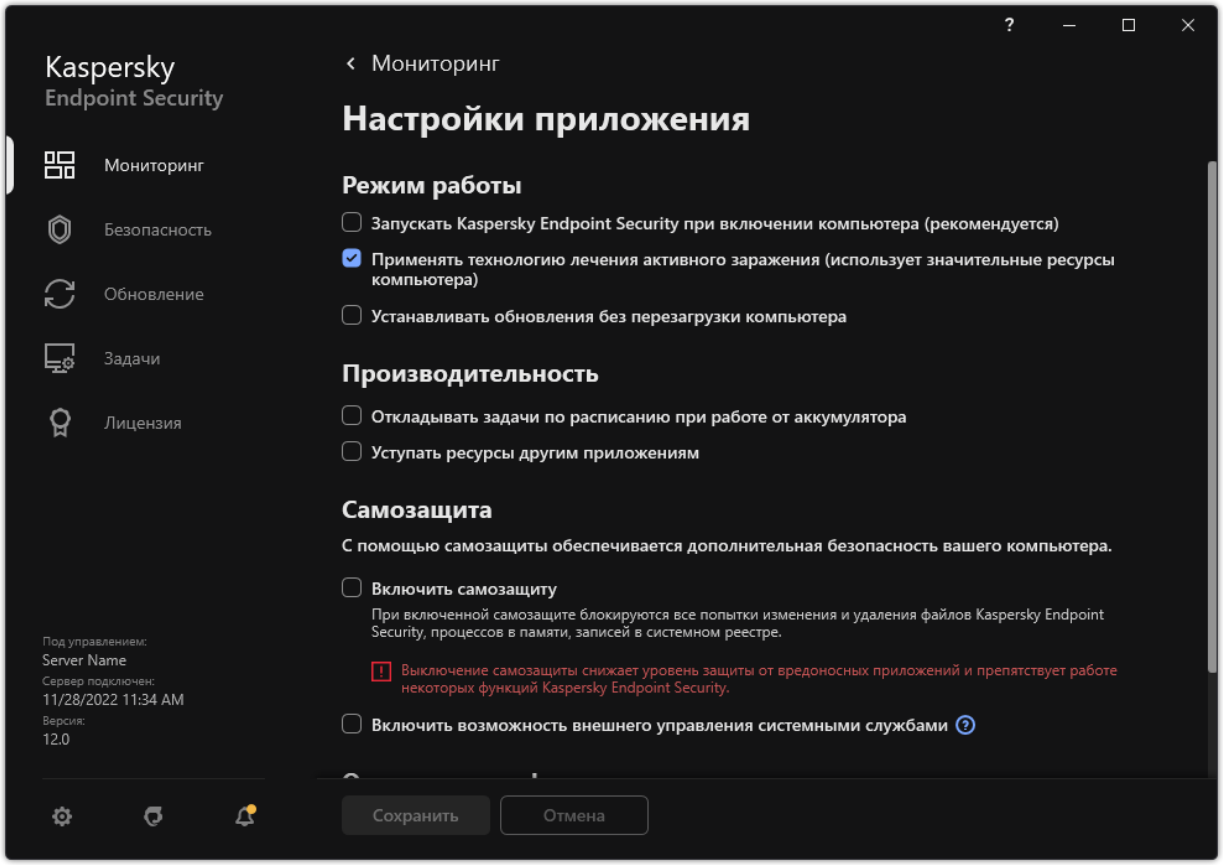


Рисунок 10. Параметры приложения Kaspersky Endpoint Security для Windows

3. С помощью флажка **Запускать Kaspersky Endpoint Security 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. 47) 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 входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, на котором вы хотите запустить или остановить приложение.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.
6. В окне свойств клиентского компьютера выберите раздел **Программы**.

   Справа в окне свойств клиентского компьютера отобразится список приложений "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите приложение Kaspersky Endpoint Security.
8. Выполните следующие действия:
   - 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 .

Как запустить или остановить Kaspersky Endpoint Security через командную строку

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. Для запуска приложения в командной строке введите `klpsm.exe start_avp_service`.
4. Для остановки приложения в командной строке введите `klpsm.exe stop_avp_service`.

Для завершения работы приложения из командной строки необходимо включить внешнее управление системными службами (см. раздел "Защита служб приложения от внешнего управления" на стр. 313).

Рисунок 11. Запуск и завершение работы программы из командной строки

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. 40):

- 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. 276).
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.

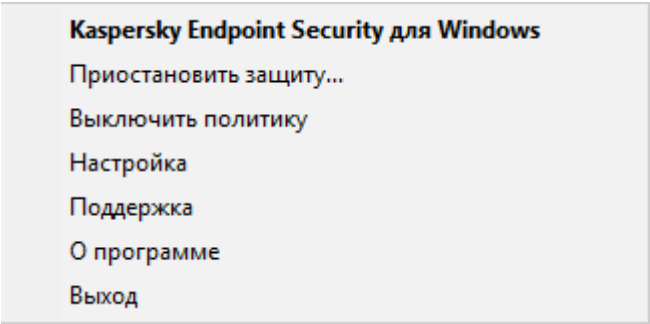


Рисунок 12. Контекстное меню значка программы

► *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.

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. 58). 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;
- почтовый ящик Microsoft Outlook;
- жесткие, съемные и сетевые диски;

- любой выбранный файл.

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

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

В этом разделе

Проверка компьютера 50
Проверка съемных дисков при подключении к компьютеру 56
Фоновая проверка 58
Проверка из контекстного меню 58
Проверка целостности приложения 63
Формирование области проверки 65
Запуск проверки по расписанию 66
Запуск проверки с правами другого пользователя 69
Оптимизация проверки 69

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. 98) 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. 58). 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. 66).

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. 32).

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 дополнительно проверяет файлы почтовых форматов. • **Рекомендуемый**. Приложение Kaspersky Endpoint Security проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты. Приложение не проверяет архивы и установочные пакеты. • **Низкий**. Приложение Kaspersky Endpoint Security проверяет только новые и измененные файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера. Приложение не проверяет составные файлы. 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 все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет. **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 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. 298). 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 "Включение и выключение технологии лечения активного заражения" на стр. 93). 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.
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, почтовые базы, жесткий, съемный или сетевой диск, папка или файл.

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 проверки, как только это станет возможным. Задача проверки может быть пропущена, например, если в установленное время запуска задачи проверки был выключен компьютер. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи проверки, а выполняет следующую задачу проверки по установленному расписанию.
Выполнять только во время простоя компьютера	Отложенный запуск задачи проверки, 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.
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. 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. 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 файлы, если их проверка длится более N секунд	Ограничение длительности проверки одного объекта. По истечении заданного времени приложение прекращает проверку файла. Это позволит сократить время выполнения проверки.
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. 56). • Проверка из контекстного меню (на стр. 58). • Проверка важных областей, запущенная в результате обнаружения индикатора компрометации (IOC). Если флажок снят, Kaspersky Endpoint Security позволяет запускать несколько задач проверки одновременно. Запуск нескольких задач проверки требует больше ресурсов компьютера.

Параметр	Описание
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 сторонних приложений.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Kaspersky Endpoint Security проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
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/Outlook Express, 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. 65). 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.
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. 32).

Таблица 4. Параметры задачи Проверка съемных дисков

Параметр	Описание
Действие при подключении съемного диска	**Подробная проверка**. Если выбран этот элемент, 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. 405), наиболее подверженные заражению, а также не распаковывает составные объекты.
Максимальный размер съемного диска	Если флажок установлен, то Kaspersky Endpoint Security выполняет действие, выбранное в раскрывающемся списке **Действие при подключении съемного диска**, над съемными дисками, размер которых не превышает указанный максимальный размер. Если флажок снят, то Kaspersky Endpoint Security выполняет действие, выбранное в раскрывающемся списке **Действие при подключении съемного диска**, над съемными дисками любого размера.
Отображать ход 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 остановку задачи 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.

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. 50) 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. 32).

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.

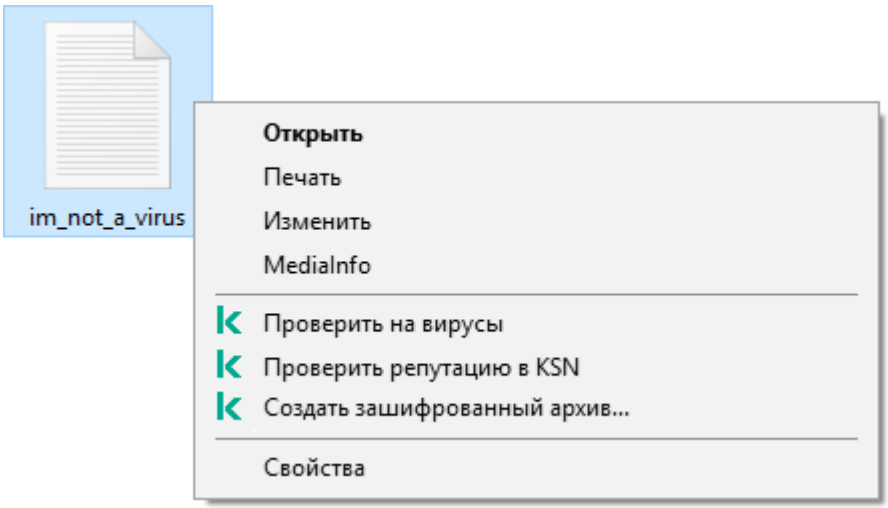


Рисунок 13. Контекстное меню файла

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. 32).

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 дополнительно проверяет файлы почтовых форматов. • **Рекомендуемый**. Приложение Kaspersky Endpoint Security проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты. Приложение не проверяет архивы и установочные пакеты. • **Низкий**. Приложение Kaspersky Endpoint Security проверяет только новые и измененные файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера. Приложение не проверяет составные файлы.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет. **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 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. 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. 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 файлы, если их проверка длится более N секунд	Ограничение длительности проверки одного объекта. По истечении заданного времени приложение прекращает проверку файла. Это позволит сократить время выполнения проверки.
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. Kaspersky Endpoint Security 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/Outlook Express, 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. 65). 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.
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*. Запускайте задачу *Проверка целостности*, если приложение Kaspersky Endpoint Security обнаружило вредоносный объект и не обезвредило его.

Вы можете создать задачу *Проверка целостности* 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 приложения через Консоль администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Сервер администрирования** → **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 (12.3)** → **Проверка целостности**.

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 или при обнаружении вирусной атаки.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Проверка целостности приложения после заражения компьютера*.

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 Kaspersky Endpoint Security выполнит проверку целостности приложения. Вы также можете настроить расписание проверки целостности приложения в свойствах задачи (см. таблицу ниже).

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* 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* не отображается, администратор запретил использование локальных задач в политике (см. раздел "Управление задачами" на стр. 32).

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 проверки, как только это станет возможным. Задача проверки может быть пропущена, например, если в установленное время запуска задачи проверки был выключен компьютер. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи проверки, а выполняет следующую задачу проверки по установленному расписанию.
Выполнять только во время простоя компьютера	Отложенный запуск задачи проверки, 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.

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.

> 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:

- **Моя почта**.

  Файлы, связанные с работой почтового клиента Outlook: файлы данных (PST), автономные файлы данных (OST).

- **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**.

  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. 282)

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. 32).

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.

Параметр	Описание
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу проверки, как только это станет возможным. Задача проверки может быть пропущена, например, если в установленное время запуска задачи проверки был выключен компьютер. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи проверки, а выполняет следующую задачу проверки по установленному расписанию.
Выполнять только во время простоя компьютера	Отложенный запуск задачи проверки, 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.
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.
Остановить задачу, если она выполняется более чем N (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. 65) или оптимизировать проверку (см. раздел "Оптимизация проверки" на стр. 69).
Активировать устройство перед запуском задачи функцией Wake-on-LAN за N (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.

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. 58).

Настроить права пользователя для запуска проверки съемных дисков (см. раздел "Проверка съемных дисков при подключении к компьютеру" на стр. 56), фоновой проверки (см. раздел "Фоновая проверка" на стр. 58) и проверки целостности (см. раздел "Проверка целостности приложения" на стр. 63) 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. 32).

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 проверки** 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 файлы, если их проверка длится более N секунд**. Ограничение длительности проверки одного объекта. По истечении заданного времени приложение прекращает проверку файла. Это позволит сократить время выполнения проверки.
   - **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 проверки одного объекта. По истечении заданного времени приложение прекращает проверку файла. Это позволит сократить время выполнения проверки.

   > 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. 32).

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.

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. 303).

В этом разделе

Схема обновления с серверного хранилища 73

Запуск и остановка задачи обновления 76

Запуск задачи обновления с правами другого пользователя 76

Выбор режима запуска для задачи обновления 78

Добавление источника обновлений 79

Обновление модулей приложения 82

Использование прокси-сервера при обновлении 83

Откат последнего обновления 87

Обновление антивирусных баз в ручном режиме 89

Устранение уязвимостей и установка критических обновлений в приложении 90

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-, HTTP-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.

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/14.2/ru-RU/180697.htm.

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

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

Настроить групповую задачу *Обновление* 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. 32).

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

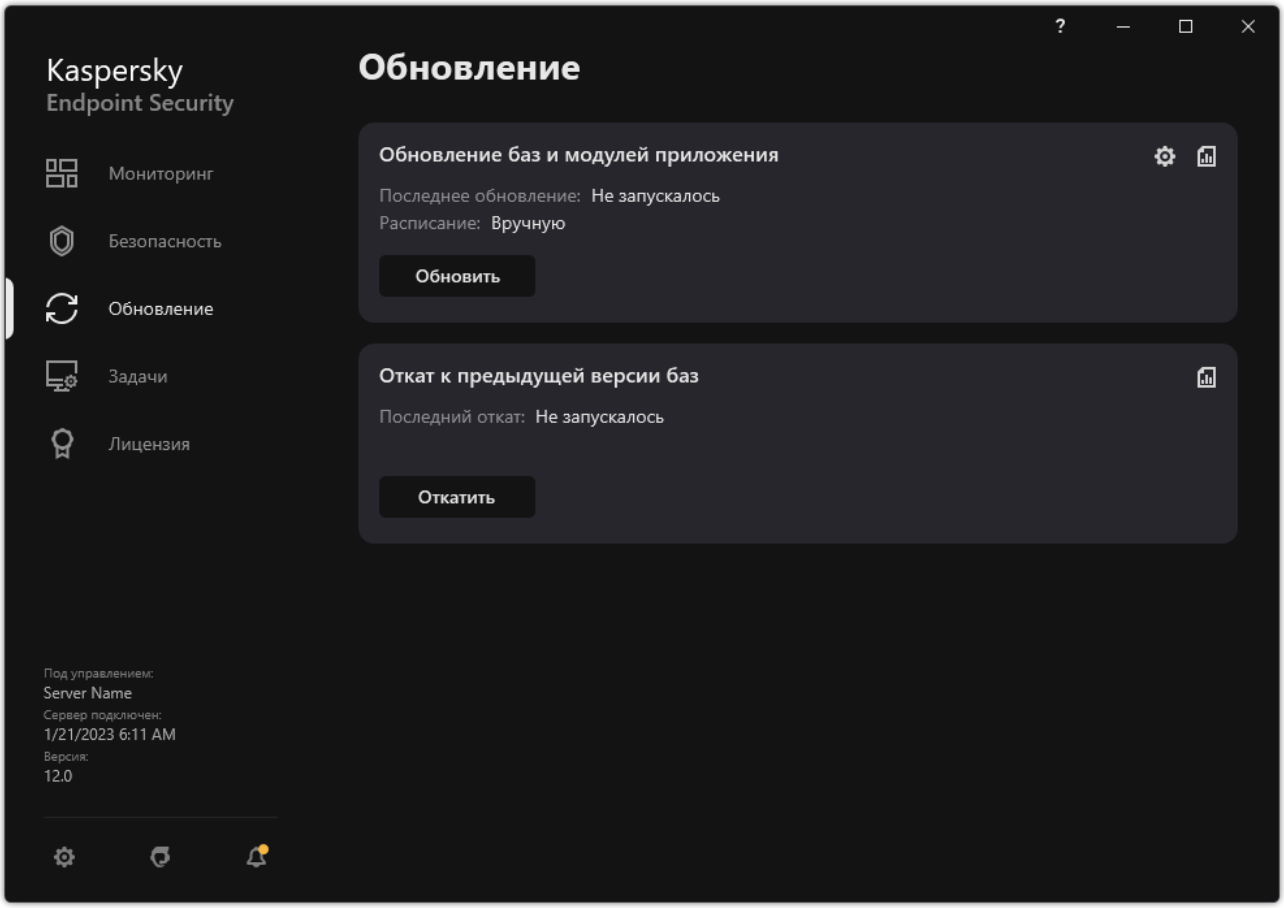


Рисунок 14. Локальные задачи обновления

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**.

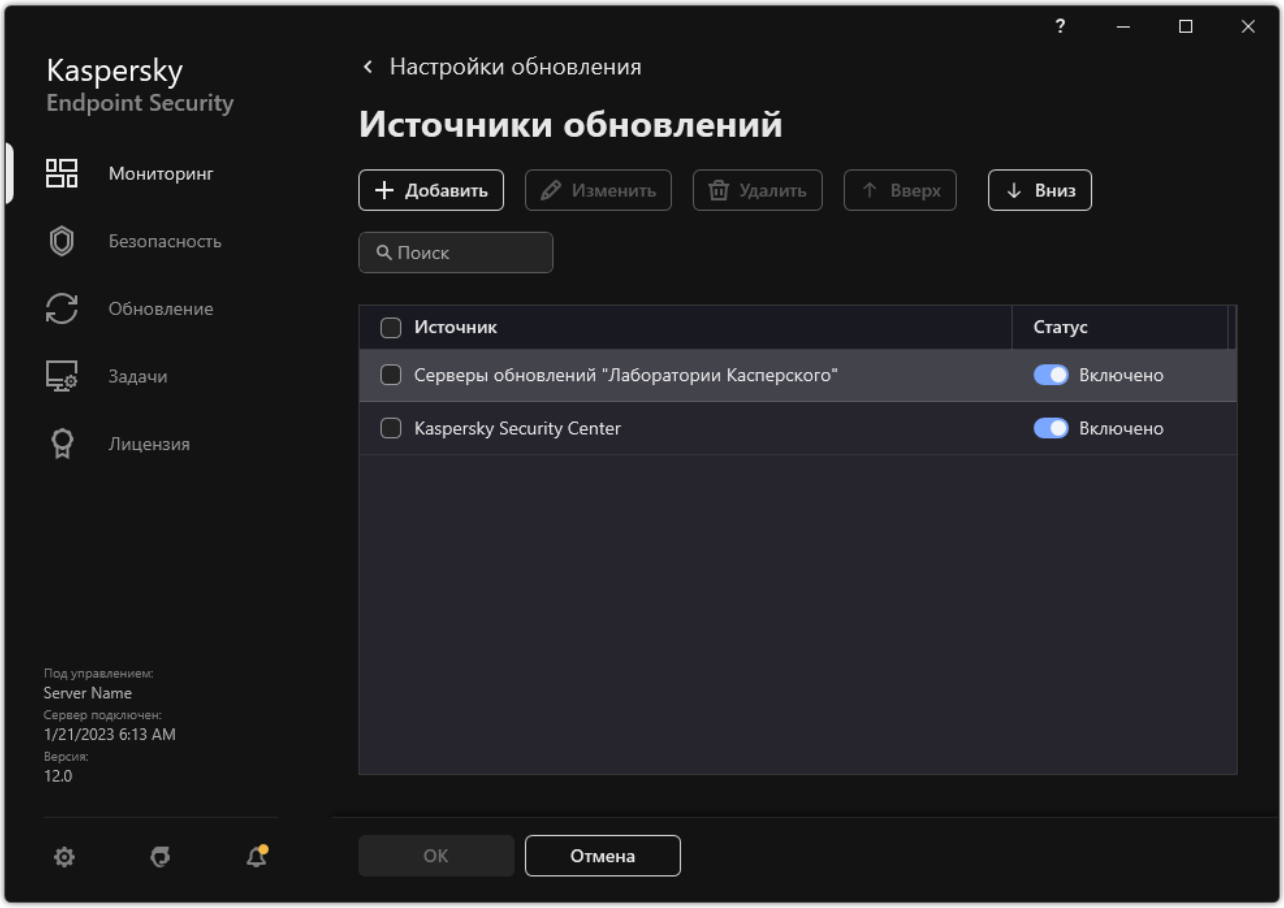


Рисунок 15. Источники обновлений

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.

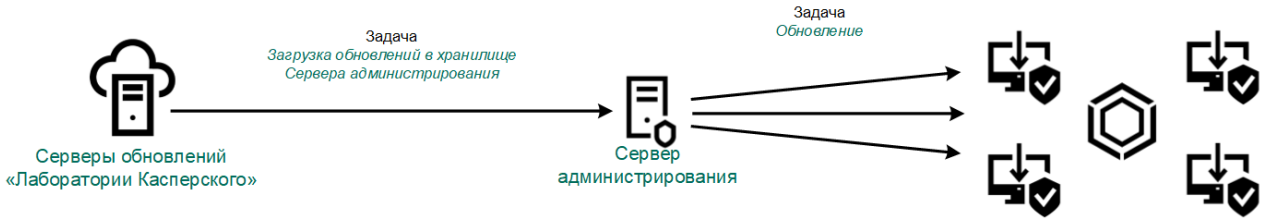


Рисунок 16. Обновление с серверного хранилища

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.

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:*

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

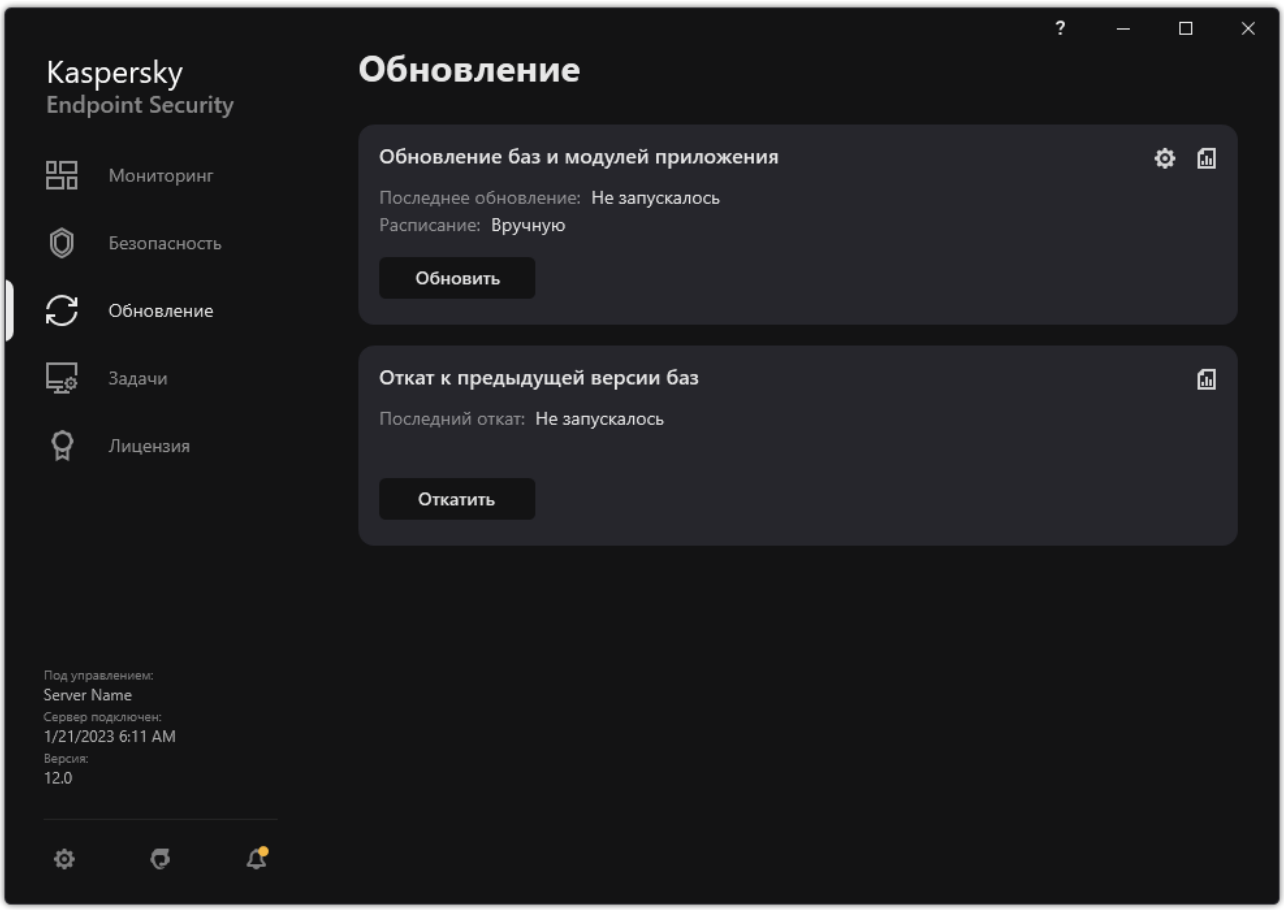


Рисунок 17. Локальные задачи обновления

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:*

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

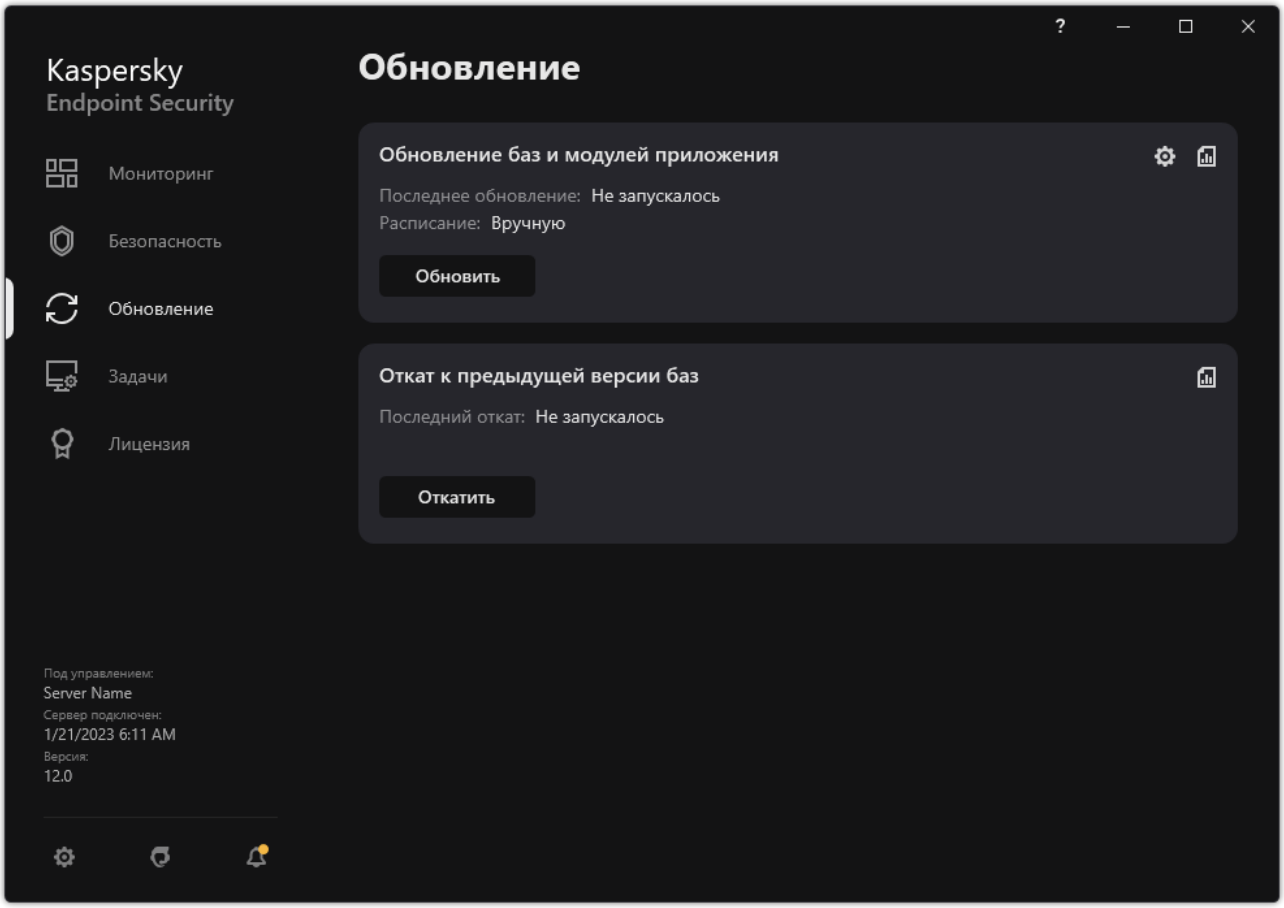


Рисунок 18. Локальные задачи обновления

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.
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* выбраны серверы "Лаборатории Касперского" в качестве первого источника обновления, так как у приложения может отсутствовать доступ к серверу Kaspersky Security Center.

Как добавить источник обновлений в интерфейсе приложения

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

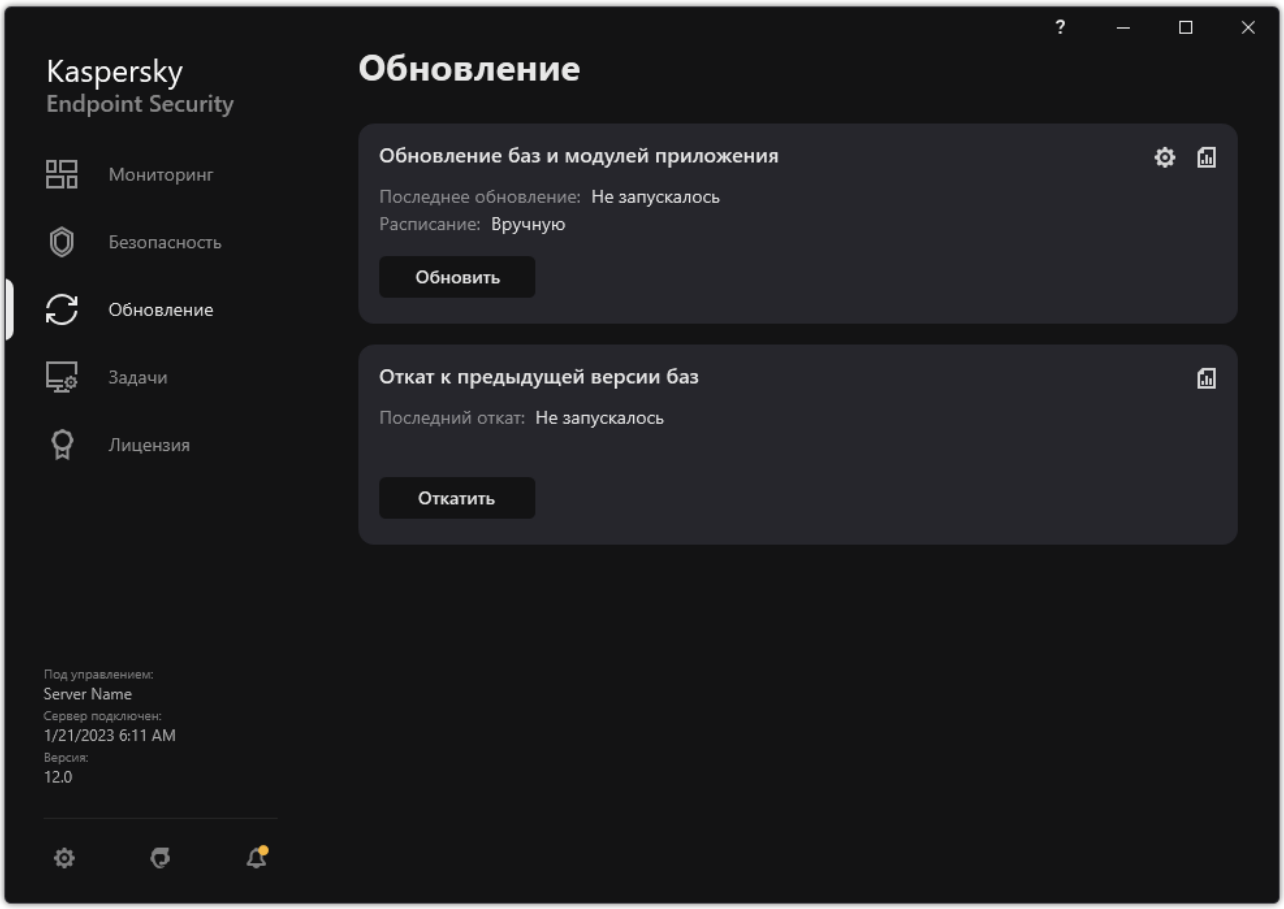


Рисунок 19. Локальные задачи обновления

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**.

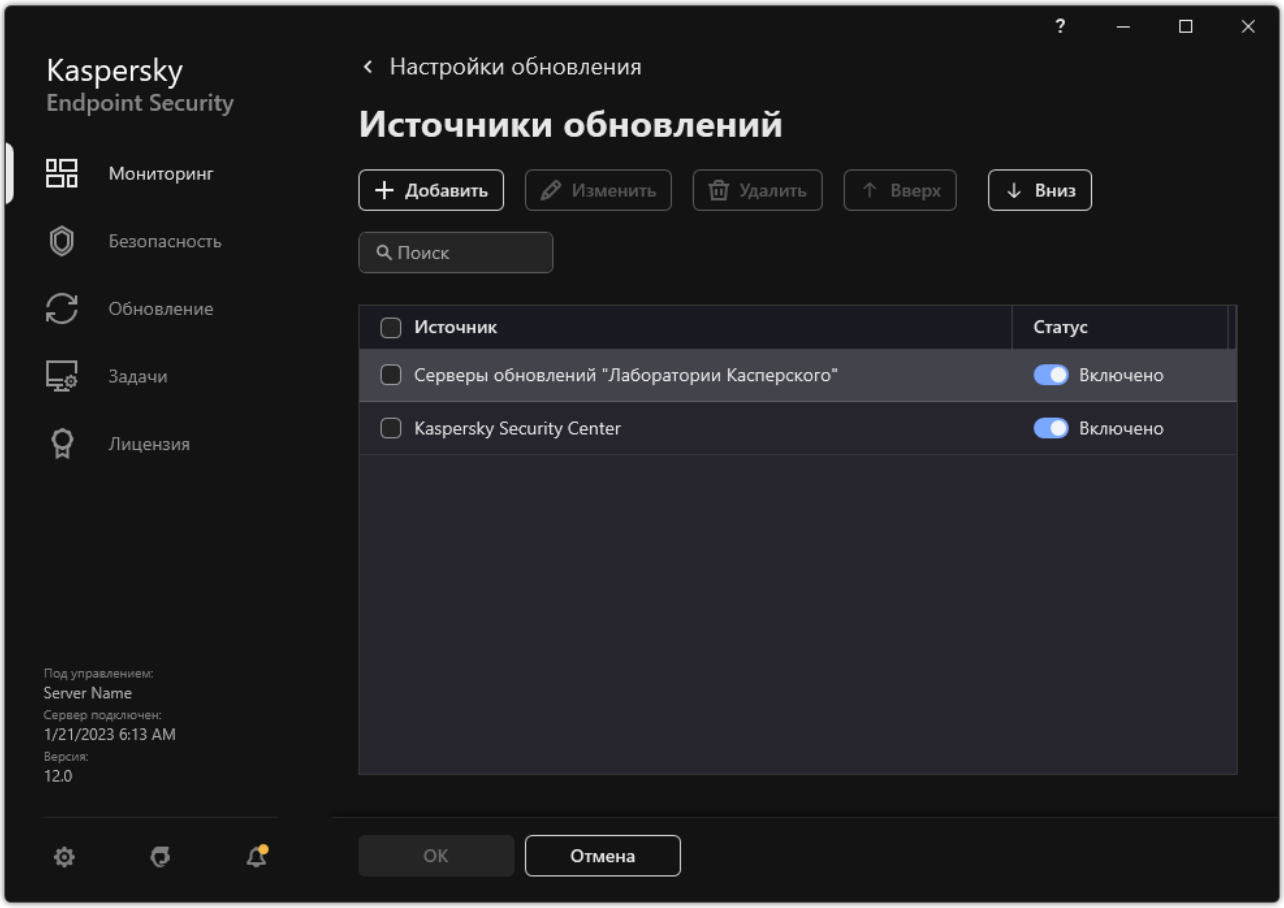


Рисунок 20. Источники обновлений

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://<имя пользователя>:<пароль>@<узел>:<порт>`.

   - 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\AVP11\Update distribution\`.

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

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. Подробнее об отслеживании обновлений модулей приложения и подтверждении обновления в Kaspersky Security Center см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/14.2/ru-RU/index.htm.

После установки обновления приложения может потребоваться перезагрузка компьютера.

► *Чтобы настроить обновление модулей приложения, выполните следующие действия:*

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

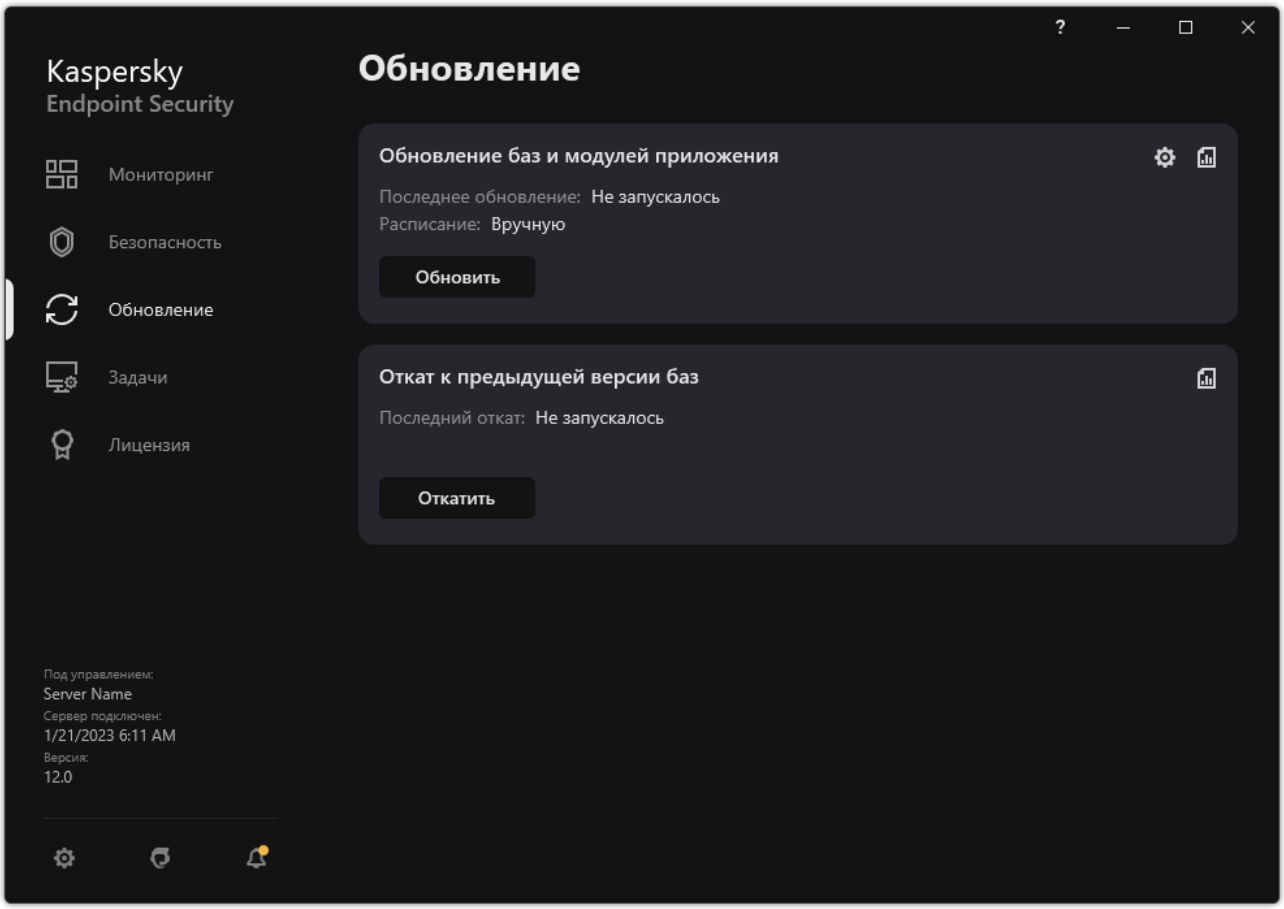


Рисунок 21. Локальные задачи обновления

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

   Откроется окно свойств задачи.

3. В 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** и нажмите на плитку **Настройки сети**.

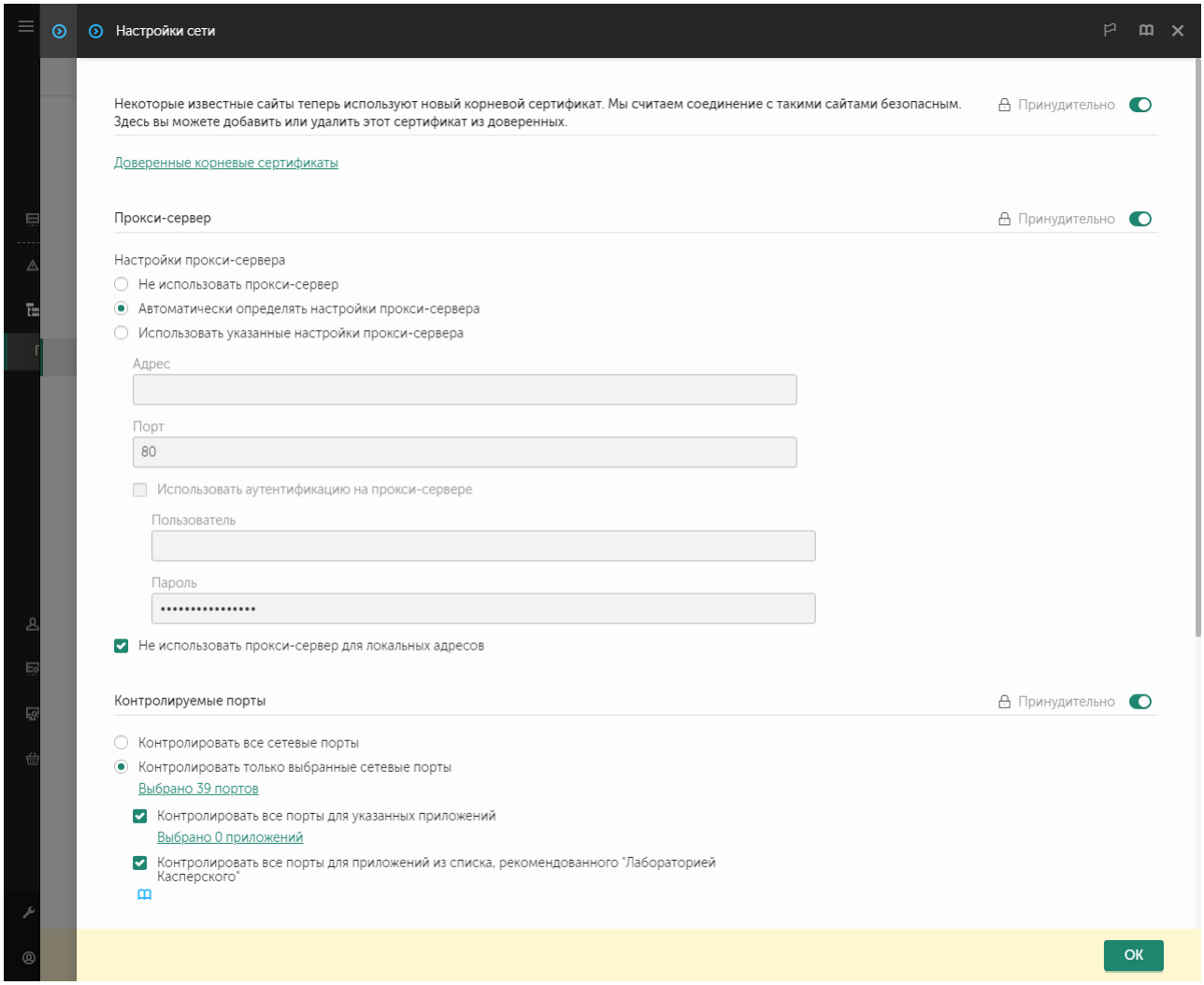


Рисунок 22. Параметры сети приложения Kaspersky Endpoint Security для Windows

5. В блоке **Настройки прокси-сервера** выберите вариант **Не использовать прокси-сервер для локальных адресов**.
6. 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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

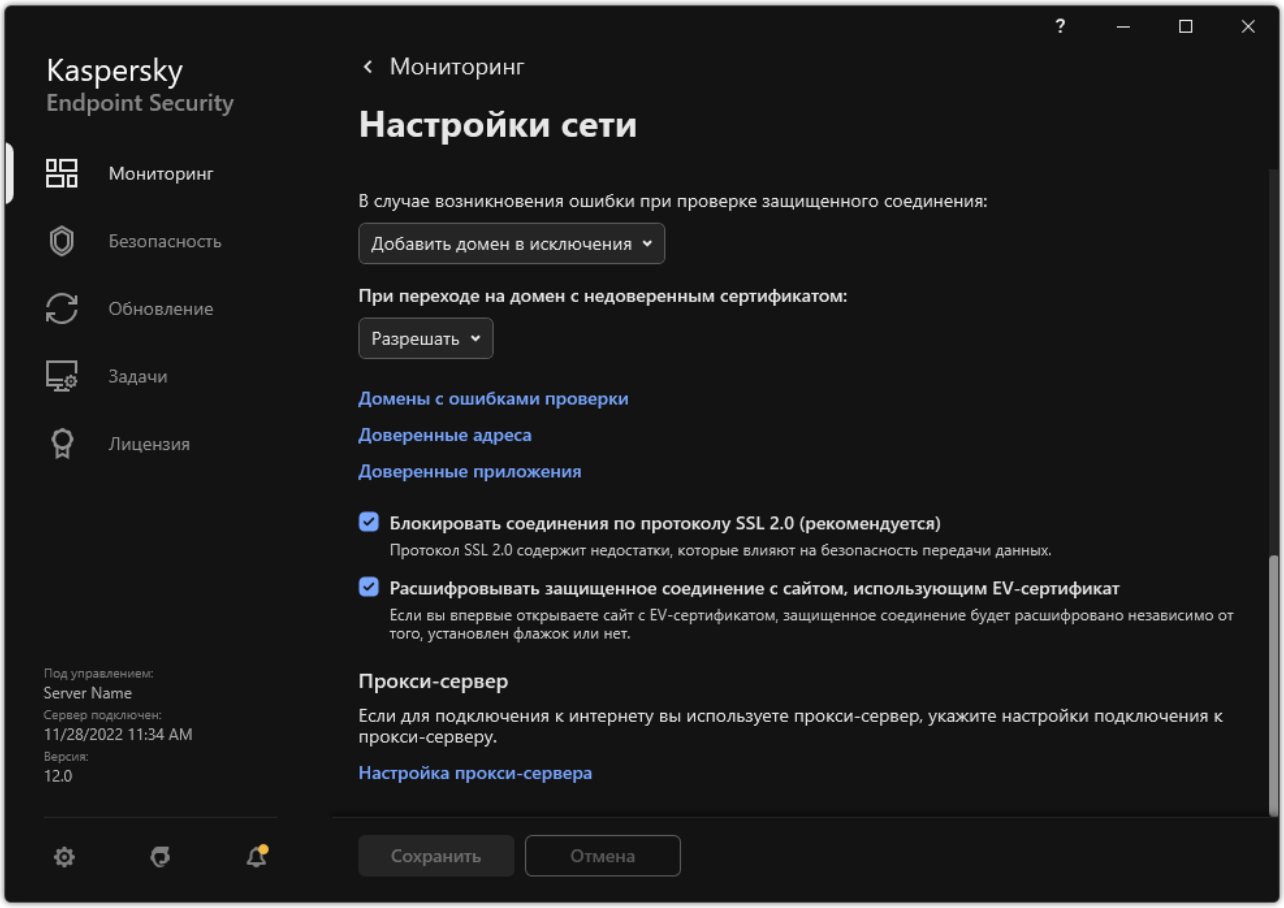


Рисунок 23. Параметры сети приложения

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

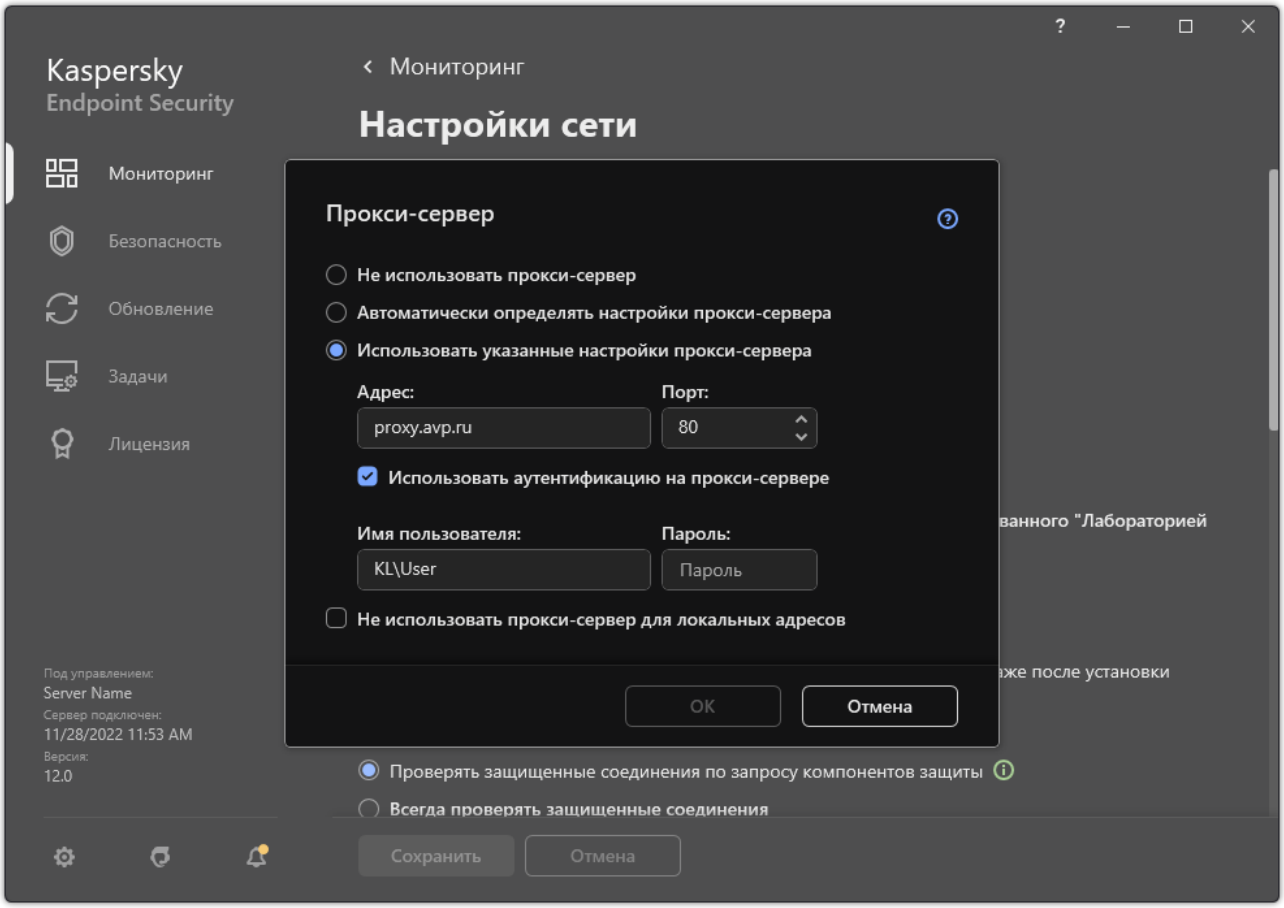


Рисунок 24. Параметры подключения к прокси-серверу

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

     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. Если вы хотите включить использование аутентификации на прокси-сервере, установите флажок **Использовать аутентификацию на прокси-сервере** и укажите учетные данные 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.

