

KASPERSKY

Kaspersky Security Center 10

Руководство по эксплуатации

643.46856491.00069-05 90 01

Версия программы: 10.5.1781.0

Уважаемый пользователь!

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

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

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

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

Документ может быть изменен без предварительного уведомления.

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

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

Дата редакции документа: 11.05.2018

Обозначение документа:

© АО "Лаборатория Касперского", 2018.

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

Содержание

Об этом документе	16
Источники информации о программе	17
Источники для самостоятельного поиска информации	17
Обсуждение программ "Лаборатории Касперского" на форуме	19
О программе	20
Настройка прав. Роли пользователей	20
Добавление роли пользователя	21
Назначение роли пользователю или группе пользователей	22
Права доступа к Серверу администрирования и его объектам	23
Управление Серверами администрирования	25
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования	26
Подключение к Серверу администрирования и переключение между Серверами администрирования	31
Условия подключения к Серверу администрирования через интернет	33
Защищенное подключение к Серверу администрирования	34
Аутентификация Сервера при подключении устройства	34
Аутентификация Сервера при подключении Консоли администрирования	35
Сертификат Сервера администрирования	35
Отключение от Сервера администрирования	36
Добавление Сервера администрирования в дерево консоли	36
Удаление Сервера администрирования из дерева консоли	36
Добавление виртуального Сервера администрирования в дерево консоли	37
Смена учетной записи службы Сервера администрирования. Утилита klsrvswch	38
Просмотр и изменение параметров Сервера администрирования	40
Настройка общих параметров Сервера администрирования	40
Обработка и хранение событий на Сервере администрирования	41
Контроль возникновения вирусных эпидемий	42
Ограничение трафика	42
Настройка параметров Веб-сервера	44

Работа с внутренними пользователями	44
Управление группами администрирования.....	45
Создание групп администрирования.....	46
Перемещение групп администрирования	48
Удаление групп администрирования	49
Автоматическое создание структуры групп администрирования.....	50
Автоматическая установка программ на устройства группы администрирования.....	52
Автономные пользователи.....	52
Создание профиля подключения к Серверу администрирования для автономных пользователей.....	54
Создание правила переключения Агента администрирования по сетевому местоположению	59
Удаленное управление программами	62
Управление политиками.....	62
Создание политики.....	64
Отображение унаследованной политики во вложенной группе	66
Активация политики.....	66
Автоматическая активация политики по событию "Вирусная атака"	67
Применение политики для автономных пользователей.....	67
Изменение политики. Откат изменений	68
Сравнение политик.....	68
Удаление политики.....	70
Копирование политики	70
Экспорт политики.....	71
Импорт политики	71
Конвертация политик.....	72
Управление профилями политик.....	72
О профиле политики	73
Создание профиля политики.....	77
Изменение профиля политики	78
Удаление профиля политики.....	79
Создание правила активации профиля политики.....	80
Управление задачами	86
Создание задачи	90

Создание задачи Сервера администрирования	90
Создание задачи для набора устройств	92
Создание локальной задачи	93
Отображение унаследованной групповой задачи в рабочей области вложенной группы	94
Автоматическое включение устройств перед запуском задачи	94
Автоматическое выключение устройства после выполнения задачи	95
Ограничение времени выполнения задачи	95
Экспорт задачи	96
Импорт задачи	96
Конвертация задач	97
Запуск и остановка задачи вручную	98
Приостановка и возобновление задачи вручную	99
Наблюдение за ходом выполнения задачи	99
Просмотр результатов выполнения задач, хранящихся на Сервере администрирования.....	99
Настройка фильтра информации о результатах выполнения задачи.....	100
Изменение задачи. Откат изменений.....	100
Сравнение задач	101
Учетные записи для запуска задач	103
Установка программы с помощью групповых политик Active Directory.....	103
Просмотр и изменение локальных параметров программы.....	105
Управление клиентскими устройствами.....	106
Подключение клиентских устройств к Серверу администрирования	108
Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover	110
Туннелирование соединения клиентского устройства с Сервером администрирования.....	112
Удаленное подключение к рабочему столу клиентского устройства.....	113
Подключение к устройствам с помощью Windows Desktop Sharing.....	115
Настройка перезагрузки клиентского устройства	116
Аудит действий на удаленном клиентском устройстве	117
Проверка соединения клиентского устройства с Сервером администрирования.....	119
Автоматическая проверка соединения клиентского устройства с Сервером администрирования.....	119

Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk	120
Проверка времени соединения устройства с Сервером администрирования.....	121
Идентификация клиентских устройств на Сервере администрирования	122
Перемещение устройств в состав группы администрирования	122
Смена Сервера администрирования для клиентских устройств	123
Кластеры и массивы серверов	124
Удаленное включение, выключение и перезагрузка клиентских устройств	125
Доступ к локальным задачам и статистике, флажок "Не разрывать соединение с Сервером администрирования"	126
Форсирование синхронизации	127
О менеджере соединений	127
Отправка сообщения пользователям устройств	128
Работа с программой Kaspersky Security для виртуальных сред.....	128
Контроль изменения состояния виртуальных машин	129
Настройка переключения статусов устройств	130
Отслеживание состояния антивирусной защиты с помощью информации в системном реестре	136
Назначение тегов устройствам и просмотр назначенных тегов.....	138
Автоматическое назначение тегов устройствам	140
Просмотр и настройка тегов, назначенных устройству	142
Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center	143
Подключение утилиты удаленной диагностики к клиентскому устройству ...	144
Включение и выключение трассировки, загрузка файла трассировки	146
Загрузка параметров программ	147
Загрузка журналов событий.....	148
Запуск диагностики и загрузка ее результатов	148
Запуск, остановка и перезапуск программ.....	149
Устройства с защитой на уровне UEFI	149
Параметры управляемого устройства	150
Параметры политики Агента администрирования	158
Управление учетными записями пользователей.....	173
Работа с учетными записями пользователей.....	174
Добавление учетной записи пользователя.....	175

Настройка проверки уникальности имени внутреннего пользователя	176
Добавление группы пользователей.....	178
Добавление пользователя в группу	179
Назначение пользователя владельцем устройства.....	179
Рассылка сообщений пользователям	180
Просмотр списка мобильных устройств пользователя.....	181
Установка сертификата пользователю	182
Просмотр списка сертификатов, выписанных пользователю	183
Об администраторе виртуального Сервера	183
Работа с отчетами, статистикой и уведомлениями.....	184
Работа с отчетами	184
Создание шаблона отчета	185
Создание и просмотр отчета	186
Сохранение отчета	186
Создание задачи рассылки отчета.....	187
Шаг 1. Выбор типа задачи	188
Шаг 2. Выбор типа отчета.....	188
Шаг 3. Действия с отчетом	188
Шаг 4. Выбор учетной записи для запуска задачи.....	190
Шаг 5. Настройка расписания задачи	190
Шаг 6. Определение названия задачи.....	195
Шаг 7. Завершение создания задачи.....	196
Работа со статистической информацией.....	196
Настройка параметров уведомлений о событиях	197
Создание сертификата для SMTP-сервера	199
Выборки событий	200
Просмотр выборки событий.....	201
Настройка параметров выборки событий.....	201
Создание выборки событий.....	202
Экспорт выборки событий в текстовый файл	202
Удаление событий из выборки	203
Настройка экспорта событий в SIEM-систему	203
Выборки устройств	205
Просмотр выборки устройств	205

Настройка параметров выборки устройств	206
Экспорт параметров выборки устройств в файл.....	206
Создание выборки устройств	207
Создание выборки устройств по импортированным параметрам	207
Удаление устройств из групп администрирования в выборке	208
Параметры условий выборки устройств	209
Политики.....	224
Задачи	225
Работа с ревизиями объектов.....	225
О ревизиях объектов	228
Просмотр раздела История ревизий	228
Сравнение ревизий объекта	229
Просмотр ревизии объекта	231
Сохранение ревизии объекта в файле	232
Откат изменений.....	232
Добавление описания ревизии	233
Нераспределенные устройства	233
Опрос сети.....	234
Просмотр и изменение параметров опроса сети Windows.....	235
Просмотр и изменение параметров опроса групп Active Directory	236
Просмотр и изменение параметров опроса IP-диапазонов	236
Работа с доменами Windows. Просмотр и изменение параметров домена.....	237
Работа с IP-диапазонами	237
Создание IP-диапазона.....	238
Просмотр и изменение параметров IP-диапазона.....	238
Работа с группами Active Directory. Просмотр и изменение параметров группы	238
Создание правил автоматического перемещения устройств в группы администрирования.....	239
Использование динамического режима VDI на клиентских устройствах.....	239
Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования	241
Поиск устройств, являющихся частью VDI	241
Перемещение в группу администрирования устройств, являющихся частью VDI	242