► *Чтобы откатить последнее обновление, выполните следующие действия:*

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

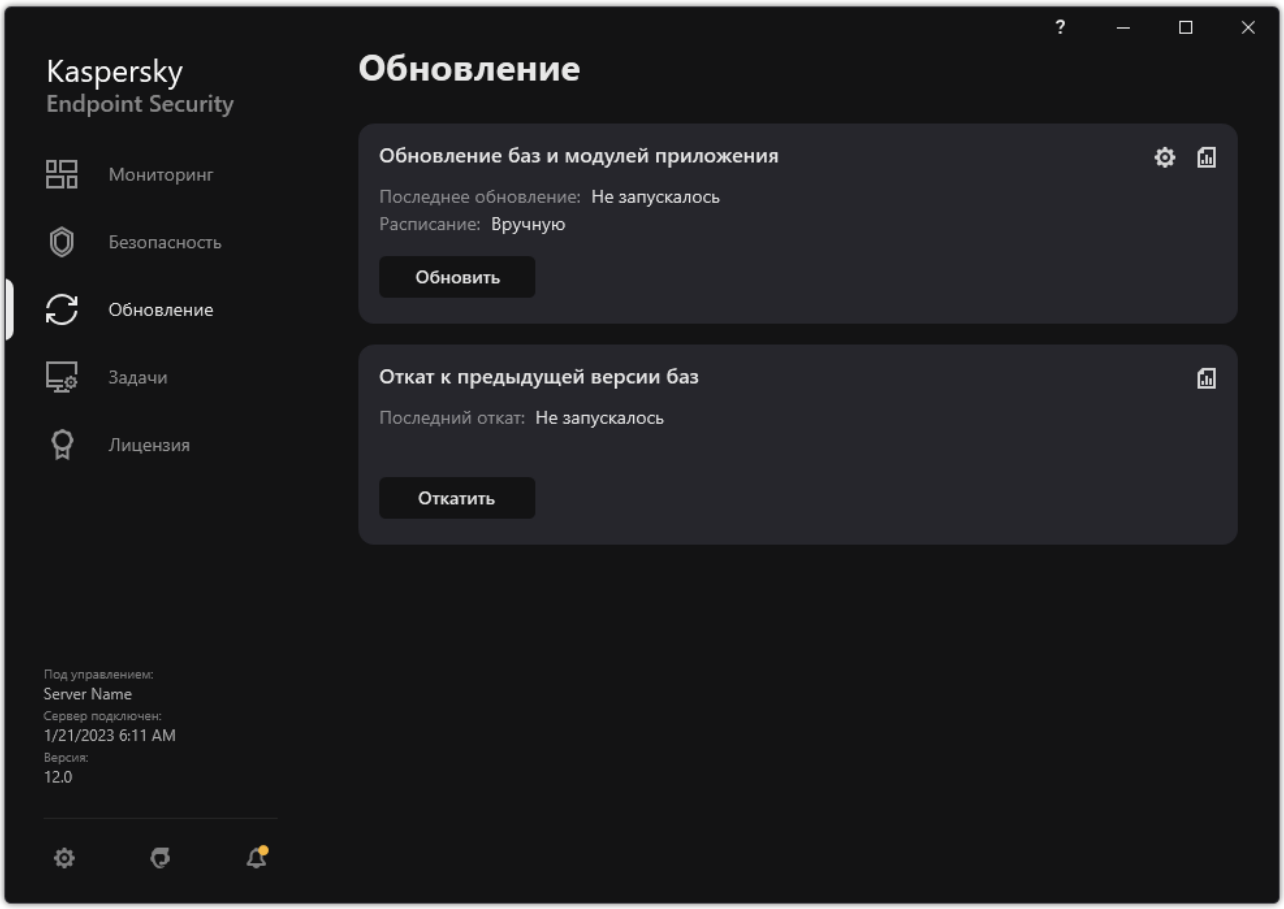


Рисунок 25. Локальные задачи обновления

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**.

► *Чтобы запустить или остановить задачу отката 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 отката обновления, чтобы запустить ее.
   - Выберите запущенную задачу отката обновления, чтобы остановить ее.
   - Выберите остановленную задачу отката обновления, чтобы возобновить ее или запустить ее заново.

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.

Если вам недоступны серверы обновлений "Лаборатории Касперского" (например, нет доступа к интернету), обратитесь в Службу технической поддержки "Лаборатории Касперского" для получения обновлений приложения на дисках.

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.

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:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

Работа с активными угрозами

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). Для работы с активными угрозами Kaspersky Endpoint Security использует технологию лечения активного заражения (см. раздел "Включение и выключение технологии лечения активного заражения" на стр. 93). 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. 50) и в параметрах приложения (см. раздел "Включение и выключение технологии лечения активного заражения" на стр. 93).

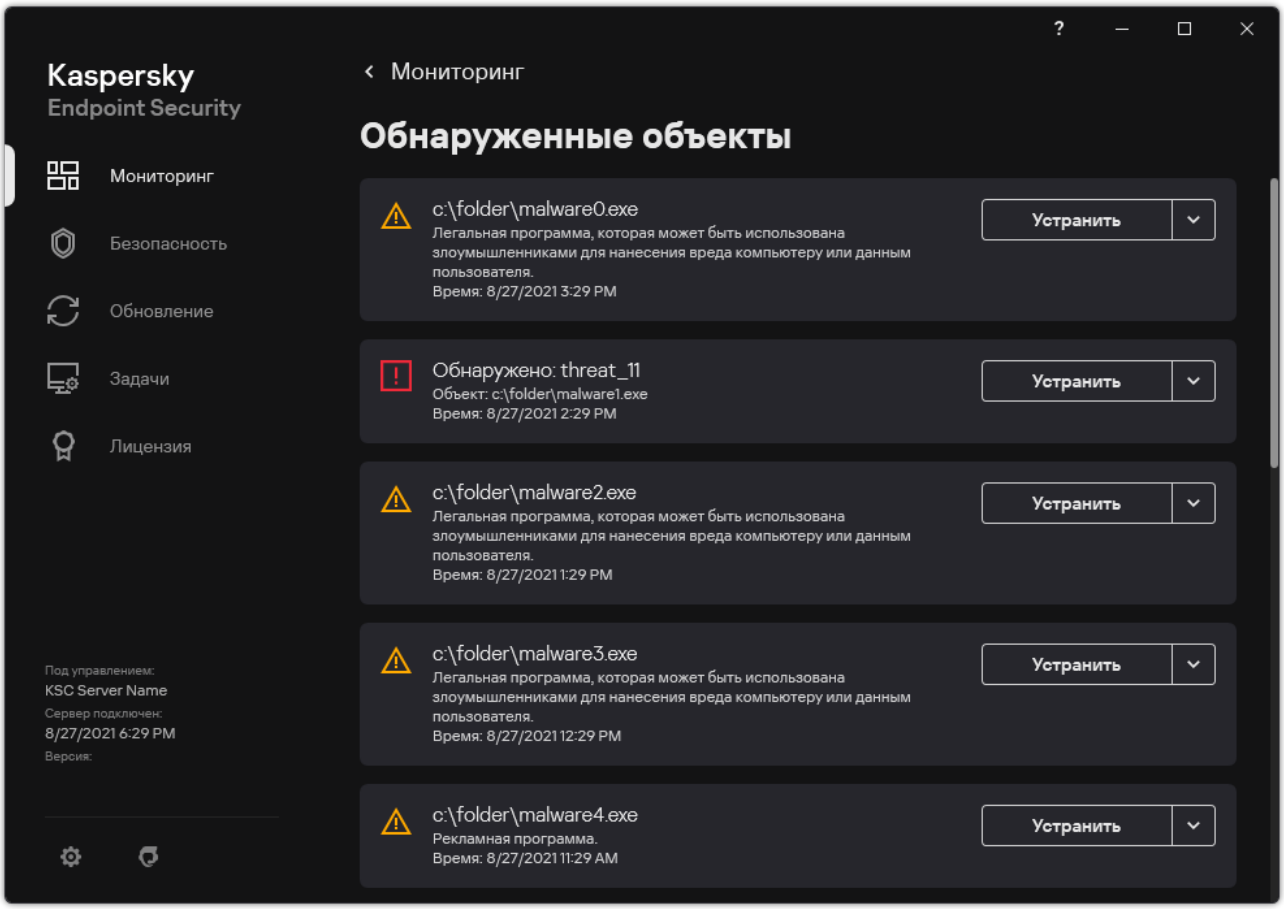


Рисунок 26. Список активных угроз

В этом разделе

Лечение активных угроз на рабочих станциях 92

Лечение активных угроз на серверах 93

Включение и выключение технологии лечения активного заражения 93

Обработка активных угроз 94

Лечение активных угроз на рабочих станциях

Для работы с активными угрозами на рабочих станциях вам нужно включить технологию лечения активного заражения (см. раздел "Включение и выключение технологии лечения активного заражения" на стр. 93) в параметрах приложения. Далее вам нужно настроить взаимодействие приложения с пользователем в свойствах задачи *Поиск вредоносного ПО* (см. раздел "*Проверка компьютера*" на стр. 50). 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 "Включение и выключение технологии лечения активного заражения" на стр. 93).

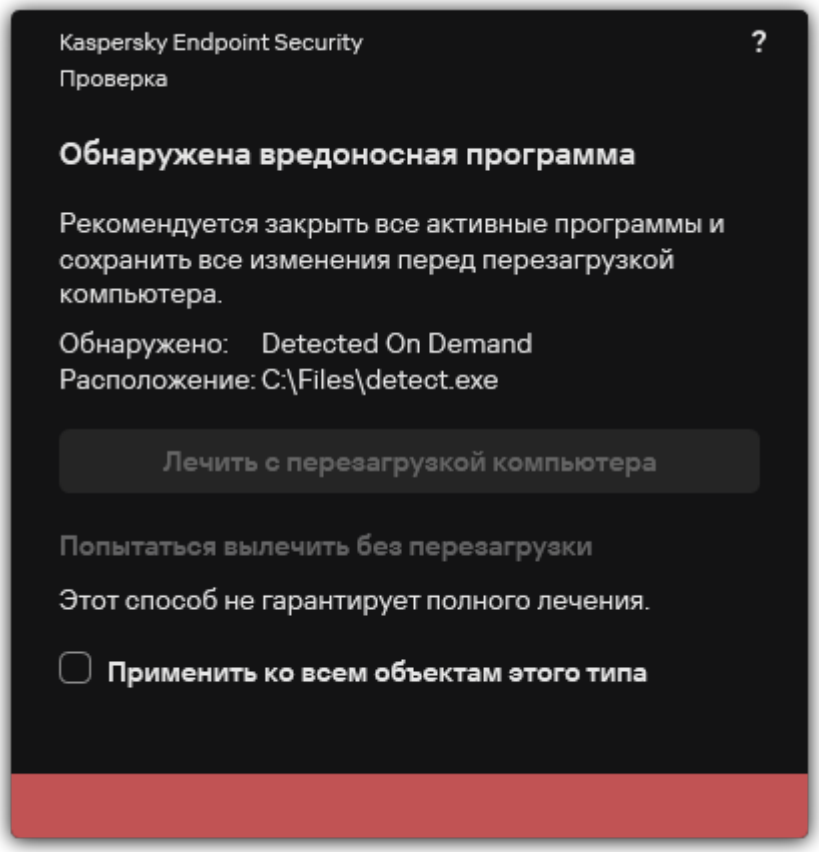


Рисунок 27. Уведомление об активной угрозе

Лечение активных угроз на серверах

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

- включите технологию лечения активного заражения (см. раздел "Включение и выключение технологии лечения активного заражения" на стр. 93) в параметрах приложения;
- включите немедленное лечение активного заражения (см. раздел "Проверка компьютера" на стр. 50) 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 "Включение и выключение технологии лечения активного заражения" на стр. 93) в параметрах приложения и включить немедленное лечение активного заражения (см. раздел "Проверка компьютера" на стр. 50) в свойствах задачи *Поиск вредоносного ПО*. Далее вам нужно запустить задачу *Поиск вредоносного ПО*.

Включение и выключение технологии лечения активного заражения

Если Kaspersky Endpoint Security не может остановить выполнение вредоносного приложения, вы можете использовать технологию лечения активного заражения. По умолчанию технология лечения активного заражения выключена, так как технология использует значительные ресурсы компьютера. Таким образом, вы можете включать технологию лечения активного заражения только при работе с активными угрозами (см. раздел "Работа с активными угрозами" на стр. 91).

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. 50) 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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

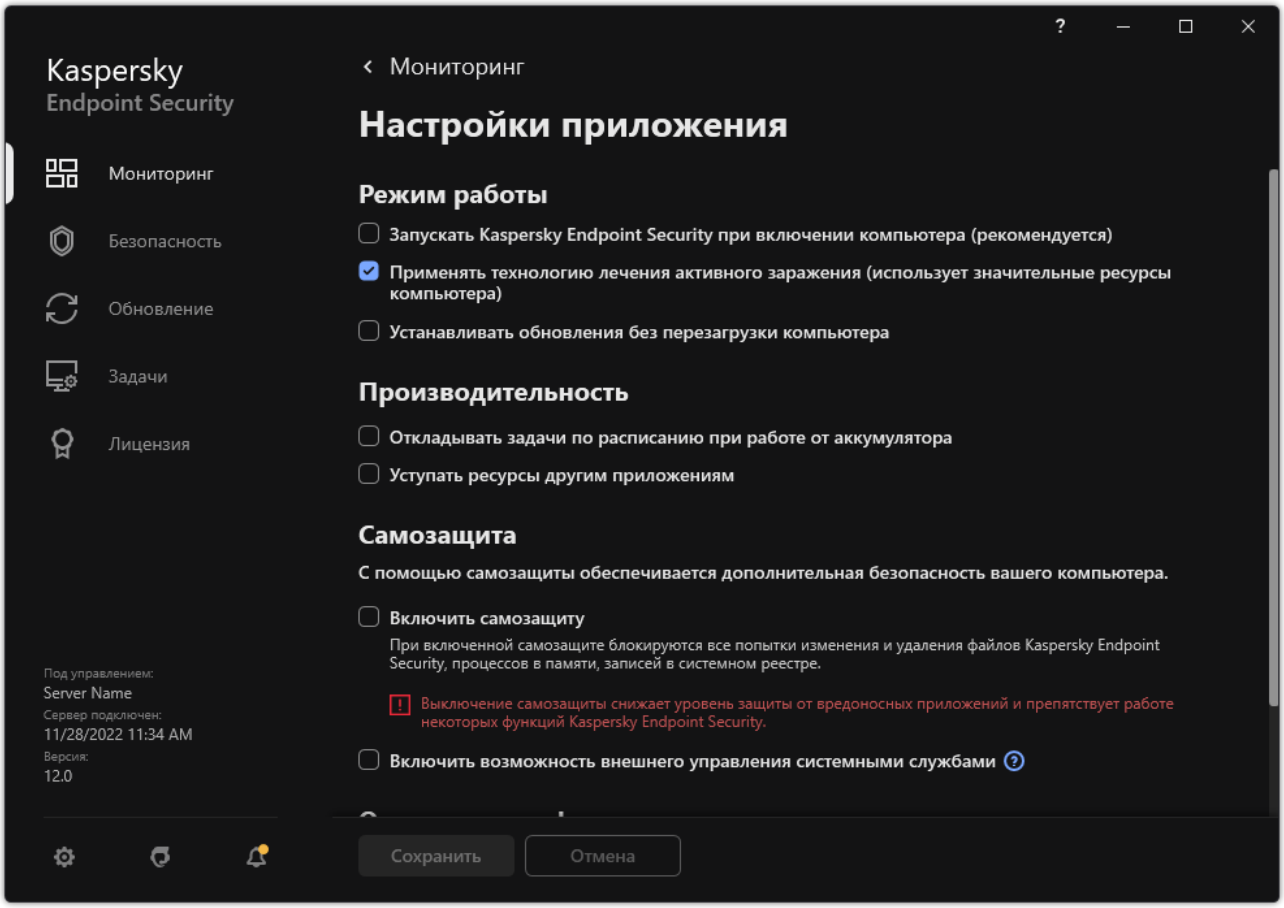


Рисунок 28. Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Режим работы** 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.

Обработка 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. 50) 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 устранить.
3. Выберите способ устранения угрозы:
   - **Устранить**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет.
   - **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. 282). 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 Вирусной энциклопедии "Лаборатории Касперского" https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/.

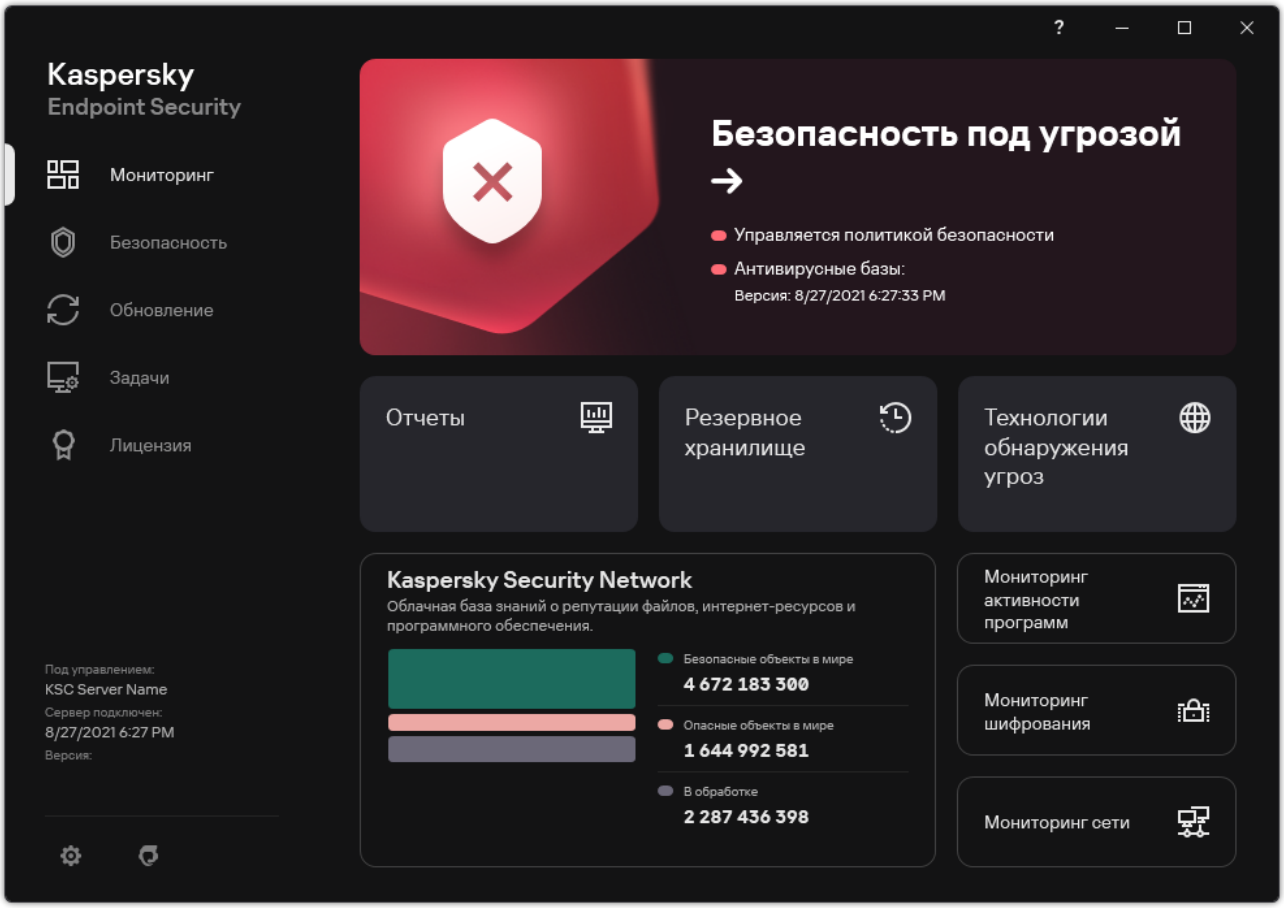


Рисунок 29. Главное окно приложения при обнаружении угрозы

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 98

Ограничения работы с Локальным KSN 99

Включение и выключение облачного режима для компонентов защиты 99

Настройка KSN Proxy 100

Проверка репутации файла в Kaspersky Security Network 101

Включение и выключение использования Kaspersky Security Network

► *Чтобы включить или выключить использование Kaspersky Security Network, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

   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.
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 приложение "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. 282)). 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. 138).

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".

При использовании Kaspersky Private Security Network функциональность облачного режима доступна начиная с версии Kaspersky Private Security Network 3.0.

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

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

Настройка KSN Proxy

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 связи с внешней сетью и ускоряя получение компьютером пользователя запрошенной информации.

По умолчанию после включения использования KSN и принятия Положения об использовании KSN приложение использует прокси-сервер для связи с Kaspersky Security Network. В качестве прокси-сервера приложение использует Сервер администрирования Kaspersky Security Center и TCP-порт 13111. Таким образом, если KSN Proxy недоступен, вам нужно проверить следующие параметры:

- На Сервере администрирования запущена служба *ksnproxy*.
- На компьютере Сетевой экран не блокирует порт 13111.

Вы можете настроить использование KSN Proxy: включить или включить KSN Proxy, настроить порт для соединения. Для этого вам нужно открыть свойства Сервера администрирования. Подробнее о настройке KSN Proxy см. в справке Kaspersky Security Center. Также вы можете включить или выключить KSN Proxy для отдельных компьютеров в политике Kaspersky Endpoint Security.

Как включить или выключить KSN Proxy 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 **Продвинутая защита** → **Kaspersky Security Network**.
5. В блоке **Настройки KSN Proxy** используйте флажок **Использовать Сервер администрирования как прокси-сервер KSN**, чтобы включить или выключить KSN Proxy.
6. Если требуется, установите флажок **Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен**.

   Если флажок установлен, Kaspersky Endpoint Security использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как в "Лаборатории Касперского", так и на сторонних серверах, в случае использования Kaspersky Private Security Network.
7. Сохраните внесенные изменения.

Адрес KSN Proxy совпадает с адресом Сервера администрирования. При изменении доменного имени Сервера администрирования необходимо обновить адрес KSN Proxy вручную.

► *Чтобы настроить адрес KSN Proxy, выполните следующие действия:*

1. В Консоли администрирования перейдите в папку **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Свойства**.
3. В открывшемся окне укажите новый адрес прокси-сервера KSN на закладке **Общие**.
4. Сохраните внесенные изменения.

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. 98).

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

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

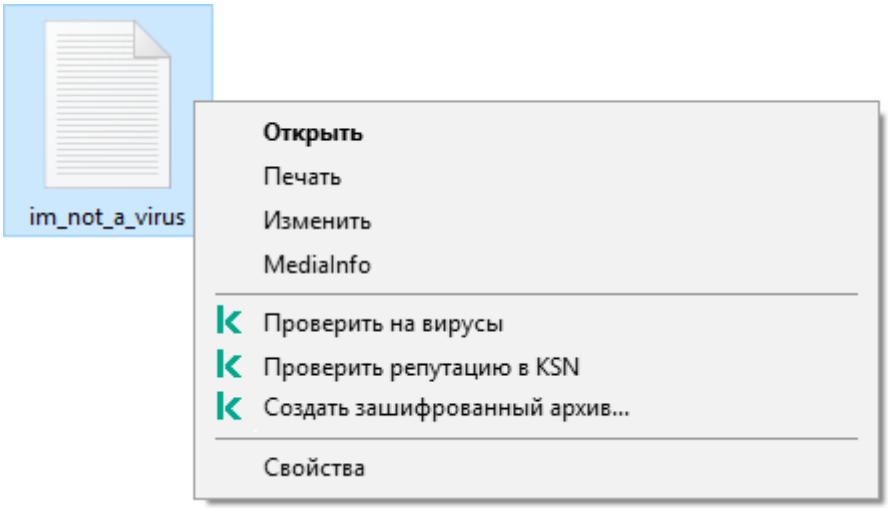


Рисунок 30. Контекстное меню файла

Kaspersky Endpoint Security отображает репутацию файла:

Доверенная (Kaspersky Security Network). Большинство пользователей Kaspersky Security Network подтвердили, что файл доверенный.

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. 287).

Недоверенная (Kaspersky Security Network). Вирус или другое приложение, представляющее угрозу (см. раздел "Работа с активными угрозами" на стр. 91).

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).

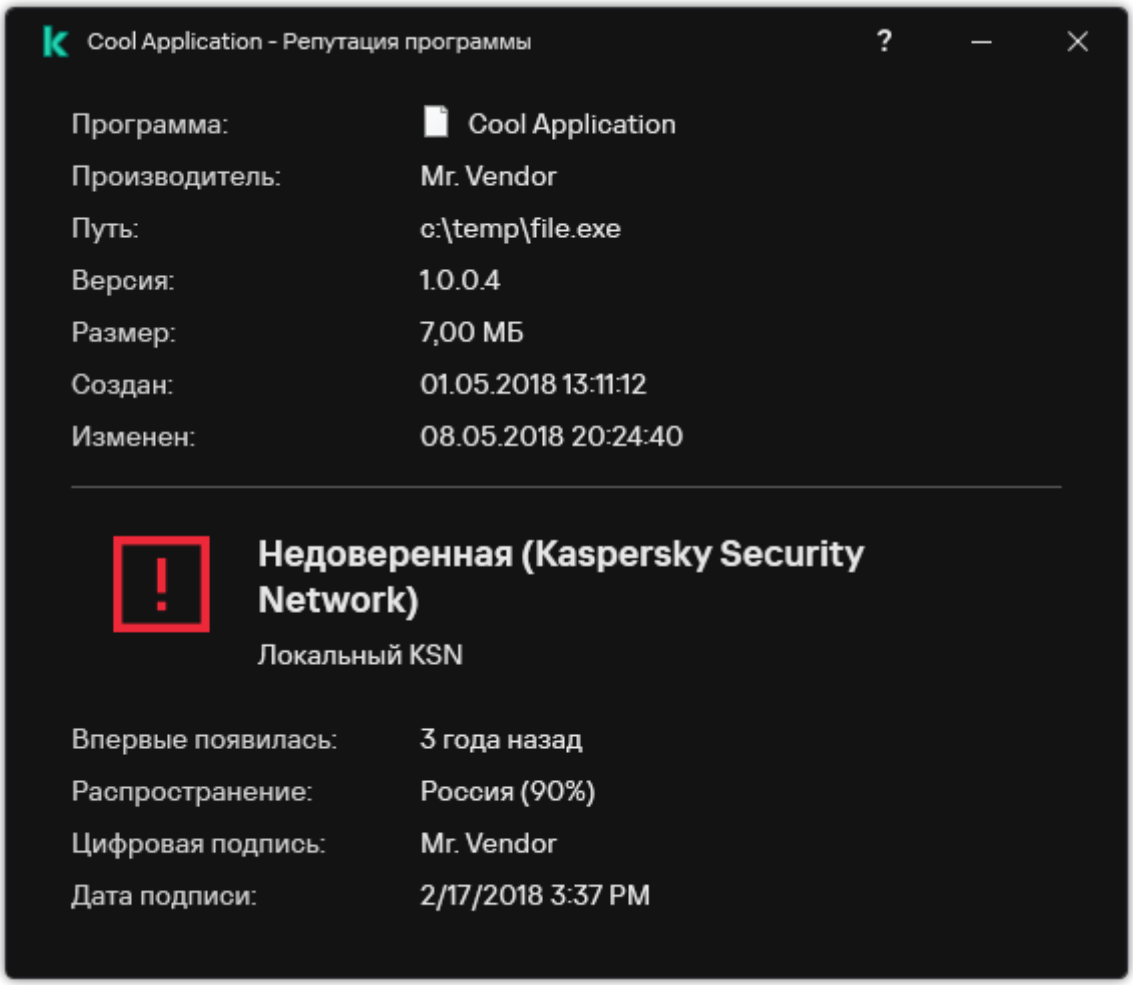


Рисунок 31. Репутация файла в Kaspersky Security Network

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. Если активность приложения совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

В этом разделе

Включение и выключение Анализа поведения 104

Выбор действия при обнаружении вредоносной активности приложения 106

Защита папок общего доступа от внешнего шифрования 107

Включение и выключение Анализа поведения

По умолчанию Анализ поведения включен и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Анализ поведения при необходимости.

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.

► *Чтобы включить или выключить Анализ поведения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Анализ поведения**.

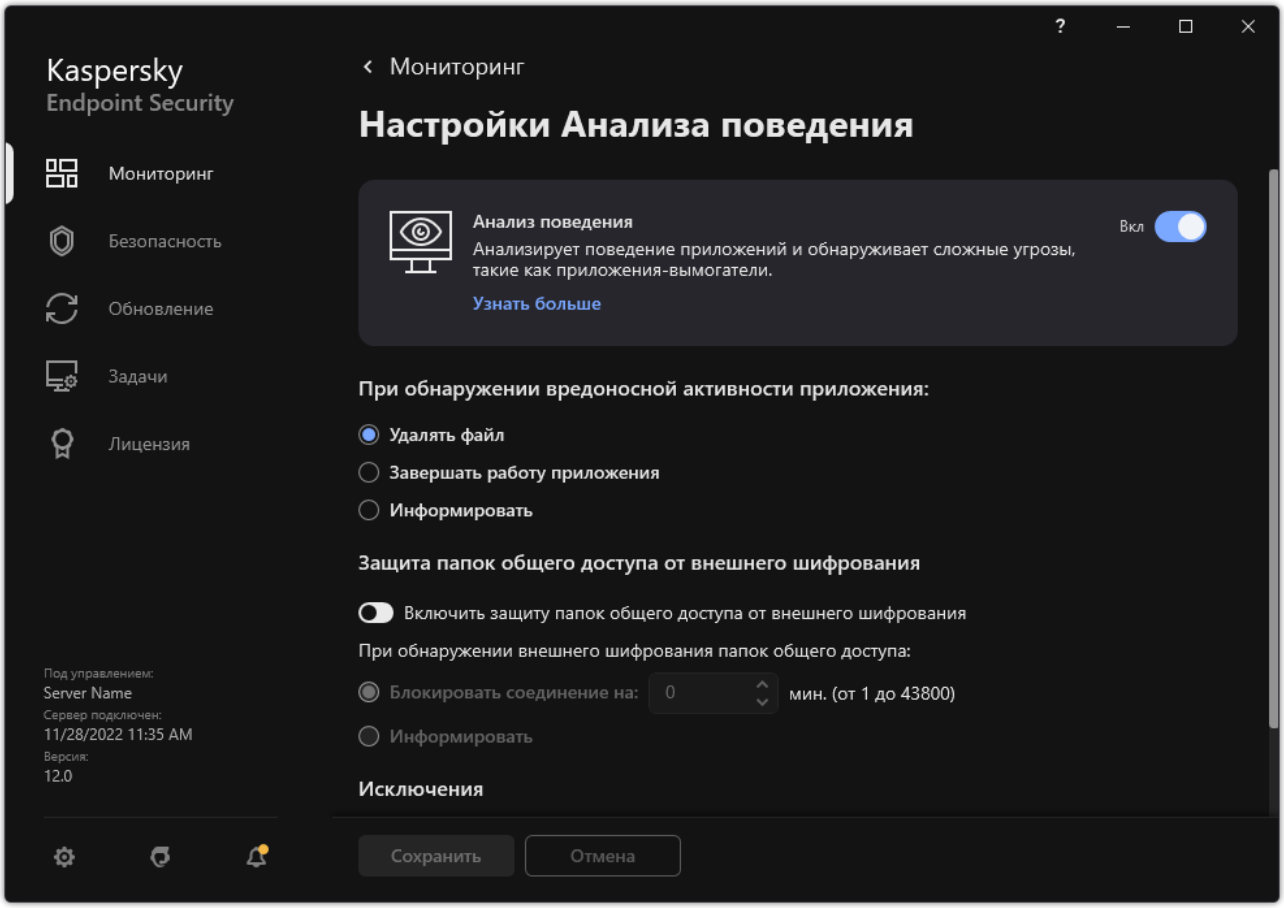


Рисунок 32. Параметры Анализа поведения

3. Используйте переключатель **Анализ поведения**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

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

Выбор действия при обнаружении вредоносной активности приложения

► *Чтобы выбрать действие при обнаружении вредоносной активности приложения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Анализ поведения**.

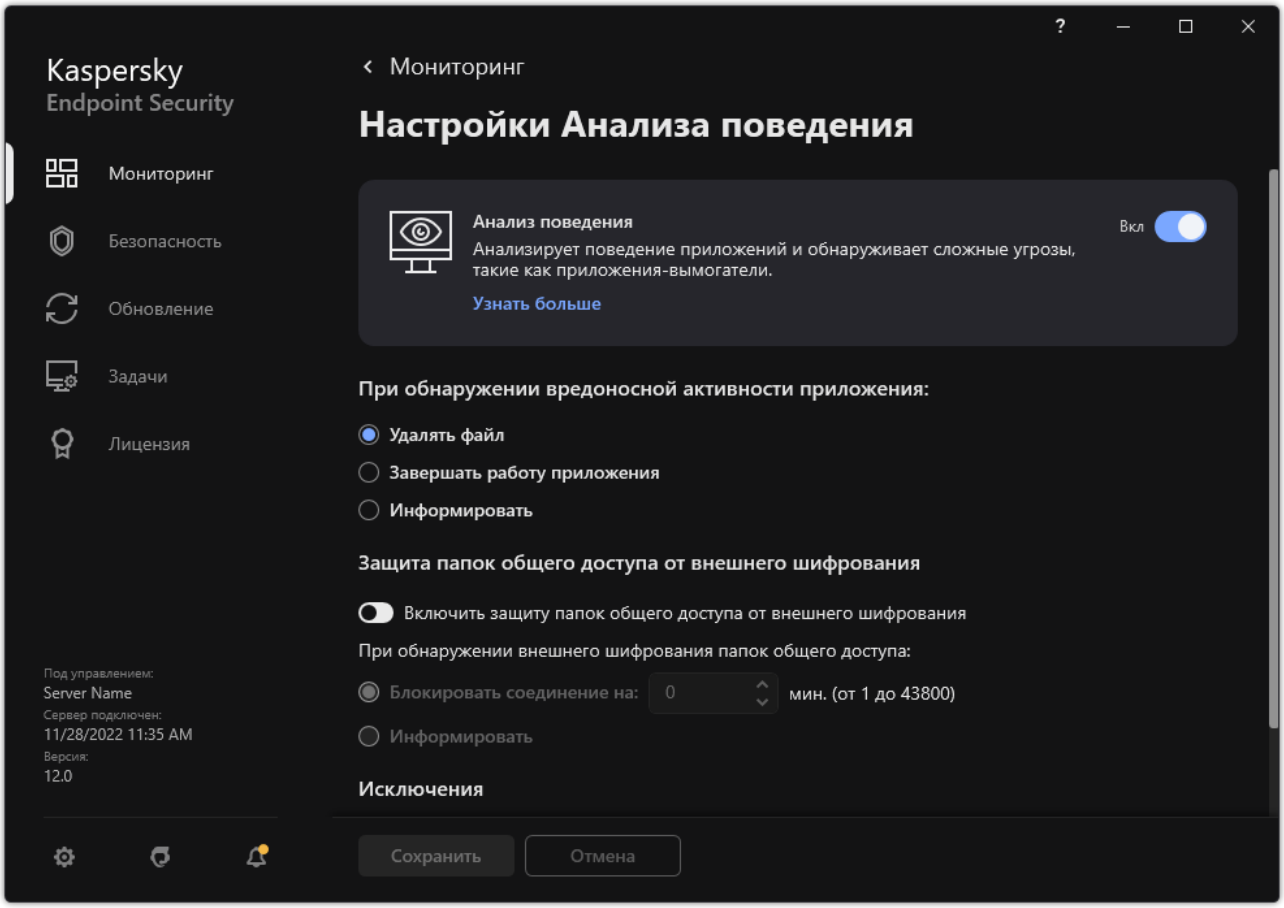


Рисунок 33. Параметры Анализа поведения

3. В блоке **Действие при обнаружении вредоносной активности** выберите нужное действие:
   - **Удалять файл**. 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.

4. Сохраните внесенные изменения.

Защита папок общего доступа от внешнего шифрования

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

Функция защиты папок общего доступа от внешнего 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.

По умолчанию защита папок общего доступа от внешнего шифрования выключена.

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

В этом разделе

Включение и выключение защиты папок общего доступа от внешнего шифрования 107
Выбор действия при обнаружении внешнего шифрования папок общего доступа 109
Создание исключения для защиты папок общего доступа от внешнего шифрования 111
Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования 112

Включение и выключение защиты папок общего доступа от внешнего шифрования

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

► *Чтобы включить или выключить защиту папок общего доступа от внешнего шифрования, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Анализ**

поведения.

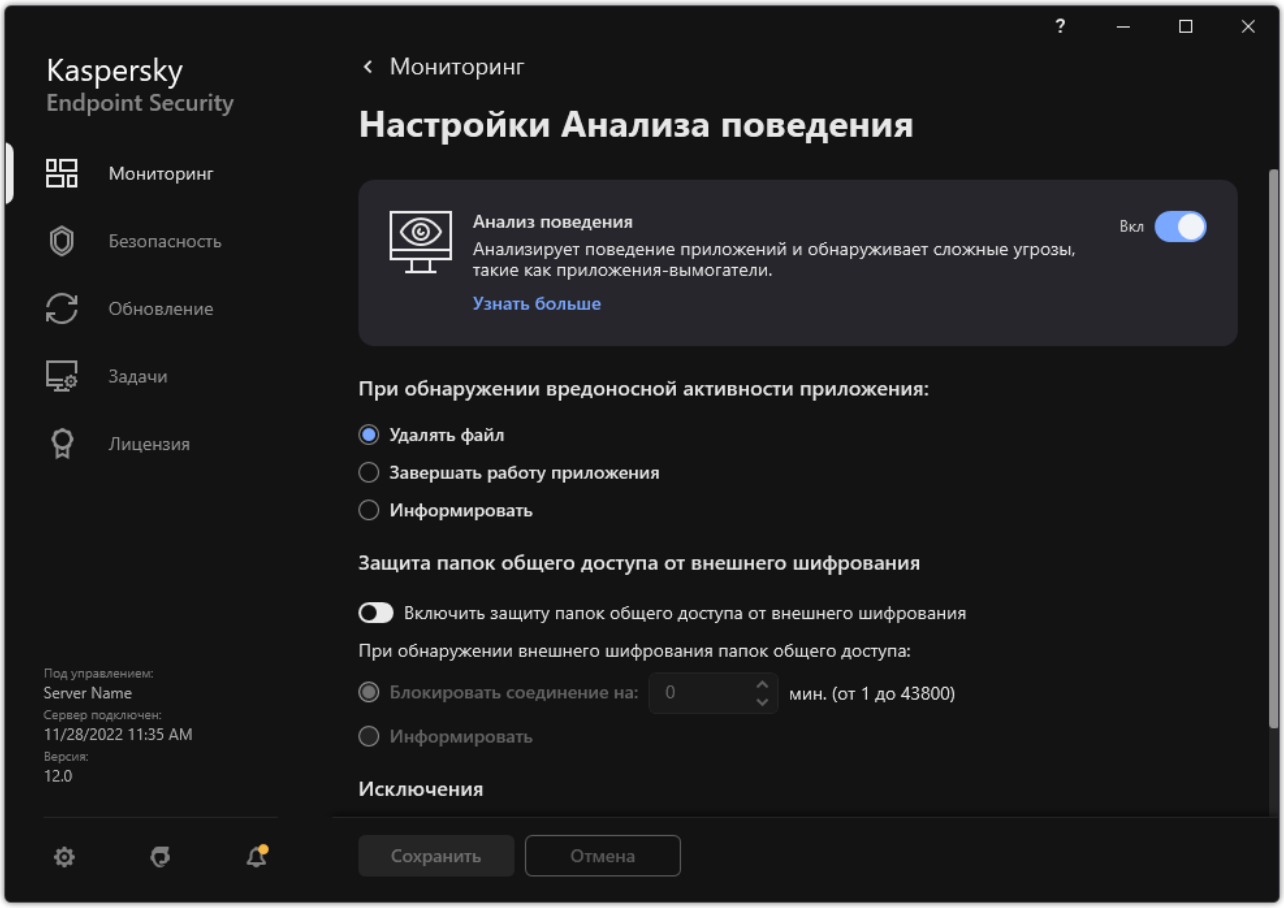


Рисунок 34. Параметры Анализа поведения

3. Используйте переключатель **Включить защиту папок общего доступа от внешнего шифрования**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении внешнего шифрования папок общего доступа

► *Чтобы выбрать действие при обнаружении внешнего шифрования папок общего доступа, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Анализ поведения**.

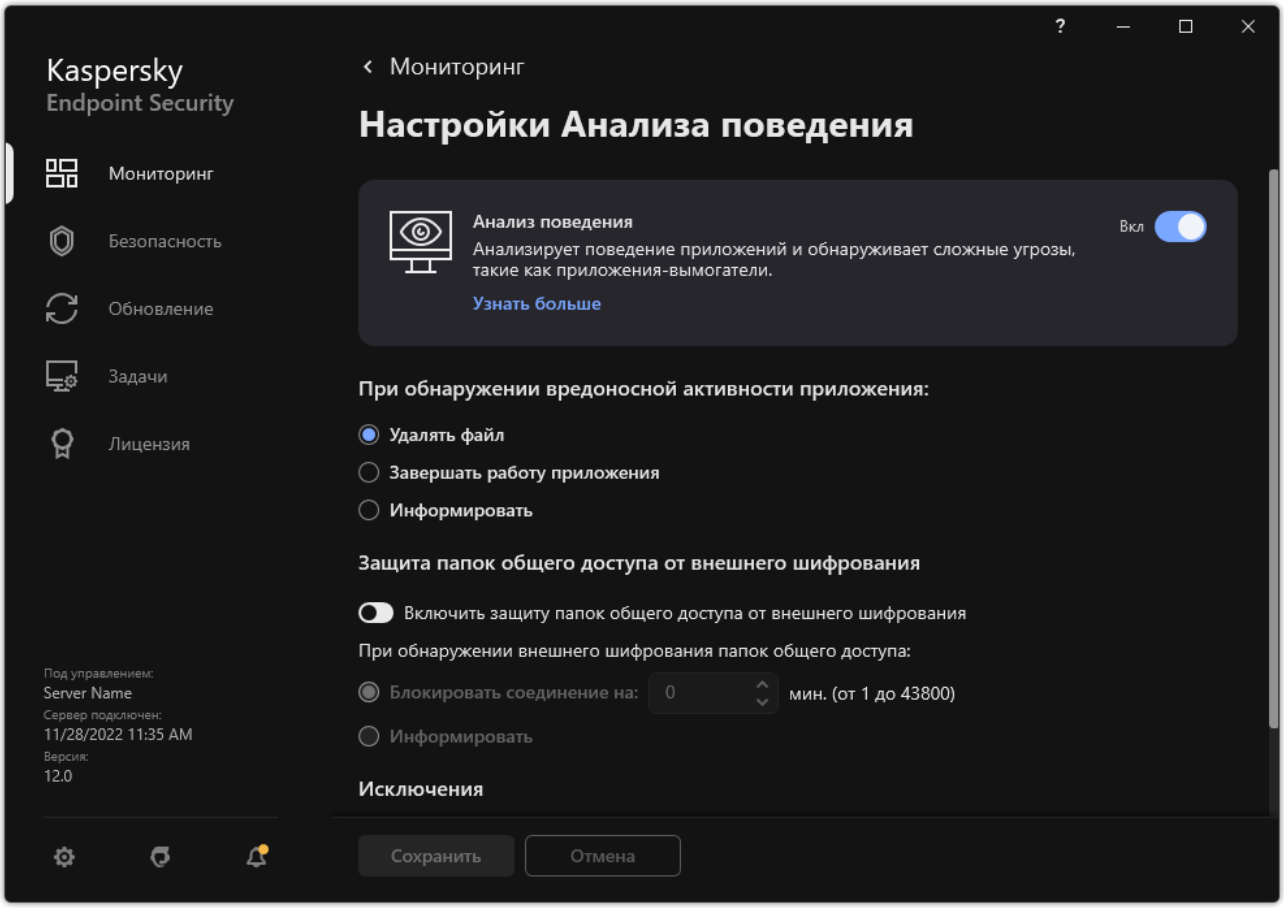


Рисунок 35. Параметры Анализа поведения

3. В блоке **Защита папок общего доступа от внешнего шифрования** выберите нужное действие:
   - **Блокировать соединение на N мин. (от 1 до 43800)**. Если выбран этот вариант, то 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. 303);
- 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. 129), то выполняется восстановление измененных файлов из резервных копий.

- **Информировать**. Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security выполняет следующие действия:
  - добавляет запись в отчеты локального интерфейса приложения (см. раздел "Работа с отчетами" на стр. 303);
  - добавляет запись в список активных угроз;
  - отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

4. Сохраните внесенные изменения.

Создание исключения для защиты папок общего доступа от внешнего шифрования

Исключение папки 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.

Как создать исключение для защиты папок общего доступа в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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**.
4. Нажмите на кнопку **Добавить**.
5. Выберите папку общего доступа, нажав на кнопку **Обзор**.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает 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 `C:\Users\*\Folder\`.

6. В блоке **Компоненты защиты** выберите компонент **Анализ поведения**.
7. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.
8. Установите статус для исключения **Активно**.

   Вы можете в любое время остановить работу исключения с помощью переключателя.
9. Сохраните внесенные изменения.

Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования

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.

► *Чтобы исключить из защиты удаленные компьютеры, осуществляющие внешнее шифрование папок общего доступа, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Анализ поведения**.

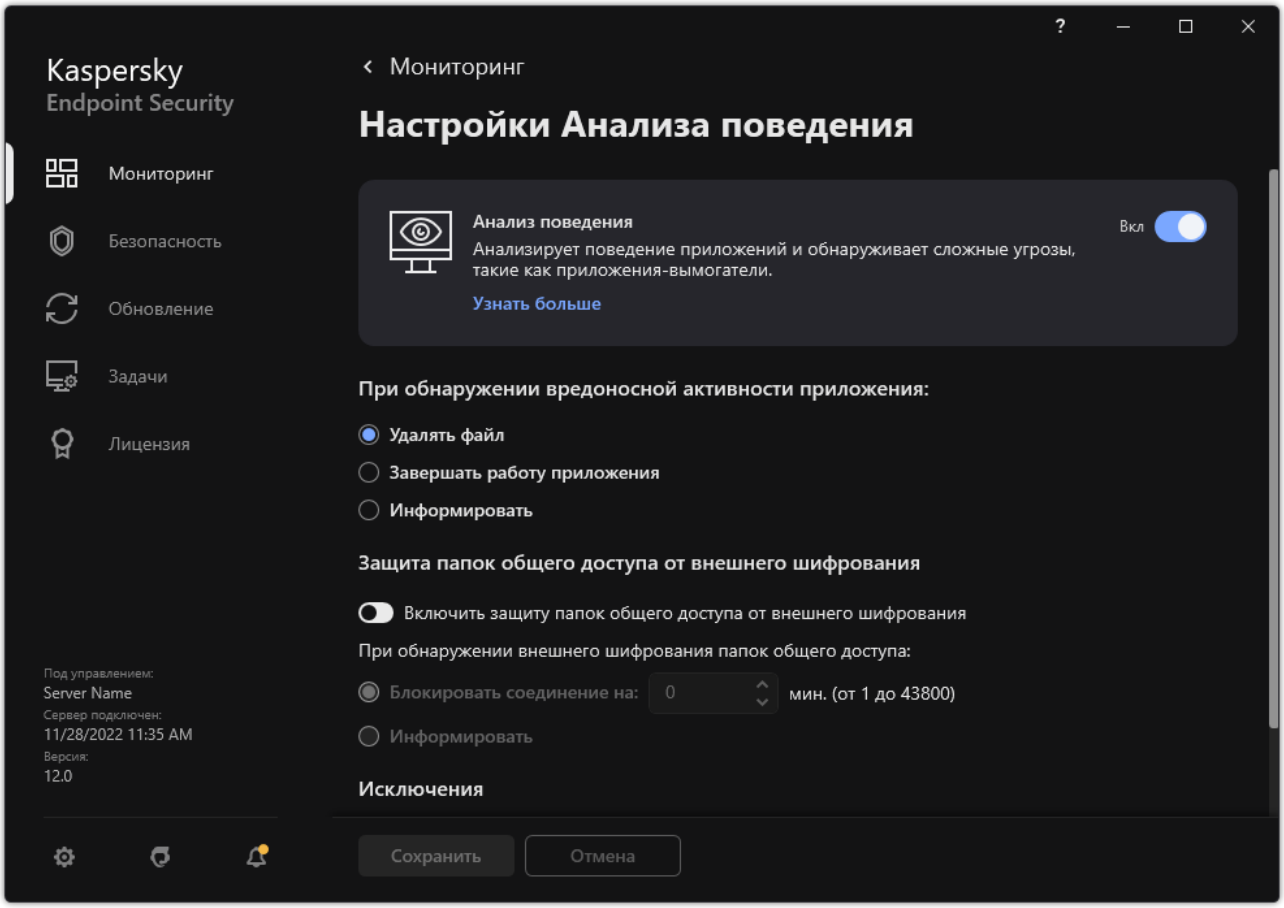


Рисунок 36. Параметры Анализа поведения

3. В блоке **Исключения** перейдите по ссылке **Настройка адресов исключений**.
4. Если вы хотите добавить IP-адрес или имя компьютера в список исключений, нажмите на кнопку **Добавить**.
5. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
6. Сохраните внесенные изменения.

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.

В этом разделе

Включение и выключение Защиты от эксплойтов 114

Защита памяти системных процессов 115

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от эксплойтов**.

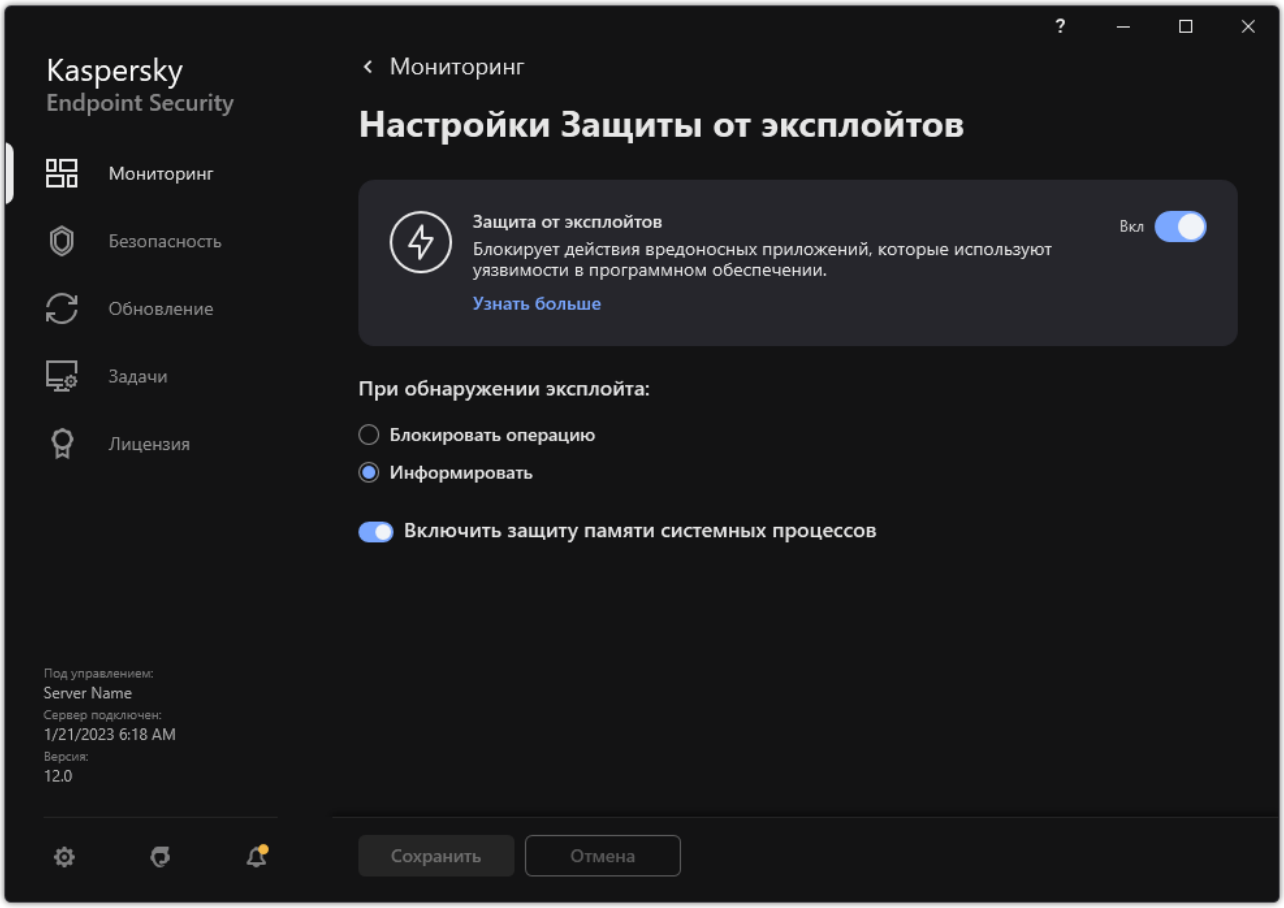


Рисунок 37. Параметры Защиты от эксплойтов

3. Используйте переключатель **Защита от эксплойтов**, чтобы включить или выключить компонент.
4. В блоке **При обнаружении эксплойта** выберите нужное действие:
   - **Блокировать операцию**. 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 "Работа с активными угрозами" на стр. 91).
5. Сохраните внесенные изменения.

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от эксплойтов**.

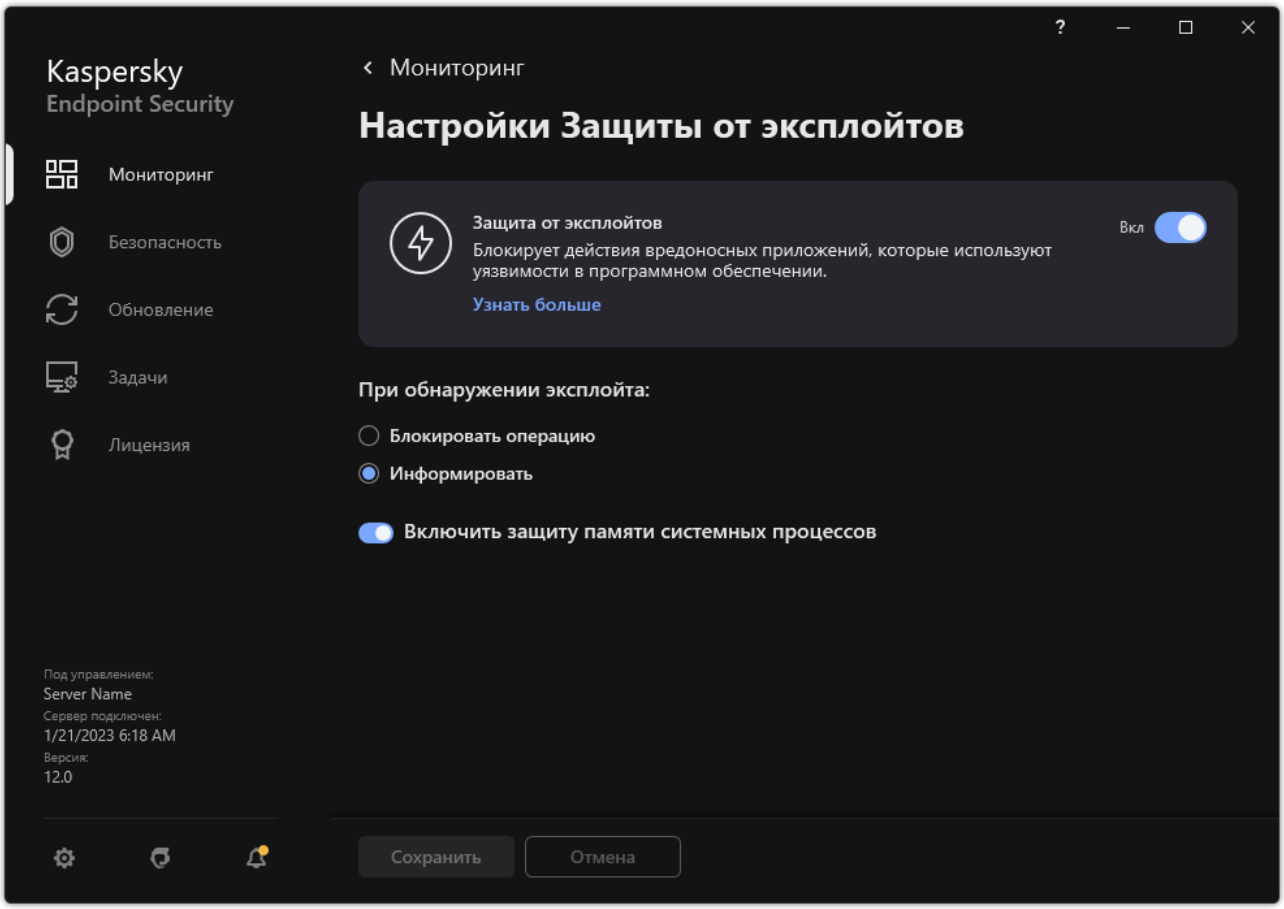


Рисунок 38. Параметры Защиты от эксплойтов

3. Используйте переключатель **Включить защиту памяти системных процессов**, чтобы включить или выключить функцию.
4. Сохраните внесенные изменения.

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. HIPS – Host Intrusion Prevention System) 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. 98).

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. 404), 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. 121). 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 118
Работа с группами доверия приложений 119
Работа с правами приложений 122
Защита ресурсов ОС и персональных данных 124
Удаление информации о неиспользуемых приложениях 125
Мониторинг работы Предотвращения вторжений 126
Защита доступа к аудио и видео 126

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. 38) 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. 404) 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.

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. 404).

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. 121). 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. 121).

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 119

Настройка прав группы доверия 120

Выбор группы доверия для приложений, запускаемых до Kaspersky Endpoint Security 121

Выбор группы доверия для неизвестных приложений 121

Выбор группы доверия для приложений с цифровой подписью 122

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. 404).

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. 122).

Как изменить группу доверия для приложения в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. 404). 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. 38) 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. 38) 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 начала работы Kaspersky Endpoint Security для Windows** выберите нужную группу доверия (см. раздел "Приложение 2. Группы доверия приложений" на стр. 404).
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. 404) 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. 122).

Как выбрать группу доверия для неизвестных приложений в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. 98), 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. 38) 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 "Использование доверенного системного хранилища сертификатов" на стр. 295).

   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. 404) 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. 404), 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. 120), 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. 38) 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.

Параметр	Описание
Не контролировать активность приложения	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложения в операционной системе. Контроль за активностью приложения выполняют следующие компоненты: Анализ поведения (на стр. 104), Защита от эксплойтов (на стр. 114), Предотвращение вторжений (на стр. 117), Откат вредоносных действий (на стр. 129) и Сетевой экран.
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. 122) (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.
Разрешить взаимодействие с интерфейсом Kaspersky Endpoint Security для Windows	Самозащита Kaspersky Endpoint Security (на стр. 310) 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 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. 38) 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. 119).

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. 404) при первом запуске. Вы можете изменить группу доверия для приложения вручную (см. раздел "Работа с правами приложений" на стр. 122). Также вы можете настроить права для отдельного приложения вручную (см. раздел "Работа с правами приложений" на стр. 122). 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. 38) 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** 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**.

     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.

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. 122).

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 контролирует доступ приложений к аудиосигналу и видеосигналу следующим образом:

- *Доверенные* и *Слабые ограничения* – получение аудиосигнала и видеосигнала с устройств разрешено по умолчанию.
- *Сильные ограничения* и *Недоверенные* – получение аудиосигнала и видеосигнала с устройств запрещено по умолчанию.

Вы можете вручную разрешать приложениям получать аудиосигнал и видеосигнал (см. раздел "Работа с правами приложений" на стр. 122).

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. 118).
- 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. 122)) 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.

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. 131), Анализ поведения (на стр. 104) или при поиске вредоносного ПО (см. раздел "Поиск вредоносного ПО" на стр. 49).

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. 38) 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 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. 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. 98) 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 131

Автоматическая приостановка Защиты от файловых угроз 134

Изменение действия компонента Защита от файловых угроз над зараженными файлами 135

Формирование области защиты компонента Защита от файловых угроз 135

Использование методов проверки 136

Использование технологий проверки в работе компонента Защита от файловых угроз 137

Оптимизация проверки файлов 138

Проверка составных файлов 138

Изменение режима проверки файлов 139

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.

► *Чтобы включить или выключить компонент Защита от файловых угроз, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.
     - **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. 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. 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.
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. Kaspersky Endpoint Security проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.

Параметр	Значение	Описание
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 все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет.

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. 38) 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. 38) 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 все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет.
   - **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 добавляет информацию об обнаруженных зараженных файлах в список активных угроз.
   - **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. 298).

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, 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. 38) 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. 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. 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. Выберите объект для добавления в область защиты.

   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. 38) 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. 38) 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.

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. 137), 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. 38) 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. 38) 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 или файлы офисных форматов.
5. Если режим проверки только новых и измененных файлов выключен (см. раздел "Оптимизация проверки файлов" на стр. 138), 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. 38) 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.

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. 98) и эвристического анализа.

Kaspersky Endpoint Security проверяет HTTP-, HTTPS- и FTP-трафик. Kaspersky Endpoint Security проверяет URL- и IP-адреса. Вы можете задать порты, которые Kaspersky Endpoint Security будет контролировать, (см. раздел "Контроль сетевых портов" на стр. 262) или выбрать все порты.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Включение проверки защищенных соединений" на стр. 173).

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

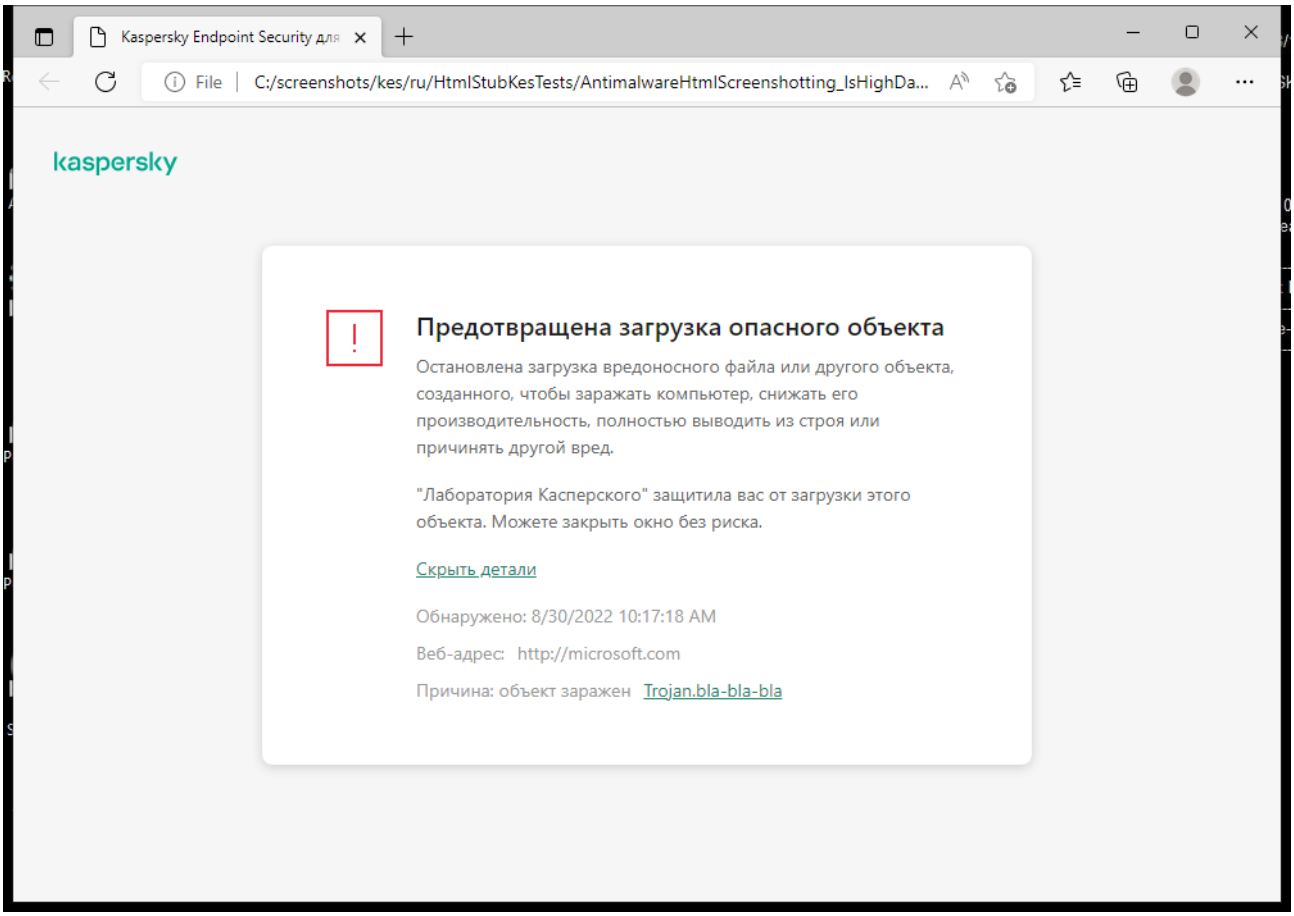


Рисунок 39. Сообщение о запрете доступа к веб-сайту

kaspersky

В этом разделе

Включение и выключение Защиты от веб-угроз 142

Настройка методов обнаружения вредоносных веб-адресов 144

Анти-Фишинг 146

Формирование списка доверенных веб-адресов 147

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.

Вы можете выбрать или настроить уровень безопасности только в Консоли администрирования (MMC) или в локальном интерфейсе приложения. Выбрать или настроить уровень безопасности в Web Console или Cloud Console невозможно.

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

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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 Kaspersky Endpoint Security 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:

   - **Запрещать загрузку**. 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. 98) 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. 173) 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. 38) 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. 38) 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.

Вы можете настроить функцию Анти-Фишинг только в Консоли администрирования (MMC) или в локальном интерфейсе приложения. Настроить функцию Анти-Фишинг в Web Console или Cloud Console невозможно. По умолчанию функция Анти-Фишинг с использованием эвристического анализа включена.

Как включить или выключить функцию Анти-Фишинг в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. 98).

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. 38) 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. 173), Веб-Контроль (на стр. 247) и Контроль сетевых портов (на стр. 262). 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. 282).

Вы также можете сформировать общий список исключений защищенных соединений (см. раздел "Исключение защищенных соединений из проверки" на стр. 180). 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.

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. 98) 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;
- Microsoft Outlook Express;
- Windows Mail.

Другие протоколы и почтовые клиенты Защита от почтовых угроз не поддерживает.

Защита от почтовых угроз не всегда может получить доступ к сообщениям на *уровне протокола* (например, при использовании решения Microsoft Exchange). Поэтому дополнительно в состав Защиты от почтовых угроз включено расширение для Microsoft Office Outlook. Расширение позволяет проверять сообщения на *уровне почтового клиента*. Расширение компонента Защита от почтовых угроз поддерживает работу с Outlook 2010, 2013, 2016, 2019.

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 149

Изменение действия над зараженными сообщениями электронной почты 152

Формирование области защиты компонента Защита от почтовых угроз 153

Проверка составных файлов, вложенных в сообщения электронной почты 155

Фильтрация вложений в сообщениях электронной почты 156

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 Kaspersky Endpoint Security 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.

► *Чтобы включить или выключить компонент Защита от почтовых угроз выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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 Kaspersky Endpoint Security 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. 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.
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).

Параметр	Значение	Описание
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. Kaspersky Endpoint Security 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.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**	При обнаружении зараженного объекта во входящем или исходящем сообщении приложение Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение Kaspersky Endpoint Security удаляет зараженный объект. Приложение Kaspersky Endpoint Security 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. 38) 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 Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение Kaspersky Endpoint Security удаляет зараженный объект. Приложение Kaspersky Endpoint Security 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 Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение Kaspersky Endpoint Security добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение Kaspersky Endpoint Security блокирует отправку сообщения, почтовый клиент показывает ошибку.
   - **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение Kaspersky Endpoint Security добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение Kaspersky Endpoint Security блокирует отправку сообщения, почтовый клиент показывает ошибку.
4. Сохраните внесенные изменения.

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. 38) 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. 38) 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. Kaspersky Endpoint Security 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 Kaspersky Endpoint Security 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. 38) 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.

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 Kaspersky Endpoint Security блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения Kaspersky Endpoint Security. 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 158

Блокирование атакующего компьютера 159

Настройка адресов исключений из блокирования 162

Настройка защиты от сетевых атак по типам 163

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.

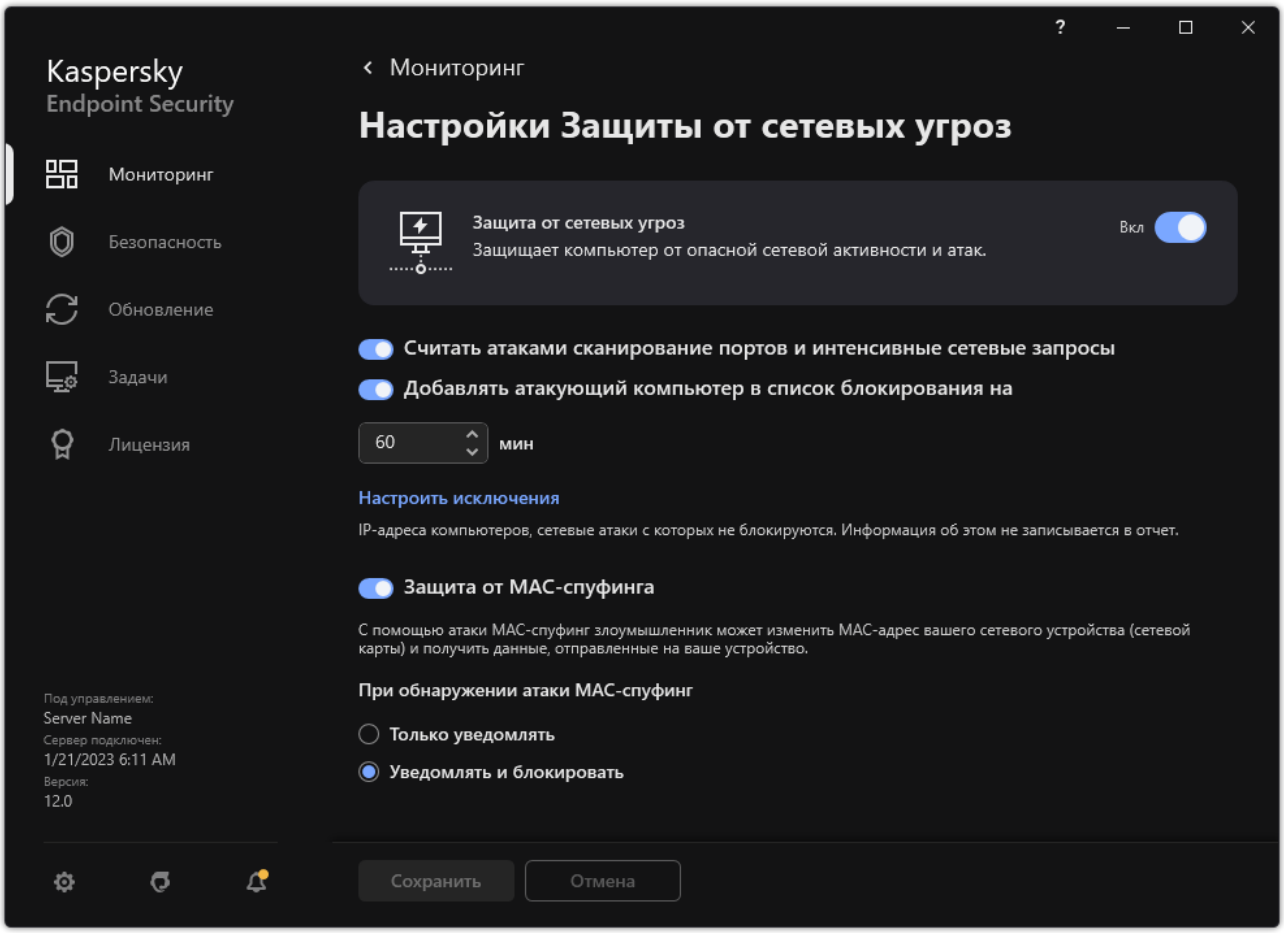


Рисунок 40. Параметры Защиты от сетевых угроз

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.

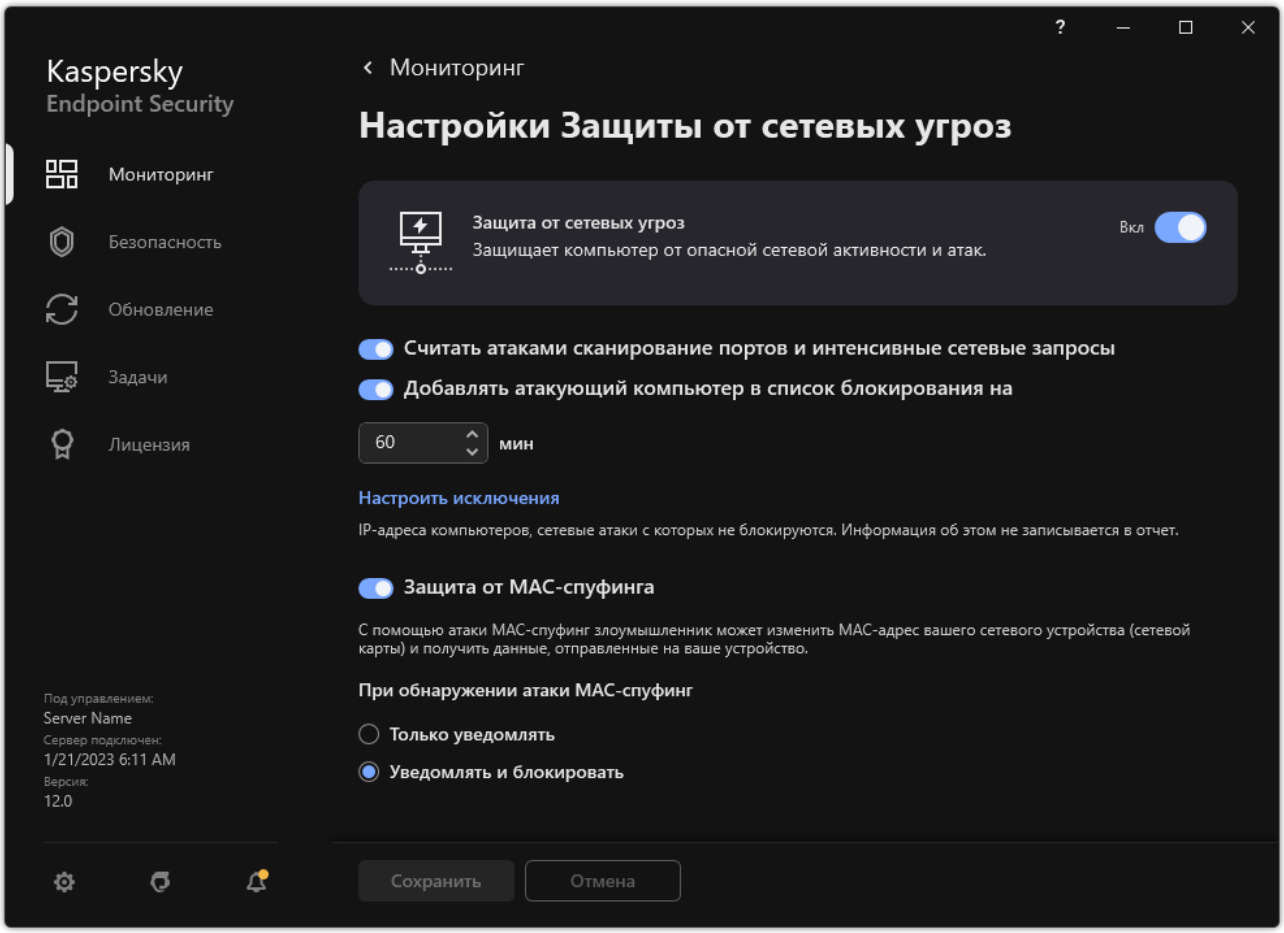


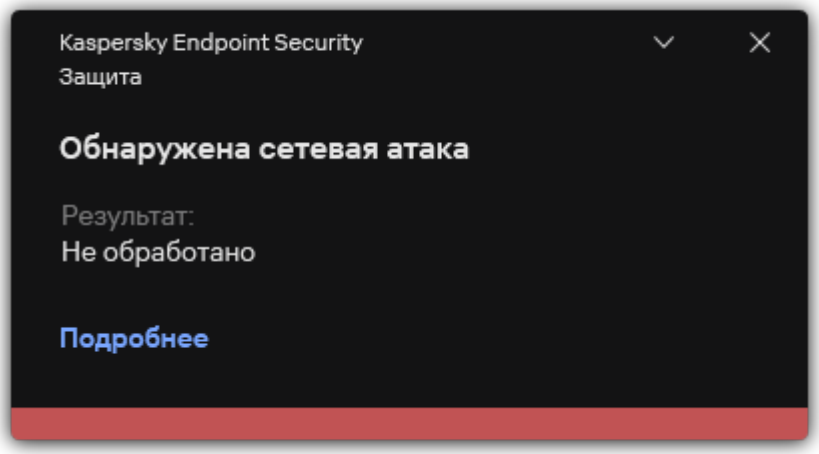
Рисунок 41. Параметры Защиты от сетевых угроз

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 события *Обнаружена сетевая атака*. Событие содержит информацию об атакующем компьютере: IP- и MAC-адреса.



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.

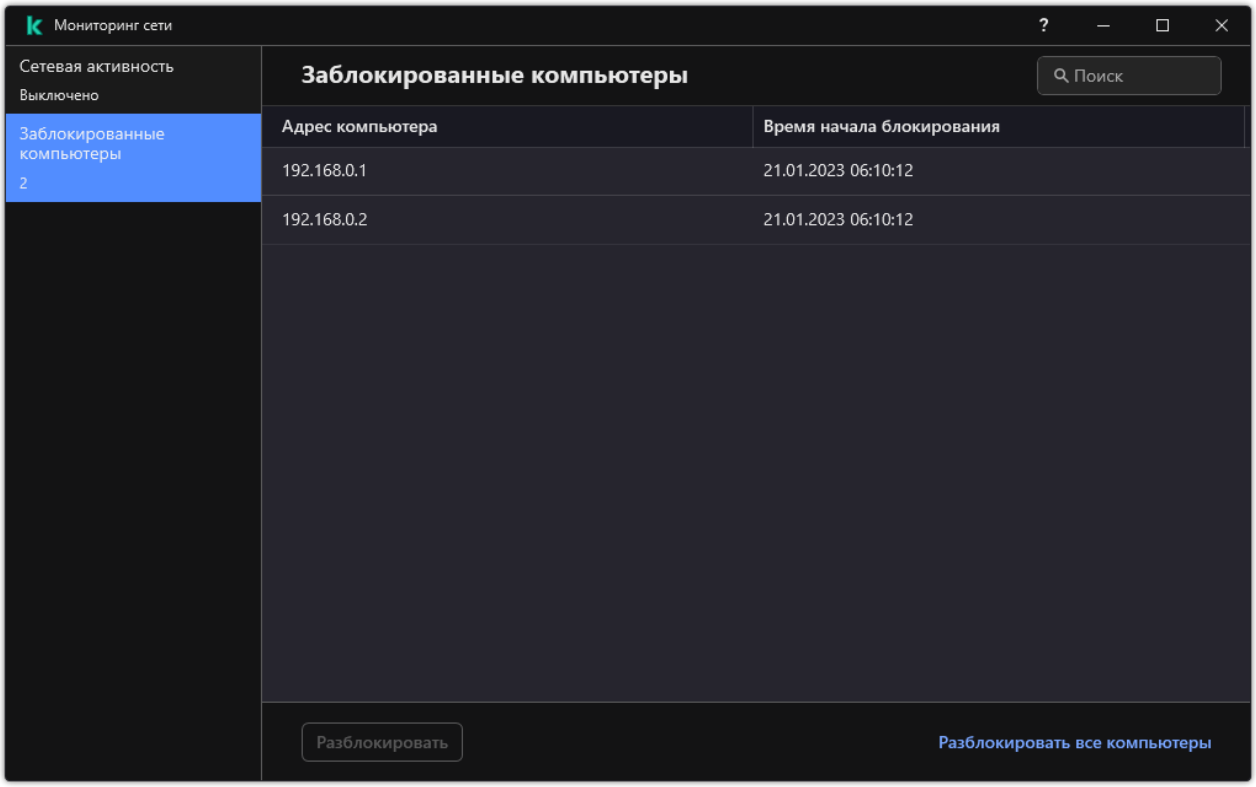
► *Чтобы разблокировать компьютер, выполните следующие действия:*

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.

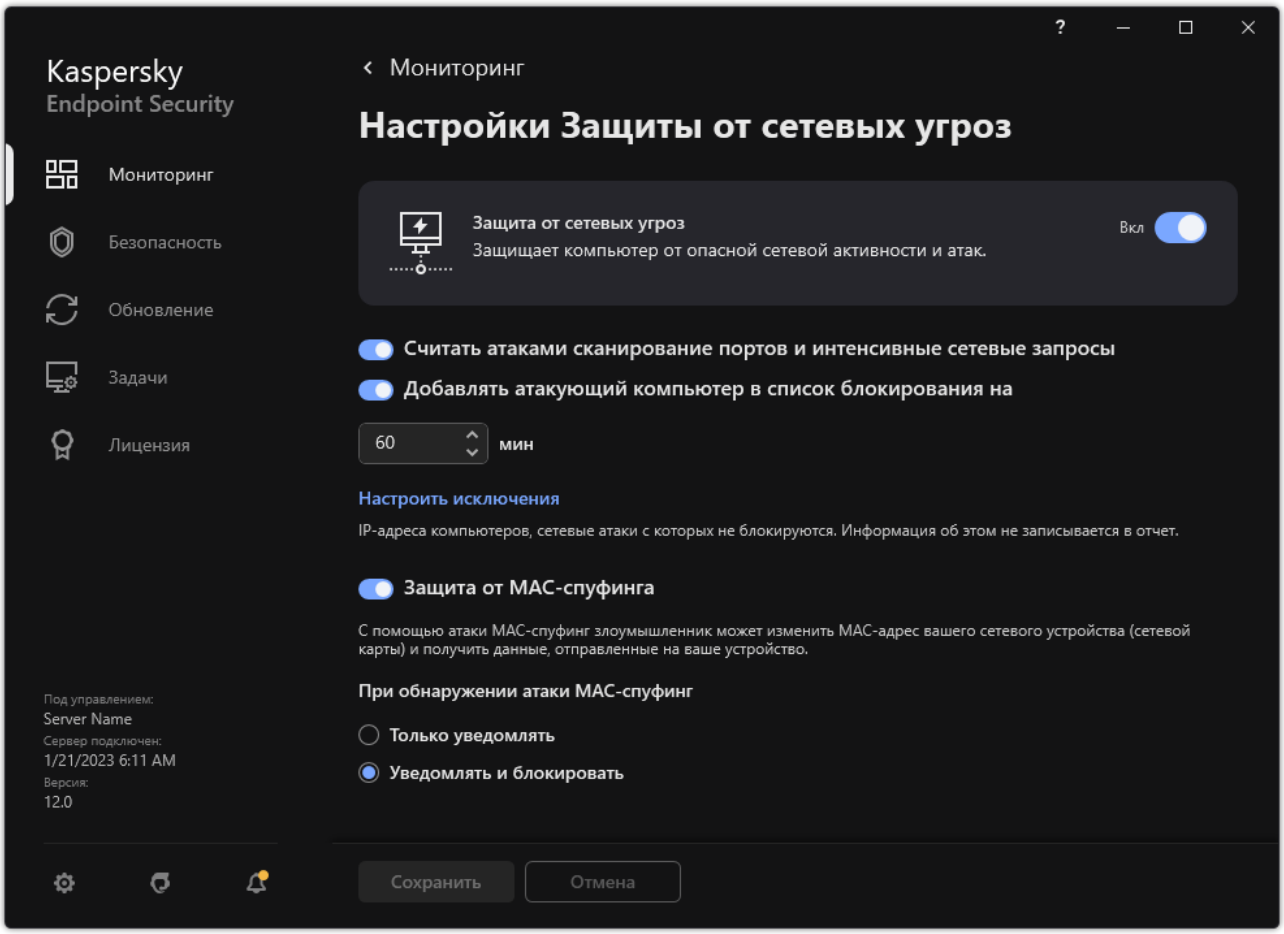


Рисунок 42. Параметры Защиты от сетевых угроз

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 атак 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.

Как настроить защиту от сетевых атак по типам в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.

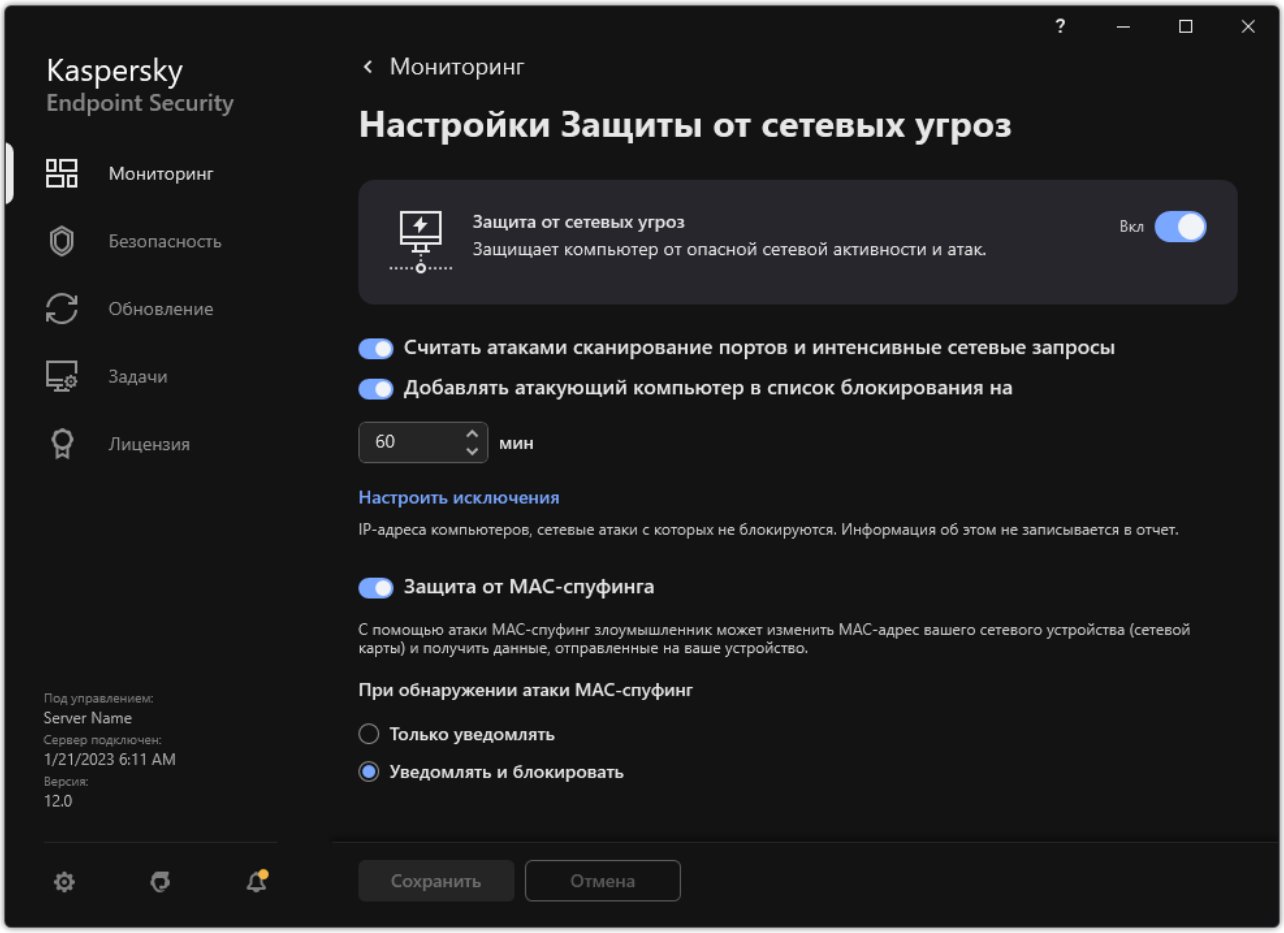


Рисунок 43. Параметры Защиты от сетевых угроз

3. Используйте переключатель **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение атак.

   Если переключатель включен, Kaspersky Endpoint Security контролирует сетевой трафик на наличие этих атак. При обнаружении атаки приложение уведомляет пользователя и отправляет соответствующее событие в Kaspersky Security Center. Приложение предоставляет информацию об атакующем компьютере, необходимую для принятия своевременных действий по реагированию.

4. Используйте переключатель **Защита от MAC-спуфинга**, чтобы включить или выключить обнаружение атак.

5. В блоке **При обнаружении атаки MAC-спуфинг** выберите один из следующих вариантов:

   - **Информировать**.
   - **Блокировать**.

6. Сохраните внесенные изменения.

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. 168) 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. 167). 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.

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Если вам нужен компонент Защита от атак BadUSB, вы можете добавить компонент в свойствах инсталляционного пакета перед установкой приложения или измените состав компонентов приложения после установки приложения.

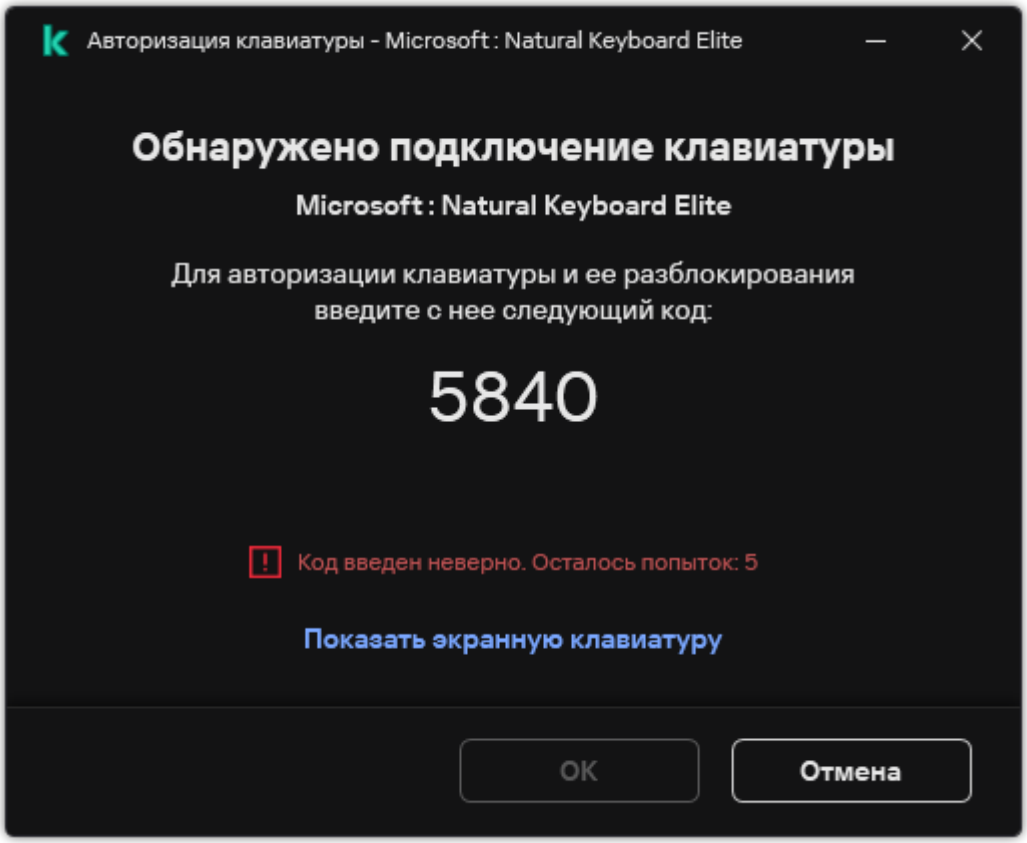


Рисунок 44. Уведомление об авторизации клавиатуры

В этом разделе

Включение и выключение Защиты от атак BadUSB 167
Использовании экранной клавиатуры при авторизации USB-устройств 168

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.

► *Чтобы включить или выключить Защиту от атак BadUSB, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** → **Защита от атак BadUSB**.
3. Используйте переключатель **Защита от атак BadUSB**, чтобы включить или выключить компонент.
4. В блоке **Авторизация USB-устройств при подключении** настройте параметры безопасности ввода кода авторизации:
   - **Максимальное количество попыток авторизации USB-устройства**. Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Endpoint Security покажет время блокировки USB-устройства. По истечении указанного времени, вам будет доступно 5 попыток ввода кода авторизации.
   - **Тайм-аут при достижении максимального количества попыток**. Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).
5. Сохраните внесенные изменения.

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 штрих-кодов). Не рекомендуется использовать экранную клавиатуру для авторизации неизвестных вам USB-устройств.

► *Чтобы разрешить или запретить использование экранной клавиатуры при авторизации, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** → **Защита от атак BadUSB**.
3. Используйте флажок **Запретить использование экранной клавиатуры для авторизации USB-устройств**, чтобы запретить или разрешить использование экранной клавиатуры 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).

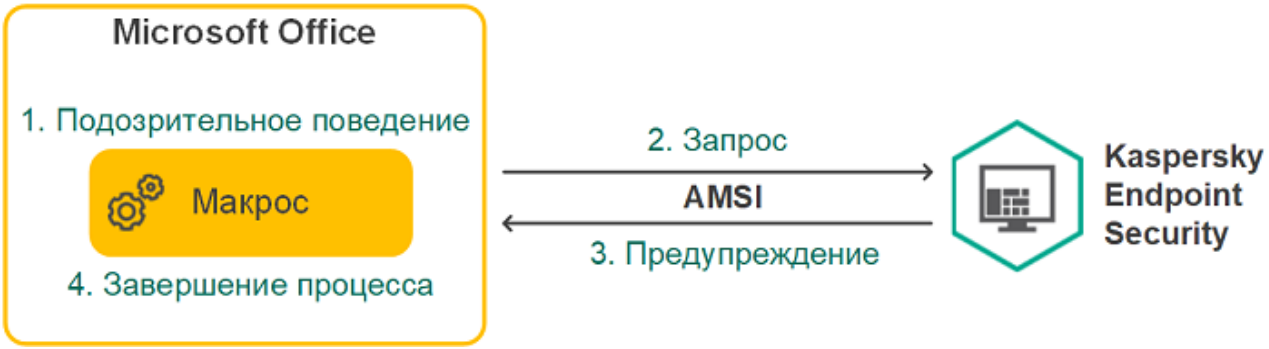


Рисунок 45. Пример работы AMSI

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. 287).

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 Core Mode);
- Windows Server 2019 Essentials / Standard / Datacenter (включая Core Mode);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая Core Mode).

В этом разделе

Включение и выключение AMSI-защиты 170
Проверка составных файлов AMSI-защитой 170

Включение и выключение AMSI-защиты

По умолчанию AMSI-защита включена.

► *Чтобы включить или выключить AMSI-защиту, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **AMSI-защита**.

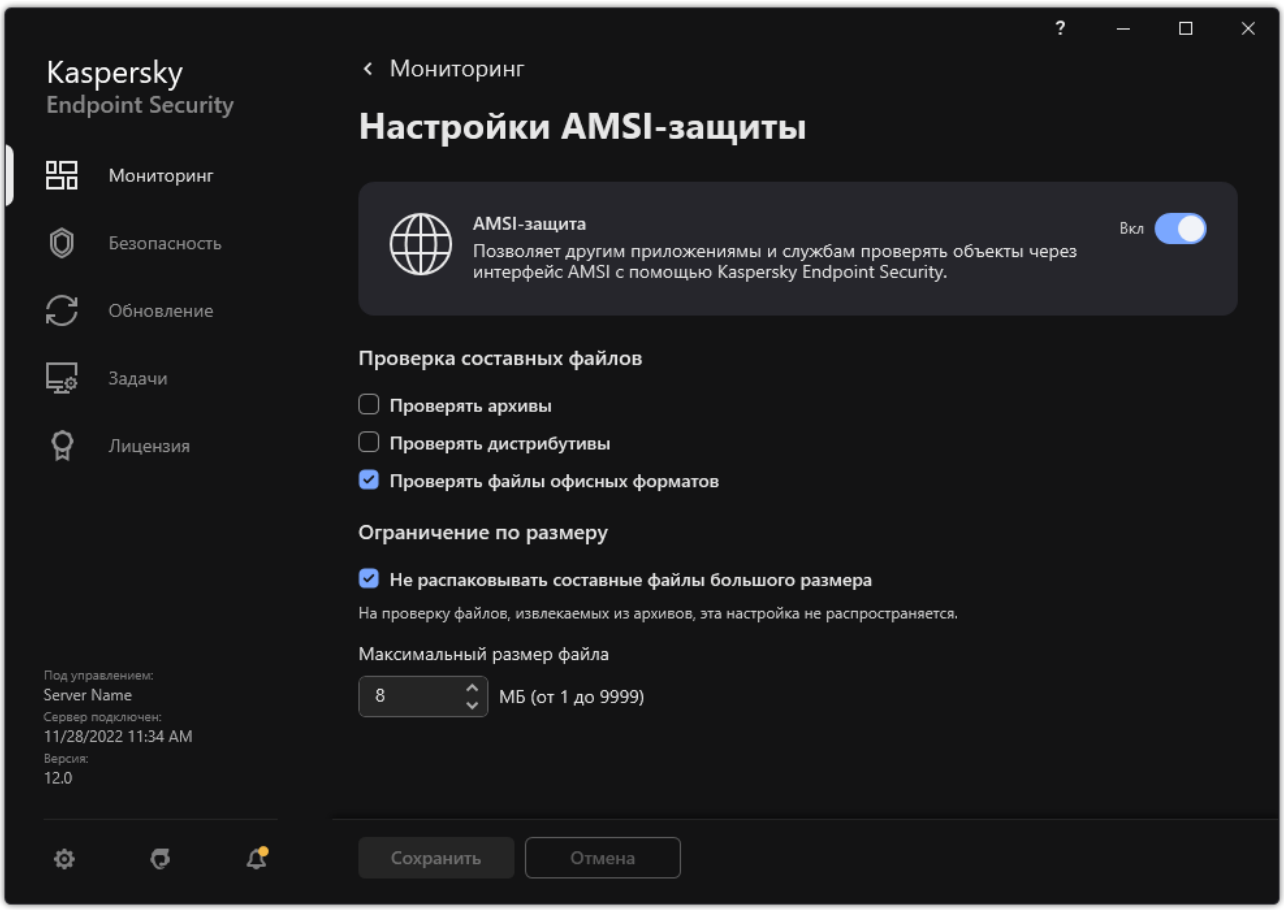


Рисунок 46. Параметры AMSI-защиты

3. Используйте переключатель **AMSI-защита**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Проверка составных файлов AMSI-защитой

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.

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

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **AMSI-защита**.

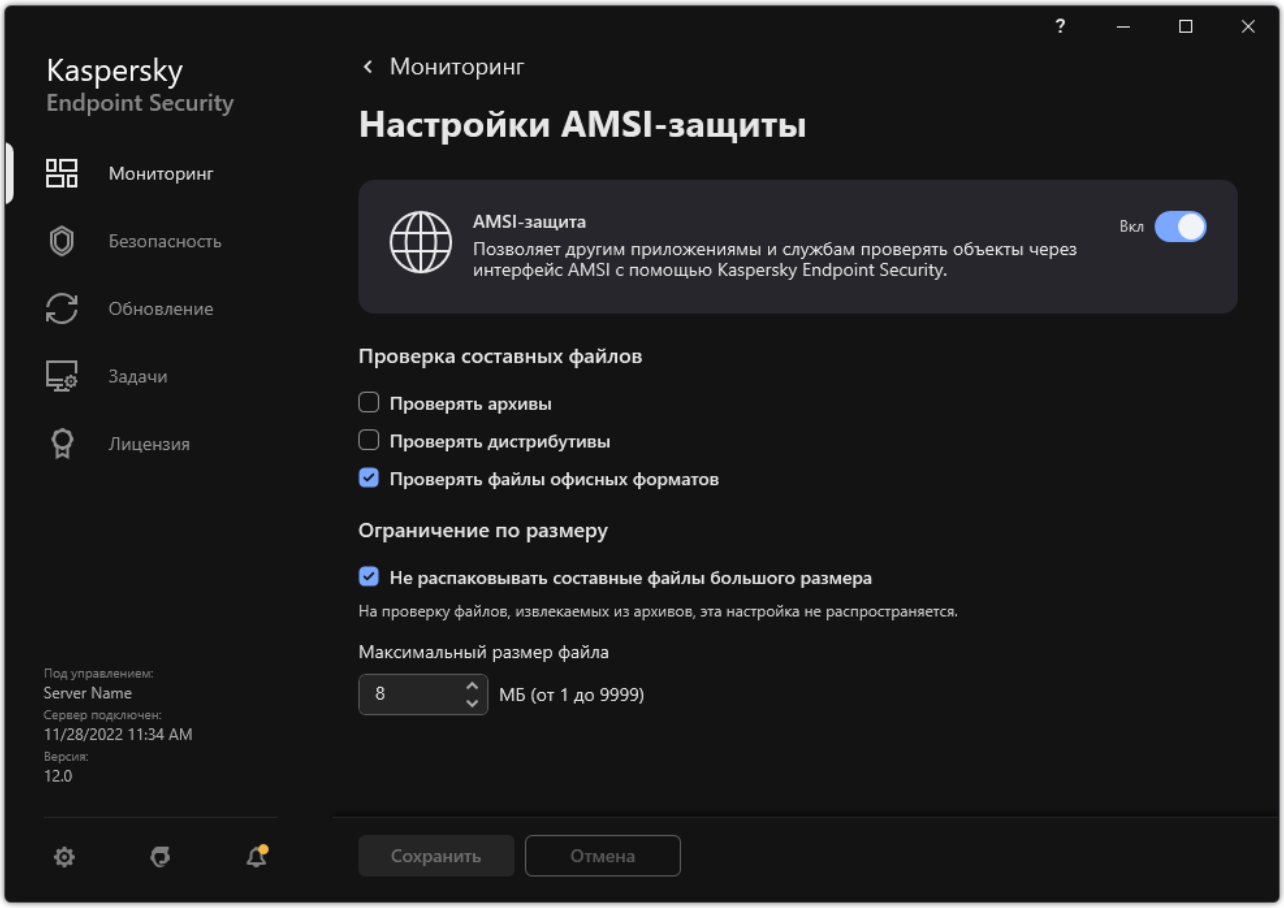


Рисунок 47. Параметры AMSI-защиты

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 в поле **Максимальный размер файла** 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.

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. 247), Защита от почтовых угроз (на стр. 149), Защита от веб-угроз (на стр. 141) 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 173

Установка доверенных корневых сертификатов 177

Проверка защищенных соединений в Firefox и Thunderbird 178

Исключение защищенных соединений из проверки 180

Включение проверки защищенных соединений

► *Чтобы включить проверку защищенных соединений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

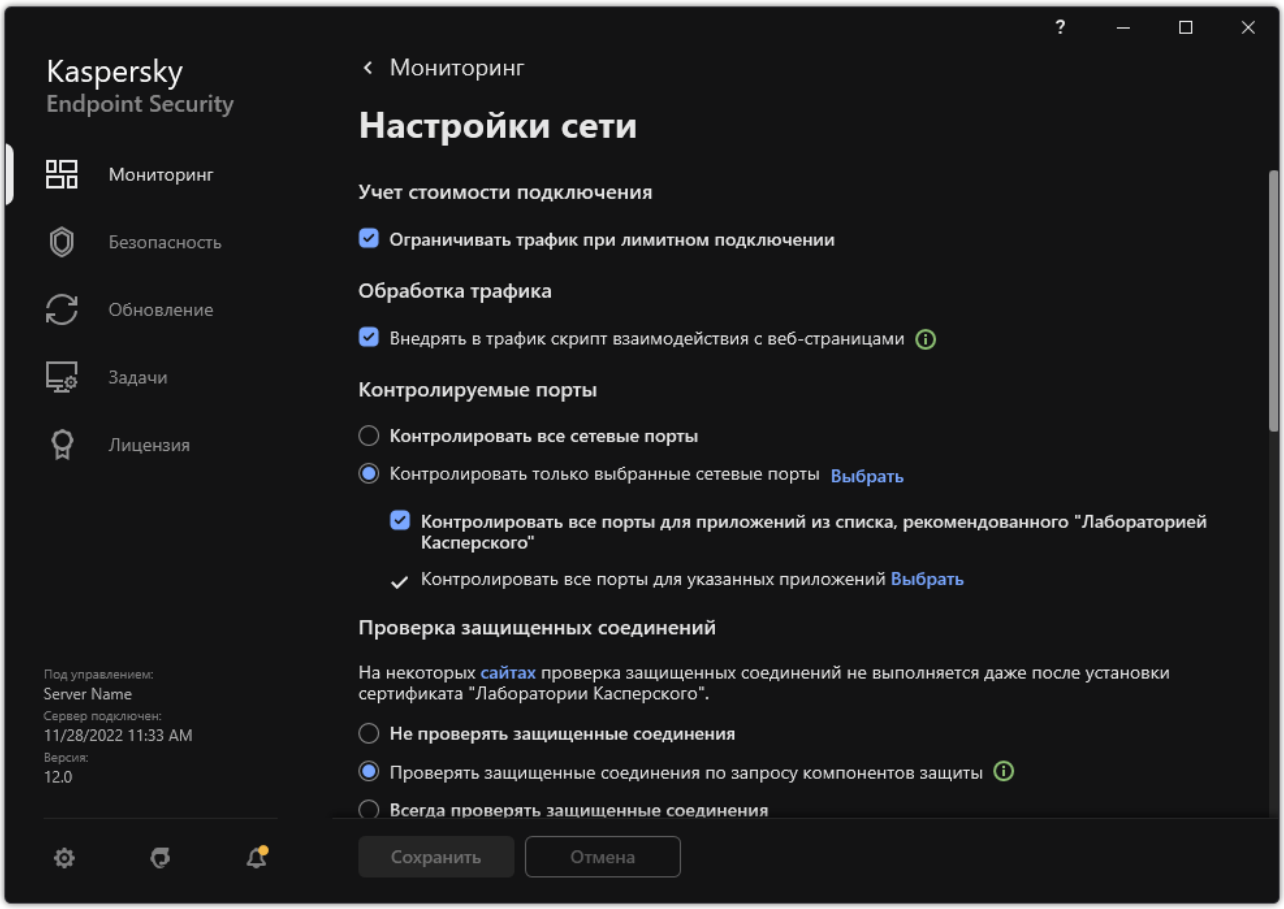


Рисунок 48. Параметры проверки защищенных соединений

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 **Error! Hyperlink reference not valid.**.
   - **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. 287). 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. 180).
5. Настройте параметры проверки защищенных соединений (см. таблицу ниже).