Управление программами на клиентских устройствах.....	242
Группы программ	243
Создание категорий программ	246
Создание пополняемой вручную категории программ	247
Создание автоматически пополняемой категории программ	250
Добавление событий в категорию программ	254
Настройка управления запуском программ на клиентских устройствах	256
Просмотр результатов статического анализа правил запуска исполняемых файлов	258
Просмотр реестра программ	259
Создание групп лицензионных программ	260
Управление ключами для групп лицензионных программ	261
Инвентаризация программного обеспечения Kaspersky Security Center	262
Инвентаризация исполняемых файлов	263
Просмотр информации об исполняемых файлах	264
Уязвимости в программах	265
Просмотр информации об уязвимостях в программах	266
Поиск уязвимостей в программах.....	267
Закрытие уязвимостей в программах.....	268
Обновления программного обеспечения	269
Просмотр информации о доступных обновлениях	271
Синхронизация обновлений Windows Update с Сервером администрирования.....	272
Шаг 1. Параметры	274
Шаг 2. Программы	275
Шаг 3. Категории обновлений.....	275
Шаг 4. Языки локализации обновлений.....	275
Шаг 5. Выбор учетной записи для запуска задачи.....	276
Шаг 6. Настройка расписания запуска задачи	276
Шаг 7. Определение названия задачи.....	281
Шаг 8. Завершение создания задачи.....	281
Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства.....	282
Офлайн-модель получения обновлений	284
Включение и выключение офлайн-модели получения обновлений	286

Установка обновлений на устройства вручную.....	288
Настройка обновлений Windows в политике Агента администрирования	291
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center	293
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	295
Отмена обновлений программного обеспечения.....	296
Удаленная установка приложений на устройства с установленным Агентом администрирования	297
Управление мобильными устройствами	298
О групповой политике управления EAS и iOS MDM-устройствами	299
Поддержка мобильных устройств.....	301
Включение поддержки мобильных устройств.....	302
Изменение параметров поддержки мобильных устройств.....	304
Выключение поддержки мобильных устройств	306
Работа с командами для мобильных устройств.....	307
Команды для управления мобильными устройствами	307
Использование Google Firebase Cloud Messaging.....	311
Отправка команд	313
Просмотр статусов команд в журнале команд	314
Работа с сертификатами.....	315
Установка сертификата.....	316
Шаг 1. Тип сертификата	317
Шаг 2. Тип устройства	317
Шаг 3. Выбор пользователя	318
Шаг 4. Источник сертификата.....	318
Шаг 5. Тег сертификата.....	319
Шаг 6. Способ уведомления пользователей.....	320
Настройка правил выпуска сертификатов	321
Интеграция с инфраструктурой открытых ключей	322
Включение поддержки Kerberos Constrained Delegation.....	324
Добавление мобильных устройств в список управляемых устройств	324
Управление мобильными устройствами Exchange ActiveSync	334
Добавление профиля управления	335
Удаление профиля управления	337

Работа с политиками Exchange ActiveSync	338
Настройка области сканирования	339
Работа с EAS-устройствами	339
Просмотр информации о EAS-устройстве.....	340
Отключение EAS-устройства от управления.....	340
Права пользователя для управления мобильными устройствами Exchange ActiveSync.....	341
Управление iOS MDM-устройствами.....	343
Выписка сертификата iOS MDM-профиля	345
Добавление конфигурационного профиля	346
Установка конфигурационного профиля на устройство	347
Удаление конфигурационного профиля с устройства	349
Добавление нового устройства посредством публикации ссылки на профиль	350
Добавление нового устройства посредством установки профиля администратором	351
Добавление provisioning-профиля.....	351
Установка provisioning-профиля на устройство.....	352
Удаление provisioning-профиля с устройства	354
Добавление управляемого приложения	355
Установка приложения на мобильное устройство	356
Удаление приложения с устройства	358
Установка приложения Kaspersky Safe Browser на мобильное устройство ..	359
Настройка параметров роуминга на мобильном устройстве iOS MDM.....	360
Просмотр информации о iOS MDM-устройстве	361
Отключение iOS MDM-устройства от управления	362
Отправка команд на устройство	363
Проверка статуса исполнения отправленных команд	363
Управление KES-устройствами	364
Создание пакета мобильных приложений для KES-устройств	364
Включение двухфакторной аутентификации KES-устройств.....	366
Просмотр информации о KES-устройстве.....	367
Отключение KES-устройства от управления.....	367
Инвентаризация оборудования, обнаруженного в сети.....	368
Добавление информации о новых устройствах	369

Настройка критериев определения корпоративных устройств	370
Настройка пользовательских полей	371
Обновление баз и программных модулей.....	372
Создание задачи загрузки обновлений в хранилище	373
Создание задачи принудительной загрузки обновлений в хранилища агентов обновлений.....	375
Настройка параметров задачи загрузки обновлений в хранилище	377
Проверка полученных обновлений.....	377
Настройка проверочных политик и вспомогательных задач	379
Просмотр полученных обновлений	381
Автоматическое распространение обновлений	381
Автоматическое распространение обновлений на клиентские устройства ..	382
Автоматическое распространение обновлений на подчиненные Серверы администрирования.....	383
Автоматическая установка обновлений программных модулей Агентов администрирования.....	384
Назначение устройства агентом обновлений вручную.....	385
Удаление устройства из списка агентов обновлений	389
Получение обновлений агентами обновлений	389
Удаление обновлений программного обеспечения из хранилища	391
Алгоритм установки патча для программы "Лаборатории Касперского" в кластерной модели	391
Работа с ключами программ	392
Просмотр информации об используемых ключах.....	393
Добавление ключа в хранилище Сервера администрирования	394
Удаление ключа Сервера администрирования.....	394
Распространение ключа на клиентские устройства	395
Автоматическое распространение ключа	396
Создание и просмотр отчета об использовании ключей	397
Хранилища данных	397
Экспорт списка объектов, находящихся в хранилище, в текстовый файл.....	398
Инсталляционные пакеты	399
Основные статусы файлов в хранилище	399
Карантин и резервное хранилище.....	401
Включение удаленного управления файлами в хранилищах	402

Просмотр свойств файла, помещенного в хранилище	403
Удаление файлов из хранилища	403
Восстановление файлов из хранилища	404
Сохранение файла из хранилища на диск	404
Проверка файлов на карантине	405
Необработанные файлы	405
Лечение необработанного файла	406
Сохранение необработанного файла на диск	407
Удаление файлов из папки "Необработанные файлы"	407
Резервное копирование и восстановление данных Сервера администрирования	408
Создание задачи резервного копирования данных	409
Утилита резервного копирования и восстановления данных (klbackup)	410
Резервное копирование и восстановление данных в интерактивном режиме	411
Резервное копирование и восстановление данных в неинтерактивном режиме	412
Перенос Сервера администрирования на другое устройство	414
Экспорт событий в SIEM-системы	416
События в Kaspersky Security Center	417
Процедура экспорта событий	420
Настройка экспорта событий в Kaspersky Security Center	421
Экспорт событий по протоколу Syslog	422
Предварительные условия	423
Включение автоматического экспорта	424
Выбор экспортируемых событий	427
Экспорт событий по протоколам CEF и LEEF	435
Предварительные условия	436
Включение автоматического экспорта общих событий	437
Экспорт событий напрямую из базы данных	440
Создание SQL-запроса с помощью утилиты klsq12	442
Просмотр имени базы данных Kaspersky Security Center	444
Настройка экспорта событий в SIEM-системе	446
Просмотр результатов экспорта	449
Общие события	449
События Сервера администрирования	450

События Агента администрирования.....	454
Kaspersky Security Network и Kaspersky Private Security Network	457
О KSN и KPSN.....	457
О предоставлении данных	459
Настройка доступа к KPSN	461
Включение и отключение KPSN	463
Просмотр статистики прокси-сервера KSN.....	464
Устранение неисправностей	466
Проблемы при удаленной установке программ	466
Неверно выполнено копирование образа жесткого диска.....	469
Проблемы с Сервером мобильных устройств Exchange ActiveSync	471
Проблемы с Сервером iOS MDM.....	473
Портал support.kaspersky.ru	473
Проверка доступности сервиса APN	473
Рекомендуемая последовательность действий для решения проблем с веб-сервисом iOS MDM.....	474
Проблемы с KES-устройствами.....	478
Портал support.kaspersky.ru	478
Проверка настроек сервиса Google Firebase Cloud Messaging	478
Проверка доступности сервиса Google Firebase Cloud Messaging	478
Обновление антивирусных баз в ручном режиме	480
Устранение уязвимостей и установка критических обновлений в программе	481
Действия после сбоя или неустранимой ошибки в работе программы	482
Приложения.....	483
Дополнительные возможности	483
Автоматизация работы Kaspersky Security Center. Утилита klakaut	484
Работа с внешними инструментами.....	484
Режим клонирования диска Агента администрирования	485
Настройка получения сообщений от компонента Контроль целостности системы	487
Обслуживание базы данных Сервера администрирования	490
Окно Способ уведомления пользователей	491
Раздел Учетная запись	492

Раздел Общие	493
Окно Выборка устройств	493
Окно Определение названия создаваемого объекта	493
Раздел Настройка событий.....	493
Раздел Категории программ	494
Особенности работы с интерфейсом управления	495
Как вернуть исчезнувшее окно свойств	495
Как перемещаться по дереву консоли	495
Как открыть окно свойств объекта в рабочей области	496
Как выбрать группу объектов в рабочей области	496
Как изменить набор граф в рабочей области.....	497
Справочная информация	497
Команды контекстного меню.....	498
Список управляемых устройств. Значение граф	504
Статусы устройств, задач и политик	509
Значки статусов файлов в Консоли администрирования	513
Поиск и экспорт данных	515
Поиск устройств.....	515
Параметры поиска устройств	517
Использование масок в строковых переменных	532
Использование регулярных выражений в строке поиска	532
Экспорт списков из диалоговых окон	534
Способы получения технической поддержки.....	534
Техническая поддержка по телефону	534
Техническая поддержка через Kaspersky CompanyAccount	535
АО "Лаборатория Касперского"	537
Информация о стороннем коде	539
Уведомления о товарных знаках	540
Соответствие терминов.....	542

Об этом документе

Настоящий документ представляет собой руководство по эксплуатации программного изделия "Kaspersky Security Center 10" (далее также "Kaspersky Security Center", "программа").

Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы. В документе также содержатся разделы с дополнительной информацией о программе.

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

Источники информации о программе

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

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В этом разделе

Источники для самостоятельного поиска информации	17
Обсуждение программ "Лаборатории Касперского" на форуме	19

Источники для самостоятельного поиска информации

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

- страница Kaspersky Security Center на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Security Center на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Для использования источников информации на веб-сайтах требуется подключение к интернету.

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

На странице Kaspersky Security Center (<http://www.kaspersky.ru/security-center>) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security Center содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Security Center в Базе знаний

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

На странице Kaspersky Security Center в Базе знаний (<https://support.kaspersky.ru/ksc10>) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

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

Электронная справка

Программа содержит файлы полной и контекстной справки.

В полной справке вы можете найти информацию о настройке и использовании Kaspersky Security Center.

В контекстной справке вы можете найти информацию об окнах Kaspersky Security Center: описание параметров Kaspersky Security Center и ссылки на описания задач, в которых используются эти параметры.

Справка может быть включена в состав программы либо располагаться онлайн на веб-ресурсе "Лаборатории Касперского". Если справка расположена онлайн, то при ее вызове будет открыто окно браузера. Для отображения онлайн-справки требуется соединение с интернетом.

Документация

В состав документации к программе входят файлы Руководства по эксплуатации и Подготовительные процедуры.

В руководстве по эксплуатации вы можете найти информацию о настройке и использовании Kaspersky Security Center.

В документе "Подготовительные процедуры" вы можете найти информацию для выполнения следующих задач:

- планирование установки программы (учитывая принципы работы программы, системные требования, типовые схемы развертывания, особенности совместимости с другими программами);
- подготовка к установке, установка и активация Kaspersky Security Center;
- настройка программы после установки.

Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем форуме (<https://forum.kaspersky.com>).

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

О программе

Программа Kaspersky Security Center (далее также "программа"), представляющее собой средство антивирусной защиты типа "А" второго класса защиты, предназначенное для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации, в том числе в изолированном периметре. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

В программе реализованы следующие функции безопасности:

- аудит безопасности программы;
- управление безопасностью;
- сигнализация;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных программ (вирусов) (БД ПКВ);
- централизованная установка компонентов САВЗ;
- поиск уязвимостей на управляемых АРМ.

Настройка прав. Роли пользователей

Вы можете гибко настраивать доступ администраторов, пользователей и групп пользователей к разным функциям программы. Предоставлять пользователям права доступа к функциям программы можно двумя способами:

- настраивать права каждого пользователя или группы пользователей индивидуально;

- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Роль пользователя – это заранее созданный и настроенный набор прав доступа к функциям программы. Роль можно предоставить пользователю или группе пользователей. Применение ролей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к программе. Права доступа в роли настраивают в соответствии с "типовыми" задачами и служебными обязанностями пользователей. Например, роль пользователя может иметь права только на чтение и отправку информационных команд на мобильные устройства других пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В программе можно создавать неограниченное количество ролей.

В этом разделе

Добавление роли пользователя.....	21
Назначение роли пользователю или группе пользователей.....	22
Права доступа к Серверу администрирования и его объектам.....	23

Добавление роли пользователя

► *Чтобы добавить роль пользователя, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Роли пользователей** и нажмите на кнопку **Добавить**.
4. В окне **Свойства: Новая роль** настройте параметры роли:
 - В разделе **Общие** укажите имя роли.

Имя роли не может превышать 100 символов.

- В разделе **Права** настройте набор прав, установив флажки **Разрешить** и **Запретить** напротив функций программы.

5. Нажмите на кнопку **ОК**.

В результате роль будет сохранена.

Роли пользователей, созданные для Сервера администрирования, отображаются в окне свойств Сервера в разделе **Роли пользователей**. Вы можете изменять и удалять роли пользователей, а также назначать роли группам пользователей (см. раздел "Назначение роли пользователю или группе пользователей" на стр. [22](#)) или отдельным пользователям.

Раздел **Роли пользователей** доступен, если в окне настройки интерфейса установлен флажок **Отображать разделы с параметрами безопасности**.

Назначение роли пользователю или группе пользователей

► *Чтобы назначить роль пользователю или группе пользователей, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.
4. В поле **Имена групп или пользователей** выберите пользователя или группу пользователей, которой нужно присвоить роль.

Если пользователь или группа отсутствует в поле, добавьте их по кнопке **Добавить**.

При добавлении пользователя по кнопке **Добавить** можно выбрать тип аутентификации пользователя (Microsoft Windows или Kaspersky Security Center). Аутентификация Kaspersky Security Center используется для выбора учетных записей внутренних пользователей.

5. Перейдите на закладку **Роли** и нажмите на кнопку **Добавить**.

Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.

6. В окне **Роли пользователей** выберите роль для группы пользователей.

7. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на закладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования.

Раздел **Безопасность** доступен, если в окне настройки интерфейса установлен флажок **Отображать разделы с параметрами безопасности**.

Права доступа к Серверу администрирования и его объектам

При установке Kaspersky Security Center автоматически формируются группы пользователей **KLAdmins** и **KLOperators**, которым предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы **KLAdmins** и **KLOperators** создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются в домене, в который входит Сервер администрирования, и на Сервере администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на Сервере администрирования.

Просмотр групп **KLAdmins** и **KLOperators** и внесение необходимых изменений в права пользователей групп **KLAdmins** и **KLOperators** можно осуществлять при помощи стандартных средств администрирования операционной системы.

Группе **KLAdmins** предоставлены все права, группе **KLOperators** – права на чтение и выполнение. Набор прав, предоставленных группе **KLAdmins**, недоступен для изменения.

Пользователи, входящие в группу **KLAdmins**, называются *администраторами Kaspersky Security Center*, пользователи из группы **KLOperators** – *операторами Kaspersky Security Center*.

Помимо пользователей, входящих в группу **KLAdmins**, права администратора Kaspersky Security Center предоставляются локальным администраторам устройств, на которых установлен Сервер администрирования.

Локальных администраторов можно исключать из списка пользователей, имеющих права администратора Kaspersky Security Center.

Все операции, запущенные администраторами Kaspersky Security Center, выполняются с правами учетной записи Сервера администрирования.

Для каждого Сервера администрирования в сети можно сформировать свою группу **KLAdmins**, обладающую правами только в рамках работы с этим Сервером.

Если устройства, относящиеся к одному домену, входят в группы администрирования разных Серверов, то администратор домена является администратором Kaspersky Security Center в рамках всех этих групп администрирования. Группа **KLAdmins** для этих групп администрирования едина и создается при установке первого Сервера администрирования. Операции, запущенные администратором Kaspersky Security Center, выполняются с правами учетной записи того Сервера администрирования, для которого они запущены.

После установки программы администратор Kaspersky Security Center может выполнять следующие действия:

- изменять права, предоставляемые группам **KLOperators**;
- определять права доступа к функциональности программы Kaspersky Security Center другим группам пользователей и отдельным пользователям, зарегистрированным на рабочем месте администратора;
- определять права доступа пользователей к работе в каждой группе администрирования.

Администратор Kaspersky Security Center может назначать права доступа к каждой группе администрирования или к другим объектам Сервера администрирования в разделе **Безопасность** окна свойств выбранного объекта.

Вы можете отследить действия пользователя при помощи записей о событиях в работе Сервера администрирования. Записи о событиях отображаются в узле **Сервер администрирования** на закладке **События**. Эти события имеют уровень важности **Информационное сообщение**; типы событий начинаются со слова **Аудит**.

Управление Серверами администрирования

Этот раздел содержит информацию о работе с Серверами администрирования и о настройке параметров Сервера администрирования.