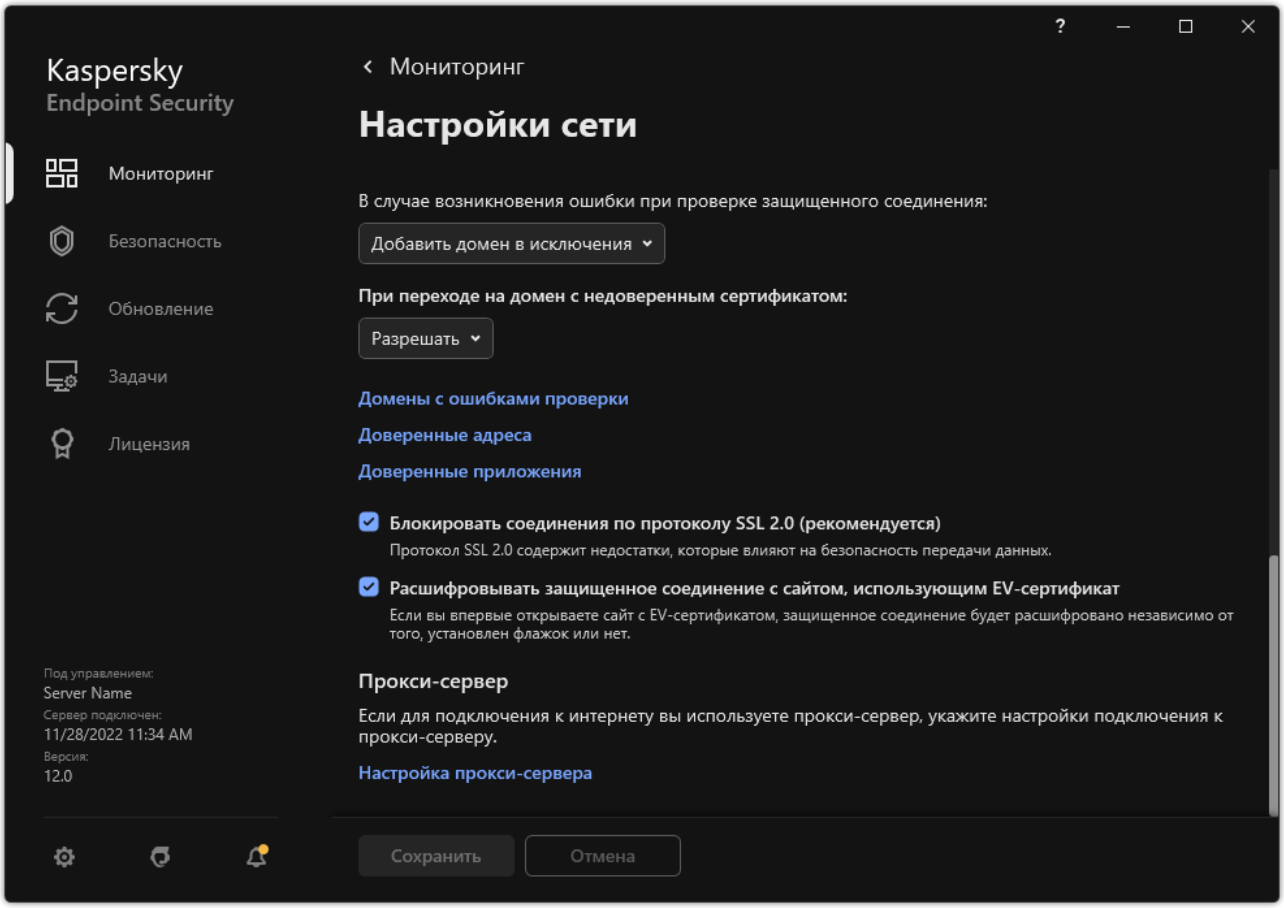


Рисунок 49. Параметры сети приложения

6. Сохраните внесенные изменения.

Таблица 12. 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.
При переходе на домен с недоверенным сертификатом	• **Разрешать**. При переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security разрешает установку сетевого соединения. 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 соединение**. 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.
В случае возникновения ошибки при проверке защищенного соединения	• **Блокировать соединение**. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение. • **Добавить 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 соединение**. Также Kaspersky Endpoint Security формирует событие об ошибке проверки защищенного соединения.

Параметр	Описание
Блокировать соединения по протоколу SSL 2.0 (рекомендуется)	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролирует сетевой трафик, передаваемый по этим соединениям.
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. 38) 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.

Проверка защищенных соединений в Firefox и Thunderbird

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Firefox и Thunderbird по умолчанию используют собственное хранилище сертификатов Mozilla, а не 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 приложениях Firefox и Thunderbird для проверки трафика этих приложений. Если к компьютеру не применена политика, вы можете выбрать хранилище сертификатов, которое будут использовать приложения Mozilla. Если вы выбрали хранилище сертификатов Mozilla, 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. 173). Если проверка защищенных соединений выключена, приложение не проверяет трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird.

Перед добавлением сертификата в хранилище Mozilla 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/15816. Подробнее о добавлении сертификата в хранилище см. 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 Firefox и Thunderbird, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Mozilla Firefox и Thunderbird** установите флажок **Использовать выбранное хранилище сертификатов для проверки защищенных соединений в приложениях Mozilla**.
4. Выберите хранилище сертификатов:
   - **Использовать хранилище сертификатов Windows (рекомендуется)**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке приложения Kaspersky Endpoint Security.
   - **Использовать хранилище сертификатов Mozilla**. 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.
5. Сохраните внесенные изменения.

Проверка защищенных соединений в Firefox и Thunderbird

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Firefox и Thunderbird по умолчанию используют собственное хранилище сертификатов Mozilla, а не 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 приложениях Firefox и Thunderbird для проверки трафика этих приложений. Если к компьютеру не применена политика, вы можете выбрать хранилище сертификатов, которое будут использовать приложения Mozilla. Если вы выбрали хранилище сертификатов Mozilla, 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. 173). Если проверка защищенных соединений выключена, приложение не проверяет трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird.

Перед добавлением сертификата в хранилище Mozilla 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/15816. Подробнее о добавлении сертификата в хранилище см. 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 Firefox и Thunderbird, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Mozilla Firefox и Thunderbird** установите флажок **Использовать выбранное хранилище сертификатов для проверки защищенных соединений в приложениях Mozilla**.
4. Выберите хранилище сертификатов:
   - **Использовать хранилище сертификатов Windows (рекомендуется)**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке приложения Kaspersky Endpoint Security.
   - **Использовать хранилище сертификатов Mozilla**. 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.
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. 173). 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. 287). 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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

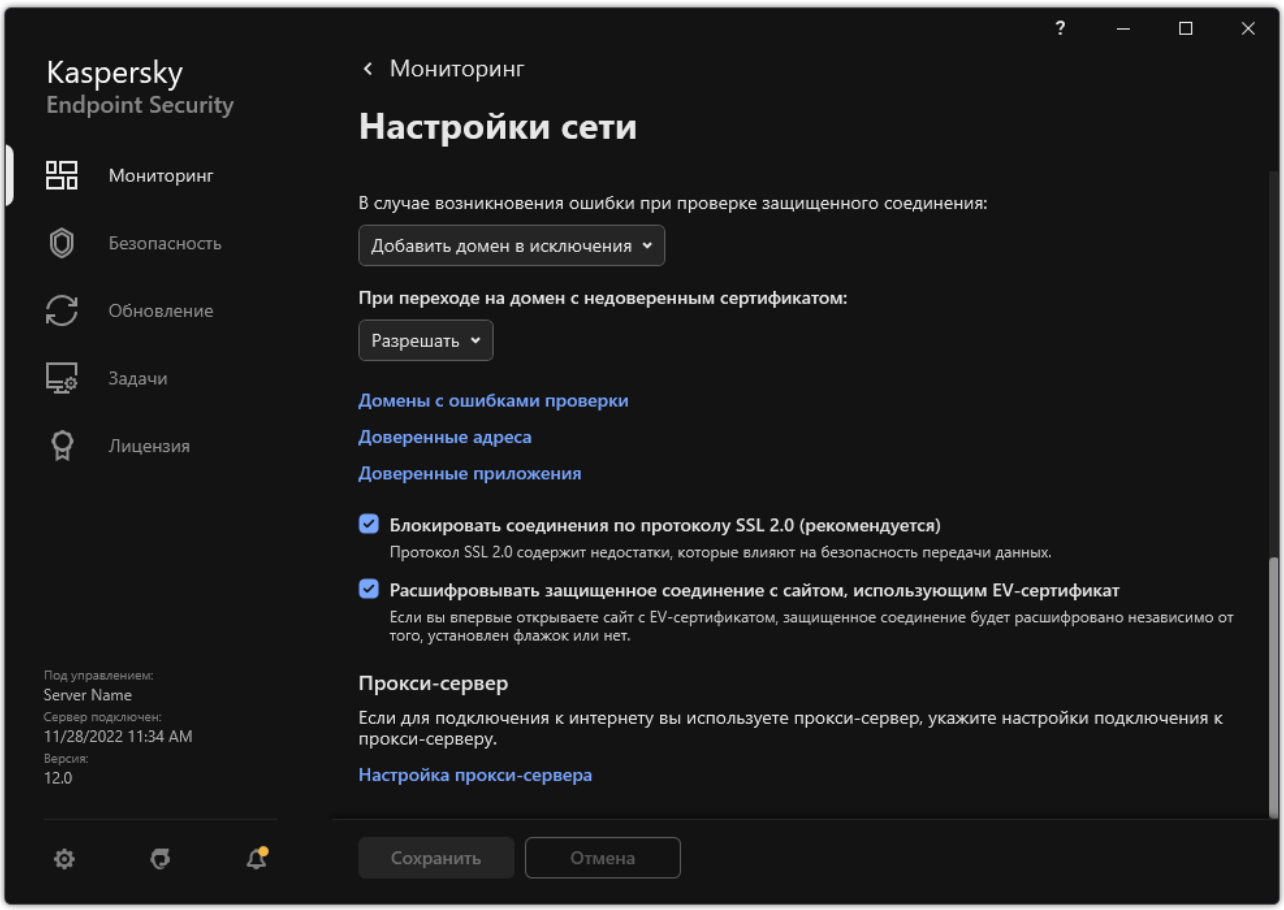


Рисунок 50. Параметры сети приложения

3. В блоке **Проверка защищенных соединений** нажмите на кнопку **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. 173). 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. 38) 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. 38) 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.

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 (см. раздел "Добавление правила Контроля приложений" на стр. 193).

   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.

3. Выбор режима работы Контроля приложений (см. раздел "Выбор режима Контроля приложений" на стр. 189).

   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.

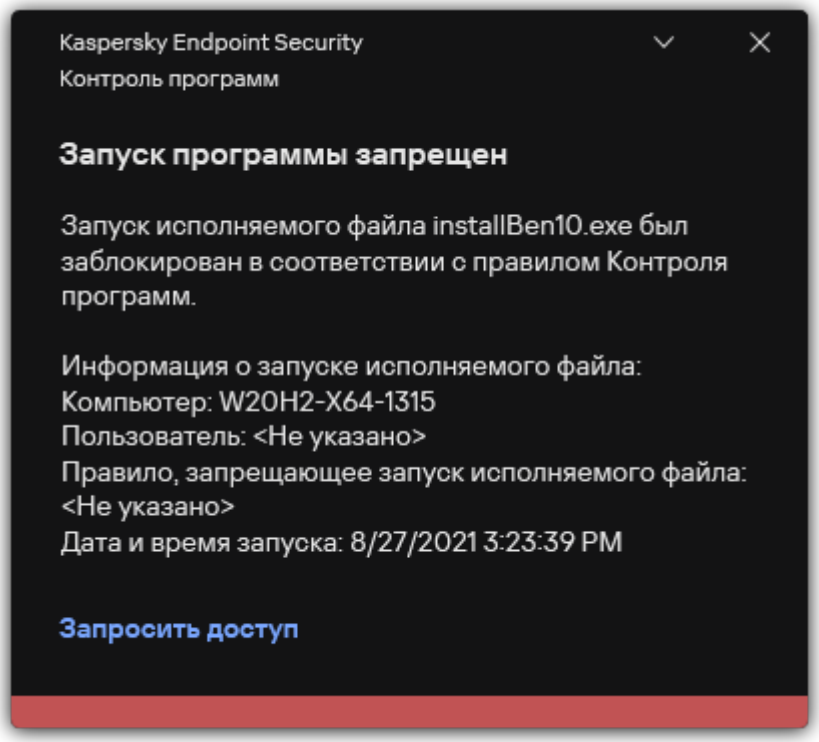


Рисунок 51. Уведомление Контроля программ

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).

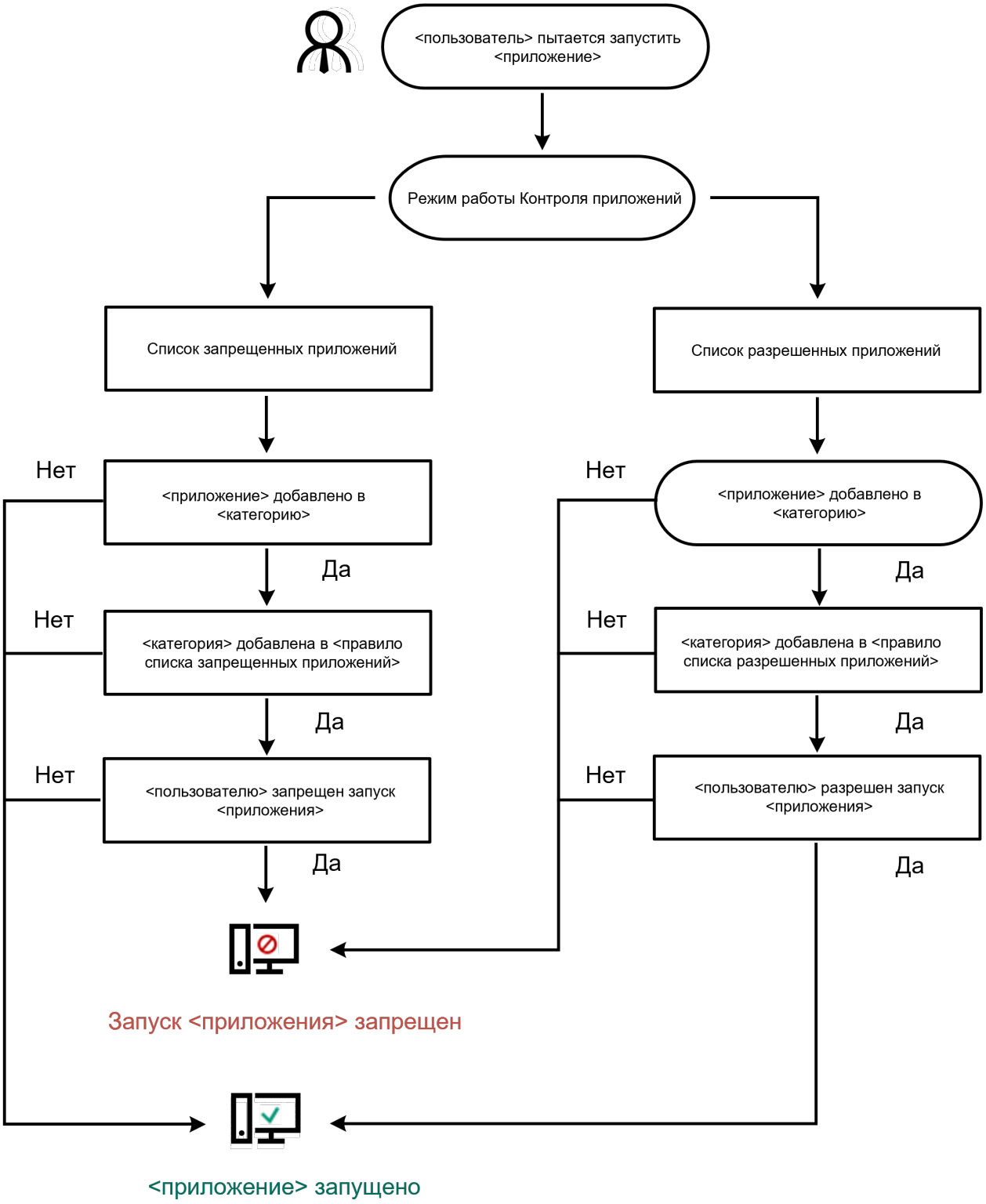


Рисунок 52. Алгоритм работы Контроля программ

kaspersky

В этом разделе

Ограничения функциональности Контроля приложений 187
Включение и выключение Контроля приложений 188
Выбор режима Контроля приложений 189
Действия с правилами Контроля приложений в интерфейсе приложения 190
Тестирование правил Контроля приложений 194
Мониторинг активности приложений 195
Правила формирования масок имен файлов или папок 195
Изменение шаблонов сообщений Контроля приложений 196

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 программы** / **Программы, 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 программы** / **Программы 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 и выключение Контроля приложений

По умолчанию Контроль приложений выключен.

► *Чтобы включить или выключить Контроль приложений выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. Используйте переключатель **Контроль приложений**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Контроль приложений включен, приложение передает в Kaspersky Security Center информацию о запущенных исполняемых файлах. Вы можете просмотреть список запущенных исполняемых файлов в Kaspersky Security Center в папке **Исполняемые файлы**. Для получения информации обо всех исполняемых файлах, а не только о запущенных файлах, запустите задачу *Инвентаризация*.

Выбор режима Контроля приложений

► *Чтобы выбрать режим Контроля приложений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. В блоке **Режим контроля запуска приложений** выберите один из следующих вариантов:
   - **Запрещенные приложения**. Если выбран этот вариант, Контроль приложений разрешает всем пользователям запуск любых приложений, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля приложений.
   - **Разрешенные приложения**. Если выбран этот вариант, Контроль приложений запрещает всем пользователям запуск любых приложений, кроме случаев, удовлетворяющих условиям разрешающих правил Контроля приложений.

     Для режима Список разрешенных приложений изначально заданы правила **Приложения ОС** и **Доверенные приложения обновления**. Эти правила Контроля приложений соответствуют KL-категориям. В KL-категорию "Приложения ОС" входят приложения, обеспечивающие нормальную работу операционной системы. В KL-категорию "Доверенные приложения обновления" входят приложения обновления наиболее известных производителей программного обеспечения. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. По умолчанию правило **Приложения ОС** включено, а правило **Доверенные приложения обновления** выключено. Запуск приложений, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

   Все правила, сформированные при выбранном режиме, сохраняются после смены режима для возможности их повторного использования. Чтобы вернуться к использованию этих правил, достаточно выбрать нужный режим.
4. В блоке **Действие при запуске приложений, запрещенных правилами** выберите, какое действие компонент должен выполнять при попытке пользователя запустить приложение, запрещенную правилами Контроля приложений.
5. Установите флажок **Контролировать загрузку DLL-модулей**, если вы хотите, чтобы приложение Kaspersky Endpoint Security контролировало загрузку DLL-модулей при запуске пользователями приложений.

   Информация о модуле и приложении, загрузившей этот модуль, будет сохранена в отчет.

   Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Перезагрузите компьютер после установки флажка, если вы хотите, чтобы приложение Kaspersky Endpoint Security контролировало все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.

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 "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.

Рекомендуется включить защиту паролем (см. раздел "Включение Защиты паролем" на стр. 276) для настройки параметров приложения, чтобы иметь возможность выключить запрещающие правила, блокирующие запуск критически важных DLL-модулей и драйверов, не изменяя при этом параметры политики Kaspersky Security Center.

6. 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 "Использование доверенного системного хранилища сертификатов" на стр. 295).

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.

В этом разделе

Добавление условия срабатывания в правило Контроля приложений 192

Добавление правила Контроля приложений 193

Изменение статуса правила Контроля приложений 194

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. 38) 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 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**. 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**.

Добавление правила Контроля приложений

► *Чтобы добавить правило Контроля приложений, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. Задайте или измените список пользователей и / или групп пользователей, которым разрешено или запрещено запускать приложения, удовлетворяющие условиям срабатывания правила. Для этого нажмите на кнопку **Добавить** в таблице **Пользователи и их права**.

      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. 192) 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.

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. 38) 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.

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

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. 38) 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. 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 **Общие настройки** → **Интерфейс**.
5. Используйте флажок **Скрыть раздел Мониторинг активности приложений**, чтобы включить или выключить доступ к инструменту.
6. 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, запрещенную правилом Контроля приложений, Kaspersky Endpoint Security выводит сообщение о блокировке запуска приложения. 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 сообщения о блокировке запуска приложения и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► *Чтобы изменить шаблон сообщения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. Уведомление о блокировке приложения см. рис. ниже.

     Настроить шаблоны сообщения для Контроля приложений в тестовом режиме (см. раздел "Тестирование правил Контроля приложений" на стр. 194) 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. 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.
4. Сохраните внесенные изменения.

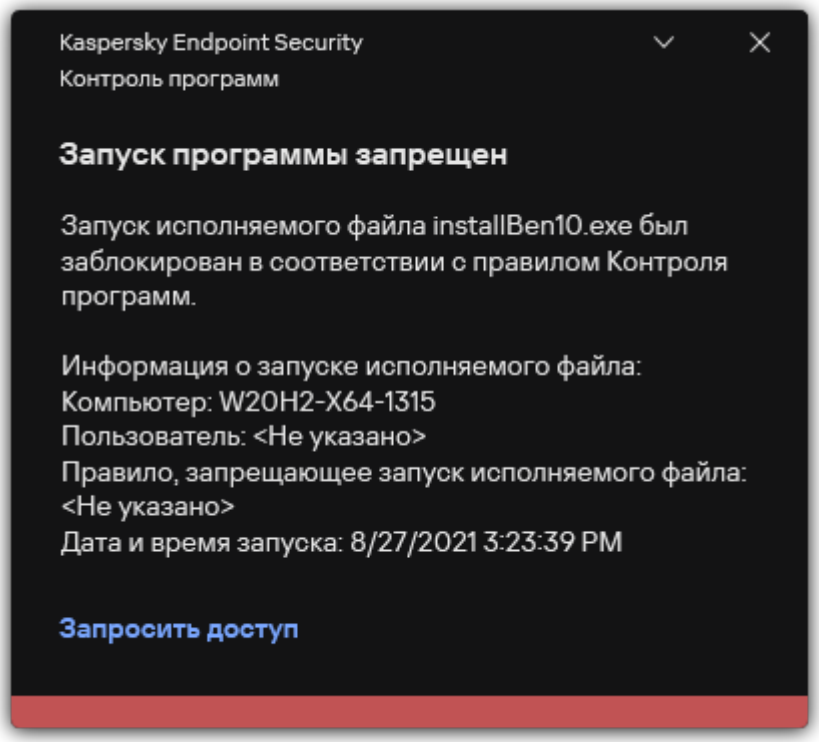


Рисунок 53. Уведомление Контроля программ

См. также:

Изменение шаблонов сообщений Веб-Контроля 258
Изменение шаблонов сообщений Контроля устройств 234
Изменение шаблонов сообщений Адаптивного контроля аномалий 245

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.

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). Таким образом, вы можете ограничить подключение всех устройств, 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).

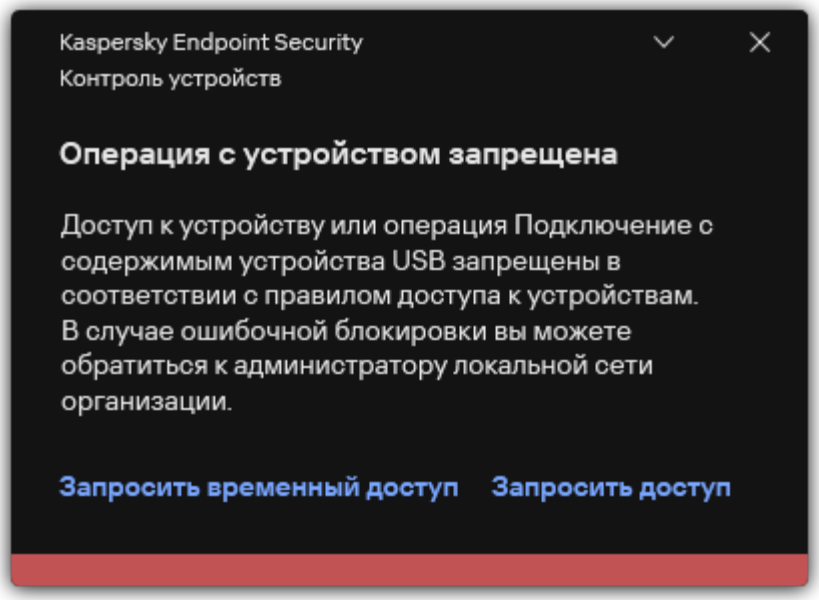


Рисунок 54. Уведомление Контроля устройств

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).

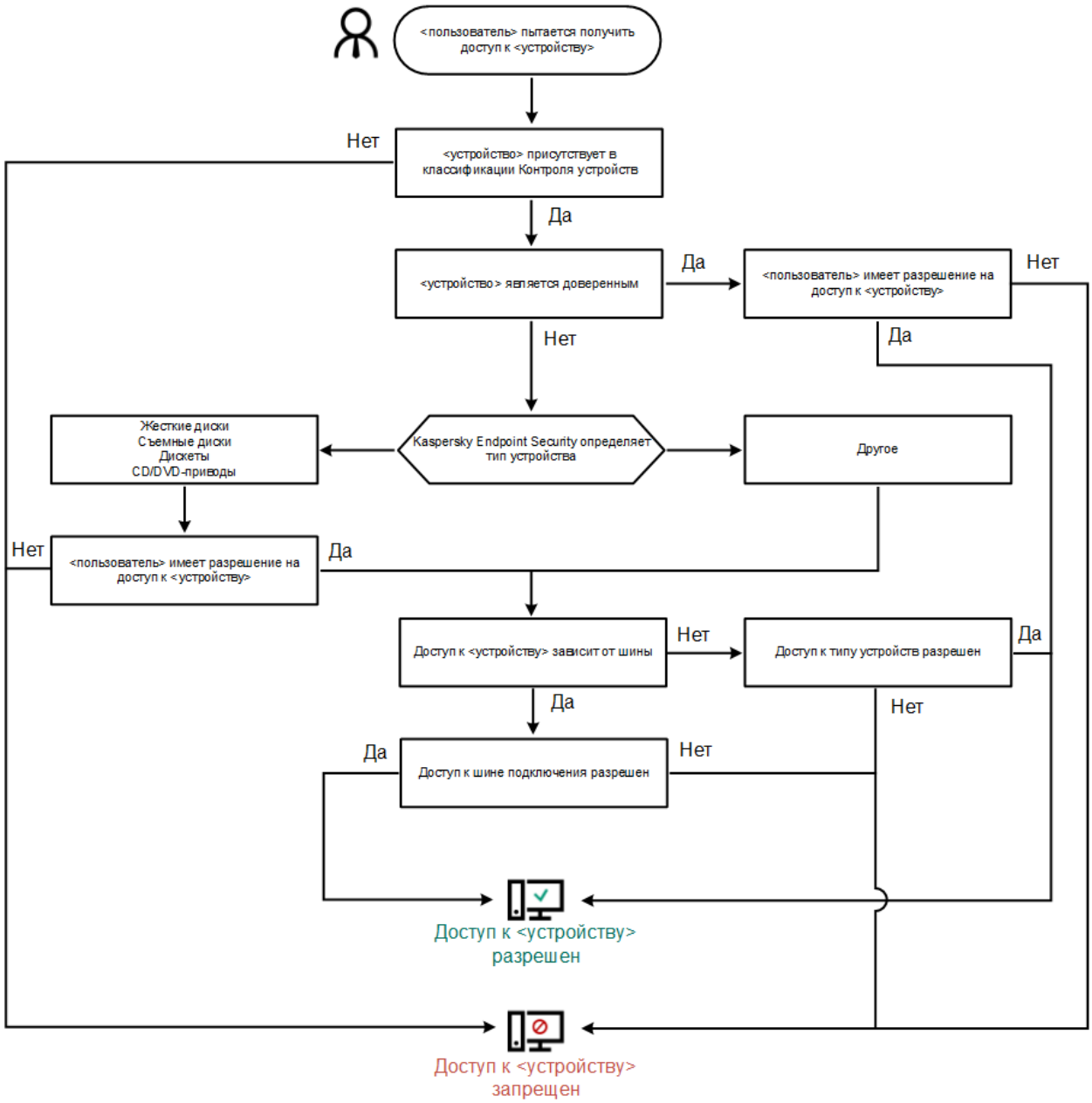


Рисунок 55. Алгоритм работы Контроля устройств

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. 229).

kaspersky

В этом разделе

Включение и выключение Контроля устройств ... 201
О правилах доступа ... 201
Изменение правила доступа к устройствам ... 203
Изменение правила доступа к шине подключения ... 206
Контроль доступа к мобильным устройствам ... 207
Контроль доступа к Bluetooth-устройствам ... 212
Контроль печати ... 214
Контроль подключения к Wi-Fi ... 218
Мониторинг использования съемных дисков ... 221
Изменение периода кеширования ... 224
Действия с доверенными устройствами ... 224
Получение доступа к заблокированному устройству ... 229
Изменение шаблонов сообщений Контроля устройств ... 234
Анти-Бриджинг ... 234

Включение и выключение Контроля устройств

По умолчанию Контроль устройств включен.

► *Чтобы включить или выключить Контроль устройств, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. Используйте переключатель **Контроль устройств**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, 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** → **Хранилище** → **Оборудование**.

О правилах доступа

Правила доступа – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам. 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 13. 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	✓	–	–	–	–
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

Правила доступа к шинам определяют только разрешение (статус ✓) или запрет (статус ⊘) на подключение устройств. Для всех шин подключения из классификации компонента Контроль устройств по умолчанию созданы правила, разрешающие доступ к шинам.

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. 166).

Изменение правила доступа к устройствам

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.

► *Чтобы изменить правило доступа к устройствам, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

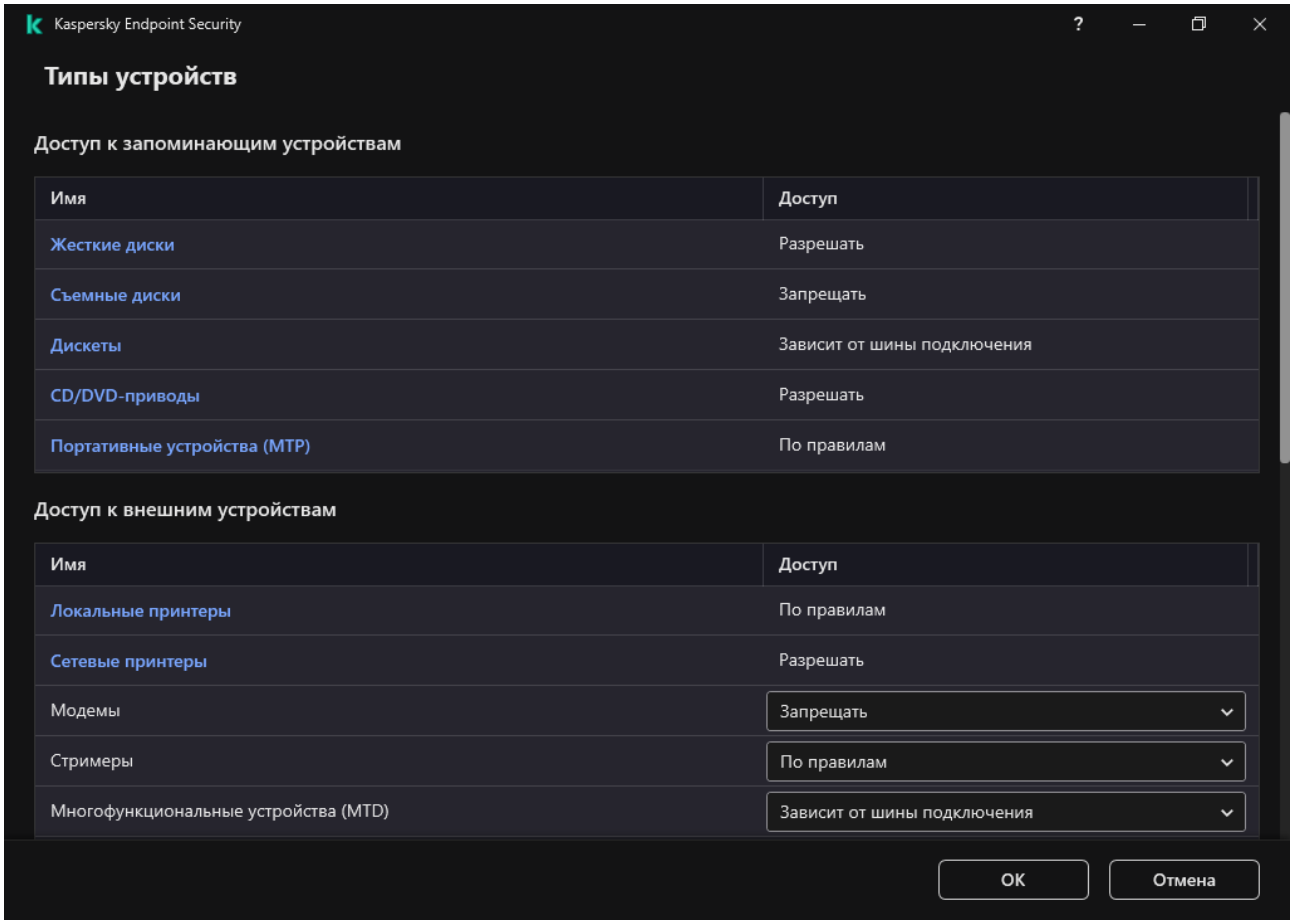


Рисунок 56. Типы устройств Контроля устройств

4. В блоке **Доступ к запоминающим устройствам** выберите правило доступа, которое хотите изменить. В блоке находятся устройства с файловой системой, для которых вы можете настроить дополнительные параметры доступа. По умолчанию правило доступа к устройствам разрешает полный доступ к типу устройств всем пользователям в любое время.

   a. В графе **Доступ** выберите доступ к устройству:

      - **Разрешать**.
      - **Запрещать**.
      - **Зависит от шины подключения**.

        Чтобы запретить или разрешить доступ к устройству, настройте доступ к шине подключения (см. раздел "Изменение правила доступа к шине подключения" на стр. 206).

      - **По правилам**.

        Этот вариант позволяет настроить права пользователей, разрешения, расписание для доступа к устройствам.

   b. В блоке **Права пользователей** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к устройствам.

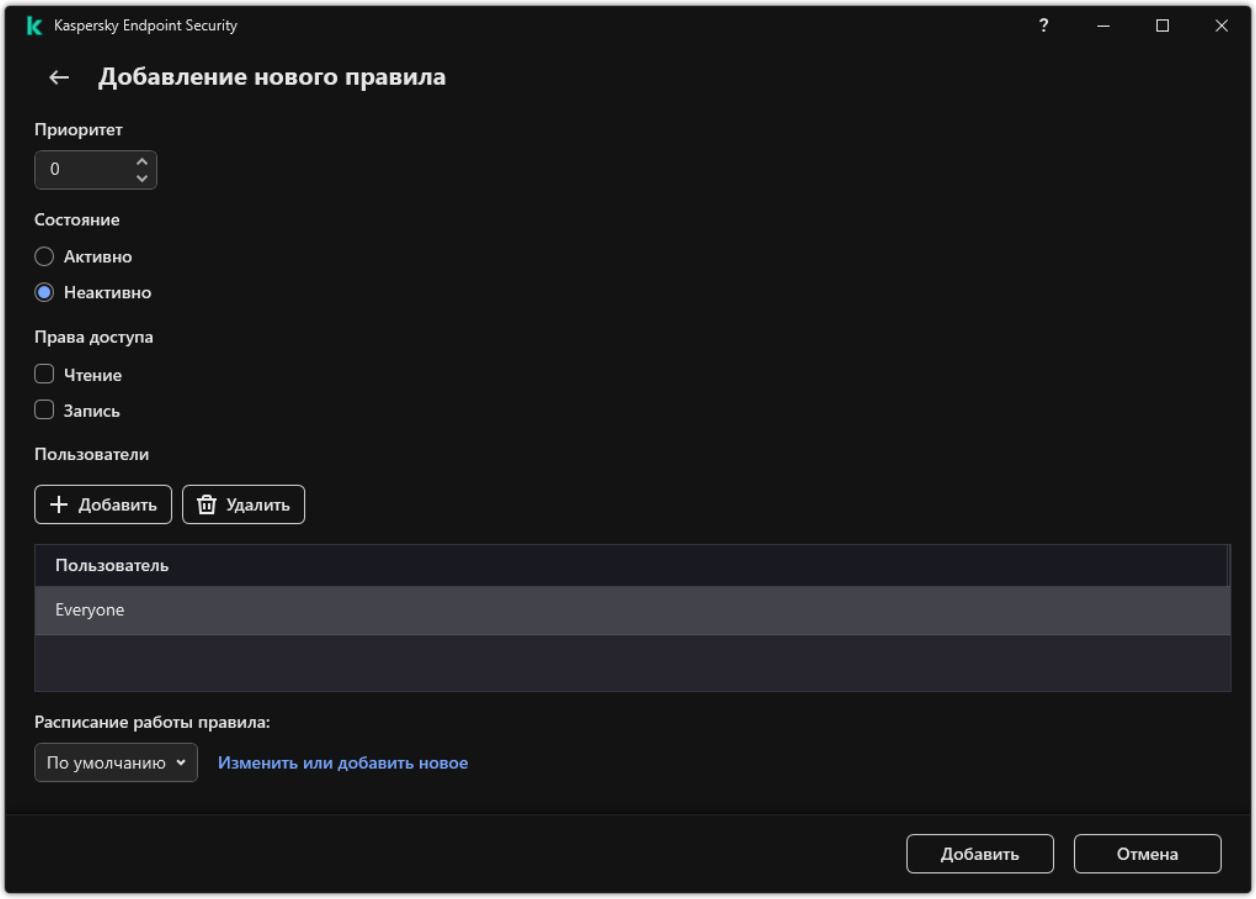


Рисунок 57. Параметры правила Контроля устройств

c. Назначьте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись) 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.

d. Установите статус правила доступа к устройствам **Включено**.

e. Настройте разрешения пользователей для доступа к устройствам: чтение, запись.

f. Выберите пользователей или группы пользователей, к которым вы хотите применить правило доступа к устройству.

g. Настройте расписание доступа к устройствам для пользователей.

h. Нажмите на кнопку **Добавить**.

5. В блоке **Доступ к внешним устройствам** выберите правило и настройте доступ: **Разрешать**, **Запрещать**, **Зависит от шины подключения**. Если требуется, настройте доступ к шине подключения (см. раздел "Изменение правила доступа к шине подключения" на стр. 206).
6. В блоке **Доступ к сетям Wi-Fi** перейдите по ссылке **Wi-Fi** и настройте доступ: **Разрешать**, **Запрещать**, **Запрещать с исключениями**. Если требуется, добавьте сети Wi-Fi в список доверенных (см. раздел "Контроль подключения к Wi-Fi" на стр. 218).

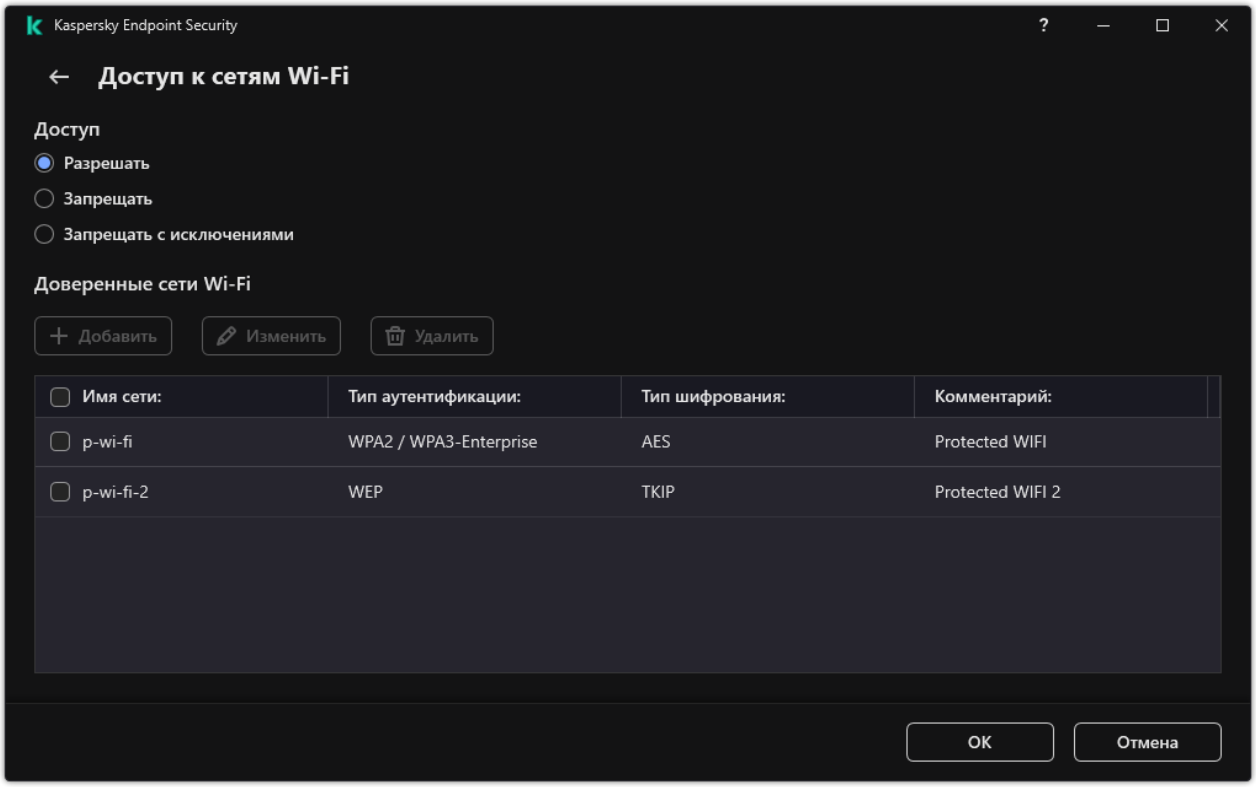


Рисунок 58. Настройки доступа к Wi-Fi

7. Сохраните внесенные изменения.

Изменение правила доступа к шине подключения

► *Чтобы изменить правило доступа к шине подключения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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 "Изменение правила доступа к устройствам" на стр. 203):

- **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 (см. раздел "Действия с доверенными устройствами" на стр. 224). 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 "Изменение правила доступа к шине подключения" на стр. 206) (**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. 38) 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.

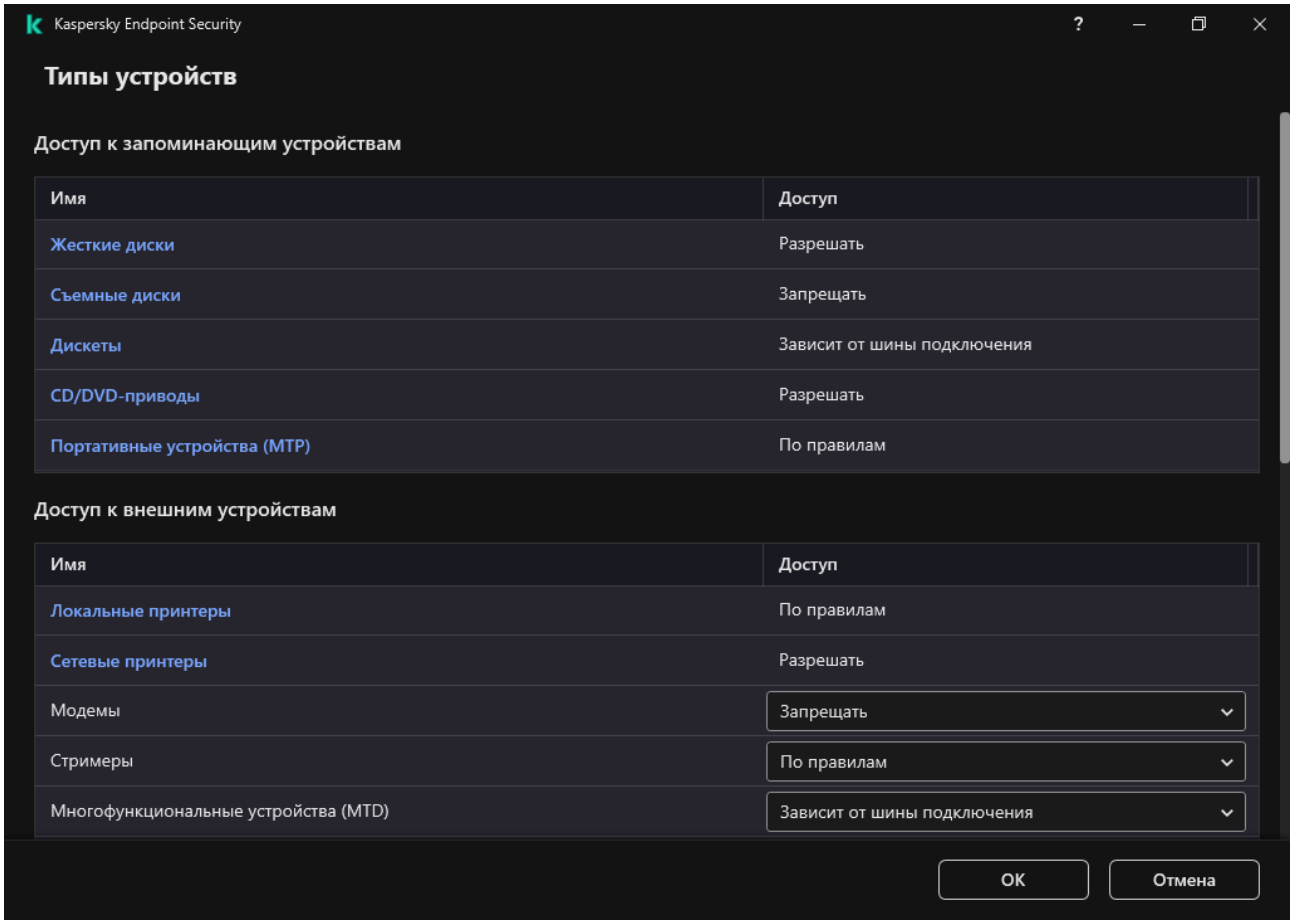


Рисунок 59. Типы устройств Контроля устройств

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.

   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

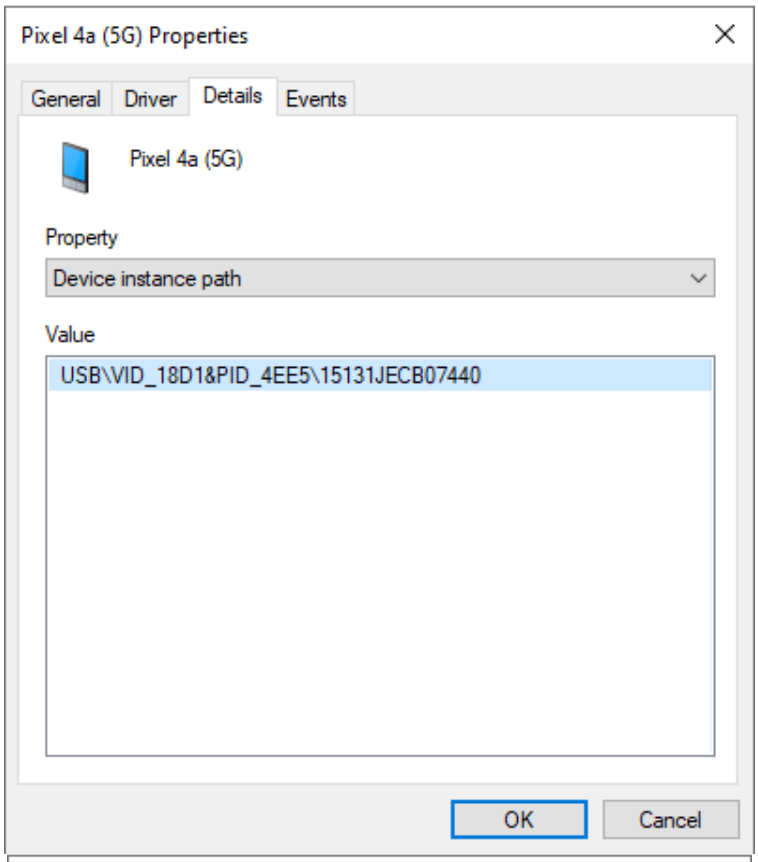
Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

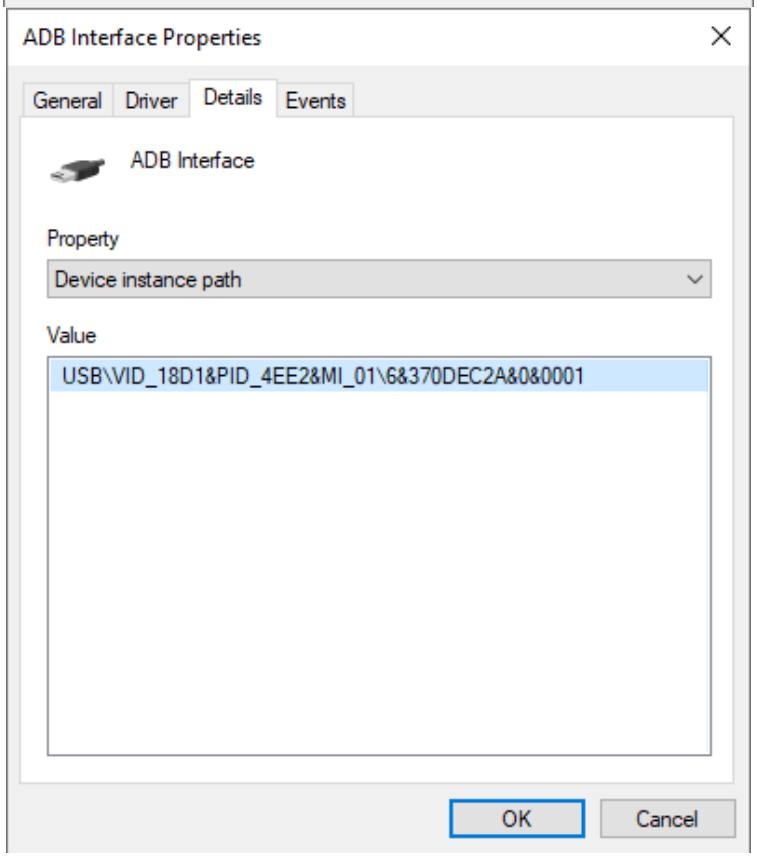
Добавление доверенного мобильного устройства (см. раздел "Действия с доверенными устройствами" на стр. 224) ничем не отличается от добавления других типов доверенных устройств. Вы можете добавить мобильное устройство по идентификатору или модели устройства.

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.


Pixel 4a (5G) Properties
General
Driver
Details
Events
Pixel 4a (5G)
Property
Device instance path
Value
USB\VID_18D1&PID_4EE5\15131JECB07440
OK
Cancel


ADB Interface Properties
General
Driver
Details
Events
ADB Interface
Property
Device instance path
Value
USB\VID_18D1&PID_4EE2&MI_01\6&370DEC2A&0&0001
OK
Cancel

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 Bluetooth-устройства к компьютеру Kaspersky Endpoint Security определяет класс устройства (англ. Class of Device – COD). Если доступ к классу устройств разрешен, приложение предоставляет доступ к подключенному устройству.

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.

Доступ к Bluetooth-устройствам

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. Приложение разрешает доступ только к доверенным Bluetooth-устройствам (см. раздел "Действия с доверенными устройствами" на стр. 224). Также 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.

  Вы можете разрешить подключение устройств ввода только в интерфейсе приложения или в Web Console. Разрешить подключение устройств ввода в Консоли администрирования (MMC) невозможно.

Доверенные Bluetooth-устройства

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Добавление доверенных Bluetooth-устройств (см. раздел "Действия с доверенными устройствами" на стр. 224) ничем не отличается от добавления других типов доверенных устройств. Вы можете добавить Bluetooth-устройства по идентификатору или модели устройства.

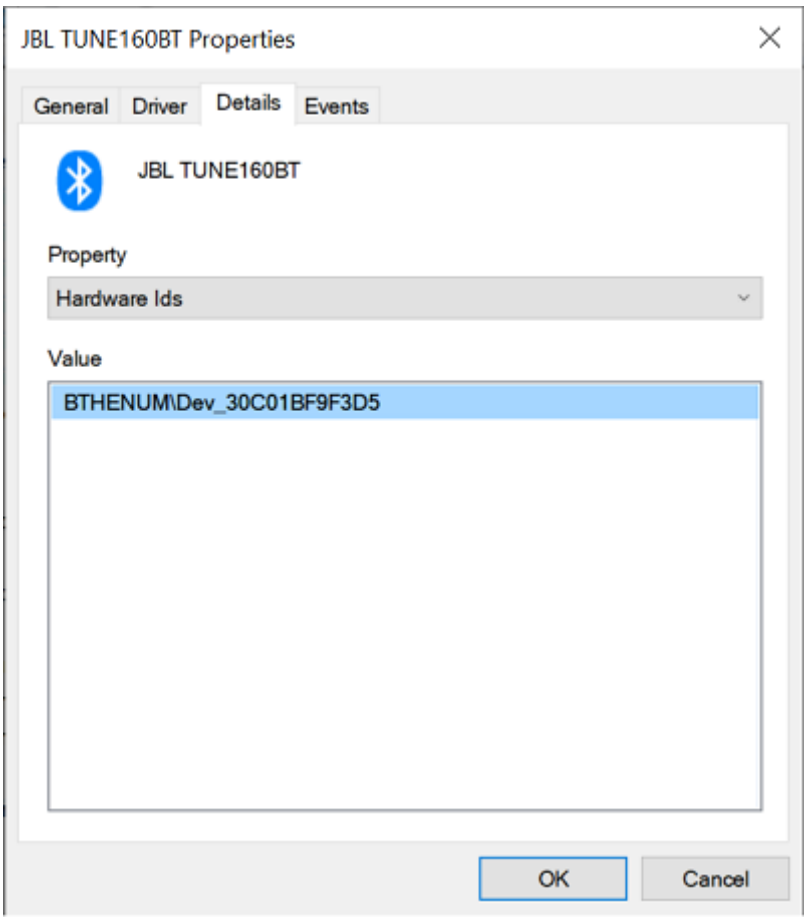
Управление доверенными Bluetooth-устройствами имеет следующие ограничения:

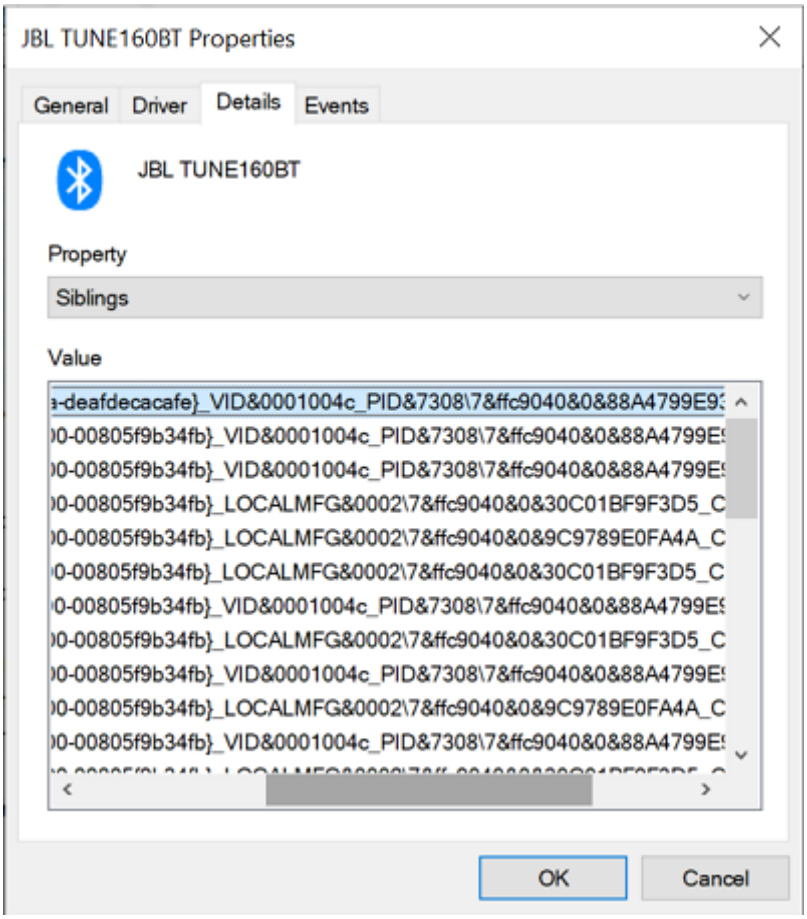
- Невозможно выбрать пользователей или группу пользователей, для которых Bluetooth-устройство будет доверенным. Если устройство в списке доверенных, то доступ разрешен для всех пользователей.