В этом разделе

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования	26
Подключение к Серверу администрирования и переключение между Серверами администрирования	31
Условия подключения к Серверу администрирования через интернет	33
Защищенное подключение к Серверу администрирования	34
Отключение от Сервера администрирования	36
Добавление Сервера администрирования в дерево консоли	36
Удаление Сервера администрирования из дерева консоли.....	36
Добавление виртуального Сервера администрирования в дерево консоли	37
Смена учетной записи службы Сервера администрирования. Утилита klsrvswch	38
Просмотр и изменение параметров Сервера администрирования.....	40

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Добавление возможно независимо от того, доступен ли Сервер, который вы хотите сделать подчиненным, для подключения через Консоль администрирования.

При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Порт 13291 необходим для приема подключений от Консоли администрирования к Серверу администрирования.

Подключение Сервера администрирования в качестве подчиненного к главному Серверу

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера с подключением к главному Серверу по порту 13000. Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования: будущего главного Сервера и будущего подчиненного Сервера.

► *Чтобы добавить Сервер администрирования, доступный для подключения через Консоль, в качестве подчиненного Сервера, выполните следующие действия:*

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.
2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
4. В рабочей области узла **Сервер администрирования** выбранной группы нажмите на ссылку **Добавить подчиненный Сервер администрирования**.

Запустится мастер добавления подчиненного Сервера администрирования.

5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования.
6. Следуйте далее указаниям мастера.

Отношение "главный Сервер – подчиненный Сервер" будет установлено. Главный Сервер будет принимать подключение от подчиненного Сервера.

Если у вас нет устройства с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования (например, если будущий

подчиненный Сервер находится в удаленном офисе, а системный администратор удаленного офиса из соображений безопасности не делает доступным порт 13291 через интернет), вы все равно можете добавить подчиненный Сервер.

► *Чтобы добавить Сервер администрирования, недоступный для подключения через Консоль, в качестве подчиненного Сервера, выполните следующие действия:*

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для подключения от подчиненных Серверов администрирования.
2. Запишите файл сертификата будущего главного Сервера администрирования на внешний носитель (например, USB-носитель) либо перешлите системному администратору того удаленного офиса, в котором находится Сервер администрирования.

Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Запишите файл сертификата будущего подчиненного Сервера администрирования на внешний носитель (например, USB-носитель). Если будущий подчиненный Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса переслать вам сертификат.

Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
5. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
6. В рабочей области узла **Сервер администрирования** нажмите на ссылку **Добавить подчиненный Сервер администрирования**.

Запустится мастер добавления подчиненного Сервера администрирования.

7. На первом шаге мастера (ввод адреса) оставьте поле **Адрес** пустым.
8. В окне **Выбор сертификата Сервера администрирования** нажмите кнопку **Обзор** и выберите сохраненный ранее файл сертификата подчиненного Сервера.
9. После завершения работы мастера подключитесь с помощью другой Консоли администрирования к будущему подчиненному Серверу администрирования. Если этот Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса подключиться к будущему подчиненному Серверу администрирования и выполнить на нем дальнейшие шаги.
10. В контекстном меню узла **Сервер администрирования** выберите **Свойства**.
11. В свойствах Сервера администрирования перейдите в раздел **Дополнительно** и затем в раздел **Иерархия Серверов администрирования**.
12. Установите флажок **Данный Сервер администрирования является подчиненным**.
Поля ввода станут доступными для ввода и редактирования.
13. В поле **Адрес главного сервера** введите сетевое имя будущего главного Сервера администрирования.
14. Выберите ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.
15. Нажмите на кнопку **ОК**.

Отношение "главный Сервер – подчиненный Сервер" будет установлено. Вы сможете подключаться к подчиненному Серверу через Консоль администрирования. Главный Сервер будет принимать подключение от подчиненного Сервера.

Подключение главного Сервера администрирования к подчиненному Серверу

Вы можете добавить новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу по порту 13000. Это целесообразно, например, если вы размещаете подчиненный Сервер в демилитаризованной зоне.

Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования: будущего главного Сервера и будущего подчиненного Сервера.

► *Чтобы добавить новый Сервер администрирования в качестве подчиненного и подключить главный Сервер к нему по порту 13000, выполните следующие действия:*

1. Убедитесь, что порт 13000 будущего подчиненного Сервера доступен для приема подключений от главного Сервера администрирования.
2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер.
4. В рабочей области узла **Серверы администрирования** нужной группы администрирования нажмите на ссылку **Добавить подчиненный сервер администрирования**.

Запустится мастер добавления подчиненного Сервера администрирования.

5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования, и установите флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.
6. Если вы подключаетесь к будущему подчиненному Серверу через прокси-сервер, на первом шаге мастера установите флажок **Использовать прокси-сервер** и введите параметры подключения.
7. Следуйте далее указаниям мастера.

Будет установлена иерархия Серверов администрирования. Подчиненный Сервер будет принимать подключение от главного Сервера.

Подключение к Серверу администрирования и переключение между Серверами администрирования

При запуске программа Kaspersky Security Center предпринимает попытку соединения с Сервером администрирования. Если в сети существует несколько Серверов администрирования, запрашивается тот Сервер, с которым было установлено соединение во время предыдущего сеанса работы программы Kaspersky Security Center.

Если программа запускается в первый раз после установки, выполняется попытка соединения с Сервером администрирования, указанным при установке Kaspersky Security Center.

После соединения с Сервером администрирования структура папок этого Сервера отображается в дереве консоли.

Если в дерево консоли добавлено несколько Серверов администрирования, вы можете переключаться между ними.

Для работы с каждым Сервером администрирования необходима Консоль администрирования. Перед первым подключением к новому Серверу администрирования убедитесь, что на нем открыт порт 13291, по которому принимаются подключения от Консоли, и все остальные порты для связи Сервера администрирования с другими компонентами Kaspersky Security Center.

► *Чтобы переключиться на другой Сервер администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню узла выберите пункт **Подключиться к Серверу администрирования**.
3. В открывшемся окне **Параметры подключения** в поле **Адрес сервера** укажите имя Сервера администрирования, к которому вы хотите подключиться. В качестве имени Сервера администрирования вы можете указать IP-адрес или имя устройства в сети

Windows. При нажатии на кнопку **Дополнительно** в нижней части окна вы можете настроить параметры подключения к Серверу администрирования (см. рис. ниже).

Для подключения к Серверу администрирования через порт, отличный от установленного по умолчанию, в поле **Адрес сервера** требуется ввести значение в формате <Имя Сервера администрирования>:<Порт>.

Пользователям, не обладающим правами на **Чтение**, будет отказано в доступе к Серверу администрирования.

Параметры подключения

KASPERSKY®

Адрес сервера:
localhost

Использовать SSL-соединение

Имя пользователя: WIN7DOC1\tester

Пароль: ●●●●●●●●

Запомнить учетные данные

Использовать сжатие данных

Использовать прокси-сервер

Адрес:

Имя пользователя:

Пароль:

OK Отмена Дополнительно <<

Рисунок 1. Установка соединения с Сервером администрирования

4. Нажмите на кнопку **ОК** для завершения переключения между Серверами.

После соединения с Сервером администрирования структура папок соответствующего ему узла в дереве консоли обновляется.

Условия подключения к Серверу администрирования через интернет

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет. Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления программами и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 100 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

Защищенное подключение к Серверу администрирования

Обмен информацией между клиентскими устройствами и Сервером администрирования, а также подключение Консоли администрирования к Серверу администрирования могут производиться с использованием протокола TLS (Transport Layer Security). Протокол TLS позволяет идентифицировать стороны, взаимодействующие при подключении, осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. В основе протокола TLS лежит аутентификация взаимодействующих сторон и шифрование данных по методу открытых ключей.

В этом разделе

Аутентификация Сервера при подключении устройства	34
Аутентификация Сервера при подключении Консоли администрирования	35
Сертификат Сервера администрирования	35

Аутентификация Сервера при подключении устройства

При первом подключении клиентского устройства к Серверу администрирования Агент администрирования на устройстве получает копию сертификата Сервера администрирования и сохраняет его локально.

При локальной установке Агента администрирования на устройство сертификат Сервера администрирования можно выбрать вручную.

На основании полученной копии сертификата осуществляется проверка прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем, при каждом подключении устройства к Серверу администрирования Агент администрирования запрашивает сертификат Сервера администрирования и сравнивает его

с локальной копией. Если они не совпадают, доступ Сервера администрирования к устройству не разрешается.

Аутентификация Сервера при подключении Консоли администрирования

При первом подключении к Серверу администрирования Консоль администрирования запрашивает сертификат Сервера администрирования и сохраняет его копию локально на рабочем месте администратора. На основании полученной копии сертификата при последующих подключениях Консоли администрирования к этому Серверу администрирования осуществляется идентификация Сервера администрирования.

Если сертификат Сервера администрирования не совпадает с копией сертификата, хранящейся на рабочем месте администратора, Консоль администрирования выводит запрос на подтверждение подключения к Серверу администрирования с заданным именем и на получение нового сертификата. После подключения Консоль администрирования сохраняет копию нового сертификата Сервера администрирования, которая будет использоваться для идентификации Сервера в дальнейшем.

Сертификат Сервера администрирования

Аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с устройствами осуществляется на основании *сертификата Сервера администрирования*. Сертификат используется также для аутентификации при установке соединения между главными и подчиненными Серверами администрирования.

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Сертификат Сервера администрирования создается только один раз, при установке Сервера администрирования. В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и восстановление данных (см. раздел "Резервное копирование и восстановление данных Сервера администрирования" на стр. [408](#)).

Отключение от Сервера администрирования

► *Чтобы отключиться от Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел, соответствующий Серверу администрирования, от которого нужно отключиться.
2. В контекстном меню узла выберите пункт **Отключиться от Сервера администрирования**.

Добавление Сервера администрирования в дерево консоли

► *Чтобы добавить в дерево консоли Сервер администрирования, выполните следующие действия:*

1. В главном окне программы Kaspersky Security Center выберите в дереве консоли узел **Kaspersky Security Center**.
2. В контекстном меню узла выберите пункт **Создать** → **Сервер администрирования**.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя устройства> (Не подключен)**, с которого вы можете подключиться к любому из установленных в сети Серверов администрирования.

Удаление Сервера администрирования из дерева консоли

► *Чтобы удалить Сервер администрирования из дерева консоли, выполните следующие действия:*

1. В дереве консоли выберите узел, соответствующий удаляемому Серверу администрирования.

2. В контекстном меню узла выберите пункт **Удалить**.

Добавление виртуального Сервера администрирования в дерево консоли

► Чтобы добавить в дерево консоли виртуальный Сервер администрирования, выполните следующие действия:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать виртуальный Сервер администрирования.
2. В узле Сервера администрирования выберите папку **Серверы администрирования**.
3. В рабочей области папки **Серверы администрирования** перейдите по ссылке **Добавить виртуальный Сервер администрирования**.

Запустится мастер добавления виртуального Сервера администрирования.

4. В окне **Имя виртуального Сервера администрирования** укажите имя создаваемого виртуального Сервера.

Имя виртуального Сервера администрирования не может превышать 255 символов и содержать специальные символы ("*<>?\\:|).

5. В окне **Ввод адреса подключения устройств к виртуальному Серверу** укажите адрес подключения устройств.

Адрес подключения виртуального Сервера администрирования – это сетевой адрес, по которому к нему будут подключаться устройства. Адрес подключения состоит из двух частей: сетевого адреса физического Сервера администрирования и имени виртуального Сервера, разделенных символом косой черты (слешем). Имя виртуального Сервера будет подставлено автоматически. Указанный адрес будет использоваться на этом виртуальном Сервере как адрес по умолчанию в инсталляционных пакетах Агента администрирования.

6. В окне **Создание учетной записи администратора виртуального Сервера** назначьте администратором виртуального Сервера пользователя из списка или добавьте новую учетную запись для администратора по кнопке **Создать**.

Вы можете указать несколько учетных записей.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования** – <Имя виртуального Сервера>.

Смена учетной записи службы Сервера администрирования. Утилита klsrvswch

Если вам требуется изменить учетную запись службы Сервера администрирования, заданную при установке программы Kaspersky Security Center, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования klsrvswch.

При установке Kaspersky Security Center утилита автоматически копируется в папку установки программы.

Количество запусков утилиты не ограничено.

Утилита klsrvswch позволяет менять тип учетной записи: например, если вы используете локальную учетную запись, вы можете сменить ее на доменную учетную запись либо на управляемую учетную запись службы (и наоборот).

► *Чтобы изменить учетную запись службы Сервера администрирования, выполните следующие действия:*

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center.

В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте его указаниям.

2. В окне **Учетная запись службы Сервера администрирования** выберите один из двух вариантов задания учетной записи:

- **Учетная запись системы**

Служба Сервера администрирования запускается под учетной записью и с правами *Учетная запись системы*.

Для правильной работы Kaspersky Security Center требуется, чтобы учетная запись для запуска службы Сервера администрирования обладала правами администратора ресурса для размещения информационной базы Сервера администрирования.

- **Учетная запись пользователя**

Служба Сервера администрирования запускается под учетной записью пользователя, входящего в домен. В этом случае Сервер администрирования инициирует все операции с правами этой учетной записи.

► *Чтобы выбрать пользователя, учетная запись которого будет использоваться для запуска службы Сервера администрирования, выполните следующие действия:*

1. Нажмите на кнопку **Найти** и выберите учетную запись пользователя либо управляемую учетную запись.
2. В поле **Пароль учетной записи** задайте пароль для выбранной учетной записи, если требуется. Если вы выбрали управляемую учетную запись службы, оставьте это поле пустым.

В результате работы мастера учетная запись Сервера администрирования изменяется.

При использовании SQL-сервера в режиме аутентификации учетной записи пользователя средствами Microsoft Windows требуется обеспечить доступ к базе данных. Учетная запись пользователя должна быть владельцем базы данных Kaspersky Security Center. По умолчанию требуется использовать схему dbo.

Просмотр и изменение параметров Сервера администрирования

Вы можете настраивать параметры Сервера администрирования в окне свойств Сервера администрирования.

- ▶ *Чтобы открыть окно Свойства: Сервер администрирования,*
в контекстном меню узла Сервера администрирования в дереве консоли выберите пункт **Свойства**.

В этом разделе

Настройка общих параметров Сервера администрирования.....	40
Обработка и хранение событий на Сервере администрирования	41
Контроль возникновения вирусных эпидемий	42
Ограничение трафика	42
Настройка параметров Веб-сервера.....	44
Работа с внутренними пользователями	44

Настройка общих параметров Сервера администрирования

Вы можете настраивать общие параметры Сервера администрирования в разделах **Общие**, **Параметры**, **Хранение событий** и **Безопасность** окна свойств Сервера администрирования.

Раздел **Безопасность** может не отображаться в окне свойств Сервера администрирования, если его отображение выключено в интерфейсе Консоли администрирования.

► Чтобы включить отображение раздела **Безопасность** в Консоли администрирования, выполните следующие действия:

1. В меню **Вид** главного окна программы выберите пункт **Настройка интерфейса**.
2. В открывшемся окне **Настройка интерфейса** установите флажок **Отображать разделы с параметрами безопасности** и нажмите на кнопку **ОК**.
3. В окне с сообщением программы нажмите на кнопку **ОК**.

Раздел **Безопасность** отобразится в окне свойств Сервера администрирования.

Обработка и хранение событий на Сервере администрирования

Информация о событиях в работе программы и управляемых устройств сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (Критическое событие, Отказ функционирования, Предупреждение, Информационное сообщение). В зависимости от условий, при которых произошло событие, программа может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранение событий** окна свойств Сервера администрирования вы можете настроить параметры хранения событий в базе данных Сервера: ограничить количество записей о событиях и время хранения записей. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 15 000 000 событий. Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые.

Контроль возникновения вирусных эпидемий

Kaspersky Security Center позволяет вам своевременно реагировать на возникновение угроз вирусных эпидемий. Оценка угрозы вирусной эпидемии производится путем контроля вирусной активности на устройствах.

Вы можете настраивать правила оценки угрозы вирусной эпидемии и действия в случае ее возникновения в разделе **Вирусная атака** окна свойств Сервера администрирования.

Порядок оповещения о событии *Вирусная атака* можно задать в разделе **Настройка событий** окна свойств Сервера администрирования (см. раздел "Обработка и хранение событий на Сервере администрирования" на стр. [41](#)), в окне свойств события *Вирусная атака*.

Событие *Вирусная атака* формируется при возникновении событий *Обнаружен вредоносный объект* в работе программ защиты. Поэтому для распознавания вирусной эпидемии информацию о событиях *Обнаружен вредоносный объект* требуется сохранять на Сервере администрирования.

Параметры сохранения информации о событии *Обнаружен вредоносный объект* задаются в политиках программ защиты.

При подсчете событий *Обнаружен вредоносный объект* учитывается только информация с устройств главного Сервера администрирования. Информация с подчиненных Серверов администрирования не учитывается. Для каждого подчиненного Сервера параметры события *Вирусная атака* требуется настраивать индивидуально.

Ограничение трафика

Для снижения трафика в сети предусмотрена возможность ограничения скорости передачи данных на Сервер администрирования с отдельных IP-диапазонов и IP-интервалов.

Вы можете создавать и настраивать правила ограничения трафика в разделе **Трафик** окна свойств Сервера администрирования.

Чтобы создать правило ограничения трафика, выполните следующие действия:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать правило ограничения трафика.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Трафик**.
4. Нажмите на кнопку **Добавить**.
5. В окне **Новое правило** настройте следующие параметры:

В блоке **Интервал IP-адресов, для которых нужно ограничивать трафик** можно выбрать способ задания подсети или диапазона, для которого ограничивается скорость передачи, и указать значения параметров для выбранного способа. Выберите один из следующих способов:

- **Задать интервал адресом и маской подсети**

Трафик ограничивается по параметрам подсети. Укажите в полях ввода адрес подсети и маску подсети для определения интервала, в пределах которого будет ограничен трафик.