- Так как операционная система может определять Bluetooth-устройство как несколько устройств разных типов, для доступа к устройству может потребоваться добавить несколько записей в список доверенных устройств. Также Kaspersky Endpoint Security контролирует Bluetooth-адаптер, через который подключено устройство, как отдельное устройство. Bluetooth-адаптер также нужно добавить в список доверенных устройств.
- Для предоставления временного доступа к заблокированному Bluetooth-устройству (см. раздел "Получение доступа к заблокированному устройству" на стр. 229) может потребоваться отправить несколько запросов для разных типов устройств.

Для добавления доверенного Bluetooth-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). Пример идентификатора Bluetooth-устройства: `30C01BF9F3D5`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств. Также вы можете использовать маски.

Для добавления доверенного Bluetooth-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&0001004c_PID&7308`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.





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 запретить подключение всех типов устройств к шинам COM и LPT (см. раздел "Изменение правила доступа к шине подключения" на стр. 206). Принтеры, подключенные через USB, приложение контролирует на двух уровнях: тип устройств (локальные принтеры) и шина подключения (USB). Таким образом, вы можете разрешить подключение через USB всех типов устройств кроме локальных принтеров.

Вы можете выбрать один следующих режимов доступа к локальным принтерам через USB (см. раздел "Изменение правила доступа к устройствам" на стр. 203):

- **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 (см. раздел "Действия с доверенными устройствами" на стр. 224).
- **Зависит от шины подключения** . Kaspersky Endpoint Security ограничивает доступ к локальным принтерам в соответствии со статусом подключения к шине USB (см. раздел "Изменение правила доступа к шине подключения" на стр. 206) (**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 "Изменение правила доступа к устройствам" на стр. 203):

- **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 (см. раздел "Действия с доверенными устройствами" на стр. 224).
- **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. 38) 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.

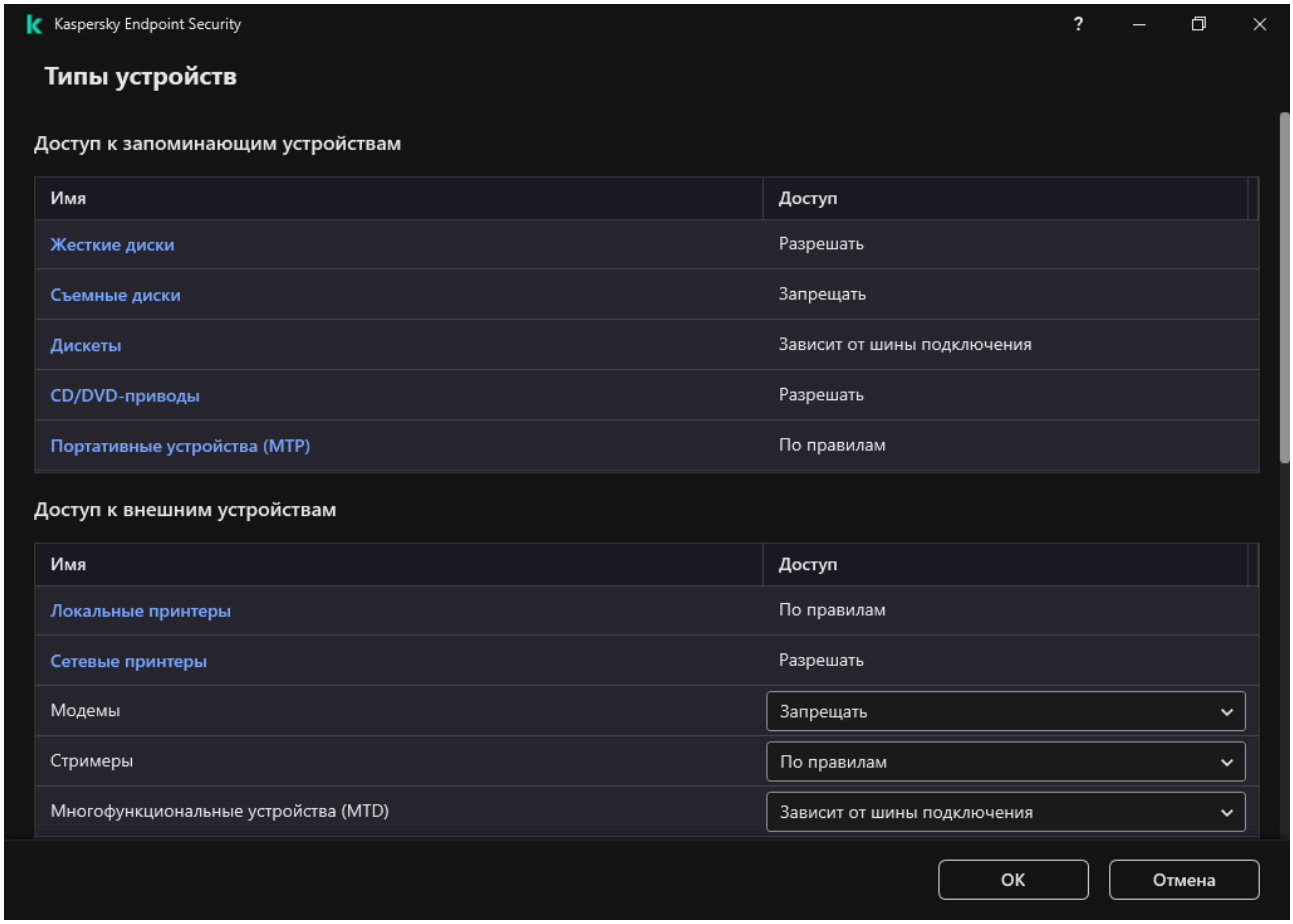


Рисунок 60. Типы устройств Контроля устройств

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.

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 (см. раздел "Действия с доверенными устройствами" на стр. 224) 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.

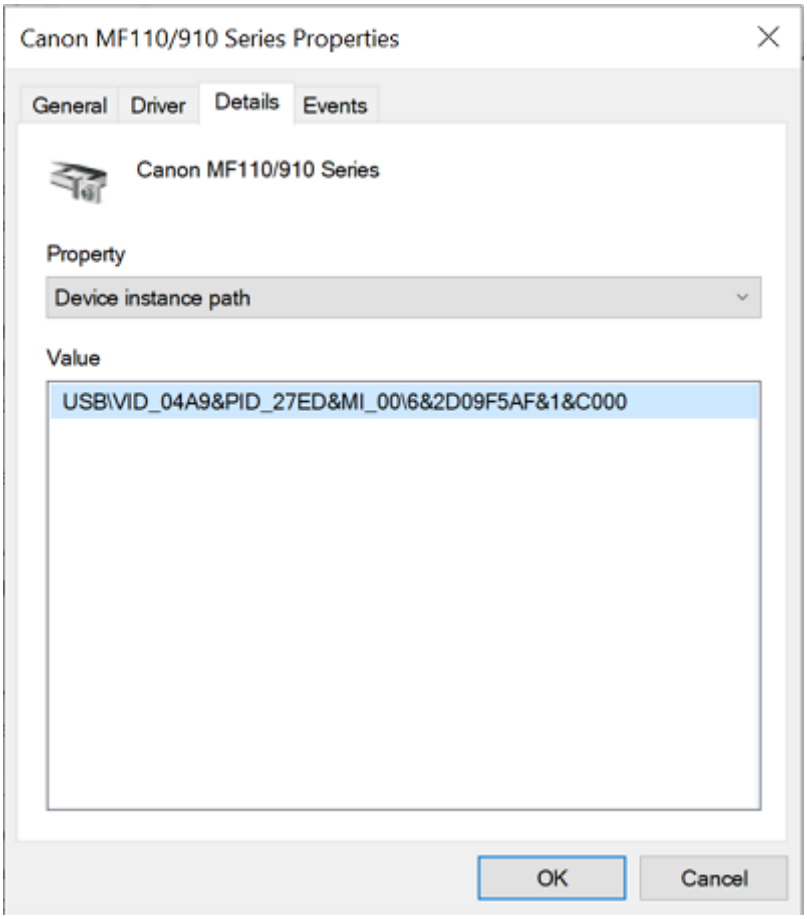


Рисунок 61. Идентификатор устройств в Диспетчере устройств

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.

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.

Как ограничить подключение к Wi-Fi в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

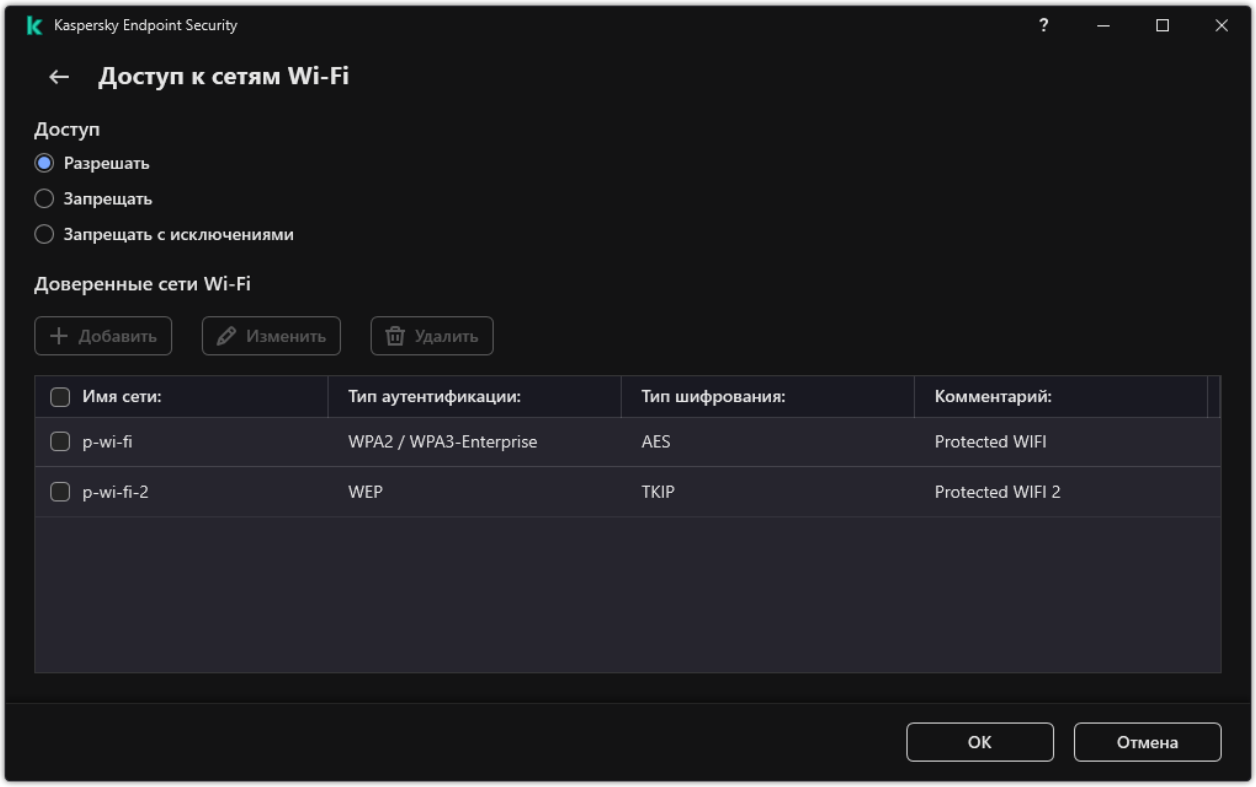


Рисунок 62. Настройки доступа к Wi-Fi

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.

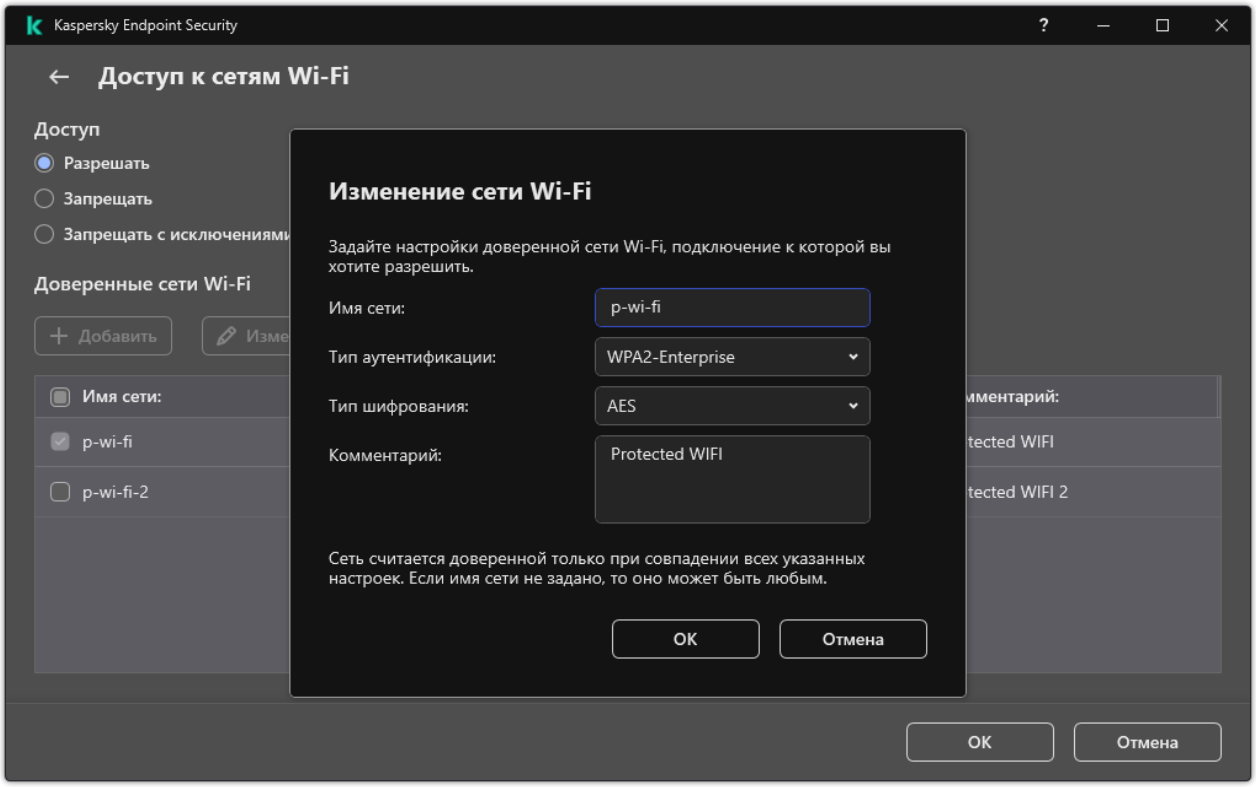


Рисунок 63. Параметры доверенной сети Wi-Fi

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).

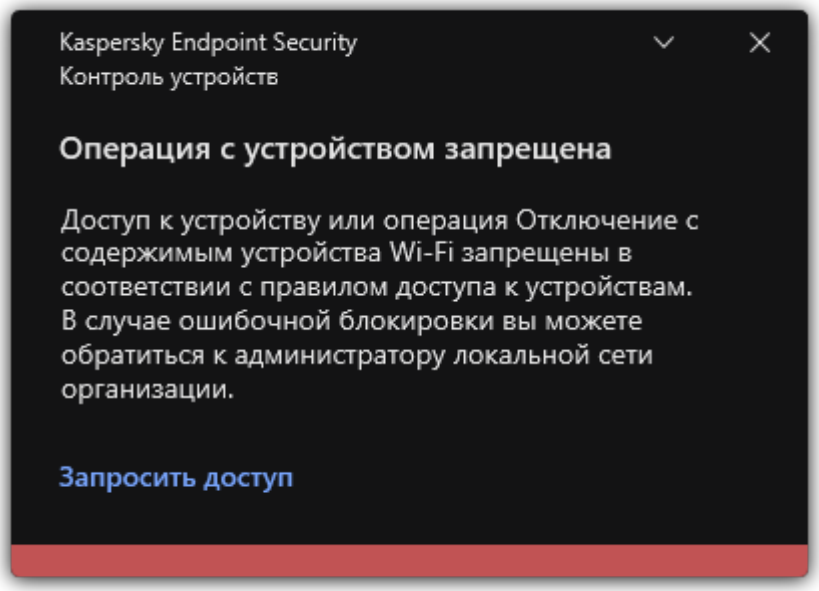


Рисунок 64. Уведомление Контроля устройств

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. 300) для компонента Контроль устройств. События имеют уровень важности *Информационное*.

► *Чтобы включить мониторинг использования съемных дисков, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

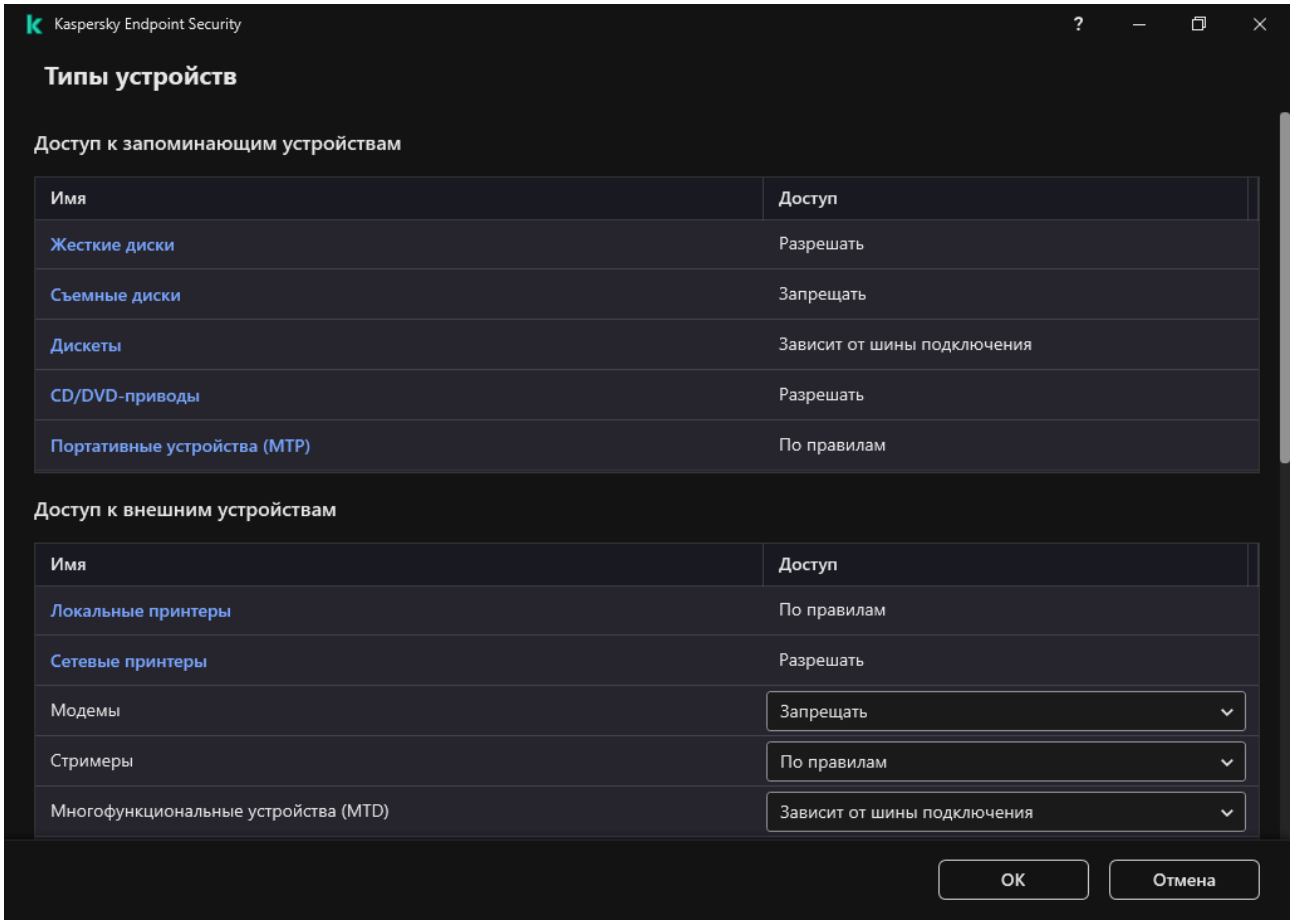


Рисунок 65. Типы устройств Контроля устройств

4. В блоке **Доступ к запоминающим устройствам** выберите элемент **Съемные диски**.
5. В открывшемся окне перейдите на закладку **Запись событий в журнал**.

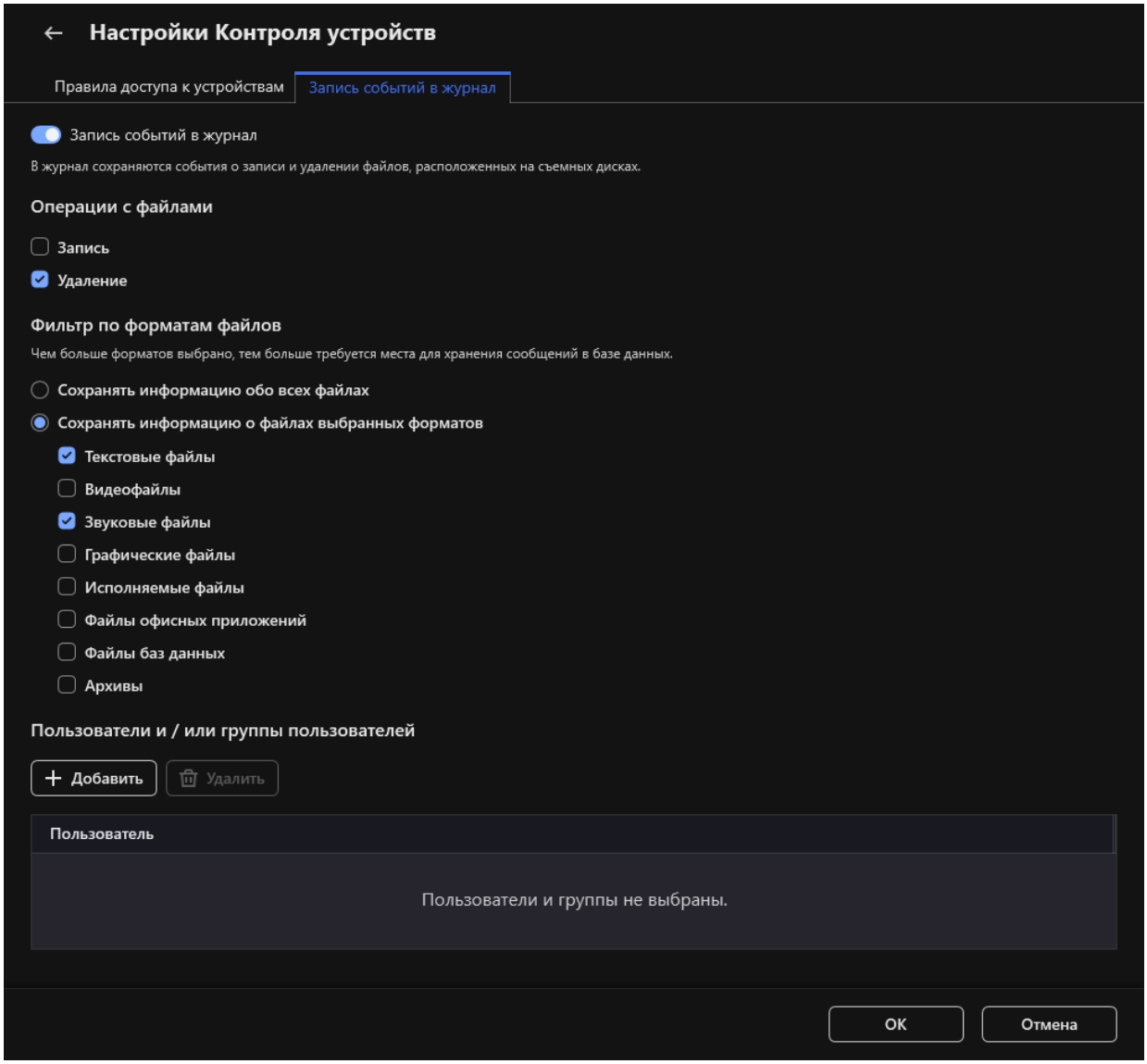


Рисунок 66. Параметры мониторинга использования съемных дисков

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. 300) 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. 311). 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.

Действия с доверенными устройствами

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.

Например, если в вашей организации запрещено использование съемных дисков, но администраторы используют съемные диски в своей работе, вы можете разрешить использование съемных дисков только для группы администраторов. Для этого необходимо добавить съемные диски в список доверенных и настроить права доступа пользователей.

Не рекомендуется добавлять более 1000 доверенных устройств, поскольку это может привести к нестабильности системы.

Kaspersky Endpoint Security позволяет добавить устройство в список доверенных следующими способами:

- Если в вашей организации не развернуто решение Kaspersky Security Center, вы можете подключить устройство к компьютеру и добавить его в список доверенных в параметрах приложения (см. раздел "Добавление устройства в список доверенных из интерфейса приложения" на стр. 225). Чтобы распространить список доверенных устройств на все компьютеры организации, вы можете включить функцию объединения списков доверенных устройств в политике или использовать процедуру экспорта / импорта (см. раздел "Экспорт и импорт списка доверенных устройств" на стр. 228).
- Если в вашей организации развернуто решение Kaspersky Security Center, вы можете обнаружить все подключенные устройства удаленно и создать список доверенных устройств в политике (см. раздел "Добавление устройства в список доверенных из Kaspersky Security Center" на стр. 226). Список доверенных устройств будет доступен на всех компьютерах, к которым применена политика.

Kaspersky Endpoint Security позволяет контролировать использование доверенных устройств (подключение и отключение). Вы можете включить запись событий в параметрах уведомлений (см. раздел "Настройка параметров журналов событий" на стр. 300) для компонента Контроль устройств. События имеют уровень важности *Информационное*.

В этом разделе

Добавление устройства в список доверенных из интерфейса приложения 225

Добавление устройства в список доверенных из Kaspersky Security Center 226

Экспорт и импорт списка доверенных устройств 228

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. 38) 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.
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.
8. Сохраните внесенные изменения.

Добавление устройства в список доверенных из Kaspersky Security Center

Kaspersky Security Center получает информацию об устройствах, если на компьютерах установлено приложение Kaspersky Endpoint Security и включен Контроль устройств (см. раздел "Включение и выключение Контроля устройств" на стр. 201). Добавить устройство в список доверенных, информации о котором в Kaspersky Security Center нет, невозможно.

Вы можете добавить устройство в список доверенных 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_*`.

► *Чтобы добавить устройства в список доверенных, выполните следующие действия:*

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 устройств**.
5. В правой части окна выберите закладку **Доверенные устройства**.
6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных устройств для всех компьютеров организации.

   Списки доверенных устройств родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные устройства родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных устройств родительской политики невозможно.
7. Нажмите на кнопку **Добавить** и выберите способ добавления устройства в список доверенных.
8. Для фильтрации устройств в раскрывающемся списке **Тип устройств** выберите тип устройств (например, **Съемные диски**).
9. В поле **Название / Модель** введите идентификатор устройства, модель (VID и PID) или маску в зависимости от выбранного способа добавления.

   > Способ добавления устройств по маске модели (VID и PID) имеет особенность. Если вы ввели маску модели, которая не соответствует ни одной модели, Kaspersky Endpoint Security проверяет идентификатор устройства (HWID) на соответствие маске. Kaspersky Endpoint Security проверяет на соответствие только часть идентификатора устройства, определяющую поставщика и тип устройства (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Если маска модели соответствует этой части идентификатора устройства, на компьютере в список доверенных устройств будут добавлены устройства удовлетворяющие маске. При этом в Kaspersky Security Center по кнопке **Обновить** отобразится пустой список устройств. Для корректного отображения списка устройств вы можете использовать способ добавления по маске идентификатора устройства.
10. Для фильтрации устройств в поле **Компьютер** введите имя компьютера или маску имени компьютера, к которому подключено устройство.

    Символ `*` заменяет любой набор символов. Символ `?` заменяет любой один символ.
11. Нажмите на кнопку **Обновить**.

    В таблице отобразится список устройств, которые удовлетворяют заданным параметрам фильтрации.

12. Установите флажки напротив названий устройств, которые вы хотите добавить в список доверенных.
13. В поле **Комментарий** введите описание причины добавления устройств в список доверенных.
14. Справа от поля **Разрешать пользователям и / или группам пользователей** нажмите на кнопку **Выбрать**.
15. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.

    По умолчанию доступ к доверенным устройствам разрешен для группы "Все".
16. Сохраните внесенные изменения.

При подключении устройства Kaspersky Endpoint Security проверяет список доверенных устройств для авторизованного пользователя. Если устройство доверенное, Kaspersky Endpoint Security разрешает доступ к устройству со всеми правами, даже если доступ к типу устройств или шине подключения запрещен. Если устройство недоверенное и доступ запрещен, вы можете запросить доступ к заблокированному устройству (см. раздел "Получение доступа к заблокированному устройству" на стр. 229).

Экспорт и импорт списка доверенных устройств

Для распространения список доверенных устройств на всех компьютеры организации вы можете использовать процедуру экспорта / импорта.

Например, если вам нужно распространить список доверенных съемных дисков, нужно выполнить следующие действия:

1. Последовательно подключите съемные диски к компьютеру.
2. В параметрах Kaspersky Endpoint Security добавьте съемные диски в список доверенных (см. раздел "Добавление устройства в список доверенных из интерфейса приложения" на стр. 225). Если требуется, настройте права доступа пользователей. Например, разрешите доступ к съемным дискам только администраторам.
3. Экспортируйте список доверенных устройств в параметрах Kaspersky Endpoint Security (см. инструкцию ниже).
4. Распространите файл с списком доверенных устройств на остальные компьютеры организации. Например, разместите файл в общей папке.
5. Импортируйте список доверенных устройств в параметрах Kaspersky Endpoint Security на остальных компьютерах организации (см. инструкцию ниже).

► *Чтобы импортировать или экспортировать список доверенных устройств, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. Для экспорта списка доверенных устройств выполните следующие действия:
   a. Выберите доверенные устройства, которые вы хотите экспортировать.
   b. Нажмите на кнопку **Экспорт**.
   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список доверенных устройств, а также выберите папку, в которой вы хотите сохранить этот файл.
   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует весь список доверенных устройств в XML-файл.
5. Для импорта списка доверенных устройств, выполните следующие действия:
   a. В раскрывающемся списке **Импорт** выберите нужное действие: **Импортировать и добавить к существующему** или **Импортировать и заменить существующий**.
   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных устройств.
   c. Откройте файл.

      Если на компьютере уже есть список доверенных устройств, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
6. Сохраните внесенные изменения.

При подключении устройства Kaspersky Endpoint Security проверяет список доверенных устройств для авторизованного пользователя. Если устройство доверенное, Kaspersky Endpoint Security разрешает доступ к устройству со всеми правами, даже если доступ к типу устройств или шине подключения запрещен.

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 (см. раздел "Действия с доверенными устройствами" на стр. 224) или временно выключить Контроль устройств (см. раздел "Включение и выключение Контроля устройств" на стр. 201).

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. 231).
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 (см. раздел "Добавление устройства в список доверенных из Kaspersky Security Center" на стр. 226).

   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.

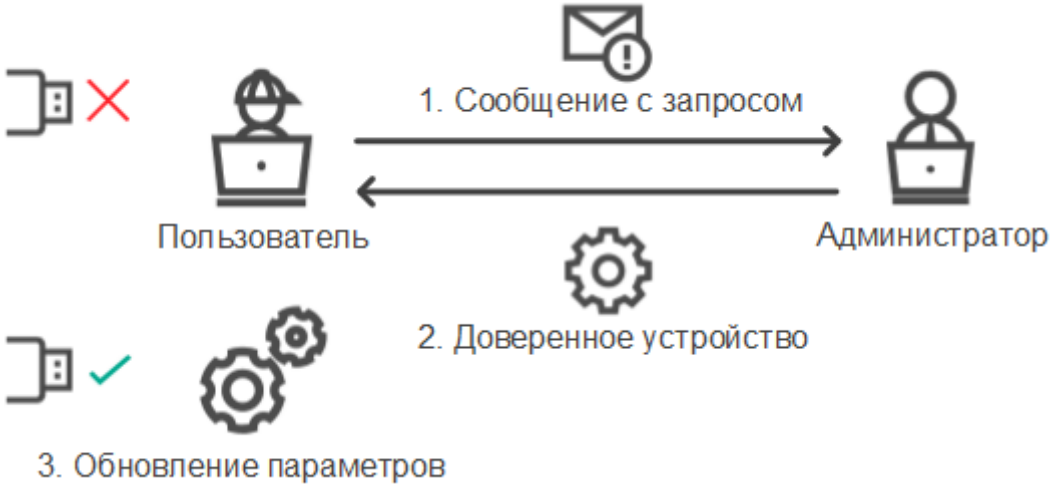


Рисунок 67. Схема предоставления доступа к устройству в онлайн-режиме

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 (см. раздел "Действия с доверенными устройствами" на стр. 224) 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.

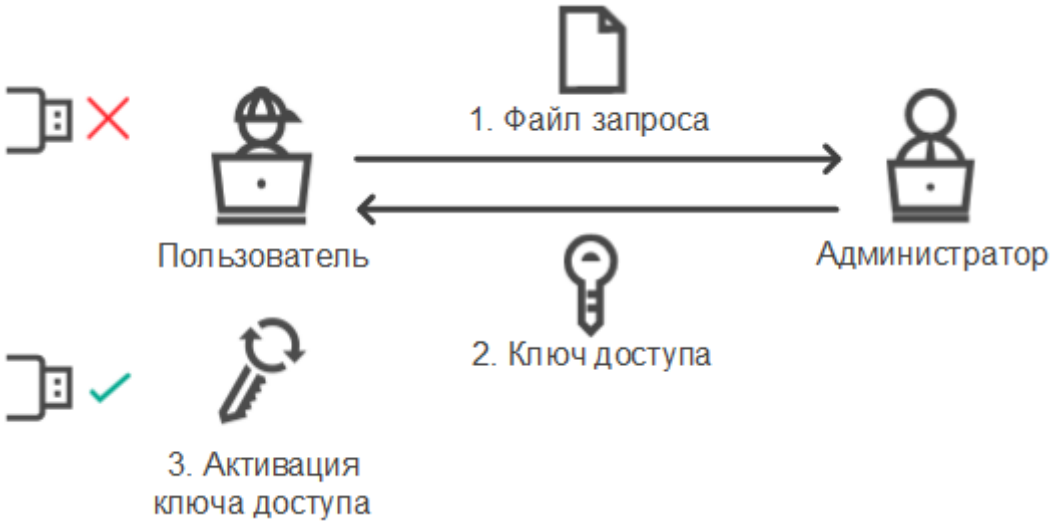


Рисунок 68. Схема предоставления доступа к устройству в офлайн-режиме

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**.

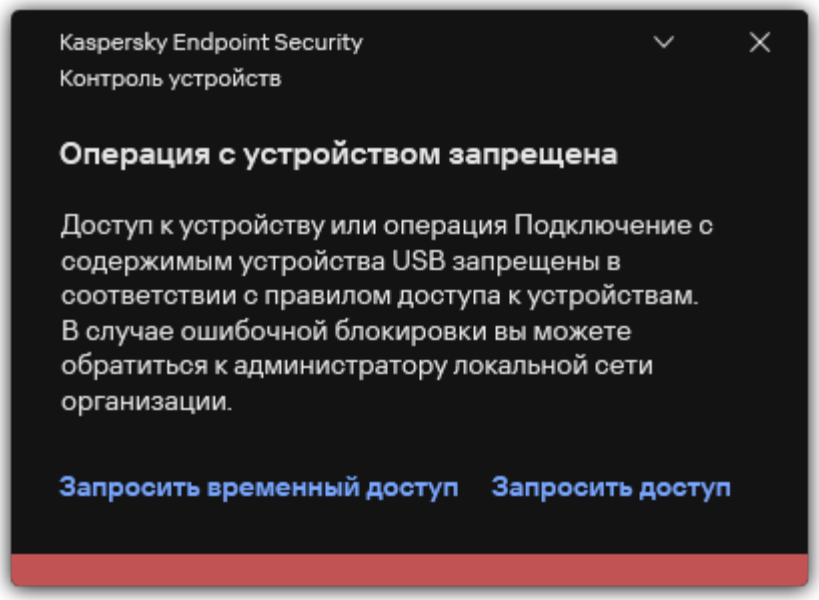


Рисунок 69. Уведомление Контроля устройств

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 (см. раздел "Действия с доверенными устройствами" на стр. 224). 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.

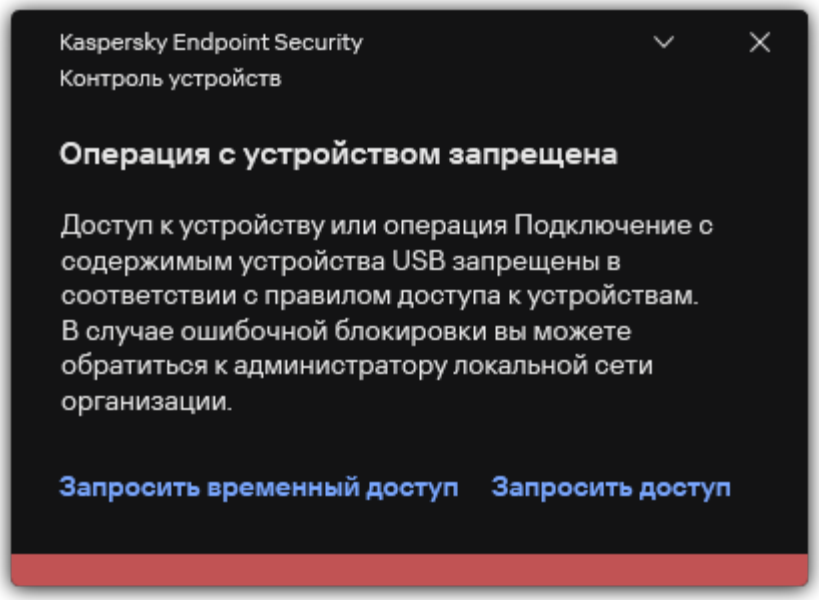


Рисунок 70. Уведомление Контроля устройств

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. 38) 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 **OK**.

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 (см. раздел "Действия с доверенными устройствами" на стр. 224).

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. 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 сообщения о блокировке доступа к устройству или запрете операции над содержимым устройства, а также для сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► *Чтобы изменить шаблоны сообщений Контроля устройств, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Шаблоны сообщений** настройте шаблоны сообщений Контроля устройств:
   - **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. 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.
4. Сохраните внесенные изменения.

См. также:

Изменение шаблонов сообщений Веб-Контроля 258

Изменение шаблонов сообщений Контроля приложений 196

Изменение шаблонов сообщений Адаптивного контроля аномалий 245

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 235

Изменение статуса правила установки соединений 235

Изменение приоритета правила установки соединений 236

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. 38) 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. 38) 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. 38) 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.

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. 244).

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 "Просмотр отчетов Адаптивного контроля аномалий" на стр. 245) и в хранилище **Срабатывание правил в состоянии Интеллектуальное обучение**.

2. Анализ отчета о срабатывании правил.

   Администратор анализирует отчет о срабатываниях правил (см. раздел "Просмотр отчетов Адаптивного контроля аномалий" на стр. 245) или содержание хранилища **Срабатывание правил в состоянии 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. Настройка Адаптивного контроля аномалий 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 **Срабатывание правил в состоянии Интеллектуальное обучение**. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища **Срабатывание правил в состоянии Интеллектуальное обучение**.

При попытке вредоносного приложения выполнить действие, Kaspersky Endpoint Security заблокирует действие и покажет уведомление (см. рис. ниже).

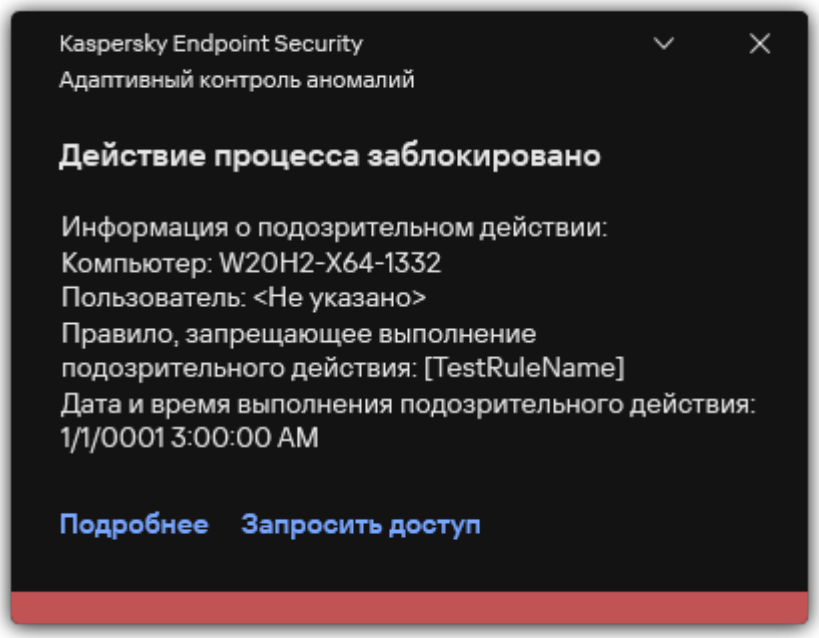


Рисунок 71. Уведомление Адаптивного контроля аномалий

Алгоритм работы Адаптивного контроля аномалий

Kaspersky Endpoint Security принимает решение о выполнении действия, связанного с правилом, по следующему алгоритму (см. рис. ниже).

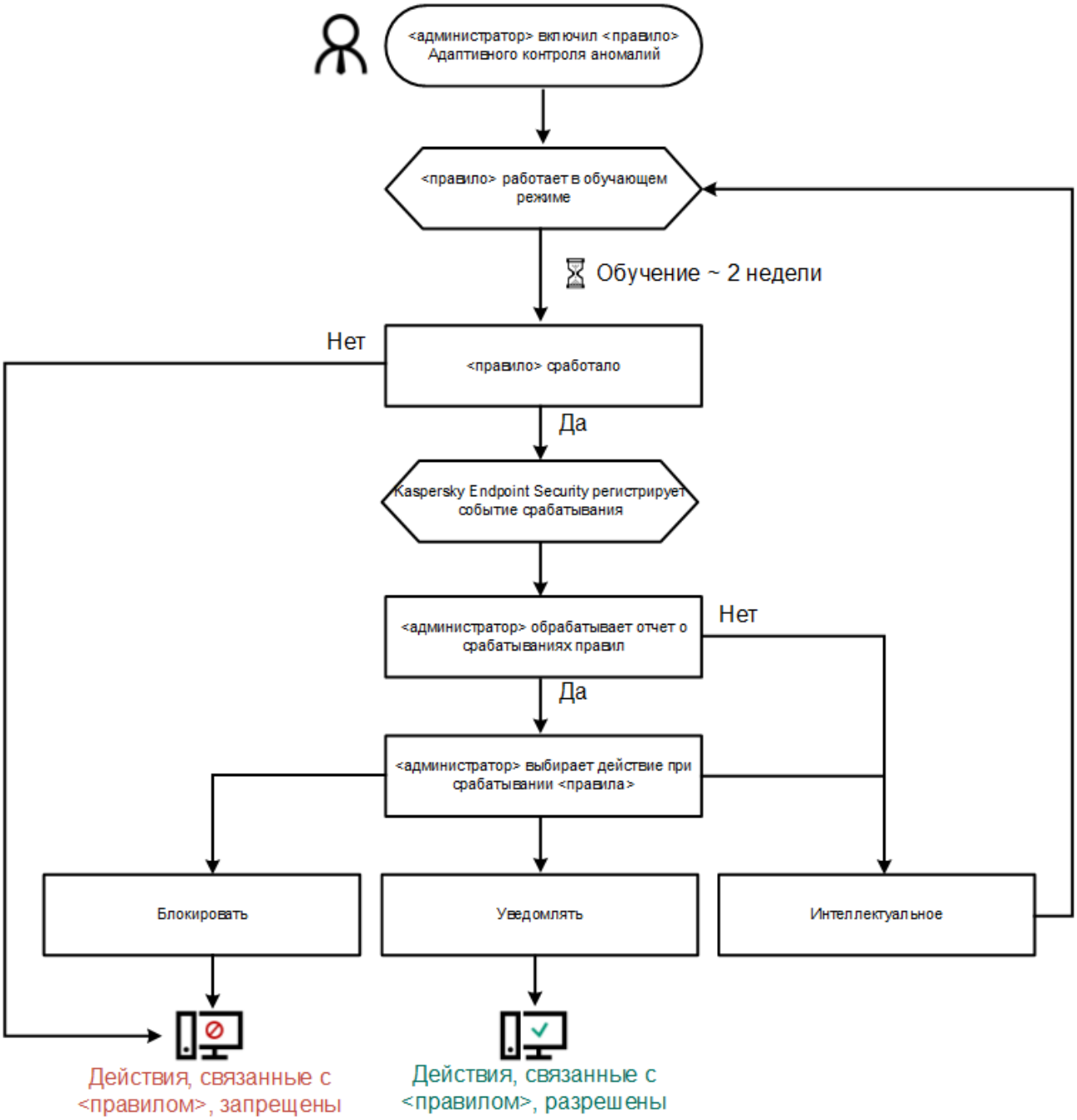


Рисунок 72. Алгоритм работы Адаптивного контроля аномалий

kaspersky

В этом разделе

Включение и выключение Адаптивного контроля аномалий ... 240

Включение и выключение правила Адаптивного контроля аномалий ... 241

Изменение действия при срабатывании правила Адаптивного контроля аномалий ... 241

Создание исключения для правила Адаптивного контроля аномалий ... 242

Экспорт и импорт исключений для правил Адаптивного контроля аномалий ... 243

Применение обновлений для правил Адаптивного контроля аномалий ... 244

Изменение шаблонов сообщений Адаптивного контроля аномалий ... 245

Просмотр отчетов Адаптивного контроля аномалий ... 245

Включение и выключение Адаптивного контроля аномалий

По умолчанию Адаптивный контроль аномалий включен.

► *Чтобы включить или выключить Адаптивный контроль аномалий, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. Используйте переключатель **Адаптивный контроль аномалий**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате Адаптивный контроль аномалий перейдет в обучающий режим. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил. После завершения обучения Адаптивный контроль аномалий блокирует действия, нехарактерные для компьютеров сети организации.

> Если в вашей организации начали использовать новые инструменты для работы, и Адаптивный контроль аномалий блокирует действия этих инструментов, вы можете сбросить результаты работы обучающего режима и повторить обучение. Для этого вам нужно изменить действие при срабатывании правила (см. раздел "Изменение действия при срабатывании правила Адаптивного контроля аномалий" на стр. 241) (например, установите значение **Информировать**). Затем вам нужно заново включить обучающий режим (установите значение **Интеллектуальное**).

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. 38) 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. 38) 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 **Срабатывание правил в состоянии 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 данном 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. 38) 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.

   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://<объект>`, где `<объект>` – 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://<команда>`, 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.

Экспорт и импорт исключений для правил Адаптивного контроля аномалий

► *Чтобы экспортировать или импортировать список исключений для выбранных правил, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. Для экспорта списка исключений выполните следующие действия:
   a. Выберите правила, исключения для которых вы хотите экспортировать.
   b. Нажмите на кнопку **Экспорт**.
   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.
   d. Подтвердите, что вы хотите экспортировать только выбранные исключения, или экспортируйте весь список.
   e. Сохраните файл.
5. Для импорта списка исключений, выполните следующие действия:
   a. Нажмите на кнопку **Импортировать**.
   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.
   c. Откройте файл.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
6. 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. 38) 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 сообщения о блокировке потенциально опасных действий и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► *Чтобы изменить шаблон сообщения, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.
4. Сохраните внесенные изменения.

См. также:

Изменение шаблонов сообщений Веб-Контроля 258

Изменение шаблонов сообщений Контроля устройств 234

Изменение шаблонов сообщений Контроля приложений 196

Просмотр отчетов Адаптивного контроля аномалий

► *Чтобы просмотреть отчеты Адаптивного контроля аномалий, выполните следующие действия:*

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** → **Адаптивный контроль аномалий**.

   В правой части окна отобразятся параметры компонента Адаптивный контроль аномалий.
5. Выполните одно из следующих действий:
   - Если вы хотите просмотреть отчет о параметрах правил Адаптивного контроля аномалий, нажмите на кнопку **Отчет о состоянии правил Адаптивного контроля аномалий**.
   - Если вы хотите просмотреть отчет о срабатываниях правил Адаптивного контроля аномалий, нажмите на кнопку **Отчет о срабатываниях правил Адаптивного контроля аномалий**.
6. Запустится процесс формирования отчета.

Отчет отобразится в новом окне.

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).

Kaspersky Endpoint Security контролирует только HTTP- и HTTPS-трафик.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Включение проверки защищенных соединений" на стр. 173).

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. 259).

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*.

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.