- **Задать интервал начальным и конечным IP-адресом**

Трафик ограничивается по интервалу IP-адресов. Укажите интервал IP-адресов в полях ввода **Начальный IP-адрес** и **Конечный IP-адрес**.

Этот вариант выбран по умолчанию.

В блоке **Ограничение трафика** можно настроить следующие параметры ограничения скорости передачи данных:

- **Период**

Временной интервал, во время которого будет действовать ограничение трафика. Границы временного интервала можно указать в полях ввода.

- **Ограничение (КБ/сек)**

Предельное значение суммарной скорости передачи входящих и исходящих данных Сервера администрирования. Ограничение действует только в течение временного интервала, заданного в поле **Период**.

- **Ограничивать трафик в остальное время (КБ/сек)**

Трафик ограничивается не только в течение интервала, указанного в поле **Период**, но и в остальное время.

По умолчанию флажок снят. Значение поля может не совпадать со значением поля **Ограничение (КБ/сек)**.

Настройка параметров Веб-сервера

Веб-сервер используется для публикации автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

Вы можете настроить параметры подключения Веб-сервера к Серверу администрирования и задать сертификат Веб-сервера в разделе **Веб-сервер** окна свойств Сервера администрирования.

Работа с внутренними пользователями

Учетные записи *внутренних пользователей* используются для работы с виртуальными Серверами администрирования. В рамках функциональности программы Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Вы можете настраивать параметры учетных записей внутренних пользователей в папке **Учетные записи пользователей** дерева консоли (см. раздел "Работа с учетными записями пользователей" на стр. [174](#)).

Управление группами администрирования

Этот раздел содержит информацию о работе с группами администрирования.

Вы можете выполнять с группами администрирования следующие действия:

- добавлять в состав группы администрирования произвольное количество вложенных групп любых уровней иерархии;
- добавлять в состав групп администрирования устройства;
- изменять иерархию групп администрирования путем перемещения отдельных устройств и целых групп в другие группы;
- удалять из состава групп администрирования вложенные группы и устройства;
- добавлять в состав групп администрирования подчиненные и виртуальные Серверы администрирования;
- переносить устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера;
- определять, какие программы "Лаборатории Касперского" будут автоматически устанавливаться на устройства, включаемые в состав группы.

В этом разделе

Создание групп администрирования.....	46
Перемещение групп администрирования.....	48
Удаление групп администрирования.....	49
Автоматическое создание структуры групп администрирования.....	50
Автоматическая установка программ на устройства группы администрирования.....	52
Автономные пользователи.....	52

Создание групп администрирования

Иерархия групп администрирования формируется в главном окне программы Kaspersky Security Center в папке **Управляемые устройства**. Группы администрирования отображаются в виде папок в дереве консоли (см. рис. ниже).

Сразу после установки Kaspersky Security Center папка **Управляемые устройства** содержит только пустую папку **Серверы администрирования**.

Наличие или отсутствие папки **Серверы администрирования** в дереве консоли определяется параметрами пользовательского интерфейса. Для включения отображения этой папки нужно перейти в меню **Вид** → **Настройка интерфейса** и в открывшемся окне **Настройка интерфейса** установить флажок **Отображать подчиненные Серверы администрирования**.

При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы. В папку **Серверы администрирования** можно добавлять подчиненные и виртуальные Серверы администрирования.

Каждая созданная группа, как и папка **Управляемые устройства**, сначала содержит только пустую папку **Серверы администрирования** для работы с подчиненными и виртуальными

Серверами администрирования этой группы. Информация о политиках, задачах этой группы, а также о входящих в ее состав устройствах отображается на соответствующих закладках в рабочей области этой группы.

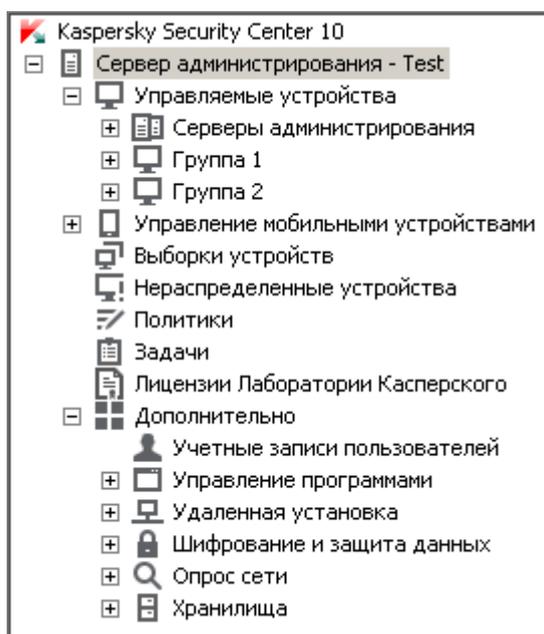


Рисунок 2. Просмотр иерархии групп администрирования

► Чтобы создать группу администрирования, выполните следующие действия:

1. В дереве консоли откройте папку **Управляемые устройства**.
2. Если вы хотите создать подгруппу существующей группы администрирования, в папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой должна входить новая группа администрирования.

Если вы создаете новую группу администрирования верхнего уровня иерархии, этот шаг можно пропустить.

3. Запустите процесс создания группы администрирования одним из следующих способов:
 - с помощью команды контекстного меню **Создать** → **Группу**;
 - по кнопке **Создать группу**, расположенной в рабочей области главного окна программы на закладке **Группы**.
4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем.

Программа позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

► *Чтобы создать структуру групп администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи** → **Создать структуру групп**.

В результате запускается мастер создания структуры групп администрирования. Следуйте его указаниям.

Перемещение групп администрирования

Вы можете перемещать вложенные группы администрирования внутри иерархии групп.

Группа администрирования перемещается вместе со всеми вложенными группами, подчиненными Серверами администрирования, устройствами, групповыми политиками и задачами. К ней будут применены все параметры, соответствующие ее новому положению в иерархии групп администрирования.

Имя группы должно быть уникальным в пределах одного уровня иерархии. Если в папке, в которую вы перемещаете группу администрирования, уже существует группа с аналогичным названием, перед перемещением название группы следует изменить. Если вы предварительно не изменили название перемещаемой группы, к ее названию при перемещении автоматически добавляется окончание вида (**<порядковый номер>**), например: **(1)**, **(2)**.

Невозможно изменить название группы **Управляемые устройства**, поскольку она является встроенным элементом Консоли администрирования.

► *Чтобы переместить группу в другую папку дерева консоли, выполните следующие действия:*

1. Выберите перемещаемую группу в дереве консоли.
2. Выполните одно из следующих действий:
 - Переместите группу с помощью контекстного меню:
 1. В контекстном меню группы выберите пункт **Вырезать**.
 2. В контекстном меню группы администрирования, в которую нужно переместить выбранную группу, выберите пункт **Вставить**.
 - Переместите группу с помощью главного меню программы:
 - a. Выберите пункт главного меню **Действие** → **Вырезать**.
 - b. Выберите в дереве консоли группу администрирования, в которую нужно переместить выбранную группу.
 - c. Выберите пункт главного меню **Действие** → **Вставить**.
 - Переместите группу в другую группу в дереве консоли с помощью мыши.

Удаление групп администрирования

Вы можете удалить группу администрирования, если она не содержит подчиненных Серверов администрирования, вложенных групп и клиентских устройств и если для нее не сформированы задачи и политики.

Перед удалением группы администрирования требуется удалить из ее состава подчиненные Серверы администрирования, вложенные группы и клиентские устройства.

► *Чтобы удалить группу, выполните следующие действия:*

1. Выберите группу администрирования в дереве консоли.
2. Выполните одно из следующих действий:
 - в контекстном меню группы выберите пункт **Удалить**;

- в главном меню программы выберите пункт **Действие** → **Удалить**;
- нажмите на клавишу **DEL**.

Автоматическое создание структуры групп администрирования

Kaspersky Security Center позволяет автоматически сформировать структуру групп администрирования с помощью мастера создания структуры групп.

Мастер создает структуру групп администрирования на основе следующих данных:

- структуры доменов и рабочих групп сети Windows;
- структуры групп Active Directory;
- содержимого текстового файла, созданного администратором вручную.

При формировании текстового файла требуется соблюдать следующие правила:

- Имя каждой новой группы должно начинаться с новой строки; разделительный символ – перевод строки. Пустые строки игнорируются.

Пример:

Офис 1

Офис 2

Офис 3

В группе назначения будут созданы три группы первого уровня иерархии.

- Имя вложенной группы следует указывать через косую черту (/).

Пример:

Офис 1/Подразделение 1/Отдел 1/Группа 1

В группе назначения будут созданы четыре вложенные друг в друга подгруппы.

- Чтобы создать несколько вложенных групп одного уровня иерархии, следует указать "полный путь к группе".

Пример:

Офис 1/Подразделение 1/Отдел 1

Офис 1/Подразделение 2/Отдел 1

Офис 1/Подразделение 3/Отдел 1

Офис 1/Подразделение 4/Отдел 1

В группе назначения будет создана одна группа первого уровня иерархии "Офис 1", в состав которой будут входить четыре вложенные группы одного уровня иерархии "Подразделение 1", "Подразделение 2", "Подразделение 3", "Подразделение 4". В состав каждой из этих групп будет входить группа "Отдел 1".

Создание структуры групп администрирования с помощью мастера не нарушает целостности сети: новые группы добавляются, а не замещают существующие. Клиентское устройство не может быть включено в состав группы администрирования повторно, поскольку при перемещении устройства в группу администрирования оно удаляется из группы **Нераспределенные устройства**.

Если при создании структуры групп администрирования устройство по каким-либо причинам не было включено в состав группы **Нераспределенные устройства** (было выключено, отключено от сети), оно не будет автоматически перенесено в группу администрирования. Вы можете добавить устройства в группы администрирования вручную после завершения работы мастера.

► Чтобы запустить автоматическое создание структуры групп администрирования, выполните следующие действия:

1. Выберите в дереве консоли папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи** → **Создать структуру групп**.

В результате запускается мастер создания структуры групп администрирования. Следуйте его указаниям.

Автоматическая установка программ на устройства группы администрирования

Вы можете указать, какие инсталляционные пакеты нужно использовать для автоматической удаленной установки программ "Лаборатории Касперского" на вновь включенные в состав группы клиентские устройства.

► Чтобы настроить автоматическую установку программ на новые устройства в группе администрирования, выполните следующие действия:

1. Выберите в дереве консоли нужную вам группу администрирования.
2. Откройте окно свойств этой группы администрирования.
3. В разделе **Автоматическая установка** выберите инсталляционные пакеты, которые следует устанавливать на новые устройства, установив флажки рядом с названиями инсталляционных пакетов нужных программ. Нажмите на кнопку **ОК**.

В результате будут созданы групповые задачи, которые будут запускаться на клиентских устройствах сразу после их добавления в группу администрирования.

Если для автоматической установки указано несколько инсталляционных пакетов одной программы, задача установки будет создана только для последней версии программы.

Автономные пользователи

В Kaspersky Security Center предусмотрена возможность переключения Агента

администрирования клиентского устройства на другие Серверы администрирования при изменении следующих характеристик сети:

- Нахождение в подсети – изменение адреса и маски подсети.
- Нахождение в DNS-домене – изменение DNS-суффикса подсети.
- Адрес основного шлюза – изменение основного шлюза сети.
- Адрес DHCP-сервера – изменение IP-адреса DHCP-сервера в сети.
- Адрес DNS-сервера – изменение IP-адреса DNS-сервера в сети.
- Адрес WINS-сервера – изменение IP-адреса WINS-сервера в сети.
- Доступность домена Windows – изменение статуса домена Windows, к которому подключено клиентское устройство.

Функциональность поддерживается для следующих операционных систем: Microsoft Windows XP / Windows Vista; Microsoft Windows Server 2003 / 2008.

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. В дальнейшем, если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение характеристик сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах программы переходят на политики для автономных пользователей.
- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах программы возвращаются к активным политикам.
- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

По умолчанию Агент администрирования переходит на политику для автономных пользователей, если Сервер администрирования недоступен более 45 минут.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

В этом разделе

Создание профиля подключения к Серверу администрирования для автономных пользователей.....	54
Создание правила переключения Агента администрирования по сетевому местоположению	59

Создание профиля подключения к Серверу администрирования для автономных пользователей

- ▶ *Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей, выполните следующие действия:*
 1. В дереве консоли выберите группу администрирования, для устройств которой требуется создать профиль подключения Агента администрирования к Серверу.
 2. Выполните одно из следующих действий:
 - Если вы хотите создать профиль подключения для всех устройств группы, в рабочей области группы на закладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.

- Если вы хотите создать профиль подключения для выбранного устройства в составе группы, в рабочей области группы на закладке **Устройства** выберите устройство и выполните следующие действия:
 - a. Откройте окно свойств выбранного устройства.
 - b. В разделе **Программы** окна свойств устройства выберите Агент администрирования.
 - c. Откройте окно свойств Агента администрирования.
- 3. В открывшемся окне свойств в разделе **Сеть** выберите вложенный раздел **Подключение**.
- 4. В блоке **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

В профиле <Офлайн-режим> не указан Сервер для подключения, и при переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах программы используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.

5. В открывшемся окне **Новый профиль** настройте параметры профиля подключения:
 - **Имя профиля**

В поле ввода можно просмотреть или изменить имя профиля подключения.

- **Адрес Сервера**

Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.

- **Номер порта**

Номер порта, по которому будет выполняться подключение.

- **Номер SSL-порта**

Номер порта, по которому будет осуществляться подключение с использованием SSL-протокола.

- **Использовать SSL-соединение**

Если флажок установлен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

По умолчанию флажок установлен.

- По ссылке **Настроить подключение через прокси-сервер** настройте параметры профиля подключения через прокси-сервер:

- **Использовать прокси-сервер**

Если флажок установлен, подключение к Серверу администрирования будет выполняться через прокси-сервер.

Если флажок снят, поля ввода параметров подключения к прокси-серверу недоступны.

По умолчанию флажок снят.

- **Адрес**

Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

- **Номер порта**

Номер порта, по которому будет выполняться подключение Kaspersky Security Center к прокси-серверу.

- **Аутентификация на прокси-сервере**

Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере. Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя** (поле доступно, если установлен флажок **Авторизация на прокси-сервере**)

Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль** (поле доступно, если установлен флажок **Авторизация на прокси-сервере**)

Пароль пользователя, через учетную запись которого выполняется подключение к прокси-серверу.

- **Адрес шлюза соединений**

Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим**

Если флажок установлен, при подключении через этот профиль программы, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. раздел "Автономные пользователи" на стр. [52](#)). В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

Если флажок снят, программы будут использовать активные политики.

По умолчанию флажок снят.

- **Использовать только для получения обновлений**

Если флажок установлен, профиль будет использоваться только при загрузке обновлений программами, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

По умолчанию флажок установлен.

- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

Если флажок установлен, Агент администрирования подключается к Серверу администрирования, используя параметры, указанные в свойствах профиля.

Если флажок снят, Агент администрирования подключается к Серверу используя исходные параметры, указанные при установке.

Флажок доступен, если флажок **Использовать только для получения обновлений** снят.

По умолчанию флажок снят.

6. Установите флажок **Включить автономный режим, когда Сервер администрирования недоступен**, чтобы при подключении программы, установленные на клиентском устройстве, использовали профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. раздел "Автономные пользователи" на стр. [52](#)), если Сервер администрирования недоступен. В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль программы, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

Создание правила переключения Агента администрирования по сетевому местоположению

► Чтобы создать правило для переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети, выполните следующие действия:

1. В дереве консоли выберите группу администрирования, для устройств которой требуется создать правило переключения Агента администрирования по описанию сетевого местоположения.
2. Выполните одно из следующих действий:
 - Если вы хотите создать правило для всех устройств группы, в рабочей области группы на закладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.
 - Если вы хотите создать правило для выбранного устройства группы, в рабочей области группы на закладке **Устройства** выберите устройство и выполните следующие действия:
 - a. Откройте окно свойств выбранного устройства.
 - b. В разделе **Программы** окна свойств устройства выберите Агент администрирования.
 - c. Откройте окно свойств Агента администрирования.
3. В открывшемся окне свойств в разделе **Сеть** выберите вложенный раздел **Подключение**.
4. В блоке **Параметры сетевого местоположения** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Новое описание** настройте параметры описания сетевого местоположения и правила переключения. Настройте следующие параметры описания сетевого местоположения:
 - **Имя описания сетевого местоположения**

Имя описания сетевого местоположения не может превышать 255 символов и содержать специальные символы ("*<>?\\:|).

- **Использовать профиль подключения**

В раскрывающемся списке можно выбрать профиль подключения Агента администрирования к Серверу администрирования. Профиль будет использоваться при выполнении условий описания сетевого местоположения. Профиль подключения содержит параметры подключения Агента администрирования к Серверу администрирования и определяет переход клиентских устройств на политики для автономных пользователей. Профиль используется только для загрузки обновлений.

6. В блоке **Условия переключения** нажмите на кнопку **Добавить**, чтобы сформировать список условий описания сетевого местоположения.

Условия в правиле соединяются по логическому "и". Чтобы правило переключения по описанию сетевого местоположения сработало, все условия переключения правила должны быть выполнены.