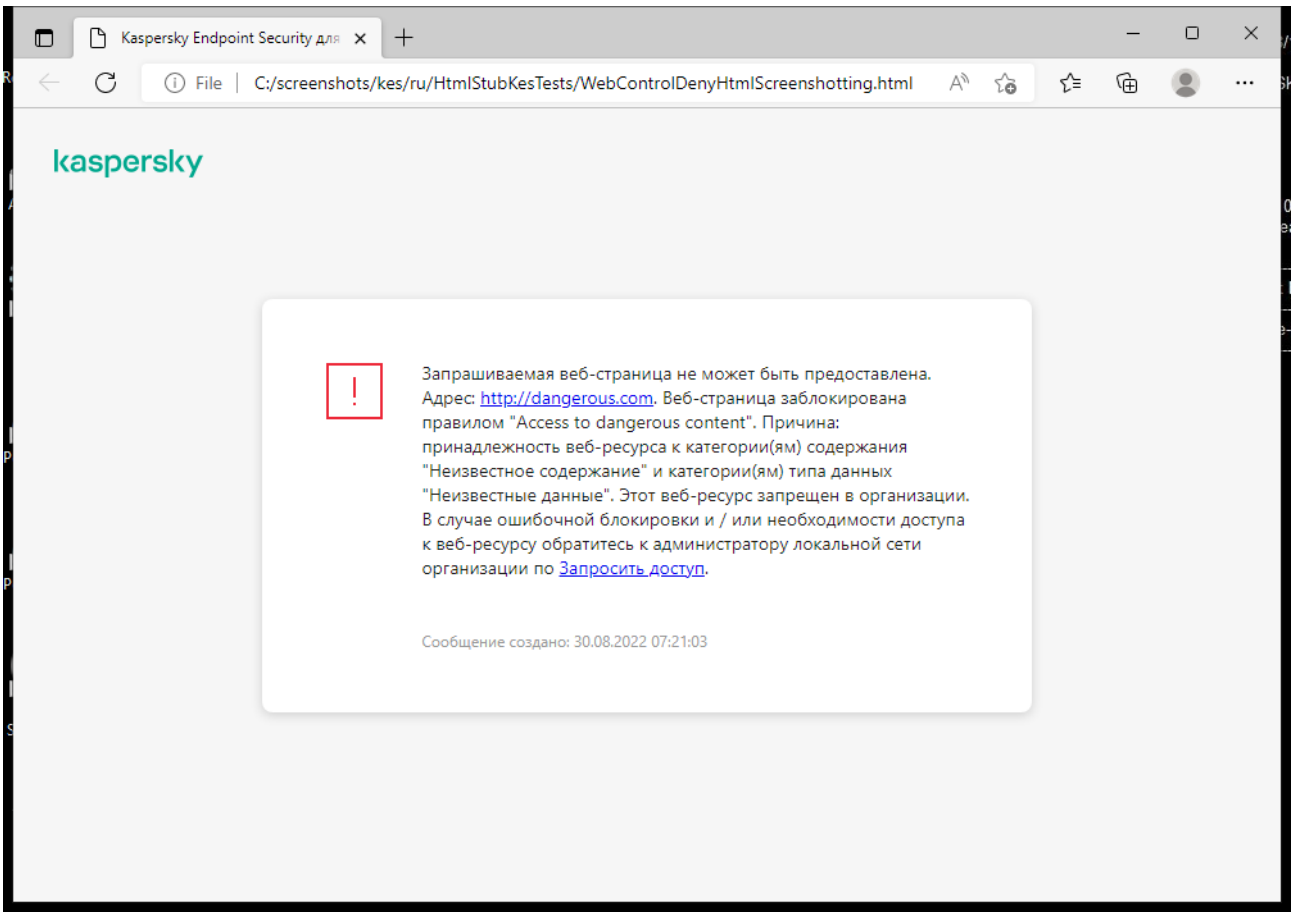
  Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

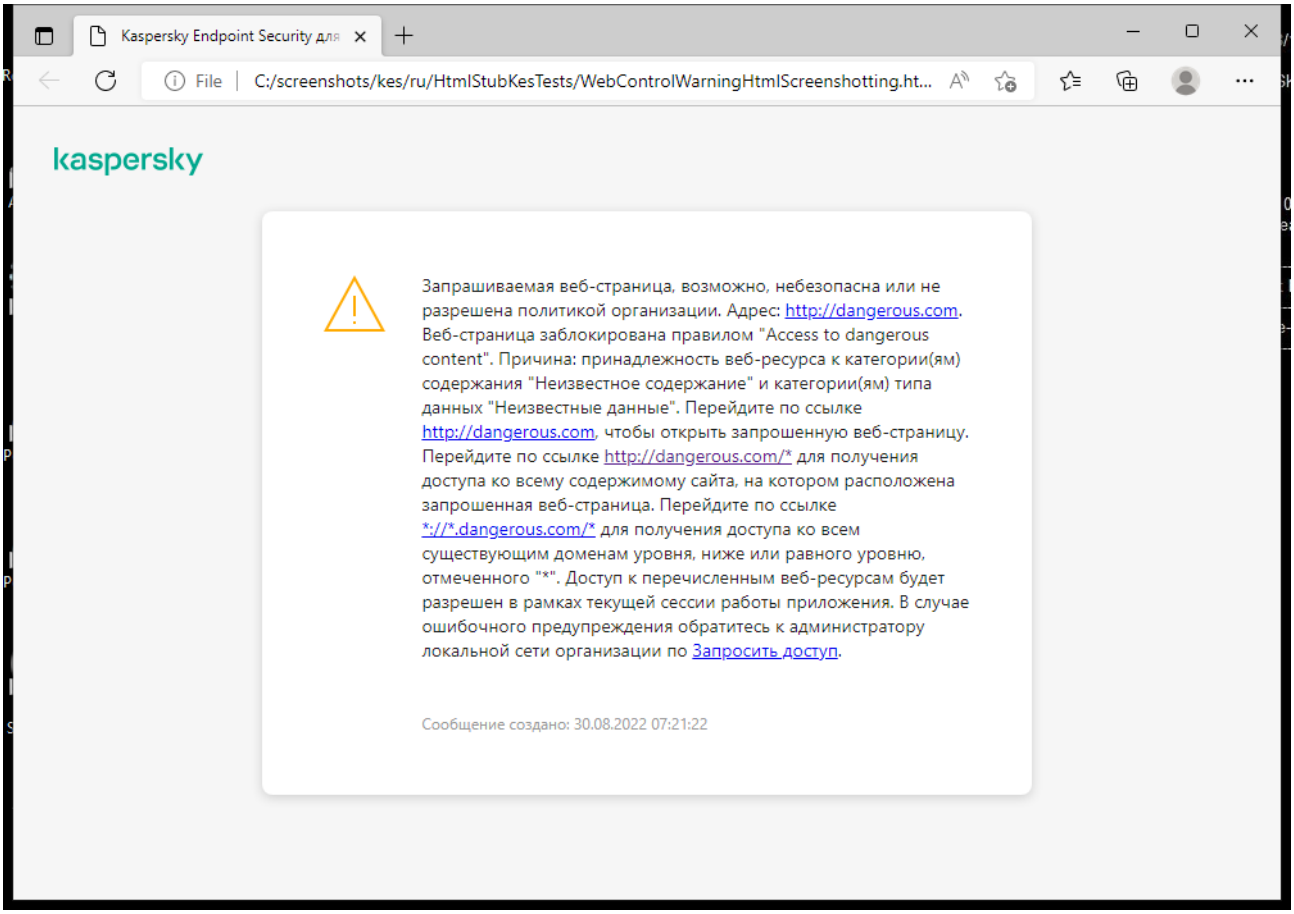
- Расписание работы правила.

  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

Включение и выключение Веб-Контроля 249
Действия с правилами доступа к веб-ресурсам 250
Экспорт и импорт списка адресов веб-ресурсов 254
Мониторинг активности пользователей в интернете 255
Изменение шаблонов сообщений Веб-Контроля 258
Правила формирования масок адресов веб-ресурсов 259

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен.

► *Чтобы включить или выключить Веб-Контроль, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.

3. Используйте переключатель **Веб-Контроль**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Действия с правилами доступа к веб-ресурсам

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. Предустановлены два правила:

- Правило "Сценарии и таблицы стилей", которое разрешает всем пользователям в любое время доступ к веб-ресурсам, адреса которых содержат названия файлов с расширением css, js, vbs. Например: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.
- *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.

kaspersky

В этом разделе

Добавление правила доступа к веб-ресурсам 251

Назначение приоритета правилам доступа к веб-ресурсам 253

Включение и выключение правила доступа к веб-ресурсам 253

Проверка работы правил доступа к веб-ресурсам 253

Добавление правила доступа к веб-ресурсам

► *Чтобы добавить или изменить правило доступа к веб-ресурсам, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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 (см. раздел "Включение и выключение правила доступа к веб-ресурсам" на стр. 253) с помощью переключателя.
7. В блоке **Действие** выберите нужный вариант:
   - **Разрешать**. Если выбрано это значение, то Kaspersky Endpoint Security разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Запрещать**. Если выбрано это значение, то Kaspersky Endpoint Security запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Предупреждать**. Если выбрано это значение, то при попытке доступа к веб-ресурсам, удовлетворяющим правилу, Kaspersky Endpoint Security 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 **Адреса** выберите нужный фильтр по адресам веб-ресурсов:

- **Ко всем адресам**. Веб-Контроль не фильтрует веб-ресурсы по адресам.
- **К отдельным адресам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Для создания список адресов веб-ресурсов выполните следующие действия:

a. Нажмите на кнопку **Добавить адрес** или **Добавить группу адресов**.

b. В открывшемся окне сформируйте список адресов веб-ресурсов. Вы можете ввести веб-адрес или использовать маски (см. раздел «Правила формирования масок адресов веб-ресурсов» на стр. 259). Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла (см. раздел «Экспорт и импорт списка адресов веб-ресурсов» на стр. 254).

c. Вернитесь в окно настройки правила доступа к веб-ресурсам.

Если Проверка защищенных соединений отключена (см. раздел "Проверка защищенных соединений" на стр. 173), для протокола HTTPS доступна фильтрация только по имени сервера.

10. 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 веб-ресурсы только для отдельных пользователей. 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.

11. 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.

12. Сохраните внесенные изменения.

Назначение приоритета правилам доступа к веб-ресурсам

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.

Вы можете назначить приоритет каждому правилу из списка правил, расположив их в определенном порядке.

► *Чтобы назначить правилам доступа к веб-ресурсам приоритет, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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 выберите правило, приоритет которого вы хотите изменить.
5. С помощью кнопок **Вверх** и **Вниз** переместите правило на нужную позицию в списке правил доступа к веб-ресурсам.
6. Сохраните внесенные изменения.

Включение и выключение правила доступа к веб-ресурсам

► *Чтобы включить или выключить правило доступа к веб-ресурсам, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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 выберите правило, которое вы хотите включить или выключить.
5. В графе **Состояние** выполните следующие действия:
   - Если вы хотите включить использование правила, выберите значение **Активно**.
   - Если вы хотите выключить использование правила, выберите значение **Не активно**.
6. Сохраните внесенные изменения.

Проверка работы правил доступа к веб-ресурсам

Чтобы оценить, насколько согласованы правила Веб-Контроля, вы можете проверить их работу. Для этого в рамках компонента Веб-Контроль предусмотрена функция "Диагностика правил".

► *Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

Экспорт и импорт списка адресов веб-ресурсов

Если в правиле доступа к веб-ресурсам вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл формата TXT. В дальнейшем вы можете импортировать список из этого файла, чтобы при настройке правила не создавать список адресов веб-ресурсов вручную. Возможность экспорта и импорта списка адресов веб-ресурсов может понадобиться, например, если вы создаете правила со сходными параметрами.

► *Чтобы импортировать или экспортировать список адресов веб-ресурсов в файл, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. Выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать или импортировать.
5. Для экспорта списка доверенных веб-ресурсов в блоке **Адреса** выполните следующие действия:
   a. Выберите адреса, которые вы хотите экспортировать.

      Если вы не выбрали ни одного адреса, Kaspersky Endpoint Security экспортирует все адреса.
   b. Нажмите на кнопку **Экспорт**.
   c. В открывшемся окне введите имя файла формата TXT, в который вы хотите экспортировать список адресов веб-ресурсов, а также выберите папку, в которой вы хотите сохранить этот файл.
   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список адресов веб-ресурсов в TXT-файл.
6. Для импорта списка веб-ресурсов в блоке **Адреса** выполните следующие действия:
   a. Нажмите на кнопку **Импорт**.

      В открывшемся окне выберите TXT-файл, из которого вы хотите импортировать список веб-ресурсов.
   b. Откройте файл.

      Если на компьютере уже есть список адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из TXT-файла.
7. Сохраните внесенные изменения.

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. 303), 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 *Критические события*);
- посещение нерекомендованного веб-сайта (статус *Предупреждения*);
- посещение разрешенного веб-сайта (статус *Информационные сообщения*).

Перед включением мониторинга активности пользователей в интернете 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. 173).

► *Чтобы внедрить в трафик скрипт взаимодействия с веб-страницами, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

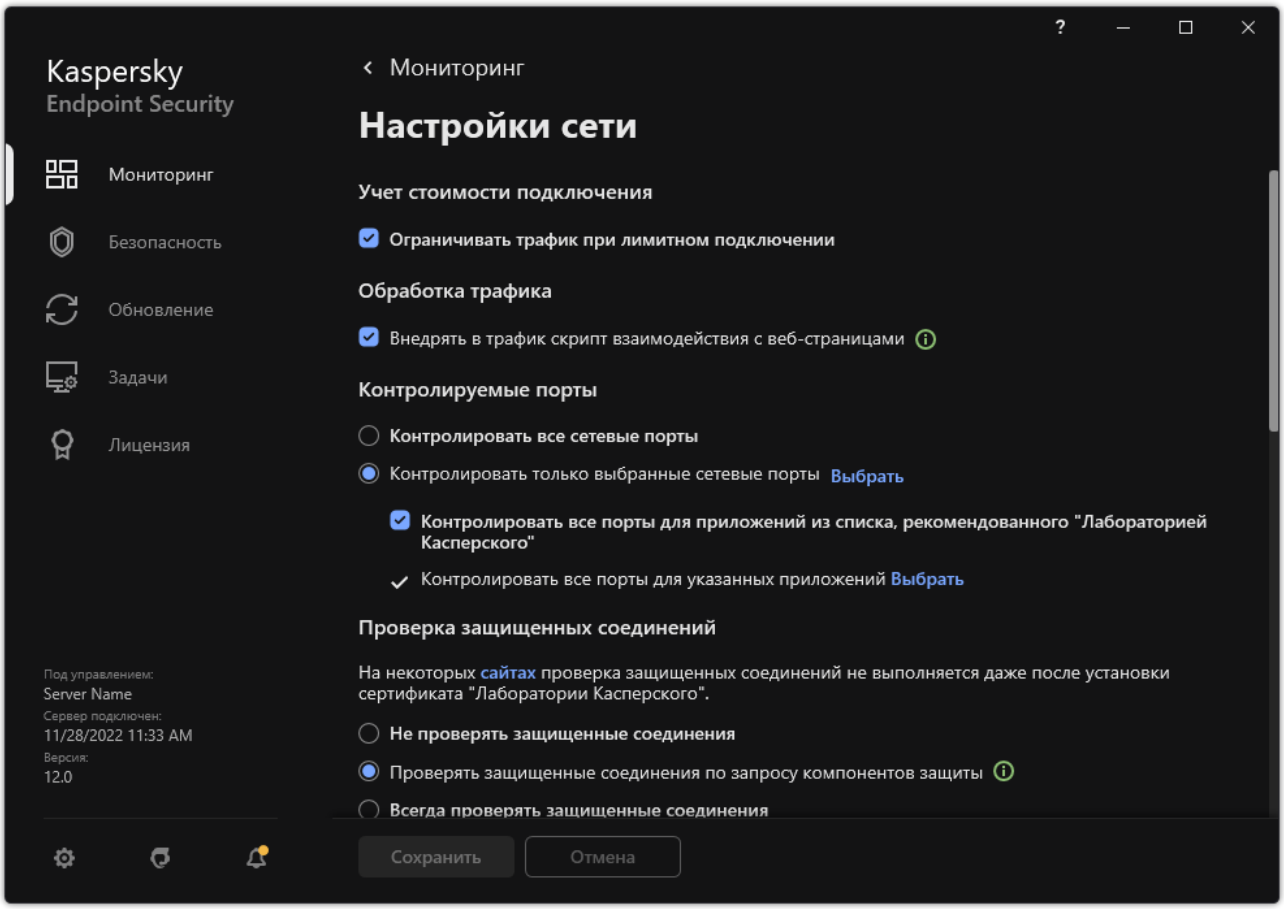


Рисунок 73. Параметры проверки защищенных соединений

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. 303).

► *Чтобы настроить запись событий Веб-Контроля на компьютере пользователя, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настройка уведомлений**.
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/14.2/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.

► *Чтобы включить запись событий посещения разрешенных веб-сайтов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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, 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. Вы можете изменять их содержание.

► *Чтобы изменить шаблон сообщений Веб-Контроля, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.
4. Сохраните внесенные изменения.

См. также:

Изменение шаблонов сообщений Контроля устройств 234
Изменение шаблонов сообщений Контроля приложений 196
Изменение шаблонов сообщений Адаптивного контроля аномалий 245

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 14. 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.
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.

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
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.

Контроль сетевых портов

Во время работы Kaspersky Endpoint Security компоненты Веб-Контроль (на стр. 247), Защита от почтовых угроз (на стр. 149), Защита от веб-угроз (на стр. 141) 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.

В этом разделе

Включение контроля всех сетевых портов 262

Формирование списка контролируемых сетевых портов 263

Формирование списка приложений, для которых контролируются все сетевые порты 264

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

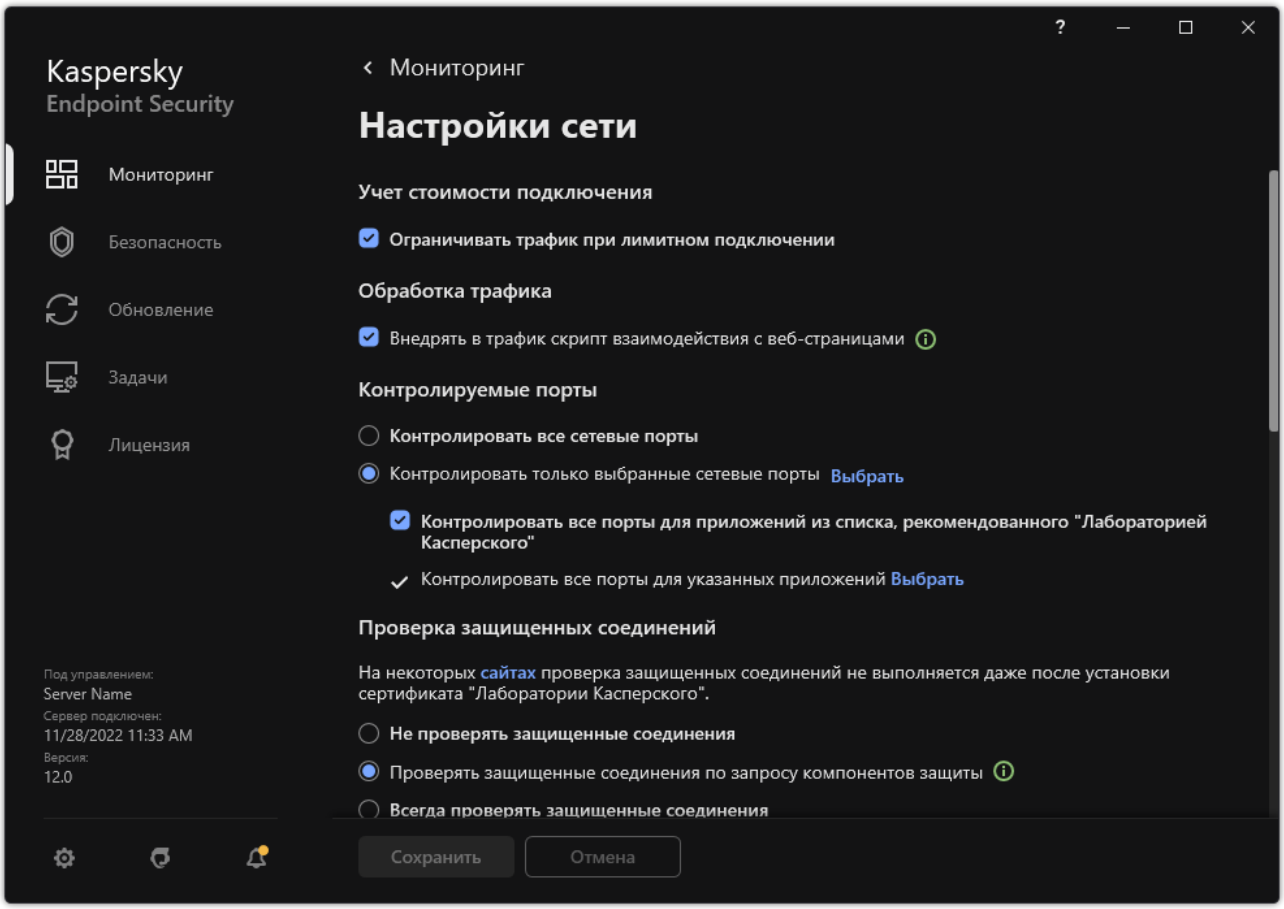


Рисунок 74. Параметры проверки защищенных соединений

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. 38) 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. 262) 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. 264).

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. 38) 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.

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. 267). Для работы предустановленных правил приложение использует эвристический анализ. Также вы можете добавить собственные правила (см. раздел "Добавление пользовательских правил" на стр. 268) (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).

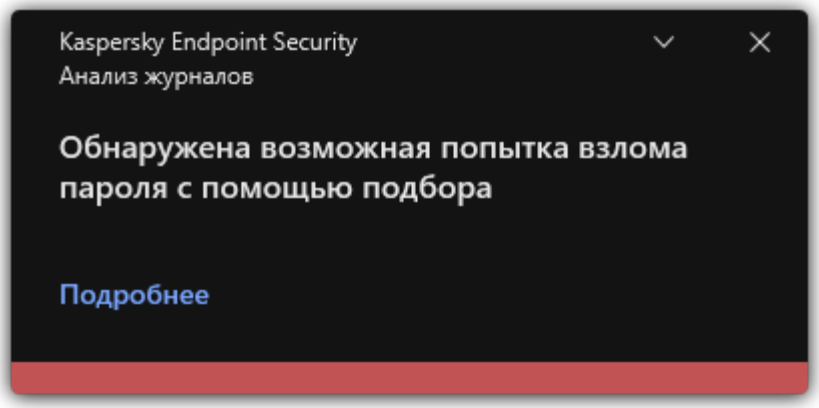


Рисунок 75. Уведомление Анализа журналов

В этом разделе

Настройка предустановленных правил 267
Добавление пользовательских правил 268

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. 38) 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).

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*.

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. 38) 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:
   - **Имя 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*).

- **Идентификаторы 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*.

Мониторинг файловых операций

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.
Мониторинг файловых операций работает только на серверах с файловой системой NTFS или ReFS.

Начиная с версии Kaspersky Endpoint Security для Windows 11.11.0 добавлена поддержка компонента Мониторинг файловых операций. Мониторинг файловых операций обнаруживает изменения объектов (файлов и папок) в заданной области мониторинга. Эти изменения могут указывать на нарушение безопасности компьютера. При обнаружении изменения объектов приложение информирует администратора.

Для работы Мониторинга файловых операций требуется настроить область действия компонента (см. раздел "Формирование области мониторинга" на стр. 270), то есть выбрать объекты, за состоянием которых должен следить компонент.

Вы можете посмотреть информацию о результатах работы компонента Мониторинг файловых операций (см. раздел "Просмотр информации о целостности системы" на стр. 272) в Kaspersky Security Center и в интерфейсе Kaspersky Endpoint Security для Windows.

В этом разделе

Формирование области мониторинга 270
Просмотр информации о целостности системы 272

Формирование области мониторинга

Мониторинг файловых операций не может работать без заданной области мониторинга. То есть вам нужно указать пути к файлам и папкам, изменения которых Мониторинг файловых операций будет контролировать. Рекомендуется добавлять в область мониторинга объекты, изменения в которых происходят редко, или, доступ к которым имеет только администратор. Это позволит уменьшить количество событий Мониторинга файловых операций.

Также для уменьшения количества событий вы можете добавить исключения в правила мониторинга. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга. Например, в организации используется приложение, целостность файлов которого вы хотите контролировать. Для этого вам нужно добавить путь к папке с приложением (например, `C:\Users\Testadmin\Desktop\Utilities`). Вы можете исключить из правила мониторинга файлы журналов, так как эти файлы не влияют на безопасность системы. Кроме того приложение постоянно вносит изменения в файлы журналов, и в результате вы можете получить большое количество однотипных событий. Чтобы это избежать, добавьте файлы журналов в исключения (например, `C:\Users\Testadmin\Desktop\Utilities\*.log`).

Как сформировать область мониторинга в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Мониторинг файловых операций**.
3. Убедитесь, что переключатель **Мониторинг файловых операций** включен.
4. В блоке **Правила мониторинга** нажмите **Настроить правила**.
5. В блоке **Правила мониторинга** нажмите на кнопку **Добавить**.
6. В открывшемся окне нажмите настройте параметры правила мониторинга:
   - **Название правила**. Введите название правила, например, *Мониторинг приложения А*.
   - **Уровень важности событий**. Выберите уровень важности событий, которые будет регистрировать Мониторинг файловых операций: *Информационное* ⓘ, *Предупреждение* ⚠, *Критическое* ⓘ.
   - **Область мониторинга**. Введите путь к папке или файлу.

     При задании области мониторинга убедитесь, что путь к папке или файлу начинается с буквы диска или системной переменной среды. Приложение не поддерживает пользовательские переменные среды. Если путь к папке или файлу указан не верно, Kaspersky Endpoint Security не добавит указанную область 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.
   - **Исключения**. Введите путь к папке или файлу. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. Записи исключений имеют более высокий приоритет, чем записи области мониторинга.
7. Нажмите на кнопку**OK**.

   В список правил мониторинга будет добавлено новое правило. Вы можете выключить правило из мониторинга, не удаляя его из списка правил. Для этого выключите переключатель рядом с ним.
8. Сохраните внесенные изменения.

Просмотр информации о целостности системы

Информация о результатах работы Мониторинга файловых операций отображается следующими способами:

События в консоли Kaspersky Security Center и интерфейсе Kaspersky Endpoint Security

Kaspersky Endpoint Security отправляет событие в Kaspersky Security Center, если обнаруживает изменение в файлах. Вы можете настроить выборку событий, чтобы посмотреть события от компонента Мониторинг файловых операций. Подробнее о настройке выборки событий см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/14.2/ru-RU/166234.htm.

В интерфейсе Kaspersky Endpoint Security предусмотрен отдельный отчет для компонента Мониторинг файловых операций (см. раздел "Просмотр отчетов" на стр. 304).

Kaspersky Endpoint Security имеет инструменты агрегации событий для уменьшения количества событий Мониторинга файловых операций. Kaspersky Endpoint Security включает агрегацию событий в следующих случаях:

- слишком частое изменение одного объекта (более пяти раз в минуту);
- слишком частое срабатывание одного правила мониторинга (более 10 раз в минуту).

В результате Kaspersky Endpoint Security создает отдельные события об изменении объектов до тех пор, пока не сработают инструменты агрегации. Далее Kaspersky Endpoint Security включает агрегацию событий и создает соответствующее событие. Kaspersky Endpoint Security выполняет агрегацию событий в течение суток (период агрегации) или до остановки Kaspersky Endpoint Security. После перезапуска Kaspersky Endpoint Security или после окончания периода агрегации приложение формирует специальные события: *Отчет о подозрительном событии за период агрегации* и *Отчет об изменениях объекта за период агрегации*. Эти отчеты содержат информацию о начале и окончании периода агрегации и количестве агрегированных событий.

Статус компьютера в консоли Kaspersky Security Center

При получении от компонента Мониторинг файловых операций событий с уровнем важности *Критическое* или *Предупреждение* Kaspersky Security Center изменяет статус компьютера на *Критический* или *Предупреждение*.

> Получение статуса компьютера от управляемого приложения (условие **Статус устройства определен программой**) должно быть включено в Kaspersky Security Center в списках условий назначения статусов *Критическое* и *Предупреждение*. Условия назначения статусов устройства настраиваются в окне свойств группы администрирования.

Статус компьютера и все причины изменения статуса отображаются в списке устройств, входящих в группу администрирования. Подробнее о статусах компьютера см. в справке Kaspersky Security Center https://support.kaspersky.com/help/KSC/14.2/ru-RU/191051.htm.

Отчеты в консоли Kaspersky Security Center

В Kaspersky Security Center предусмотрено два типа отчетов:

- 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.

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.

- 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.

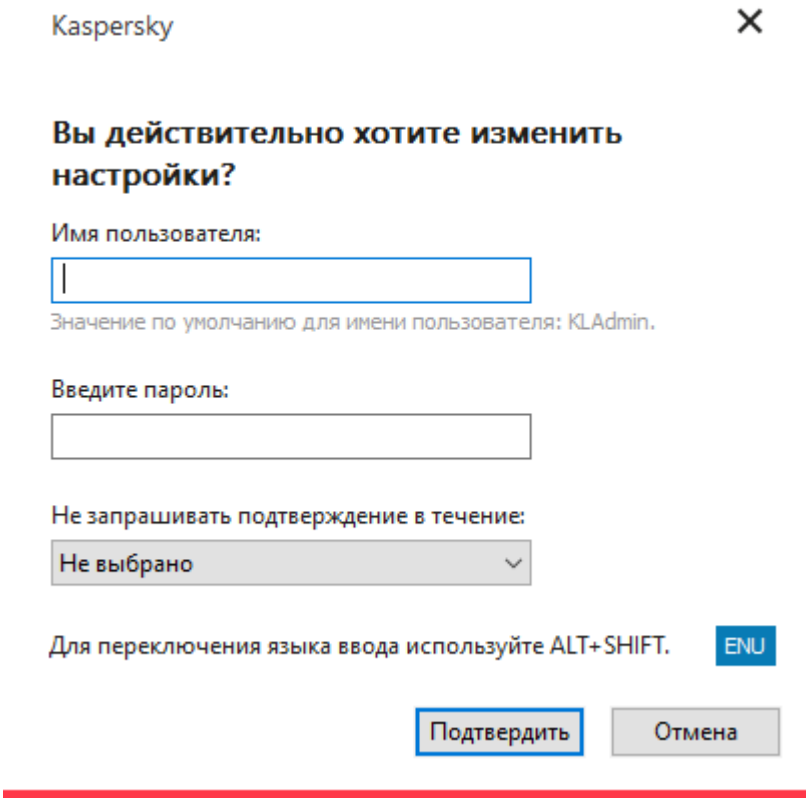


Рисунок 76. Запрос пароля для доступа к Kaspersky Endpoint Security

Имя пользователя и пароль

Для доступа к Kaspersky Endpoint Security необходимо ввести данные доменной 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.
- **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).

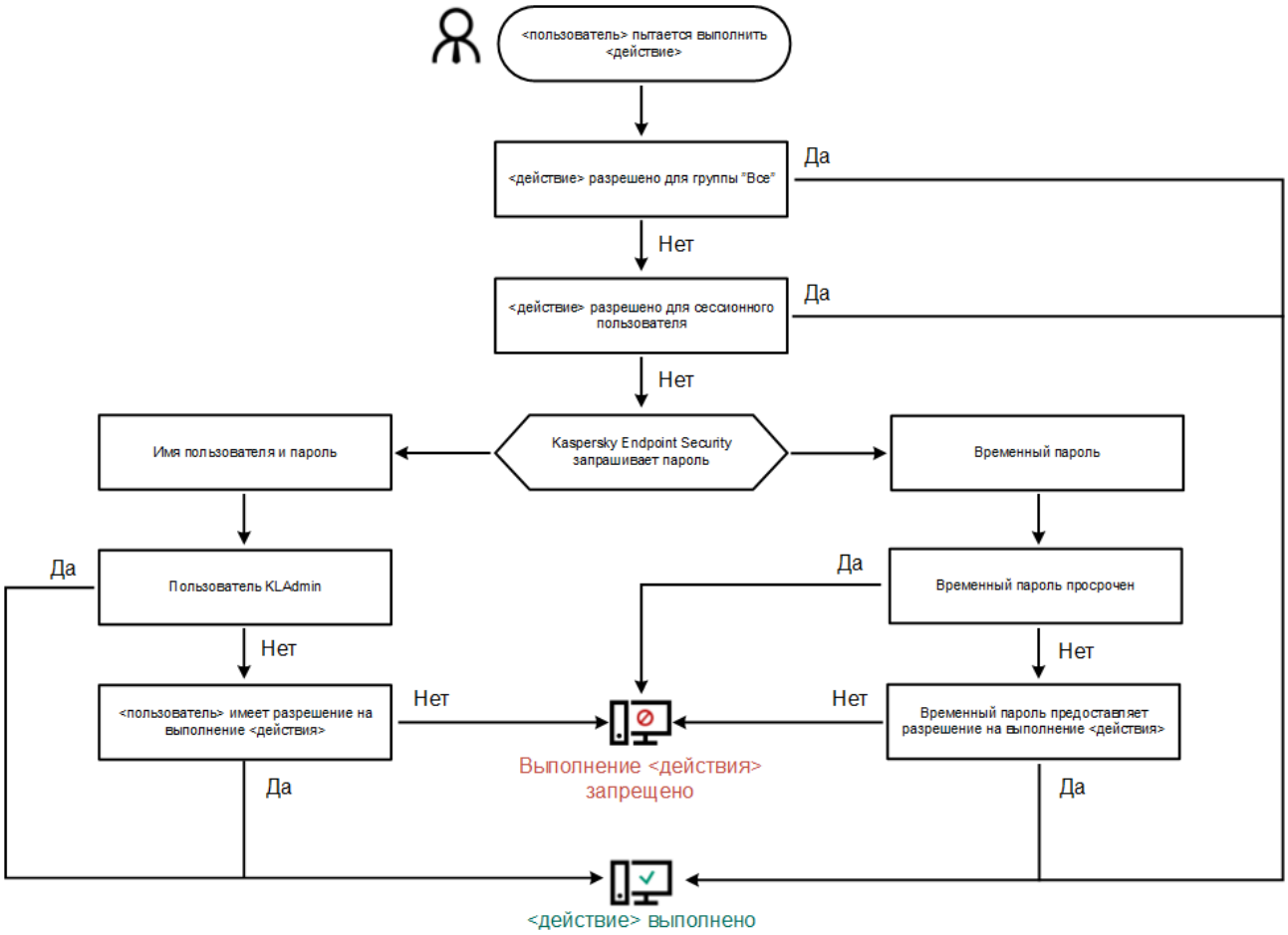


Рисунок 77. Алгоритм работы Защиты паролем

kaspersky

В этом разделе

Включение Защиты паролем 276

Предоставление разрешений для отдельных пользователей или групп 277

Использование временного пароля для предоставления разрешений 278

Особенности разрешений Защиты паролем 279

Сброс пароля KLAdmin 280

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. 38) 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. 280). 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 программы** 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. 277) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 278).

Разрешения Защиты паролем имеют ряд особенностей (см. раздел "Особенности разрешений Защиты паролем" на стр. 279). 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. 277) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 278).

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

Вы можете предоставить доступ к Kaspersky Endpoint Security для отдельных пользователей или групп. 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. 278).

Как предоставить разрешение для отдельных пользователей или групп в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. В открывшемся окне нажмите на кнопку **Выбрать**.

   Откроется стандартное окно Windows для выбора пользователей или групп.
5. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.
6. 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 программы** 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. 277) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 278).

Разрешения Защиты паролем имеют ряд особенностей (см. раздел "Особенности разрешений Защиты паролем" на стр. 279). Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

7. 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 **Программы**.
6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows** 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 **Настройка**.
10. Откроется окно **Создание временного пароля**.
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.

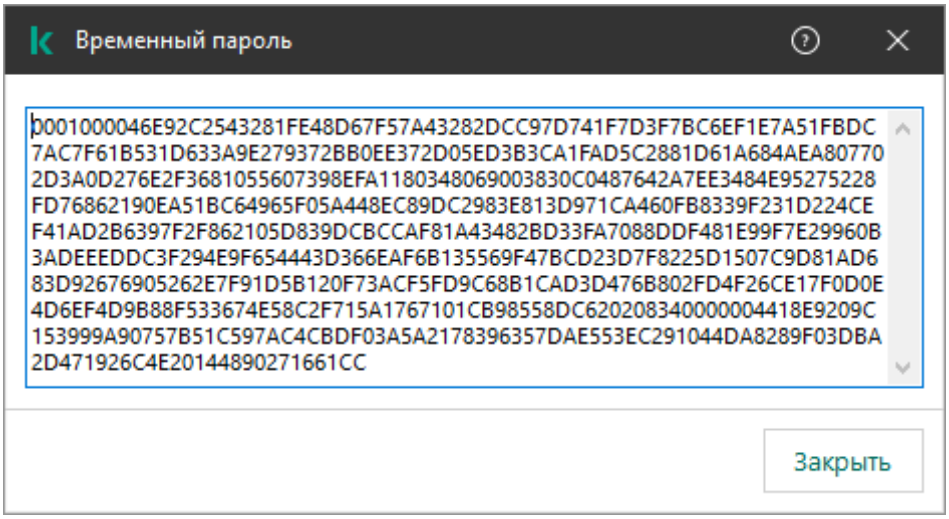


Рисунок 78. Временный пароль

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. 277) 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. 277) 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. 277) 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.

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. 278). 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. 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 **Общие настройки** → **Интерфейс**.
5. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
6. В открывшемся окне снимите флажок **Включить защиту паролем**.
7. Сохраните внесенные изменения.
8. Повторно установите флажок **Включить защиту паролем**.
9. Нажмите на кнопку **OK**.

   Откроется окно для ввода пароля администратора.
10. Задайте новый пароль для учетной записи KLAdmin и подтвердите его.
11. Сохраните внесенные изменения.

В результате пароль для учетной записи KLAdmin будет обновлен после применения политики.

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.

В этом разделе

Создание исключения из проверки 282

Выбор типов обнаруживаемых объектов 286

Формирование списка доверенных приложений 287

Создание локальной доверенной зоны 291

Использование доверенного системного хранилища сертификатов 295

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. 104).
- Защита от эксплойтов (см. раздел "Защита от эксплойтов" на стр. 114).
- Предотвращение вторжений (см. раздел "Предотвращение вторжений" на стр. 117).
- Защита от файловых угроз (см. раздел "Защита от файловых угроз" на стр. 131).
- Защита от веб-угроз (см. раздел "Защита от веб-угроз" на стр. 141).
- Защита от почтовых угроз (см. раздел "Защита от почтовых угроз" на стр. 149).
- Задача *Поиск вредоносного ПО* (см. раздел "*Поиск вредоносного ПО*" на стр. 49).

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. 38) 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**.

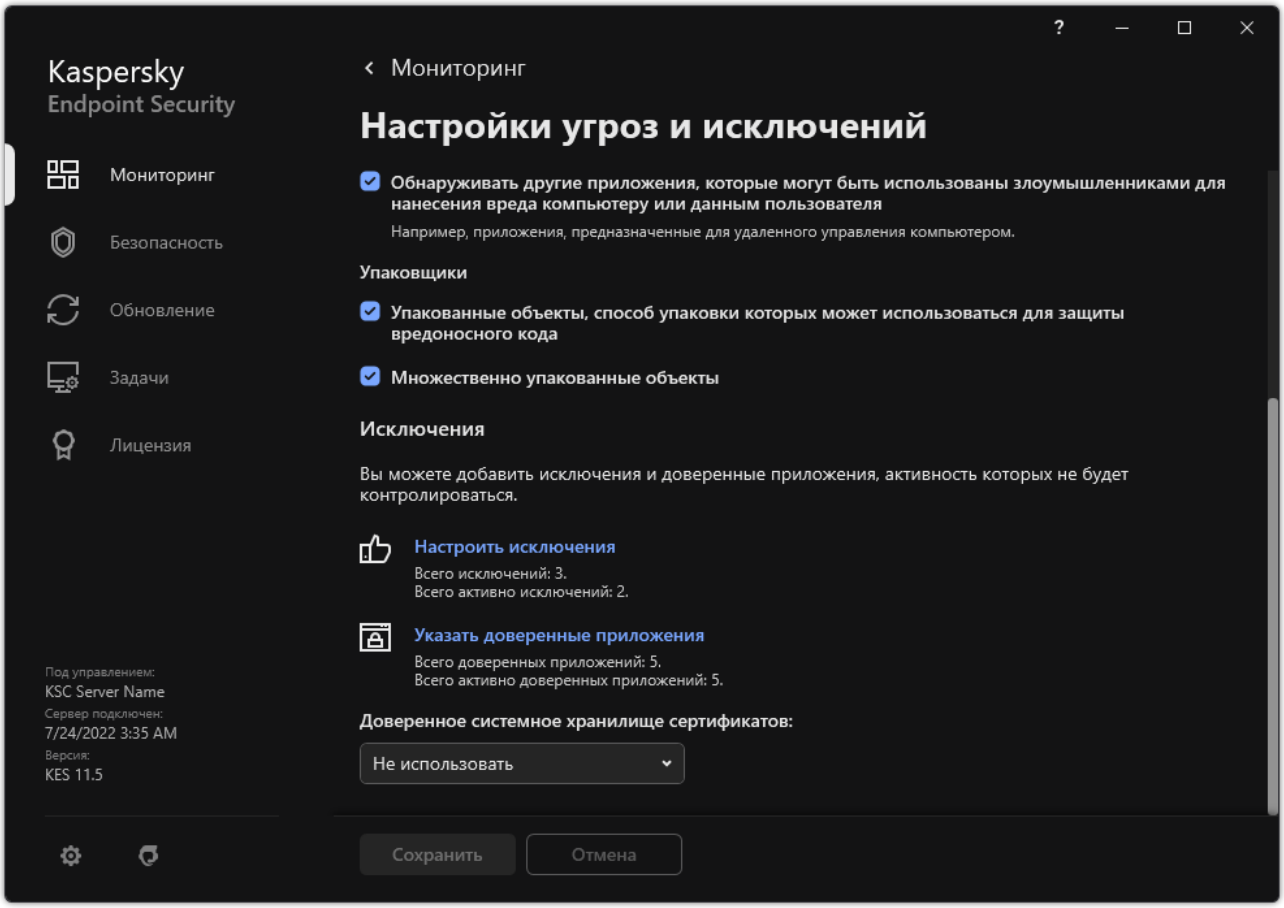


Рисунок 79. Параметры исключений

4. Нажмите на кнопку **Добавить**.
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 `C:\Users\*\Folder\`.

6. Если вы хотите исключить из проверки тип объектов, в поле **Объект** 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 файла** 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**.

    Вы можете в любое время остановить работу исключения с помощью переключателя (см. рис. ниже).

11. Сохраните внесенные изменения.

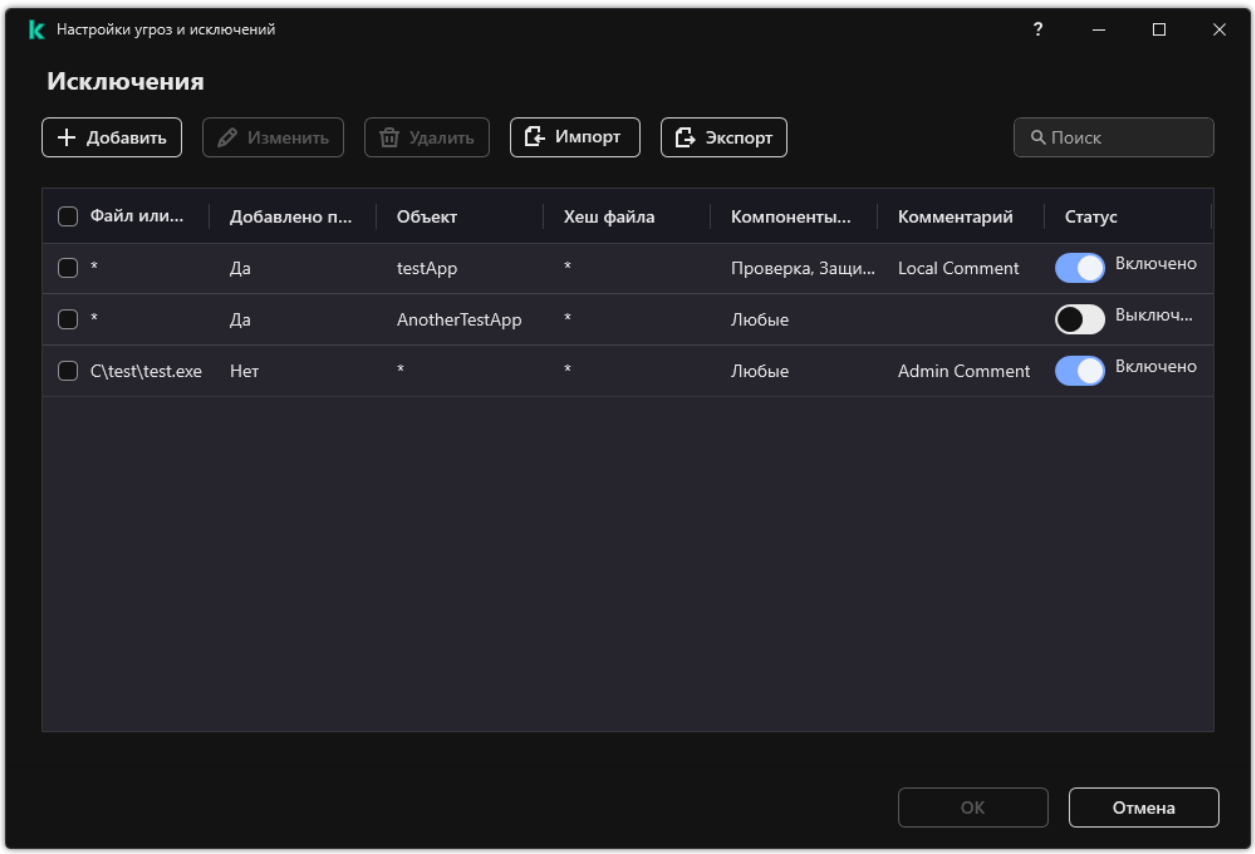


Рисунок 80. Список исключений

Примеры масок пути:

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\, но не в подпапках папки C:\dir\;
- маска `C:\dir\` будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
- 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.

Выбор типов обнаруживаемых объектов

► *Чтобы выбрать типы обнаруживаемых объектов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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:
   - **Вирусы и черви**;
   - **Троянские приложения (в том числе приложения-вымогатели)**;
   - **Вредоносные утилиты**;
   - **Рекламные приложения**;
   - **Приложения автодозвона**;
   - **Обнаруживать другие 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**.
4. Сохраните внесенные изменения.

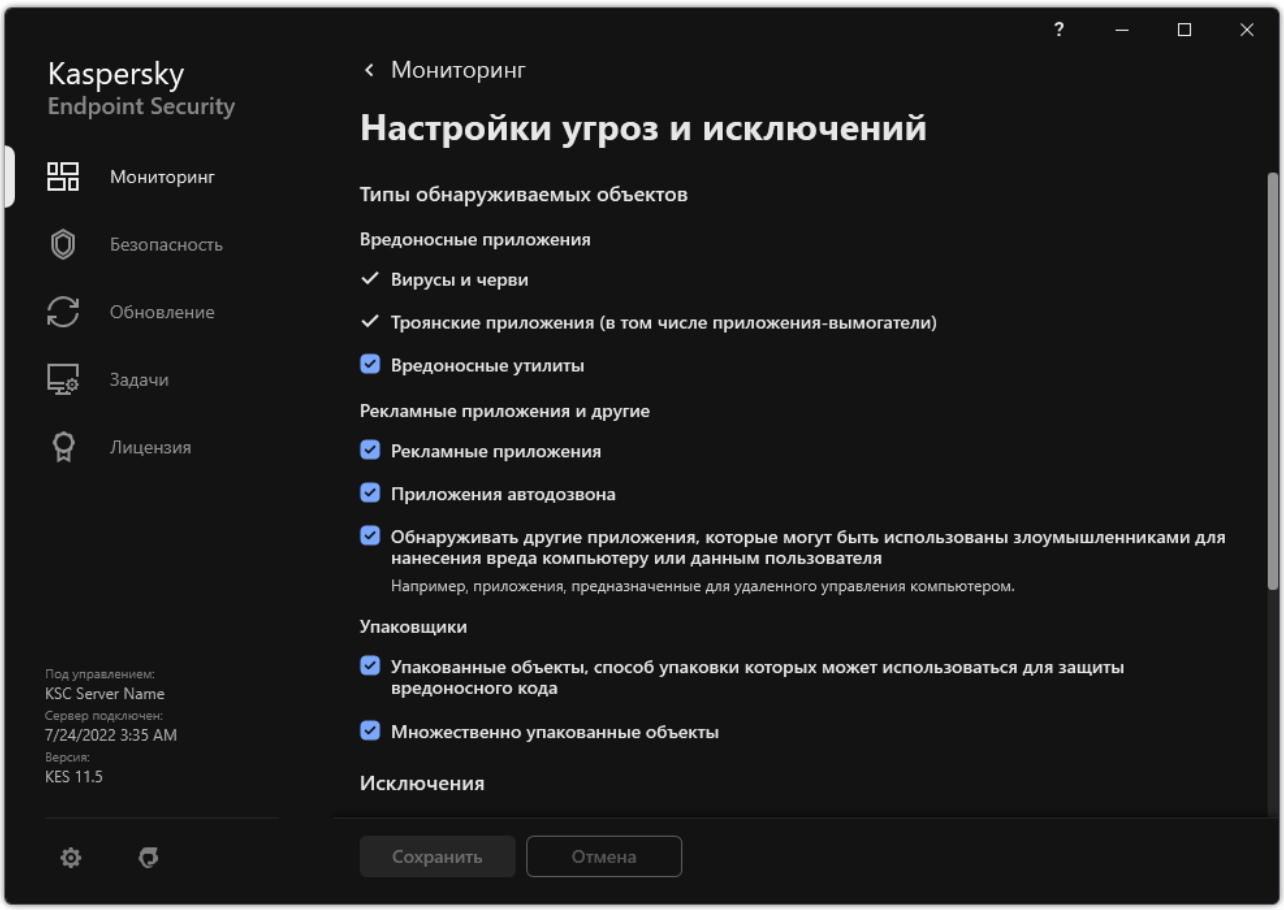


Рисунок 81. Типы обнаруживаемых объектов

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. 282).

Как добавить приложение в список доверенных в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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**.

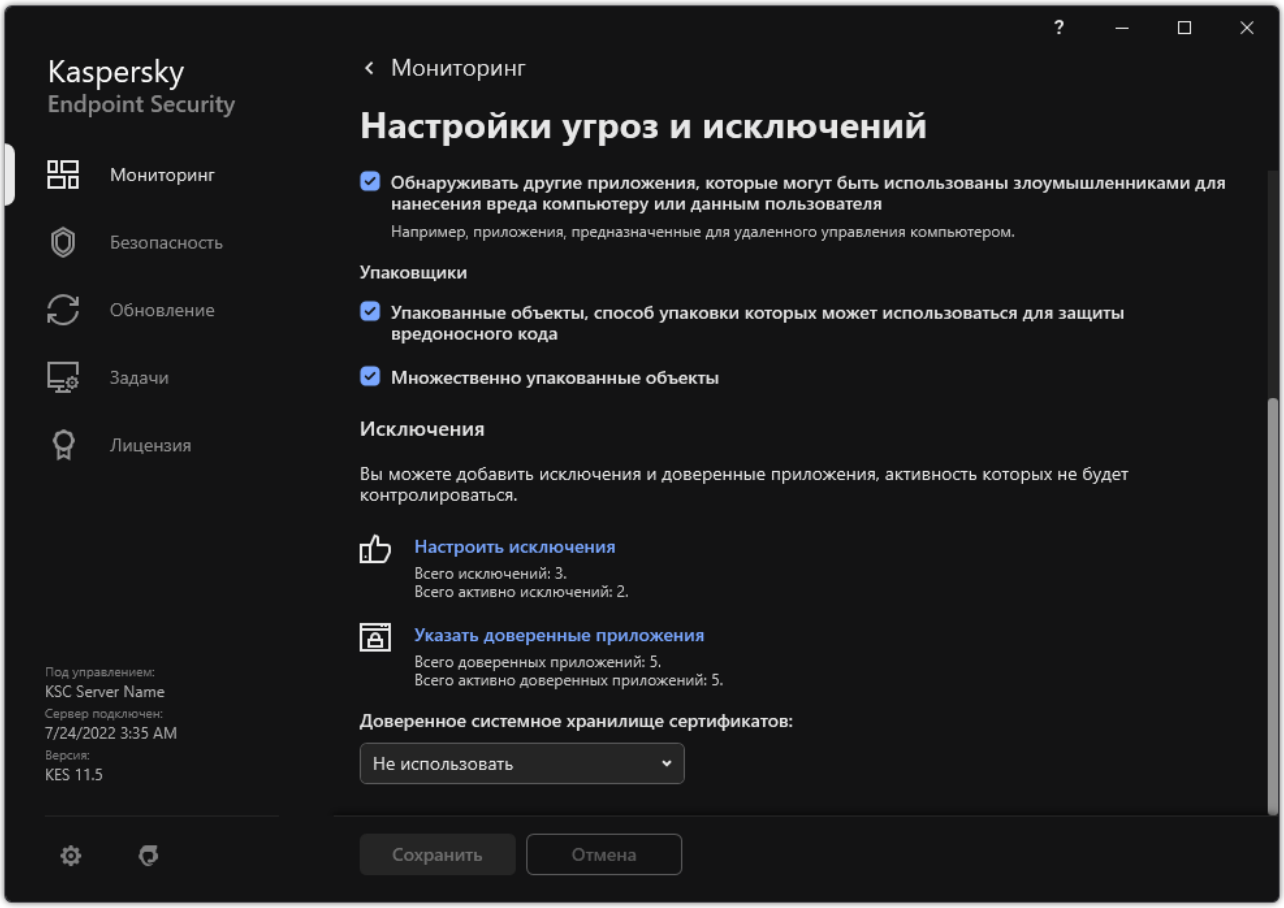


Рисунок 82. Параметры исключений

4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Выберите исполняемый файл доверенного приложения.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

   > 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. 287).
7. Вы можете в любое время исключить приложение из доверенной зоны (см. раздел "Создание локальной доверенной зоны" на стр. 291) с помощью переключателя (см. рис. ниже).

8. Сохраните внесенные изменения.

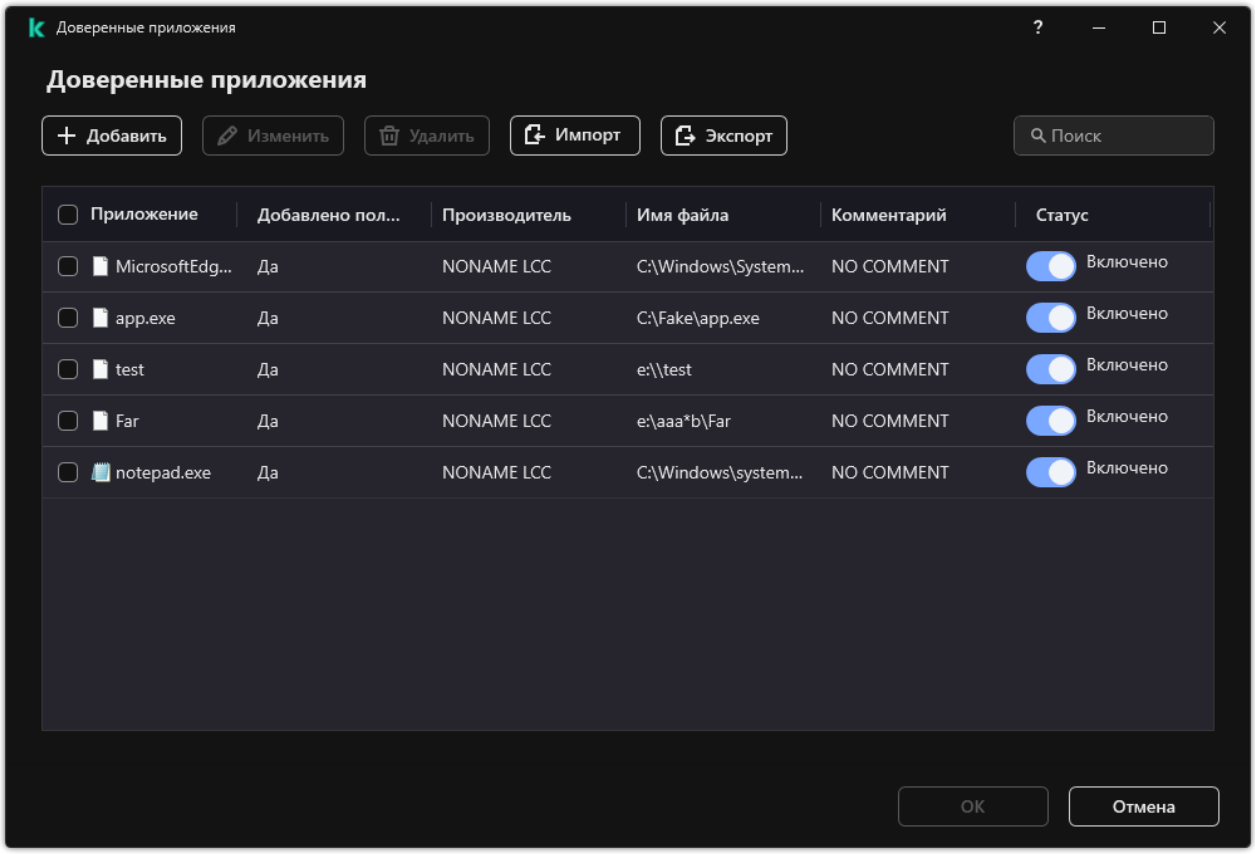


Рисунок 83. Список доверенных приложений

Таблица 15. 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.
Не контролировать активность приложения	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложения в операционной системе. Контроль за активностью приложения выполняют следующие компоненты: Анализ поведения (на стр. 104), Защита от эксплойтов (на стр. 114), Предотвращение вторжений (на стр. 117), Откат вредоносных действий (на стр. 129) и Сетевой экран.
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. 122) (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.

Параметр	Описание
Разрешить взаимодействие с интерфейсом приложения	Самозащита Kaspersky Endpoint Security (на стр. 310) 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. 169).
Не собирать телеметрию по операциям консольного ввода	Kaspersky Endpoint Security не отправляет данные телеметрии об управлении приложением через консоль. Данные телеметрии использует Kaspersky Anti Targeted Attack Platform (EDR) (на стр. 324).
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.
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.

Создание локальной доверенной зоны

У пользователя есть возможность формировать собственную локальную доверенную зону для отдельного компьютера. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений из проверки и доверенных приложений. Администратор может разрешить или запретить использование локальных исключений или локальных доверенных приложений в параметрах политики. Для этого предназначены флажки **Разрешить использование локальных исключений** и **Разрешить использование локальных доверенных приложений** в разделе политики **Исключения**.

Если администратор разрешил формировать локальную доверенную зону, пользователь может добавлять собственные исключения из проверки (см. раздел "Создание исключения из проверки" на стр. 282) и доверенные приложения (см. раздел "Формирование списка доверенных приложений" на стр. 287) в интерфейсе приложения. При этом у пользователя нет прав на изменение или удаление объектов из доверенной зоны, заданной в политике. Также администратор может просматривать, добавлять, изменять или удалять элементы списка в консоли Kaspersky Security Center, если необходимо добавить исключения для отдельного компьютера.

Как создать локальное исключение из проверки в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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**.

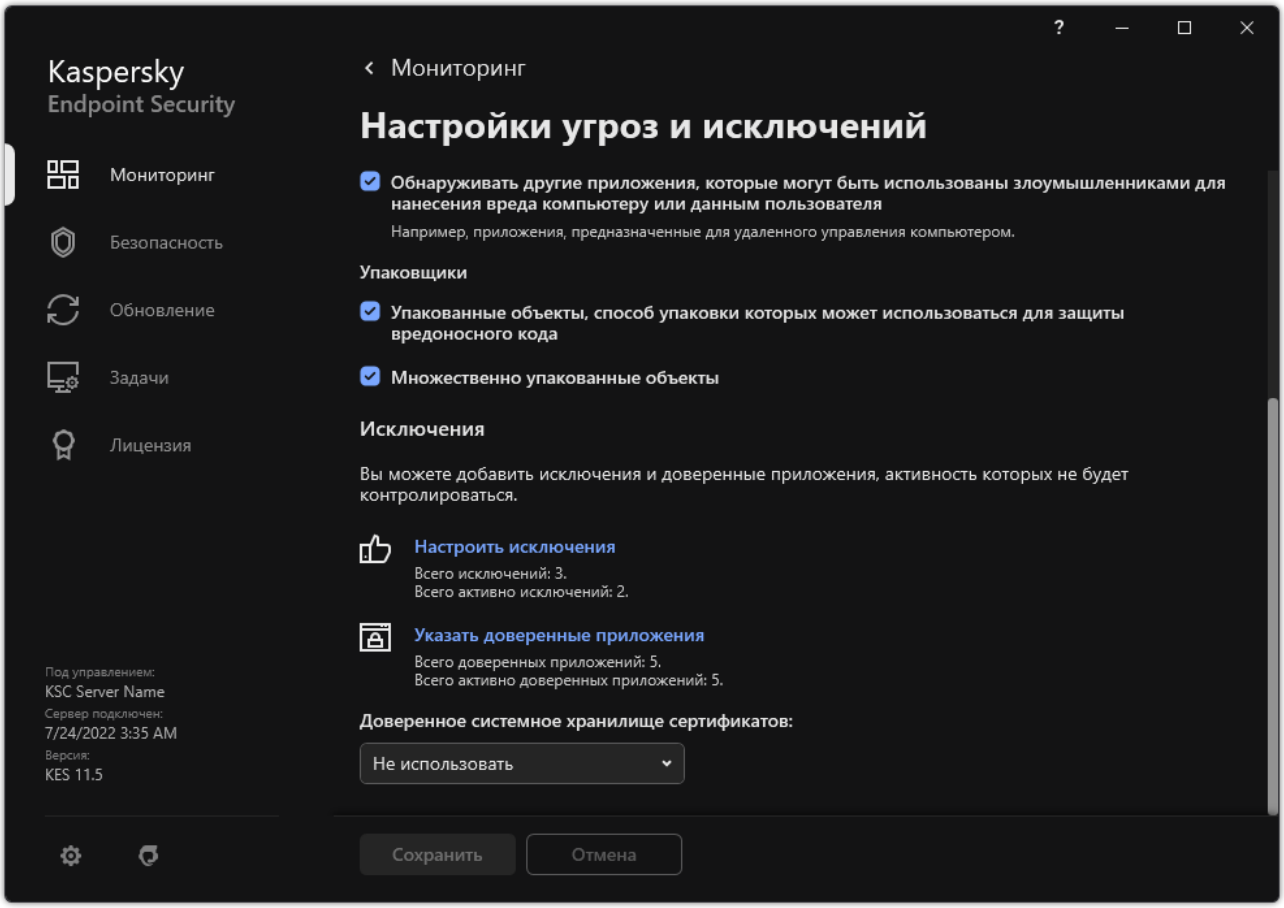


Рисунок 84. Параметры исключений

4. Нажмите на кнопку **Добавить**.
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 `C:\Users\*\Folder\`.

6. Если вы хотите исключить из проверки тип объектов, в поле **Объект** 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 файла** 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**.

    Вы можете в любое время остановить работу исключения с помощью переключателя (см. рис. ниже).

11. Сохраните внесенные изменения.

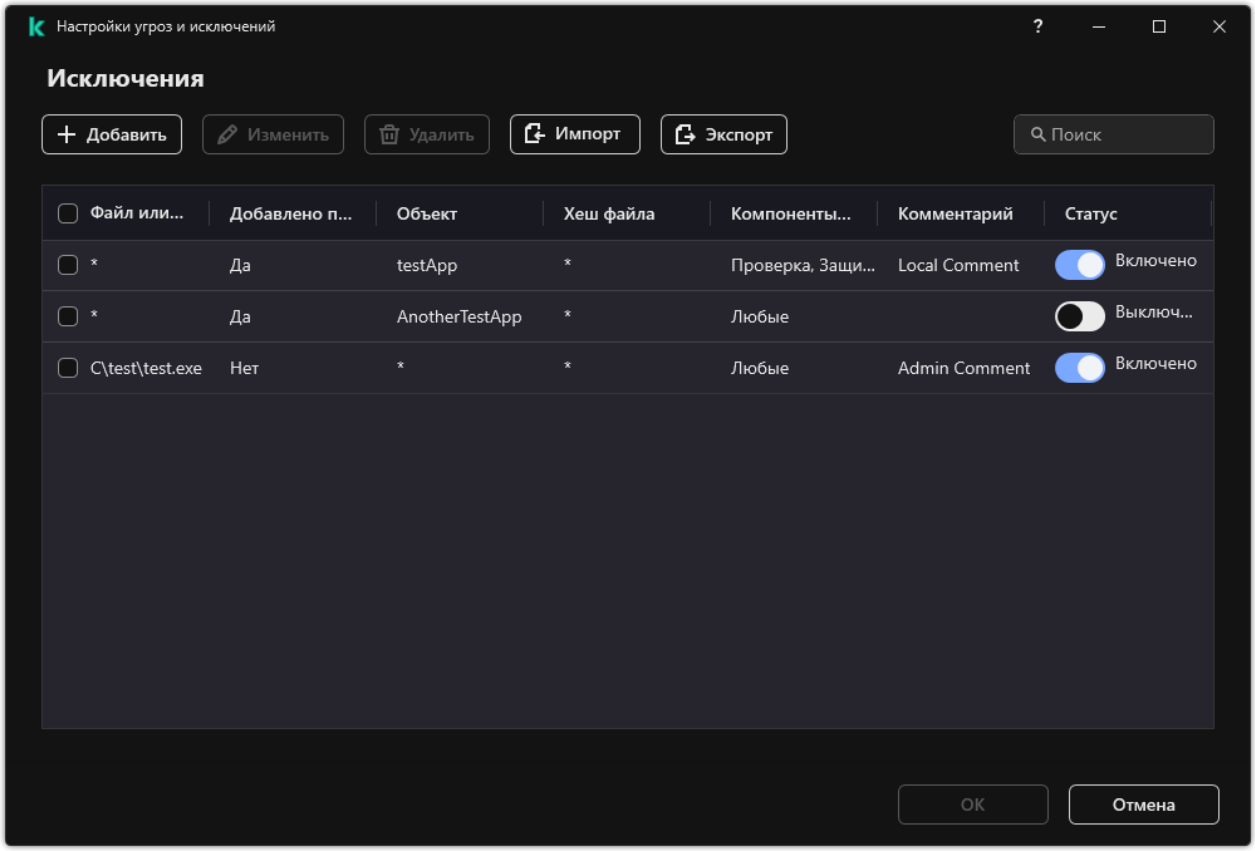


Рисунок 85. Список исключений

Как добавить приложение в список локальных доверенных приложений в интерфейсе приложения

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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**.

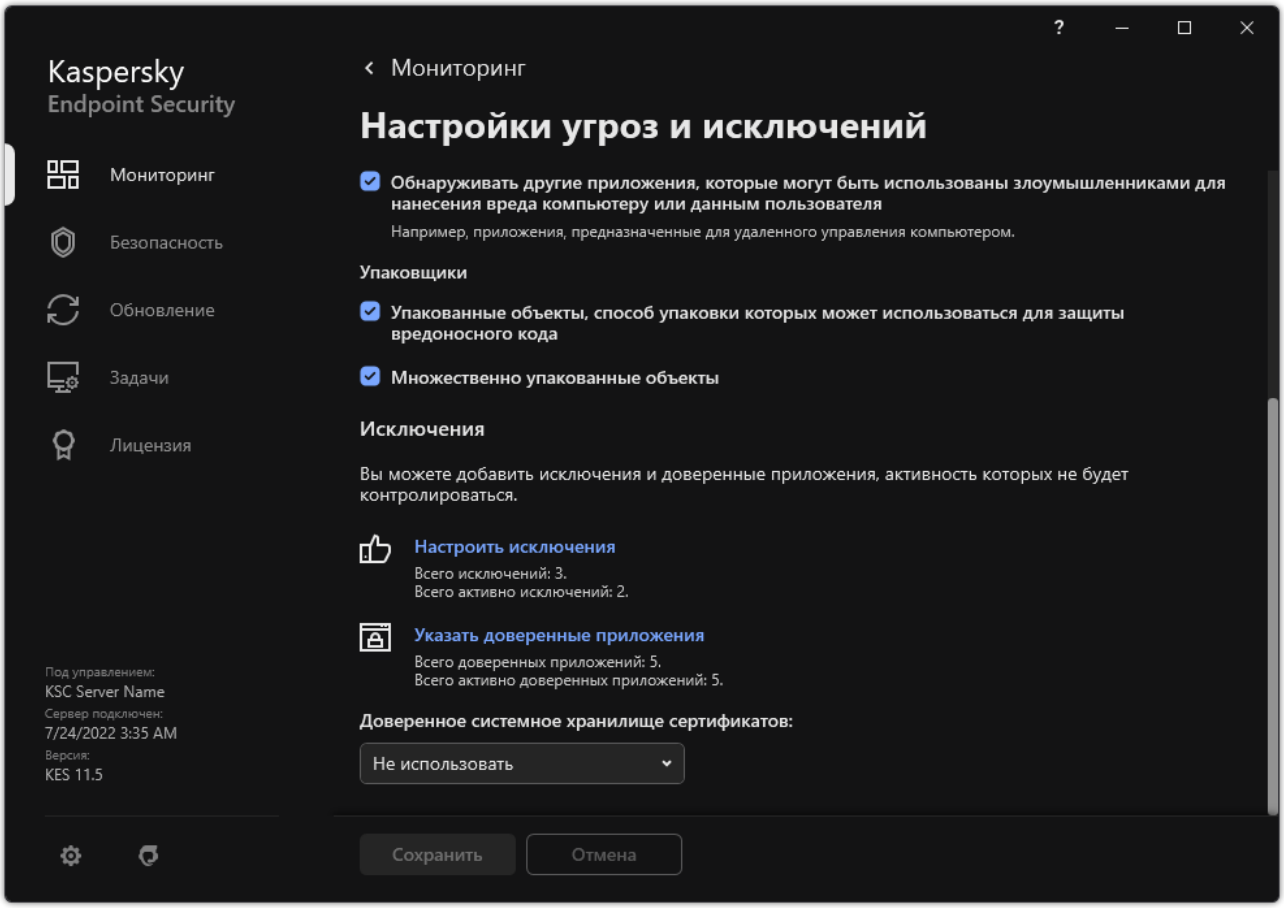


Рисунок 86. Параметры исключений

4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Выберите исполняемый файл доверенного приложения.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

   > 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. 287).
7. Вы можете в любое время исключить приложение из доверенной зоны (см. раздел "Создание локальной доверенной зоны" на стр. 291) с помощью переключателя (см. рис. ниже).
8. Сохраните внесенные изменения.

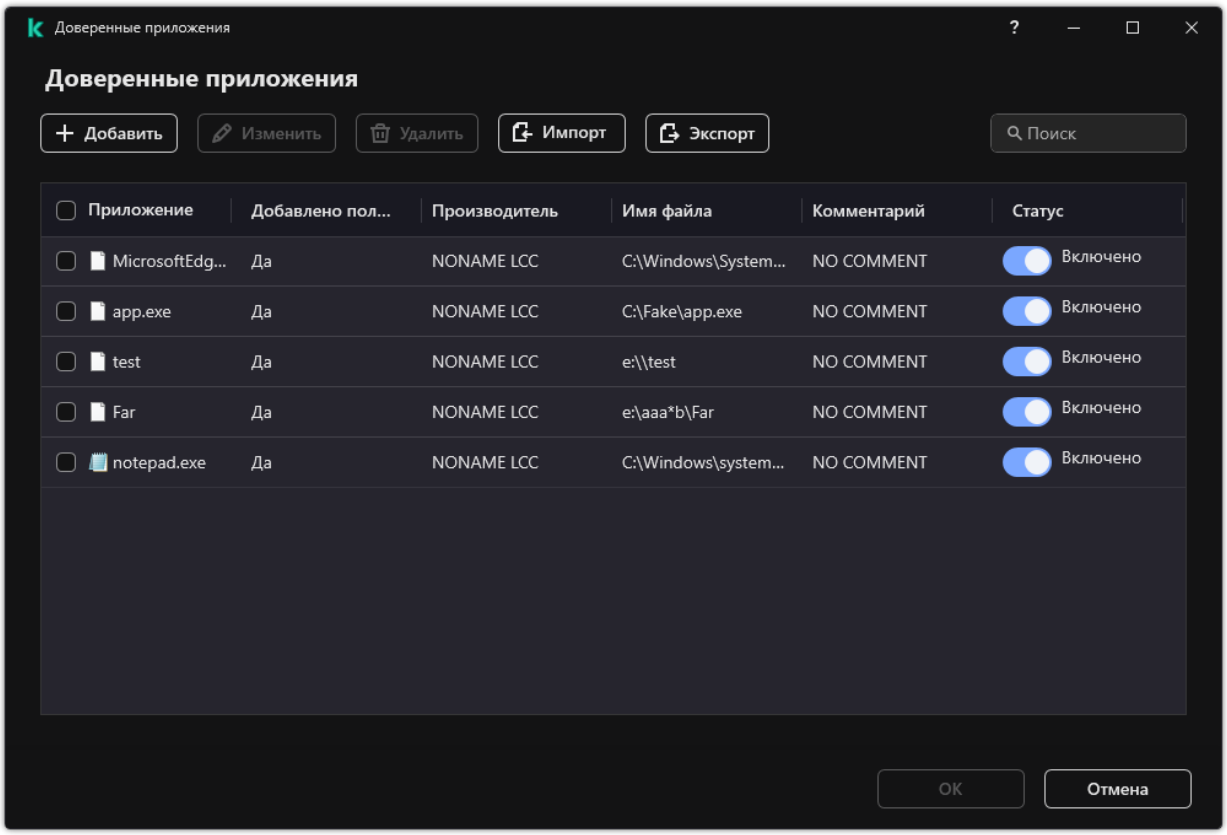


Рисунок 87. Список доверенных приложений

Использование доверенного системного хранилища сертификатов

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки приложения, подписанные доверенной цифровой подписью. Kaspersky Endpoint Security автоматически помещает такие приложения в группу *Доверенные*.

► *Чтобы начать использовать доверенное системное хранилище сертификатов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

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.21.15\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 296

Настройка максимального размера резервного хранилища 297

Восстановление файлов из резервного хранилища 298

Удаление резервных копий файлов из резервного хранилища 299

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.

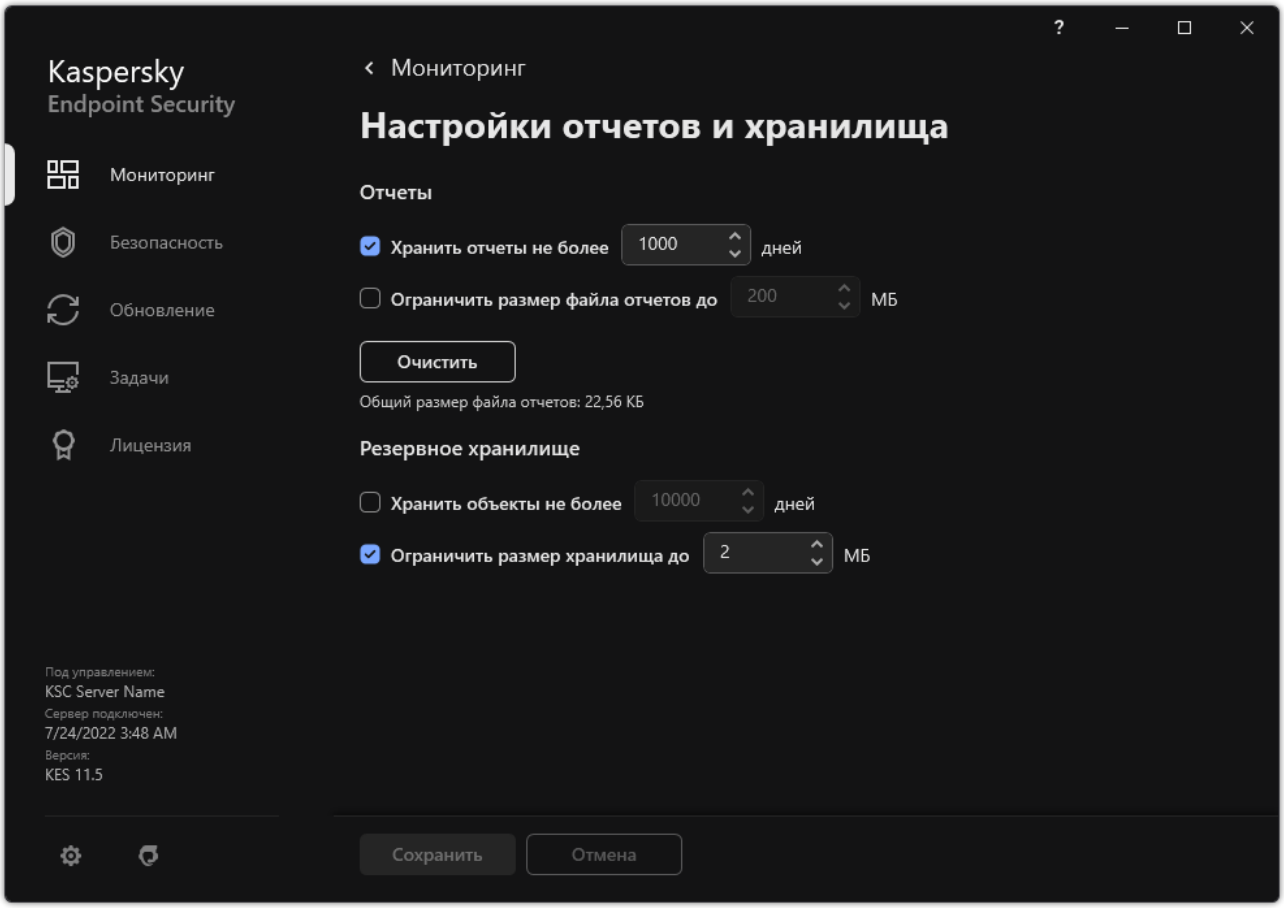


Рисунок 88. Параметры резервного хранилища

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.

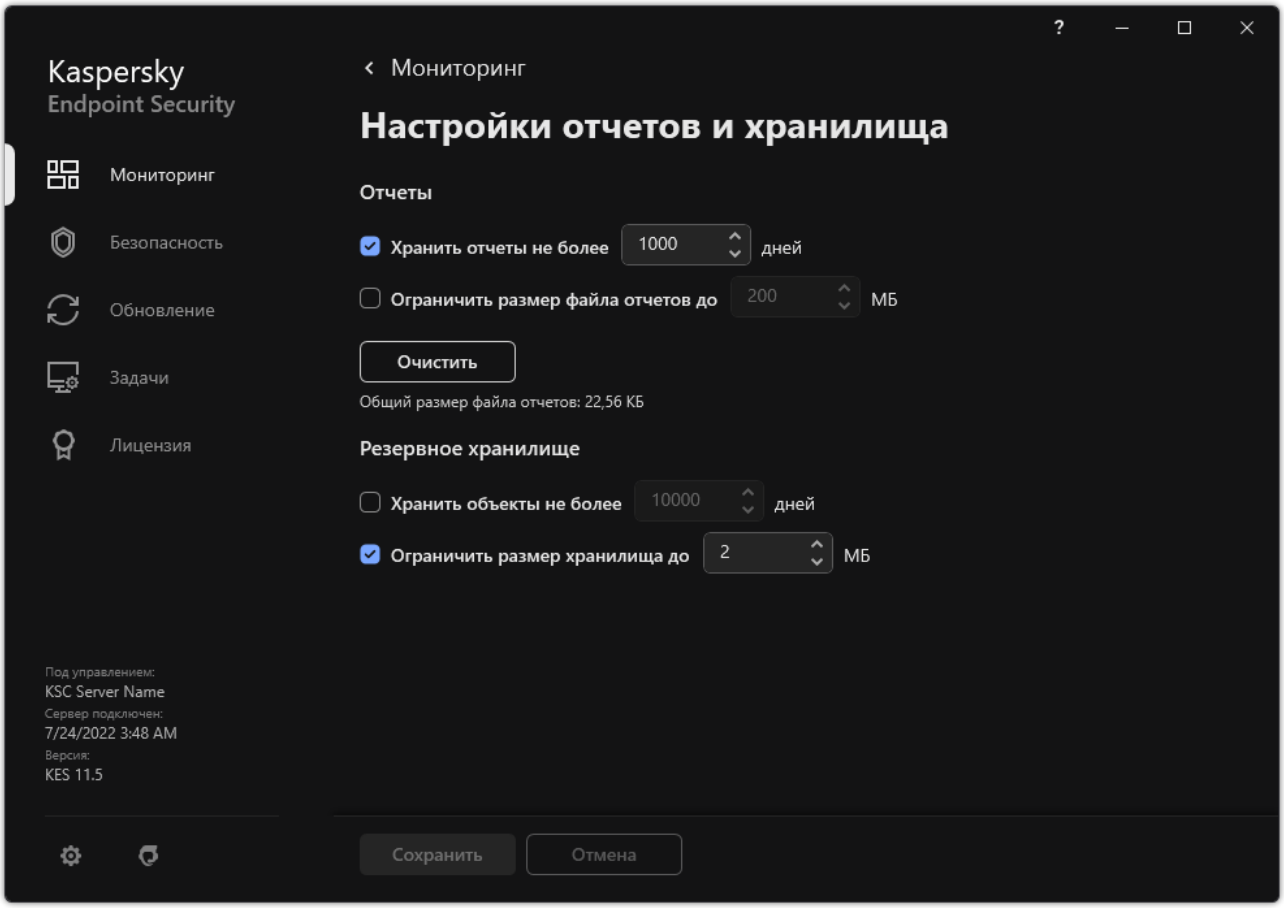


Рисунок 89. Параметры резервного хранилища

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 *Заражен*, 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 Microsoft Windows 8 (подробную информацию о восстановлении приложения Windows Store читайте в Справочной системе к Microsoft Windows 8).

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

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 300

Настройка отображения и доставки уведомлений 301

Настройка отображения предупреждений о состоянии приложения в области уведомлений 302

Настройка параметров журналов событий

► *Чтобы настроить параметры журналов событий, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настройка уведомлений**.

   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. 303). 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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настройка уведомлений**.

   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 **Настройка почтовых уведомлений**.
   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. 38) 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. 40) в области уведомлений будет меняться на или в зависимости от важности предупреждения.

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.21.15\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. 309) 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/14.2/ru-RU/index.htm).

В этом разделе

Просмотр отчетов 304

Настройка максимального срока хранения отчетов 305

Настройка максимального размера файла отчета 306

Сохранение отчета в файл 307

Удаление информации из отчетов 309

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**.

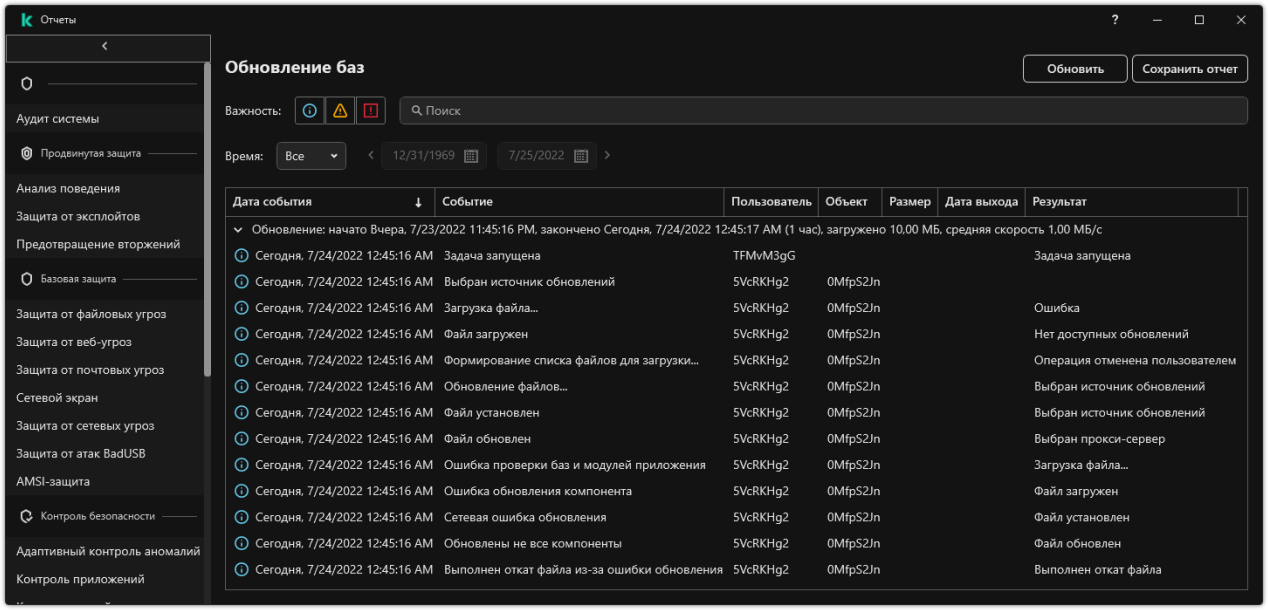


Рисунок 90. Отчеты

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.

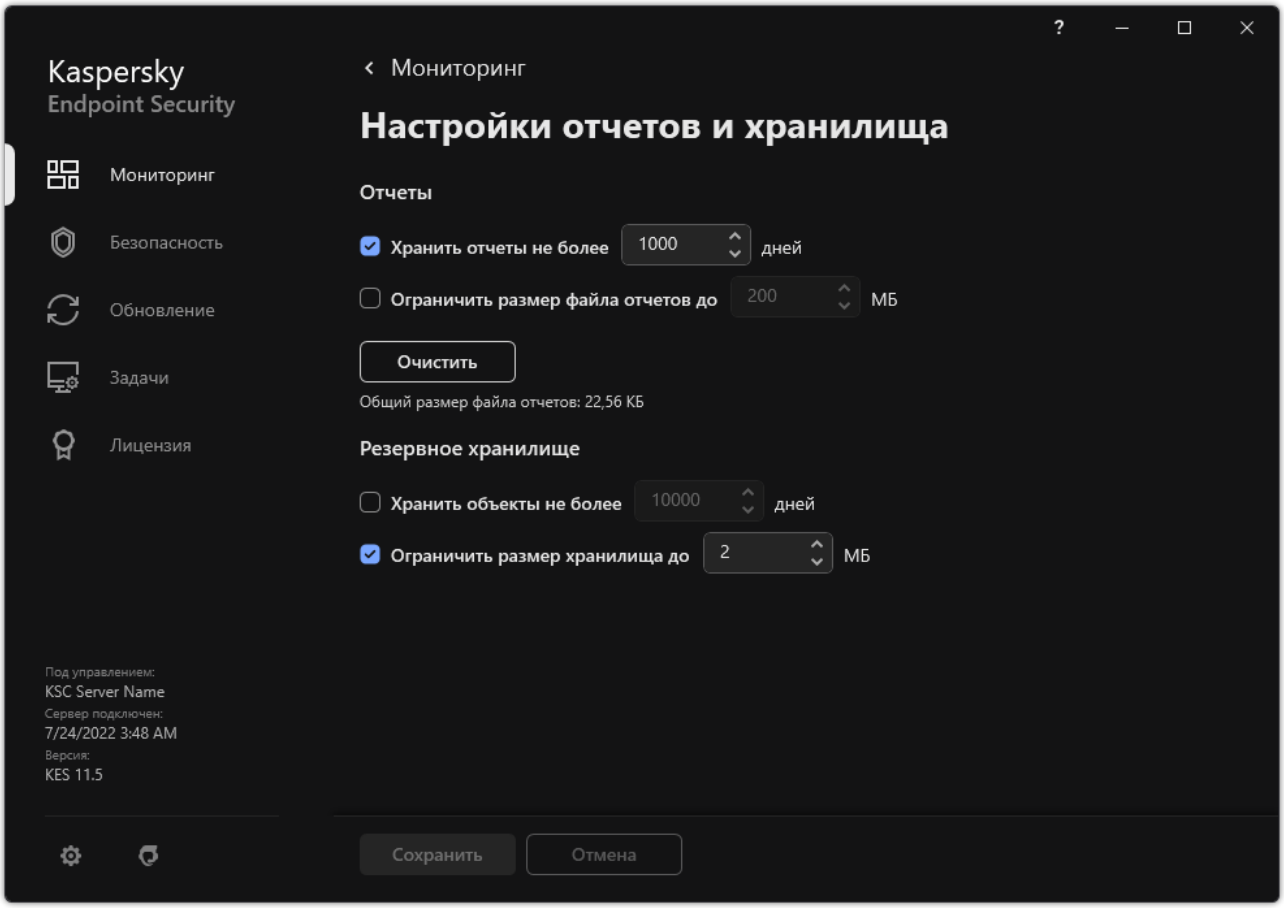


Рисунок 91. Параметры резервного хранилища

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.

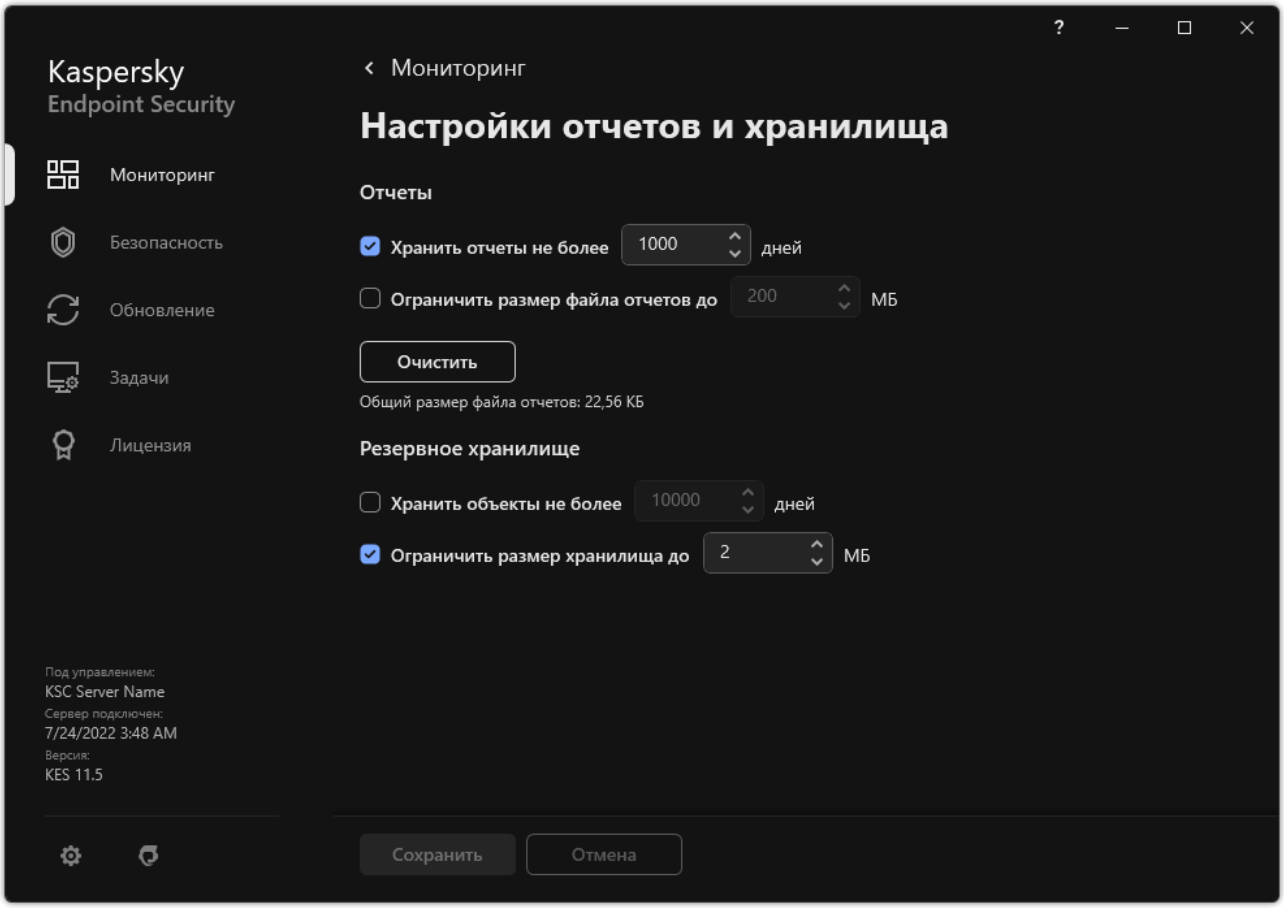


Рисунок 92. Параметры резервного хранилища

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**.

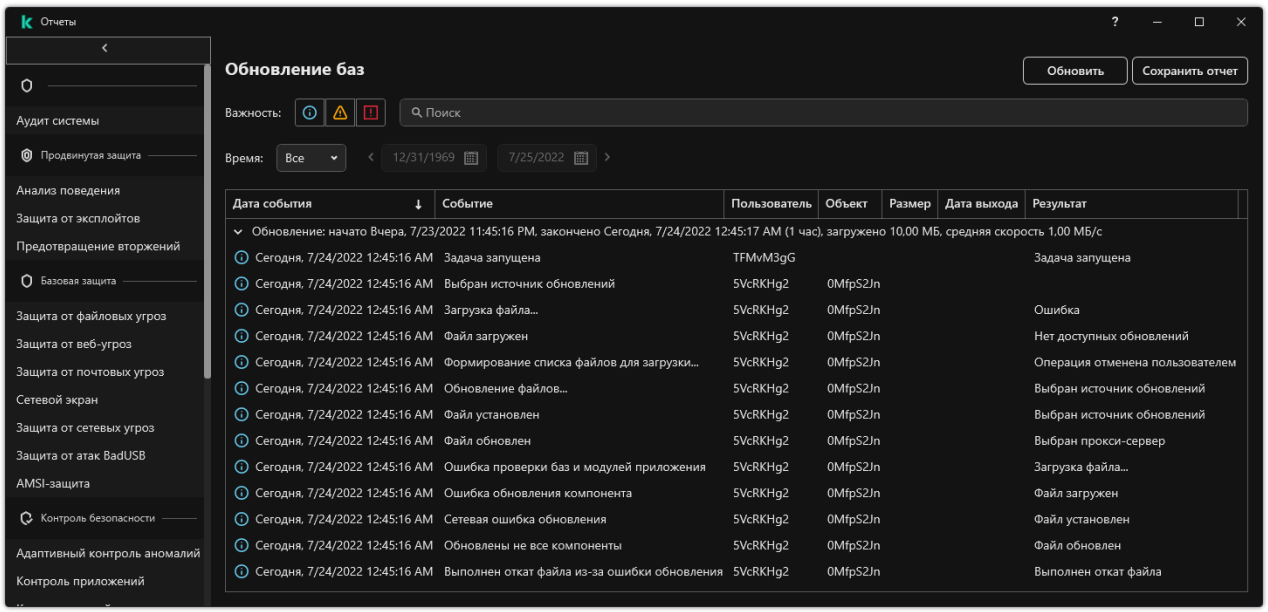


Рисунок 93. Отчеты

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. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Отчеты и хранилище**.

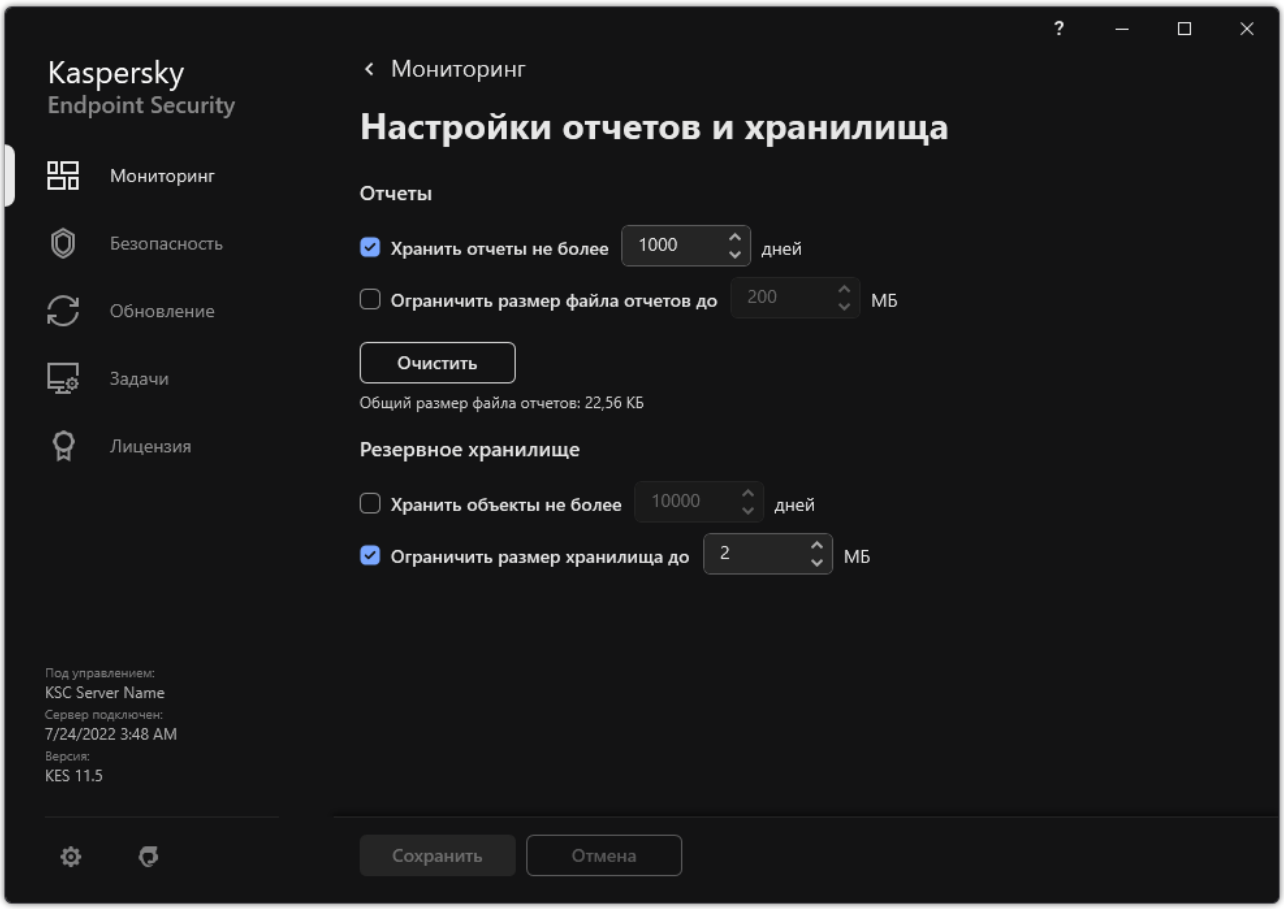


Рисунок 94. Параметры резервного хранилища

3. В блоке **Отчеты** нажмите на кнопку **Очистить**.
4. Если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 276), 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.

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).

Таблица 16. Технологии самозащиты Kaspersky Endpoint Security

Техно-логия	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://docs.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 приложениям удаленного администрирования доступ к Kaspersky Endpoint Security (например, приложения TeamViewer или RemotelyAnywhere).	✓	– (кроме Windows 7)

В этом разделе

Включение и выключение механизма самозащиты 311

Включение и выключение поддержки AM-PPL 311

Защита служб приложения от внешнего управления 313

Обеспечение работы приложений удаленного администрирования 314

Включение и выключение механизма самозащиты

По умолчанию механизм самозащиты Kaspersky Endpoint Security включен.

► *Чтобы включить или выключить механизм самозащиты, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

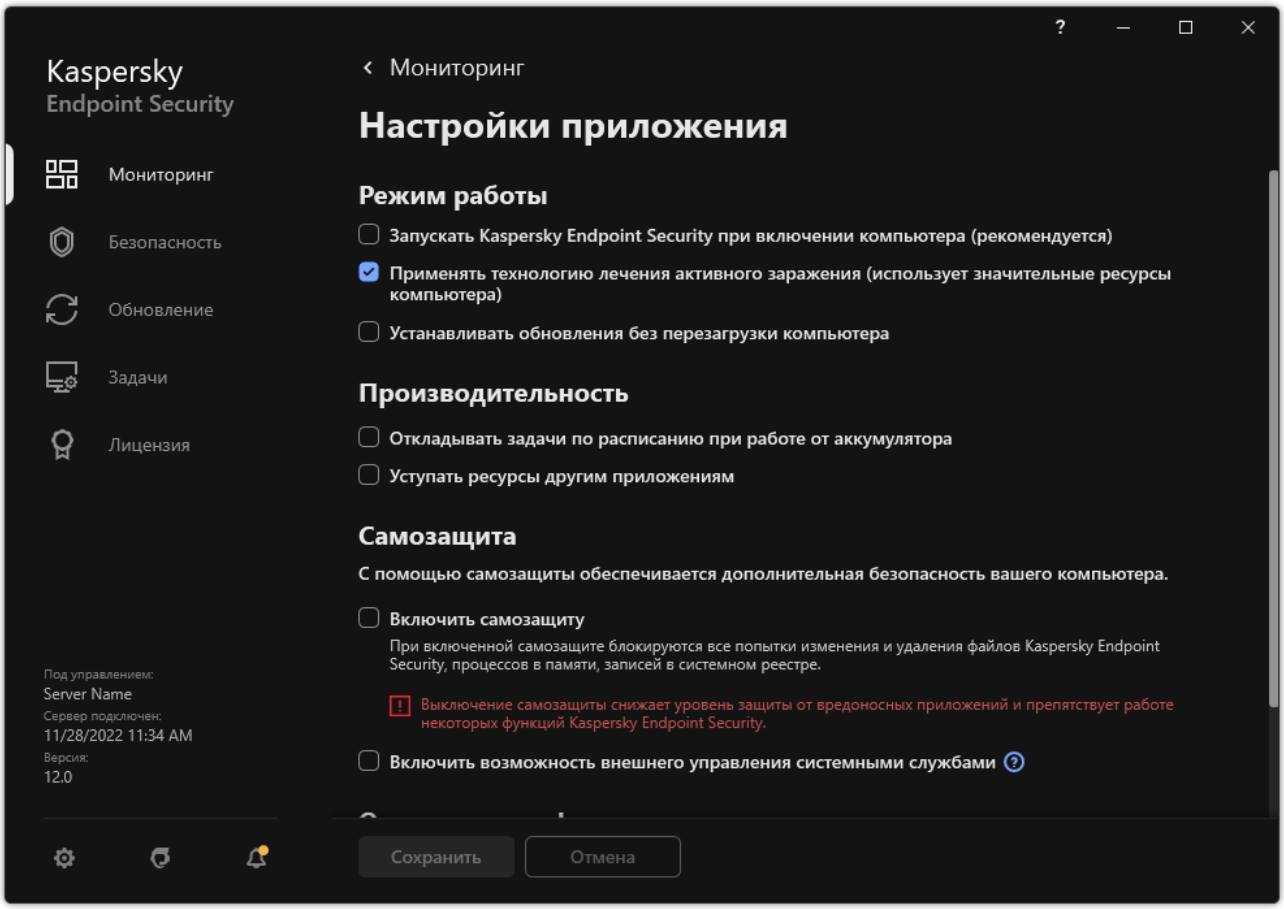


Рисунок 95. Параметры приложения Kaspersky Endpoint Security для Windows

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://docs.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.

Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.
Технология AM-PPL доступна только для компьютеров под управлением 32-разрядных операционных систем. Для компьютеров под управлением 64-разрядных операционных систем технология недоступна.

► *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. 311).

   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. 311).

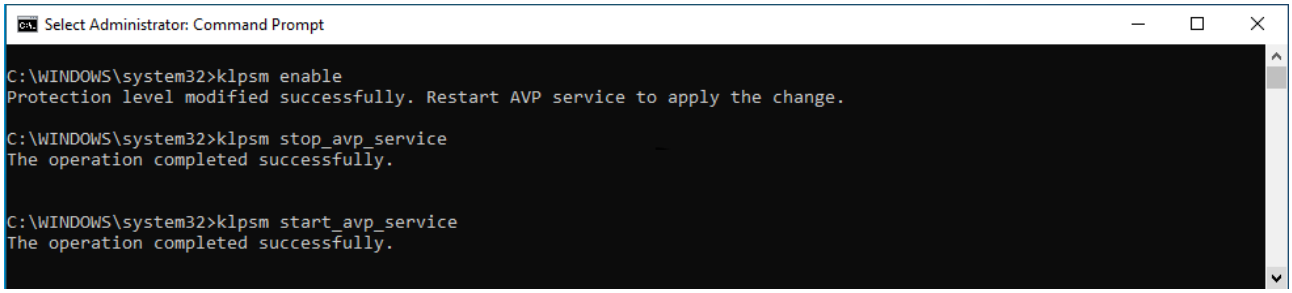


Рисунок 96. Включение поддержки технологии AM-PPL

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);
- служба Kaspersky Seamless Update Service (avpsus).

Для завершения работы приложения из командной строки необходимо, чтобы защита от внешнего управления службами Kaspersky Endpoint Security была выключена.

► *Чтобы включить или выключить защиту служб приложения от внешнего управления, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

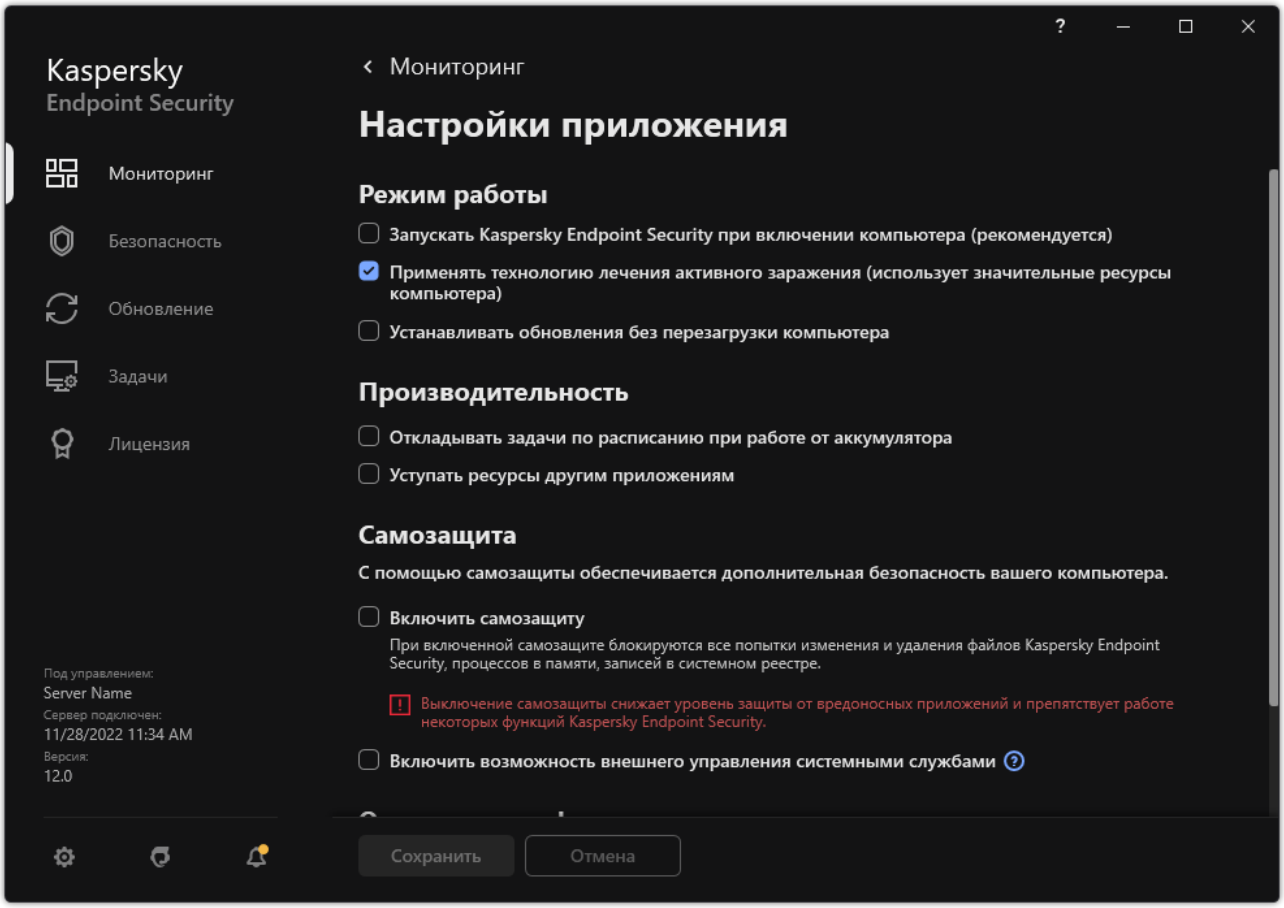


Рисунок 97. Параметры приложения Kaspersky Endpoint Security для Windows

3. Используйте флажок **Включить возможность внешнего управления системными службами**, 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. 38) 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 Kaspersky Endpoint Security**.
7. Сохраните внесенные изменения.

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 "Выбор типов обнаруживаемых объектов" на стр. 286), 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 Kaspersky Endpoint Security может сказываться на производительности других приложений. Чтобы решить проблему совместной работы при увеличении нагрузки на процессор и дисковые подсистемы, Kaspersky Endpoint Security может приостанавливать выполнение задач по расписанию и уступать ресурсы другим приложениям.

Однако существует ряд приложений, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких приложений, не следует уступать им ресурсы операционной системы.

По мере необходимости вы можете запускать эти задачи вручную.

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 "Включение и выключение технологии лечения активного заражения" на стр. 93).

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 317

Включение и выключение режима передачи ресурсов другим приложениям 319

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

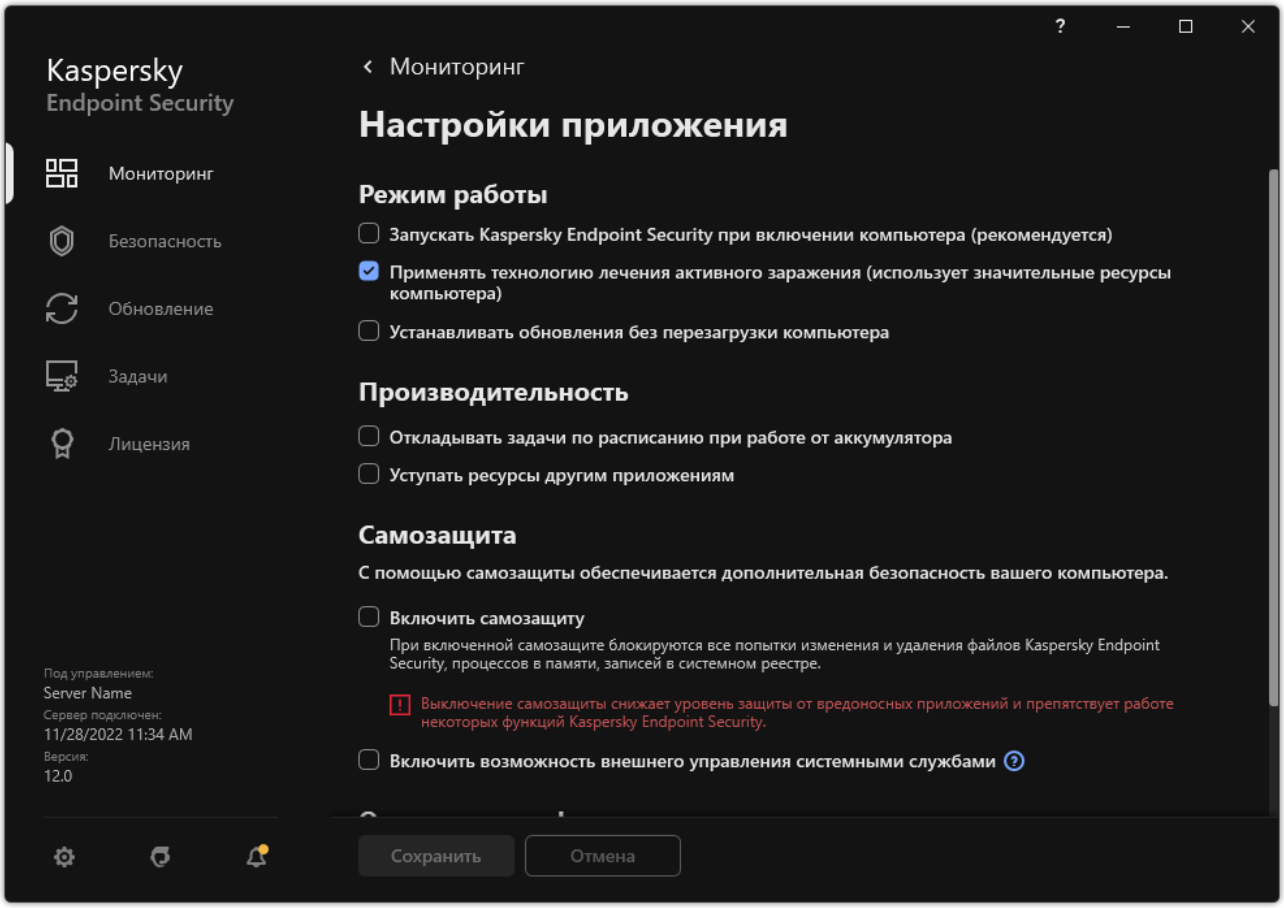


Рисунок 98. Параметры приложения Kaspersky Endpoint Security для Windows

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*;
   - *Полная проверка*;
   - *Проверка важных областей*;
   - *Выборочная проверка*;

- *Проверка целостности*;
- *Поиск IOC*.

4. Сохраните внесенные изменения.

Включение и выключение режима передачи ресурсов другим приложениям

► *Чтобы включить или выключить режим передачи ресурсов другим приложениям, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

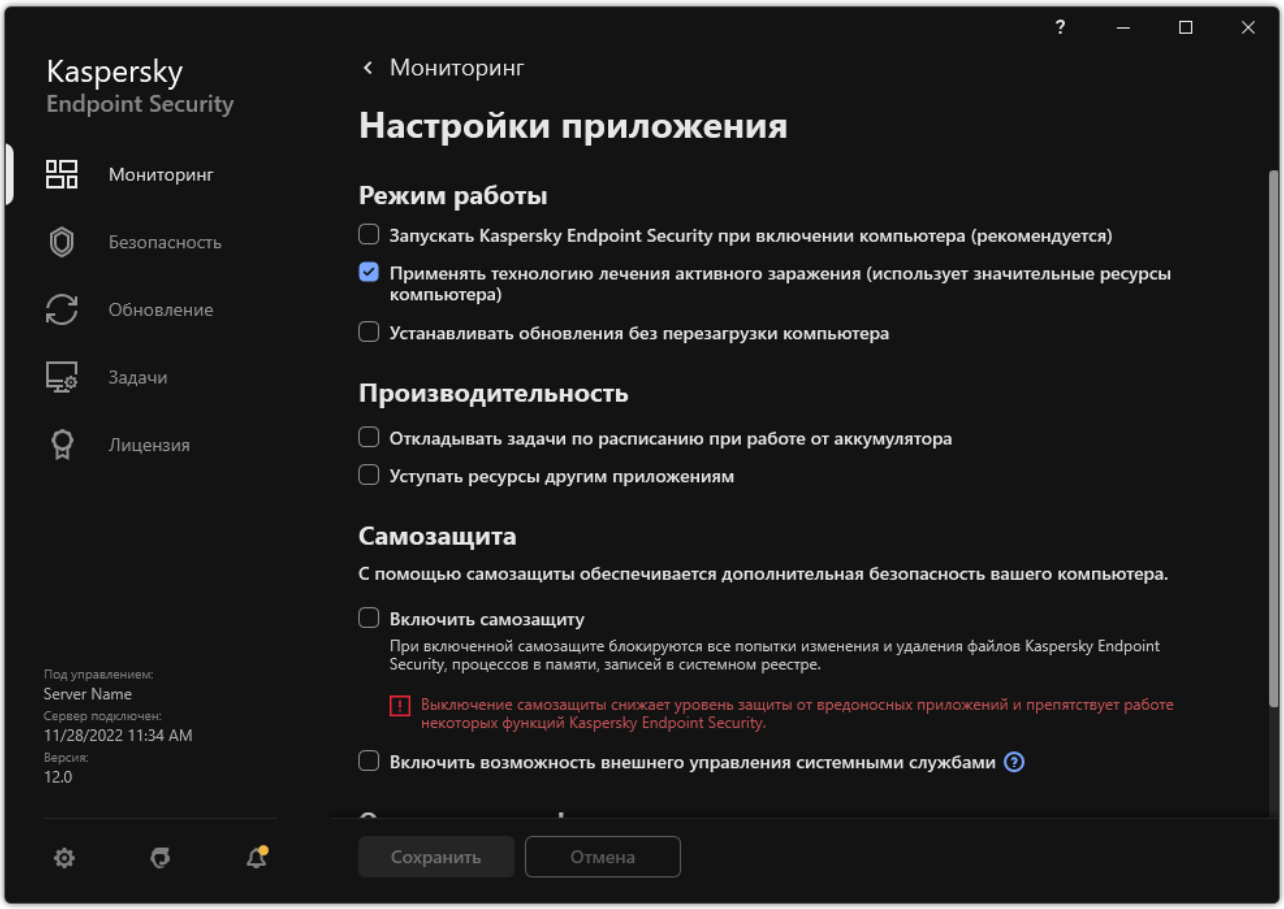


Рисунок 99. Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Производительность** используйте флажок **Уступать ресурсы другим приложениям**, чтобы включить или выключить режим передачи ресурсов другим приложениям.

При включенном режиме передачи ресурсов другим приложениям Kaspersky Endpoint Security откладывает выполнение задач, если для них задан запуск по расписанию и их выполнение замедляет работу других приложений:

- задача обновления;
- задача полной проверки;
- задача проверки важных областей;
- задача выборочной проверки;
- задача проверки целостности.

По умолчанию режим передачи ресурсов другим приложениям включен.

4. Сохраните внесенные изменения.

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 "Установка приложения" на стр. 329).

  Для этого требуется сохранить конфигурационный файл в той же папке, где находится дистрибутив.
- 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).

► *Чтобы создать конфигурационный файл, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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. Сохраните файл.

► *Чтобы импортировать параметры работы Kaspersky Endpoint Security из конфигурационного файла, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

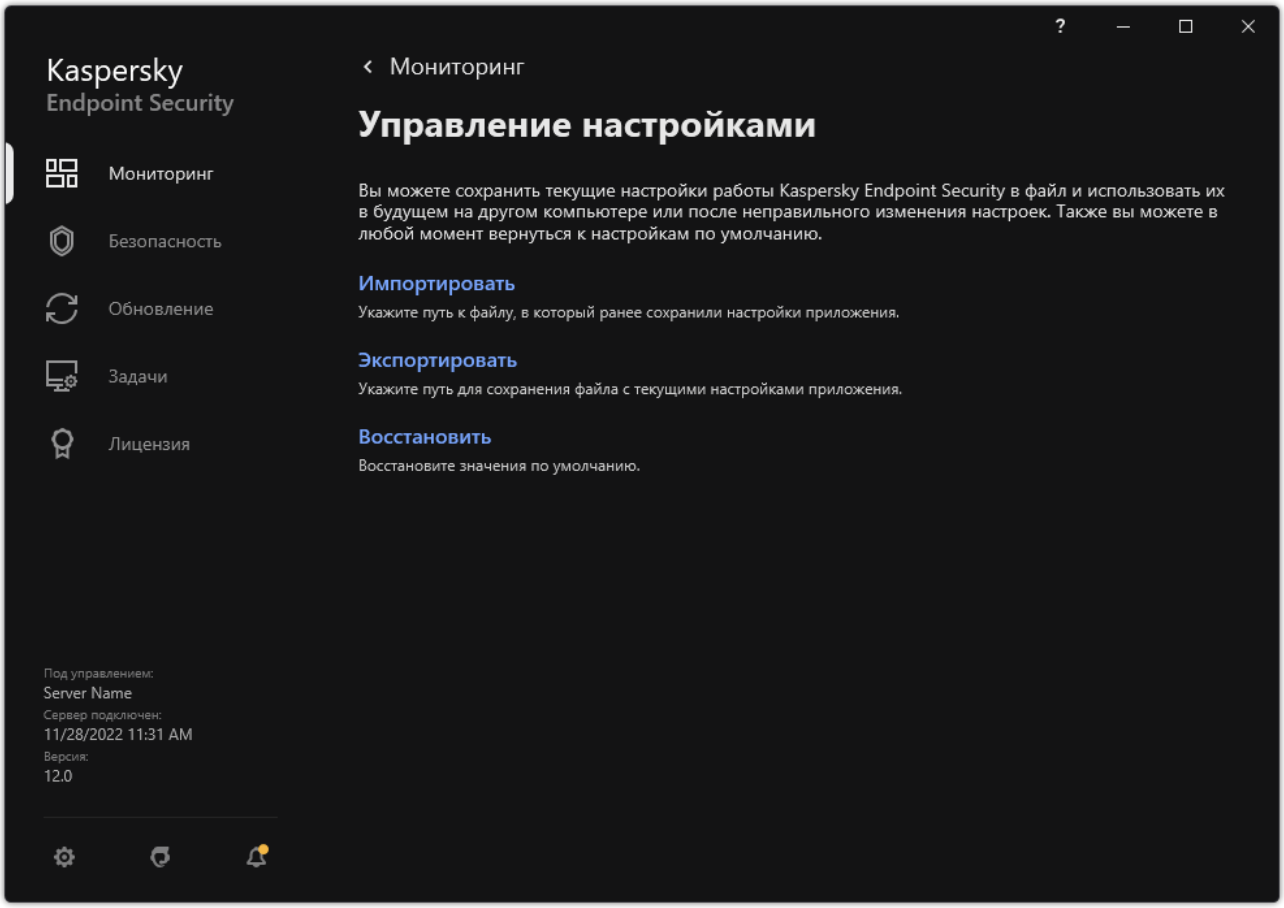


Рисунок 100. Управление настройками приложения

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 **Оптимальный**.

► *Чтобы восстановить параметры приложения по умолчанию, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

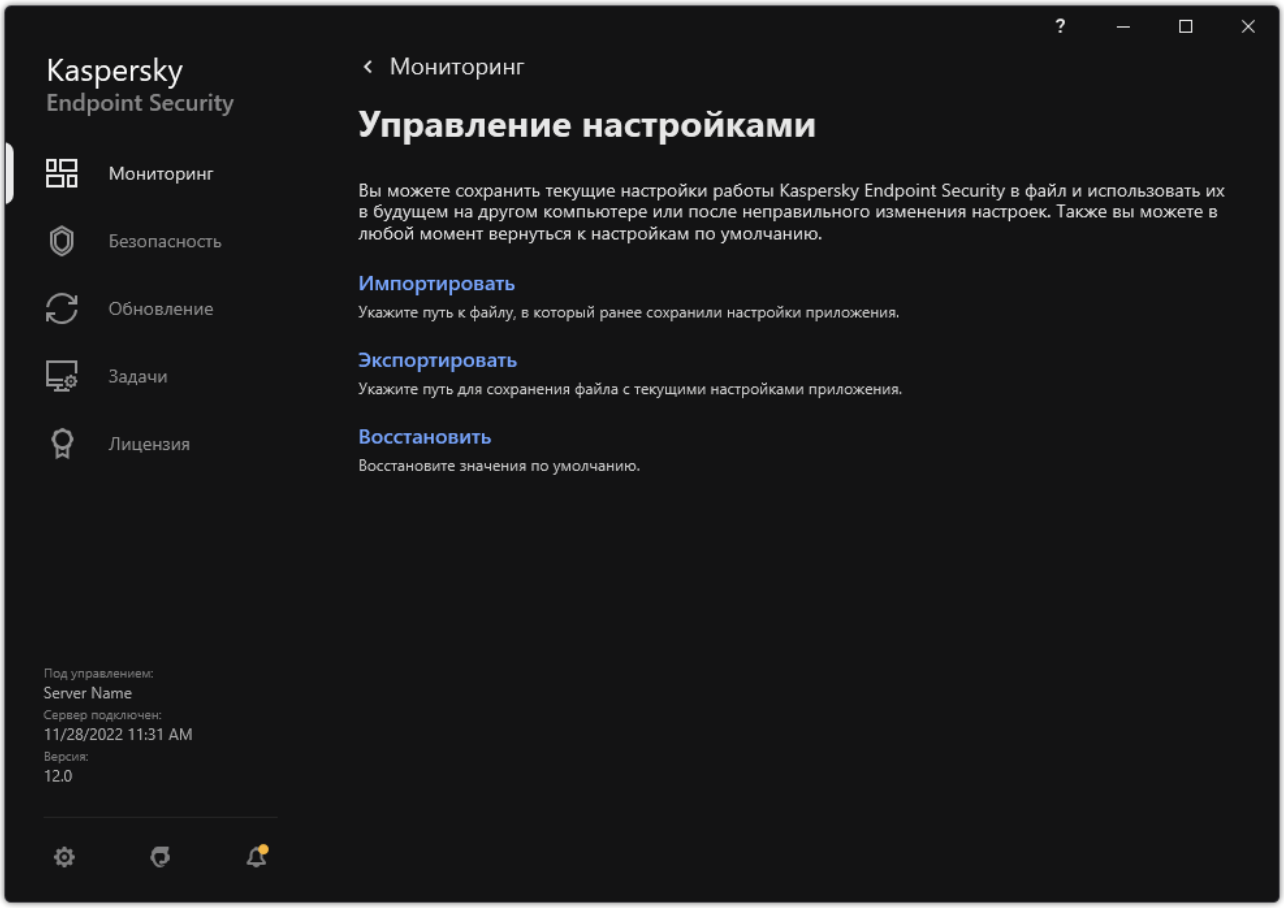


Рисунок 101. Управление настройками приложения

Kaspersky Anti Targeted Attack Platform (EDR)

Kaspersky Endpoint Security для Windows поддерживает работу с компонентом Kaspersky Endpoint Detection and Response в составе решения Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. APT – Advanced Persistent Threat), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя два функциональных блока: Kaspersky Anti Targeted Attack (далее также "*KATA*") и Kaspersky Endpoint Detection and Response (далее также "*EDR (KATA)*"). Вы можете приобрести EDR (KATA) отдельно. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform https://support.kaspersky.com/KATA/6.0/ru-RU/246841.htm.

Средства анализа угроз

Kaspersky Endpoint Detection and Response использует следующие средства анализа угроз (Threat Intelligence):

- Инфраструктура облачных служб Kaspersky Security Network (далее также "KSN"), предоставляющую доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Для работы Kaspersky Endpoint Detection and Response используется решение Kaspersky Private Security Network (KPSN), отправляющее данные на региональные серверы, не передавая данные с устройств в KSN.
- Интеграция с платформой Kaspersky Threat Intelligence Portal https://opentip.kaspersky.com/, которая содержит и отображает информацию о репутации файлов и веб-адресов.
- База угроз "Лаборатории Касперского" Kaspersky Threats https://threats.kaspersky.com/.

Принцип работы решения

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR (KATA) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в консоли Kaspersky Anti Targeted Attack Platform, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

В этом разделе

Интеграция встроенного агента с EDR (KATA) 325

Настройка отправки телеметрии 327

Интеграция встроенного агента с EDR (KATA)

Для интеграции с EDR (KATA) вам нужно добавить компонент Endpoint Detection and Response (KATA). Вы можете выбрать компонент EDR (KATA) во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

Компоненты EDR Optimum, EDR Expert и EDR (KATA) несовместимы между собой.

Для работы Endpoint Detection and Response (KATA) должны быть выполнены следующие условия:

- Kaspersky Anti Targeted Attack Platform версии 4.1 или выше.
- Kaspersky Security Center версии 13.2 или выше. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Endpoint Detection and Response (KATA).
- Приложение активировано и функциональность входит в лицензию.
- Компонент Endpoint Detection and Response (KATA) включен.
- Компоненты приложения, которые обеспечивают работу Endpoint Detection and Response (KATA), включены и работают. Работу EDR (KATA) обеспечивают следующие компоненты:
  - Защита от файловых угроз (см. раздел "Включение и выключение Защиты от файловых угроз" на стр. 131).
  - Защита от веб-угроз (см. раздел "Включение и выключение Защиты от веб-угроз" на стр. 142).
  - Защита от почтовых угроз (см. раздел "Включение и выключение Защиты от почтовых угроз" на стр. 149).
  - Защита от эксплойтов (см. раздел "Включение и выключение Защиты от эксплойтов" на стр. 114).
  - Анализ поведения (см. раздел "Включение и выключение Анализа поведения" на стр. 104).
  - Предотвращение вторжений (см. раздел "Включение и выключение Предотвращения вторжений" на стр. 118).
  - Откат вредоносных действий (на стр. 129).
  - Адаптивный контроль аномалий (см. раздел "Включение и выключение Адаптивного контроля аномалий" на стр. 240).

Интеграция с Endpoint Detection and Response (KATA) состоит из следующих этапов:

1. **Установка компонента Endpoint Detection and Response (KATA)**

   Вы можете выбрать компонент EDR (KATA) 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.

2. **Активация Endpoint Detection and Response (KATA)**

   Вам нужно приобрести отдельную лицензию на использование EDR (KATA) (Kaspersky Endpoint Detection and Response (KATA) Add-on).

Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response (KATA). В результате на компьютере будет установлено два ключа: ключ для Kaspersky Endpoint Security и ключ для Kaspersky Endpoint Detection and Response (KATA).

Лицензирование отдельной функциональности Endpoint Detection and Response (KATA) не отличается от лицензирования Kaspersky Endpoint Security.

Убедитесь, что функциональность EDR (KATA) включена в лицензию и работает в локальном интерфейсе приложения.

3. **Подключение к Central Node**

   Для работы Kaspersky Anti Targeted Attack Platform необходимо установить доверенное соединение между Kaspersky Endpoint Security и компонентом Central Node. Для настройки доверенного соединения вам нужен TLS-сертификат. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform https://support.kaspersky.com/KATA/6.0/ru-RU/247872.htm). Далее вам нужно добавить TLS-сертификат в Kaspersky Endpoint Security (см. инструкцию ниже).

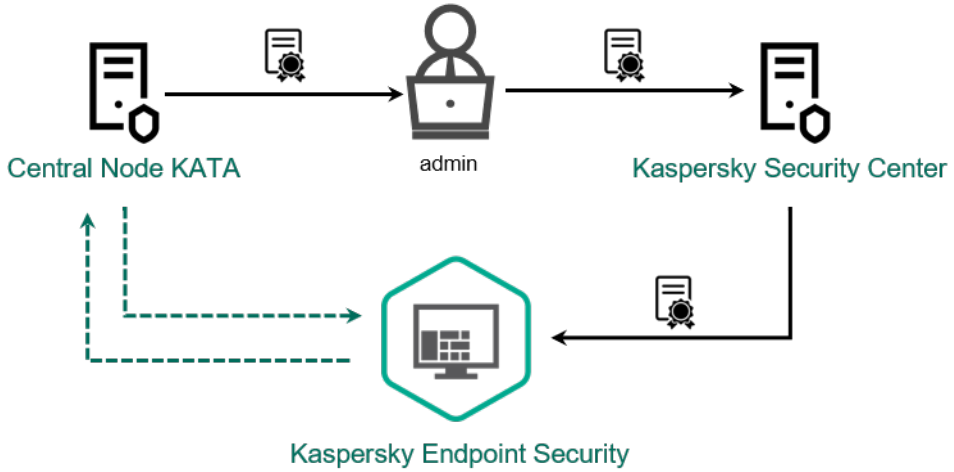


Рисунок 102. Добавление TLS-сертификата в Kaspersky Endpoint Security

   По умолчанию Kaspersky Endpoint Security проверяет только TLS-сертификат Central Node. Чтобы сделать соединение более безопасным, вы можете включить дополнительную проверку компьютера в Central Node (двусторонняя аутентификация). Для включения такой проверки вам нужно включить двустороннюю аутентификацию в параметрах Central Node и Kaspersky Endpoint Security. Также для двусторонней аутентификации вам нужен криптоконтейнер. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform https://support.kaspersky.com/KATA/6.0/ru-RU/247877.htm).

Как подключить компьютер с Kaspersky Endpoint Security к Central Node 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 **Detection and Response** → **Endpoint Detection and Response (KATA)**.
5. Установите флажок **Endpoint Detection and Response (KATA)**.
6. Нажмите на кнопку **Настройки подключения к серверам**.

7. Настройте параметры подключения к серверам:
   - **Время ожидания**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node.
   - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform https://support.kaspersky.com/KATA/6.0/ru-RU/247872.htm).
   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и Central Node. Для использования двусторонней аутентификации вам нужно в параметрах Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform https://support.kaspersky.com/KATA/6.0/ru-RU/247877.htm). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

8. Нажмите на кнопку **OK**.
9. Добавьте серверы Central Node. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.
10. Сохраните внесенные изменения.

    В результате компьютер будет добавлен в консоли Kaspersky Anti Targeted Attack Platform. 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. 304). В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Endpoint Detection and Response (KATA)**.

Настройка отправки телеметрии

Телеметрия – список событий, которые произошли на защищаемом компьютере. Kaspersky Endpoint Security анализирует данные телеметрии и отправляет их на серверы Kaspersky Anti Targeted Attack Platform во время синхронизации. События телеметрии поступают на сервер почти непрерывно. Kaspersky Endpoint Security выполняет синхронизацию с сервером при выполнении любого из следующих условий:

- Истек период синхронизации.
- Количество событий в буфере превысило максимальное значение.

Таким образом, по умолчанию приложение выполняет синхронизацию каждые 30 секунд или при накоплении в буфере 1024 события. Вы можете настроить параметры синхронизации в политике Kaspersky Endpoint Security и выбрать оптимальные значения исходя из нагрузки на сеть (см. инструкцию ниже).

Если соединение между Kaspersky Endpoint Security и сервером отсутствует, то приложение ставит новые события в очередь. При восстановлении соединения Kaspersky Endpoint Security отправляет события из очереди на сервер по порядку. При этом, чтобы не перегрузить сервер, Kaspersky Endpoint Security может отправлять не все события. Для этого вы можете оптимизировать параметры отправки событий и, например, задать максимальное количество событий в час (см. инструкцию ниже).

Если вы используете Kaspersky Anti Targeted Attack Platform совместно с другим решением, которое также использует телеметрию, вы можете выключить отправку телеметрии для KATA (EDR) (см. инструкцию выше). Это позволит оптимизировать нагрузку на серверы для этих решений. Например, если у вас развернуто решение Managed Detection and Response и KATA (EDR), вы можете использовать телеметрию MDR, а создавать задачи реагирования на угрозы в KATA (EDR).

Как настроить параметры отправки EDR-телеметрии 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 **Detection and Response** → **Endpoint Detection and Response (KATA)**.
5. Настройте параметр **Отправлять запрос на синхронизацию на сервер Kaspersky Anti Targeted Attack Platform каждые N минут**. Период отправки запросов на синхронизацию с сервером Central Node. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.
6. Убедитесь, что флажок **Отправлять телеметрию в KATA** установлен.
7. Если требуется, в блоке **Настройка передачи данных** настройте параметр **Максимальное время передачи события**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
8. Если требуется, в блоке **Регулирование количества запросов** установите флажок **Включить регулирование количества запросов**.

   Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события.
9. Настройте параметры оптимизации отправки событий на сервер:
   - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час.
   - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.
10. 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

Установка приложения ... 329
Активация приложения ... 337
Удаление приложения ... 337
Команды AVP ... 338
Команды KESCLI ... 357
Сообщения об ошибках ... 364
Коды возврата ... 367
Коды ошибок ... 373
Использование профилей задач ... 379
Профили приложения ... 380

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. 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).

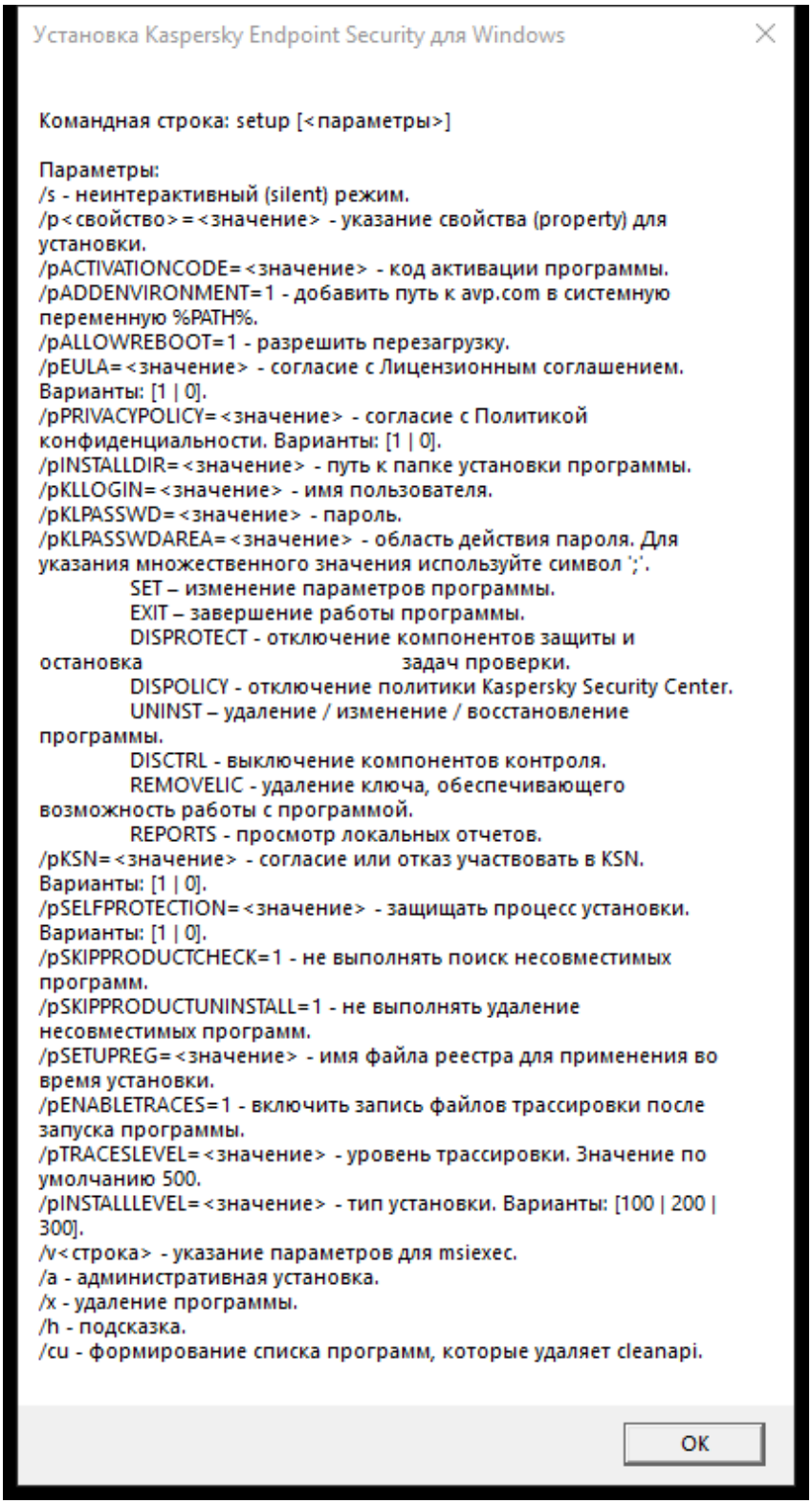


Рисунок 103. Описание параметров команды установки

► *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] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name>
/pKLPASSWD=<password> /pKLPASSWDAREA=<password scope>]
[/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing scope>] [/s]
```

или

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name>
KLPASSWD=<password> KLPASSWDAREA=<password scope>] [ENABLETRACES=1|0
TRACESLEVEL=<tracing scope>] [/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. 348).

Таблица 17. 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.
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 на наличие несовместимого ПО. Список несовместимого ПО приведен в файле incompatible.txt в комплекте поставки. Если параметр не задан, при обнаружении несовместимого ПО установка Kaspersky Endpoint Security будет прекращена.
SKIPPRODUCTUNINSTALL=1	Запрет на автоматическое удаление найденного несовместимого ПО. Если параметр не задан, Kaspersky Endpoint Security пытается удалить несовместимое ПО. Включить автоматическое удаление несовместимого ПО при установке Kaspersky Endpoint Security с помощью установщика msiexec невозможно. Для автоматического удаления несовместимого ПО используйте исполняемый файл setup_kes.exe.
CLEANERSIGNCHECK=0|1	Проверка цифровых подписей файлов найденного несовместимого ПО. Для удаления несовместимого ПО 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 несовместимого ПО. Если приложение не может проверить цифровую подпись файла найденного несовместимого 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 Agent (EDR Agent) для интеграции с решением Kaspersky Endpoint Detection and Response (KATA). 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 Kaspersky Endpoint Detection and Response (KATA) от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response Agent может быть совместим со сторонними EPP-приложениями. Вы также можете использовать EDR Agent для интеграции с решением Kaspersky Managed Detection and Response. Для этого вам нужно изменить состав компонентов приложения.
KLLOGIN	Установка имени пользователя для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (компонент Защита паролем (на стр. 273)). 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. • Например, KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT.
ENABLETRACES	Включение или выключение трассировки приложения. После запуска Kaspersky Endpoint Security приложение сохраняет файлы трассировки в папке %ProgramData%\Kaspersky Lab\KES.21.15\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://docs.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.

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=Passwor
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=60
```

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 (см. раздел "Активация приложения" на стр. 337).

Во время установки приложения или обновления версии приложения в тихом режиме поддерживается использование следующих файлов:

- setup.ini – общие параметры установки приложения;
- install.cfg (см. раздел "Создание и использование конфигурационного файла" на стр. 321) – параметры работы Kaspersky Endpoint Security;
- 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 файлов setup.ini, install.cfg и setup.reg, разместите эти файлы 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>`.

Активация приложения

► *Чтобы активировать приложение с помощью командной строки,*

введите в командной строке:

```
avp.com license /add <activation code or key file> [/login=<user name>
/password=<password>]
```

Учетные данные пользователя (`/login=<user name> /password=<password>`) нужно ввести, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 276).

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. 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. 273):

     ```
     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. 273):

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     или

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Пример:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin
KLPASSWD=!Password1 /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).

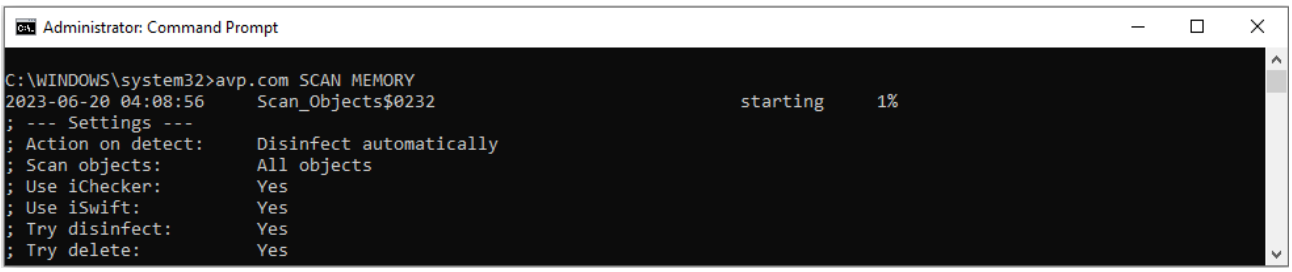


Рисунок 104. Рисунок 104. Управление программой из командной строки

kaspersky

В этом разделе

SCAN. Поиск вредоносного ПО ... 339
UPDATE. Обновление баз и модулей приложения ... 344
ROLLBACK. Откат последнего обновления ... 345
TRACES. Трассировка ... 346
START. Запуск профиля ... 347
STOP. Остановка профиля ... 348
STATUS. Статус профиля ... 348
STATISTICS. Статистика выполнения профиля ... 349
RESTORE. Восстановление файлов из резервного хранилища ... 349
EXPORT. Экспорт параметров приложения ... 350
IMPORT. Импорт параметров приложения ... 351
ADDKEY. Применение файла ключа ... 352
LICENSE. Лицензирование ... 353
RENEW. Приобретение лицензии ... 354
PBATESTRESET. Сбросить результаты проверки перед шифрованием диска ... 354
EXIT. Завершение работы приложения ... 354
EXITPOLICY. Выключение политики ... 354
STARTPOLICY. Включение политики ... 355
DISABLE. Выключение защиты ... 355
SPYWARE. Обнаружение шпионского ПО ... 355
KSN. Переключение KSN / KPSN ... 355
KATAEDR. Интеграция с EDR (KATA) ... 356

SCAN. Поиск вредоносного ПО

Запустить задачу *Поиск вредоносного ПО*.

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.
`/MEMORY`	Проверить память ядра.
`/STARTUP`	Проверить объекты, загрузка которых осуществляется при запуске операционной системы.
`/MAIL`	Проверить почтовый ящик Outlook.
`/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. 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 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 все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет. Этот вариант действия выбран по умолчанию.
/i3	Лечить обнаруженные зараженные файлы. Если лечение невозможно, удалять зараженные файлы. Также удалять составные файлы (например, архивы), если вылечить или удалить зараженный файл невозможно.
/i4	Удалять зараженные файлы. Также удалять составные файлы (например, архивы), если удалить зараженный файл невозможно.
/i8	Запрашивать действие у пользователя сразу после обнаружения угрозы.
/i9	Запрашивать действие у пользователя после выполнения проверки.

Типы файлов

/fe	**Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
/fi	**Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. 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:b	Исключение из проверки почтовых баз, входящих и исходящих сообщений электронной почты.
-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

/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 /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

См. также:

Проверка компьютера 50

Формирование области проверки 65

Scan. Поиск вредоносного ПО 358

Работа с активными угрозами 91

UPDATE. Обновление баз и модулей приложения

Запустить задачу *Обновление*.

Синтаксис команды

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Параметры задачи обновления

`local`	Запуск задачи *Обновление*, созданной автоматически после установки приложения. Вы можете изменить параметры задачи *Обновление* в локальном интерфейсе приложения или в консоли Kaspersky Security Center. Если этот параметр не установлен, Kaspersky Endpoint Security запускает задачу *Обновление* с параметрами по умолчанию или с параметрами, заданными в команде. Таким образом, вы можете настроить параметры задачи *Обновление*, следующим образом: • `UPDATE` – запуск задачи *Обновление* с параметрами по умолчанию: источник обновлений – серверы обновлений "Лаборатории Касперского", учетная запись – System, и другие. • `UPDATE local` – запуск задачи *Обновление*, созданной автоматически после установки (предустановленная задача). • `UPDATE <update settings>` – запуск задача *Обновление* 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

`/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*. 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 76

ROLLBACK. Откат последнего обновления

Откатить последние 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.

Синтаксис команды

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Режим сохранения событий в файл отчета

`/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

Включить / выключить трассировку. Файлы трассировки (см. раздел "О составе и хранении файлов трассировки" на стр. 386) 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.21.15\Traces`. По умолчанию трассировка выключена.

Синтаксис команды

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Уровень трассировки

`<уровень трассировки>` 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 `dbg`, `file` и `mem`.
`dbg`	Использовать функцию OutputDebugString и сохранять файл трассировки. Функция OutputDebugString отправляет символьную строку отладчику приложения для вывода на экран. Подробнее см. на сайте MSDN (https://msdn.microsoft.com/ru-RU/library/windows/desktop/aa363362(v=vs.85).aspx).
`file`	Сохранить один файл трассировки (без ограничений по размеру).
`rot`	Сохранить результаты трассировки в ограниченное число 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 on 500 dbg
avp.com TRACES off
avp.com TRACES on 500 dbg mem
avp.com TRACES off file
```

См. также:

Трассировка работы приложения 389
Трассировка производительности приложения 390
О составе и хранении файлов трассировки 386
Запись дампов 391
Защита файлов дампов и трассировок 391

START. Запуск профиля

Запустить выполнение профиля (например, запустить обновление баз или включить компонент защиты).

Синтаксис команды

```
avp.com START <профиль> [/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. 380) вы можете узнать по команде `HELP START`.

Режим сохранения событий в файл отчета

`/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

Остановить выполняемый профиль (например, остановить проверку съемных дисков или выключить компонент защиты).

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 276). Пользователь должен иметь разрешения **Выключение компонентов защиты**, **Выключение компонентов контроля**.

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. 380) 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. 277).

STATUS. Статус профиля

Показать информацию о состоянии профилей приложения (см. раздел "Профили приложения" на стр. 380) (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".

Синтаксис команды

```
avp.com STATUS [<profile>]
```

Если вы введете команду без профиля, Kaspersky Endpoint Security покажет состояние всех профилей приложения.

STATISTICS. Статистика выполнения профиля

Показать статистическую информацию о профиле приложения (см. раздел "Профили приложения" на стр. 380) (например, время проверки или количество обнаруженных угроз). Список доступных профилей вы можете узнать по команде `HELP STATISTICS`.

Синтаксис команды

```
avp.com STATISTICS <profile>
```

RESTORE. Восстановление файлов из резервного хранилища

Восстановить файл из резервного хранилища в папку его исходного размещения. Если по указанному пути уже существует файл с таким же именем, к имени файла добавляется суффикс "-copy". Восстанавливаемый файл копируется с исходным именем.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 276). 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.21.15\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.

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. 277).

Пример:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Экспорт параметров приложения

Экспортировать параметры Kaspersky Endpoint Security в файл. Файл будет размещен в папке `C:\Windows\SysWOW64`.

Синтаксис команды

```
avp.com EXPORT <profile> <file name>
```

Профиль

`<profile>`	Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Профили приложения" на стр. 380) вы можете узнать по команде `HELP EXPORT`.

Файл для экспорта

`<file name>`	Имя файла, в который должны быть экспортированы параметры профиля. 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.

Примеры:

```
avp.com EXPORT ids ids_config.dat
avp.com EXPORT fm fm_config.txt
```

См. также:

Создание и использование конфигурационного файла 321

IMPORT. Импорт параметров приложения

Импортировать параметры 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. 276). Пользователь должен иметь разрешение **Настройка 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. 277).

Пример:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

См. также:

Создание и использование конфигурационного файла 321

ADDKEY. Применение файла ключа

Применить файл ключа для активации Kaspersky Endpoint Security. Если приложение уже активировано, ключ будет добавлен в качестве резервного.

Синтаксис команды

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Файл ключа

`<имя файла>`	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. 273).

Пример:

```
avp.com ADDKEY file.key
```

LICENSE. Лицензирование

Выполнить операции с 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. 276). Пользователь должен иметь разрешение **Удаление ключа**.

Синтаксис команды

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Операция

`/ADD <file name>`	Применить файл ключа для активации Kaspersky Endpoint Security. 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 EDR`	Обновить статус лицензии Kaspersky Endpoint Detection and Response Add-on. В результате приложение получает актуальную информацию о статусе лицензии с серверов активации "Лаборатории Касперского".
`/DEL /login=<user name> /password=<password>`	Удалить лицензионный ключ приложения. Также будет удален резервный ключ.
`/DEL EDR /login=<user name> /password=<password>`	Удалить лицензионный ключ Kaspersky Endpoint Detection and Response Add-on. Также будет удален резервный ключ.

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. 277).

Пример:

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL EDR /login=KLAdmin /password=!Password1
```

RENEW. Приобретение лицензии

Перейти на веб-сайт "Лаборатории Касперского" для приобретения лицензии или продления ее срока действия.

PBATESTRESET. Сбросить результаты проверки перед шифрованием диска

Сбросить результаты проверки поддержки полнодискового шифрования (FDE) по технологиям Шифрование диска Kaspersky и BitLocker.

Перед запуском полнодискового шифрования приложение выполняет ряд проверок на возможность шифрования компьютера. Если полнодисковое шифрование невозможно, Kaspersky Endpoint Security сохраняет информацию о несовместимости. При следующей попытке шифрования приложение не выполняет проверки и предупреждает о том, что шифрование невозможно. Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с технологией Шифрования диска Kaspersky или BitLocker требуется сбросить информацию о несовместимости, полученную приложением при предыдущей проверке.

EXIT. Завершение работы приложения

Завершить работу 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. 276). Пользователь должен иметь разрешение **Завершение работы приложения**.

Синтаксис команды

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Выключение политики

Выключает политику 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. 276). Пользователь должен иметь разрешение **Выключение политики Kaspersky Security Center**.

Синтаксис команды

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Включение политики

Включить политику Kaspersky Security Center на компьютере. Параметры приложения будут настроены в соответствии с политикой.

DISABLE. Выключение защиты

Выключить Защиту от файловых угроз на компьютере с истекшей лицензией на Kaspersky Endpoint Security. Выполнить команду на компьютере с неактивированным приложением или с действующей лицензией невозможно.

SPYWARE. Обнаружение шпионского ПО

Включить / выключить обнаружение шпионского ПО. По умолчанию обнаружение шпионского ПО включено.

Синтаксис команды

```
avp.com SPYWARE on|off
```

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 приложение "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.

Синтаксис команды

```
avp.com KSN /global | /private <file name>
```

Конфигурационный файл Kaspersky Security Network	
`<имя файла>`	Имя конфигурационного файла с параметрами Kaspersky Private Security Network. Файл имеет разрешение PKCS7 или PEM.

Пример:

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

См. также:

Включение и выключение использования Kaspersky Security Network 98
Включение и выключение облачного режима для компонентов защиты 99
Проверка репутации файла в Kaspersky Security Network 101

KATAEDR. Интеграция с EDR (KATA)

Команды управления компонентом Endpoint Detection and Response (KATA):

- Включить или выключить компонент EDR (KATA).

  Компонент EDR (KATA) обеспечивает взаимодействие с решением Kaspersky Anti Targeted Attack Platform.
- Настроить параметры подключения к серверам Kaspersky Anti Targeted Attack Platform.
- Показать текущие параметры работы компонента.

Синтаксис команды

```
avp.com START KATAEDR
avp.com STOP KATAEDR
avp.com kataedr /set /server=<адрес сервера>:<порт> /server-certificate=<путь к TLS-сертификату> [/timeout=<время ожидания соединения с сервером Central Node (с)>] [/sync-period=<период синхронизации с сервером Central Node (мин)>]
avp.com kataedr /show
```

Операция

`stop`	Выключить компонент EDR (KATA).
`start`	Включить компонент EDR (KATA).
`set`	Настроить параметры работы компонента EDR (KATA). Вы можете настроить следующие параметры: • добавление серверов Central Node (`server=<адрес сервера>:<порт>`); • добавление TLS-сертификата (`server-certificate=<путь к TLS-сертификату>`); • установка времени ожидания соединения с сервером Central Node (`/timeout=<время ожидания соединения с сервером Central Node (с)>`); • установка периода синхронизации с сервером Central Node (`/sync-period=<период синхронизации с сервером Central Node (мин)>`).
`show`	Показать текущие параметры работы компонента.

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*).

Вы можете просмотреть список команд KESCLI с помощью команды `--help` или сокращенной команды `-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).

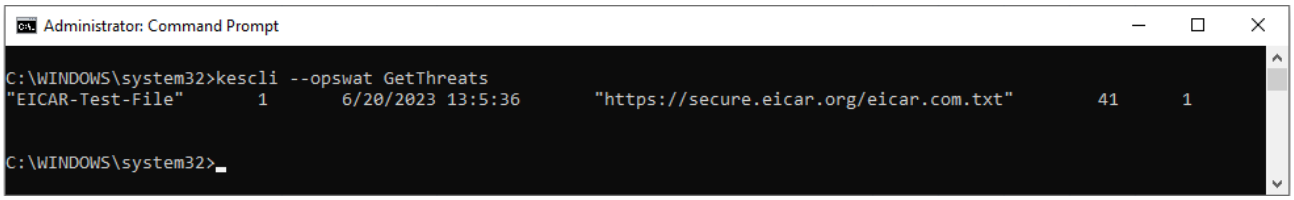


Рисунок 105. Рисунок 105. Управление приложением из командной строки

В этом разделе

Scan. Поиск вредоносного ПО 358
GetScanState. Статус выполнения проверки 359
GetLastScanTime. Определения времени выполнения проверки 360
GetThreats. Получение данных об обнаруженных угрозах 360
UpdateDefinitions. Обновление баз и модулей приложения 362
GetDefinitionState. Определение времени выполнения обновления 363
EnableRTP. Включение защиты 363
GetRealTimeProtectionState. Статус Защиты от файловых угроз 363
Version. Определение версии приложения 363

Scan. Поиск вредоносного ПО

Запустить задачу *Поиск вредоносного ПО* (Полная проверка).

> Для запуска задачи администратору нужно разрешить использование локальных задач в политике (см. раздел "Управление задачами" на стр. 32).

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. 359) и посмотреть дату и время последнего выполнения проверки с помощью команды `GetLastScanTime` (см. раздел "`GetLastScanTime. Определения времени выполнения проверки`" на стр. 360).

Область проверки

`<файлы для проверки>`	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 все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет. 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 50

Формирование области проверки 65

SCAN. Поиск вредоносного ПО 339

Работа с активными угрозами 91

GetScanState. Статус выполнения проверки

Получить информацию о статусе выполнения задачи *Поиск вредоносного ПО* (Полная проверка):

- `1` – проверка выполняется.
- `0` – проверка не запущена.

Синтаксис команды

```
kescli --opswat GetScanState
```

GetLastScanTime. Определения времени выполнения проверки

Получить информацию о дате и времени последнего выполнения задачи *Поиск вредоносного ПО* (Полная проверка).

Синтаксис команды

```
kescli --opswat GetLastScanTime
```

GetThreats. Получение данных об обнаруженных угрозах

Получить список обнаруженных угроз (*Отчет об угрозах*). Отчет содержит информацию об угрозах и вирусной активности за 30 дней до момента создания отчета.

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>
```

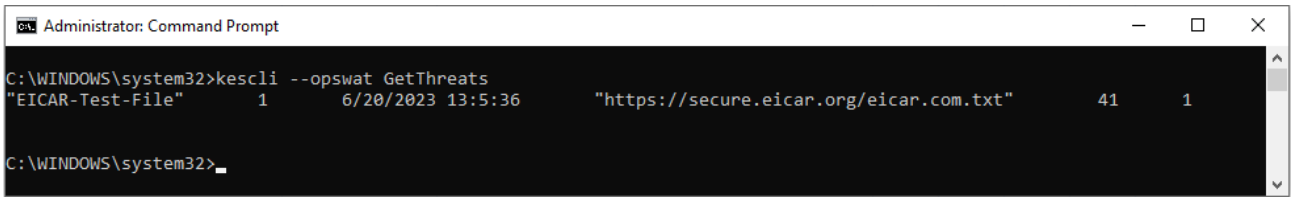


Рисунок 106. Управление приложением из командной строки

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

Запустить задачу *Обновление*. 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. 32).

Синтаксис команды

```
kescli --opswat UpdateDefinitions
```

Вы можете просмотреть дату и время выполнения последней задачи *Обновление* с помощью команды GetDefinitionsetState (см. раздел "GetDefinitionState. Определение времени выполнения обновления" на стр. 363).

GetDefinitionState. Определение времени выполнения обновления

Получить информацию о дате и времени последнего выполнения задачи *Обновление*.

Синтаксис команды

```
kescli --opswat GetDefinitionState
```

EnableRTP. Включение защиты

Включить компоненты 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).

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. 276).

Вы можете проверить статус работы Защиты от файловых угроз с помощью команды `GetRealTimeProtectionState` (см. раздел "`GetRealTimeProtectionState. Статус Защиты от файловых угроз`" на стр. 363).

GetRealTimeProtectionState. Статус Защиты от файловых угроз

Получить информацию о статусе работы компонента Защита от файловых угроз:

- `1` – компонент включен.
- `0` – компонент выключен.

Синтаксис команды

```
kescli --opswat GetRealTimeProtectionState
```

Version. Определение версии приложения

Определить версию приложения Kaspersky Endpoint Security для Windows.

Синтаксис команды

```
kescli --Version
```

Вы также можете использовать сокращенную команду `-v`.

Сообщения об ошибках

При работе с программой возможно появление следующих сообщений об ошибках:

Таблица 18. 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 19. 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

Символьные значения	Числовые значения	Доступно для команд
_Shell::_E_KEY_CORRUPTED	-8	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_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

Символьные значения	Числовые значения	Доступно для команд
errACCESS_DENIED	8000045	STOP EXITPOLICY
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 20. 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	Внутренние данные несовместимые с текущим приложением
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.21.15\profiles` или `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.21.15\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`, `EXPORT` и `IMPORT`. 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.
- `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.
- `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 ОС.
- `Scan_Removable_Drive` – Проверка съемных дисков.
- `Scan_Startup` или `STARTUP` – Проверка важных областей.
- `Updater` – Обновление.
- `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. 383).

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).

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.

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 386

Трассировка работы приложения 389

Трассировка производительности приложения 390

Запись дампов 391

Защита файлов дампов и трассировок 391

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.21.15\Traces`.

Файлы трассировки называются следующим образом:
`KES<21.15_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<21.15_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-<тип файла трассировки>.DESKTOP-<дата обновления файла>.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.

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 ротацией**. Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера. Если выбран этот режим, вы можете указать максимальное количество файлов для ротации и максимальный размер каждого файла.
   - **Записывать в один файл**. 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 (500)**.
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 "Установка приложения" на стр. 329), в том числе с помощью файла setup.ini.

В результате в папке `%ProgramData%\Kaspersky Lab\KES.21.15\Traces` будет создан файл трассировки работы приложения. После создания файла трассировки отправьте файл 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. 44).

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. 386). *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. ETW – Event Tracing for Windows). 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 ротацией**. 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.
   - **Записывать в один файл**. 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.21.15\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.21.15\Traces`.

► *Чтобы включить или выключить запись дампов, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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 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. 386). 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.

► *Чтобы включить или выключить защиту файлов дампов и файлов трассировки, выполните следующие действия:*

1. В главном окне приложения (см. раздел "Интерфейс приложения" на стр. 38) 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.

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.

Р

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их лечением или удалением.

С

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.

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.

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 21. 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

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.

Таблица 22. 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).
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.
Защита от файловых угроз	Действие при обнаружении угрозы	Лечить. Удалять, если лечение невозможно
Защита от файловых угроз → Расширенная настройка	Типы файлов	Одно из следующих значений: • Все файлы. • Файлы, проверяемые по формату.
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.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
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 атакающие 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.
Detection and Response		
Endpoint Detection and Response (KATA)	Endpoint Detection and Response (KATA)	Флажок установлен.
Сервер KATA	Адрес и порт	IP-адрес и порт сервера Central Node.
Настройки подключения к серверам	TLS-сертификат	TLS-сертификат добавлен.
Настройки подключения к серверам	Использовать двустороннюю аутентификацию	Флажок установлен. Криптоконтейнер добавлен.
Контроль безопасности		
Контроль приложений	Контроль приложений	Переключатель включен.
Контроль устройств	Контроль устройств	Переключатель включен.

Задачи		
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.
Интерфейс	Защита паролем	Переключатель включен. Администратор безопасности должен установить надежный пароль и область действия (все опции).

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.

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;

eml – сообщение электронной почты Microsoft Outlook Express;

nws – новое сообщение электронной почты Microsoft Outlook Express;

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 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;

eml – сообщение электронной почты Microsoft Outlook Express;

nws – новое сообщение электронной почты Microsoft Outlook Express;

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

Приложение Kaspersky Endpoint Security использует следующие сетевые параметры для взаимодействия с внешними службами.

Таблица 23. Сетевые параметры

Адрес	Описание
activation-v2.kaspersky.com/activationservice/activationservice.svc Протокол: HTTPS Порт: 443	Активация приложения.
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 проверки сертификата веб-ресурса при обращении по HTTPS. Если приложение Kaspersky Endpoint Security использует публичный DNS-сервер, правила обработки данных регламентируются Политикой конфиденциальности этого сервиса. Если требуется запретить приложению Kaspersky Endpoint Security использовать публичный DNS-сервер, обратитесь в Службу технической поддержки за приватным патчем.
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.

Адрес	Описание
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.
ds.kaspersky.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: Any Порт: 443, 1443	Использование Kaspersky Security Network.

Адрес	Описание
click.kaspersky.com redirect.kaspersky.com Протокол: HTTPS	Переход по ссылкам из интерфейса.

Таблица 24. Параметры, использующиеся для шифрования

Адрес	Описание
crl.kaspersky.com ocsp.kaspersky.com Протокол: HTTP Порт: 80	Инфраструктура открытых ключей (англ. Public Key Infrastructure – PKI).