7. В раскрывающемся списке выберите значение, соответствующее изменению характеристики сети, к которой подключено клиентское устройство:

- **Нахождение в подсети** – изменение адреса и маски подсети.
- **Нахождение в DNS-домене** – изменение DNS-суффикса подсети.
- **Адрес основного шлюза** – изменение основного шлюза сети.
- **Адрес DHCP-сервера** – изменение IP-адреса DHCP-сервера в сети.
- **Адрес DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Адрес WINS-сервера** – изменение IP-адреса WINS-сервера в сети.
- **Доступность Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство.

8. В открывшемся окне укажите значение условия переключения Агента администрирования на другой Сервер администрирования. Название окна зависит от выбора значения на предыдущем шаге. Настройте следующие параметры условия переключения:

- **Значение**

В поле можно добавить одно или несколько значений для создаваемого условия.

- **Соответствует хотя бы одному значению списка**

Если выбран этот вариант, условие будет выполняться при любом из значений, указанных в списке **Значение**.

По умолчанию выбран этот вариант.

- **Не соответствует ни одному из значений списка**

Если выбран этот вариант, условие будет выполняться, если его значение отсутствует в списке **Значение**.

9. В окне **Новое описание** настройте установите флажок **Описание активно**, чтобы включить использование нового описания сетевого местоположения.

В результате будет создано правило переключения по описанию сетевого местоположения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в описании профиль подключения.

Описания сетевого местоположения проверяются на соответствие характеристикам сети в том порядке, в котором они представлены в списке. Если характеристики сети соответствуют нескольким описаниям, будет использоваться первое из них. Вы можете изменить порядок следования правил в списке с помощью кнопок  и .

Удаленное управление программами

Этот раздел содержит информацию об удаленном управлении программами «Лаборатории Касперского», установленными на клиентских устройствах, при помощи политик, профилей политик, задач и настройки локальных параметров программ.

В этом разделе

Управление политиками	62
Управление задачами	86
Просмотр и изменение локальных параметров программы	105

Управление политиками

Централизованная настройка параметров программ, установленных на клиентских устройствах, осуществляется через определение политик.

Политики, сформированные для программ в группе администрирования, отображаются в рабочей области на закладке **Политики**. Перед именем каждой политики отображается значок, характеризующий ее статус (см. раздел "Статусы устройств, задач и политик" на стр. [509](#)).

После удаления политики или прекращения ее действия программа продолжает работу с параметрами, заданными в политике. В дальнейшем эти параметры можно изменить вручную.

Применение политики производится следующим образом: если на устройстве выполняются резидентные задачи (задачи постоянной защиты), их выполнение продолжается с новыми значениями параметров. Запущенные периодические задачи (проверка по требованию,

обновление баз программ) выполняются с неизменными значениями. Новый запуск периодических задач производится с измененными значениями параметров.

В случае использования иерархической структуры Серверов администрирования подчиненные Серверы получают политики с главного Сервера администрирования и распространяют их на клиентские устройства. При включенном механизме наследования параметры политики можно изменять на главном Сервере администрирования. После этого изменения, внесенные в параметры политики, распространяются на унаследованные политики на подчиненных Серверах администрирования.

При разрыве соединения между главным и подчиненным Серверами администрирования политика на подчиненном Сервере продолжает действовать с прежними параметрами. Параметры политики, измененные на главном Сервере администрирования, распространяются на подчиненный Сервер после восстановления соединения.

При отключенном механизме наследования параметры политики можно изменять на подчиненном Сервере независимо от главного Сервера.

Если происходит разрыв соединения между Сервером администрирования и клиентским устройством, на устройстве вступает в силу политика для автономного пользователя (если она определена), или политика продолжает действовать с прежними параметрами до восстановления соединения.

Результаты распространения политики на подчиненные Серверы администрирования отображаются в окне свойств политики на главном Сервере администрирования.

Результаты распространения политики на клиентские устройства отображаются в окне свойств политики Сервера администрирования, к которому они подключены.

Не используйте в параметрах политик конфиденциальные данные. Например, пароль доменного администратора.

В этом разделе

Создание политики.....	64
Отображение унаследованной политики во вложенной группе	66
Активация политики	66
Автоматическая активация политики по событию "Вирусная атака".....	67
Применение политики для автономных пользователей	67
Изменение политики. Откат изменений	68
Сравнение политик	68
Удаление политики	70
Копирование политики	70
Экспорт политики	71
Импорт политики	71
Конвертация политик	72
Управление профилями политик.....	72

Создание политики

В Консоли администрирования можно создавать политики непосредственно в папке группы администрирования, для которой создается политика, и в рабочей области папки **Политики**.

► *Чтобы создать политику в папке группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать политику.
2. В рабочей области группы выберите закладку **Политики**.

3. Запустите мастер создания политики по кнопке **Создать политику**.

В результате запускается мастер создания политики. Следуйте его указаниям.

► *Чтобы создать политику в рабочей области папки **Политики**, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.

2. Запустите мастер создания политики по кнопке **Создать политику**.

В результате запускается мастер создания политики. Следуйте его указаниям.

Для одной программы в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

При создании политики можно настроить минимальный набор параметров, без которых программа не будет работать. Остальные значения параметров устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке программы. Вы можете изменять политику после ее создания.

Не используйте в параметрах политик конфиденциальные данные. Например, пароль доменного администратора.

Параметры программ "Лаборатории Касперского", которые изменяются после применения политик, подробно описаны в Руководствах к каждой из них.

После создания политики параметры, на изменение которых наложен запрет (установлен "замок" ) , начинают действовать на клиентских устройствах независимо от того, какие параметры были определены для программы ранее.

Отображение унаследованной политики во вложенной группе

► Чтобы включить отображение унаследованных политик для вложенной группы администрирования, выполните следующие действия:

1. В дереве консоли выберите группу администрирования, для которой нужно отображать унаследованные политики.
2. В рабочей области для выбранной группы выберите закладку **Политики**.
3. В контекстном меню списка политик выберите пункт **Вид** → **Унаследованные политики**.

В результате унаследованные политики отображаются в списке политик со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования параметров изменение унаследованных политик доступно только в той группе, в которой они были созданы. Изменение унаследованных политик недоступно в той группе, которая наследует политики.

Активация политики

► Чтобы сделать политику активной для выбранной группы, выполните следующие действия:

1. В рабочей области группы на закладке **Политики** выберите политику, которую нужно сделать активной.
2. Для активации политики выполните одно из следующих действий:
 - В контекстном меню политики выберите пункт **Активная политика**.

- В окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Активная политика**.

В результате политика становится активной для выбранной группы администрирования.

При применении политики на большом количестве клиентских устройств на некоторое время существенно возрастают нагрузка на Сервер администрирования и объем сетевого трафика.

Автоматическая активация политики по событию "Вирусная атака"

► Чтобы политика активировалась автоматически при наступлении события "Вирусная атака", выполните следующие действия:

1. В окне свойств Сервера администрирования откройте раздел **Вирусная атака**.
2. Откройте окно **Активация политик** по ссылке **Настроить активацию политик по событию "Вирусная атака"** и добавьте политику в выбранный список политик, активируемых при обнаружении вирусной атаки.

В случае активации политики по событию *Вирусная атака* вернуться к предыдущей политике можно только вручную.

Применение политики для автономных пользователей

Политика для автономных пользователей вступает в силу на устройстве в случае его отключения от сети организации.

- Чтобы применить выбранную политику для автономных пользователей, в окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Политика для автономных пользователей**.

В результате политика начинает действовать на устройствах в случае их отключения от сети организации.

Изменение политики. Откат изменений

► *Чтобы изменить политику, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Применить**.

Изменения политики будут сохранены в свойствах политики, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения политики.

► *Чтобы откатить изменения политики, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. Выберите политику, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств политики.
3. В окне свойств политики выберите раздел **История ревизий**.
4. В списке ревизий политики выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Сравнение политик

Вы можете сравнивать две политики для одной управляемой программы. В результате сравнения политик вы получаете отчет, показывающий, какие параметры политик

совпадают, а какие различаются. Сравнить политики бывает нужно, например, если разные администраторы в своих локальных офисах создали несколько политик для одной управляемой программы или если одна политика верхнего уровня была наследована и изменена для каждого локального офиса. Вы можете сравнить политики двумя способами: выбрать одну политику и сравнить с другой или сравнить две политики из списка политик.

► *Чтобы сравнить политику с другой политикой, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику, которую нужно сравнить с другой политикой.
3. В контекстном меню политики выберите пункт **Сравнить политику с другой политикой**.
4. В окне **Выбор политики** выберите политику, с которой нужно провести сравнение.
5. Нажмите на кнопку **ОК**.

Отобразится отчет сравнения двух политик для программы в формате HTML.

► *Чтобы сравнить две политики из списка политик, выполните следующие действия:*

1. В папке **Политики** в списке политик с помощью клавиши **SHIFT** или **CTRL** выберите две политики для одной управляемой программы.
2. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения двух политик для программы в формате HTML.

В отчете сравнения параметров политик для программы Kaspersky Endpoint Security 10 для Windows выполняется также сравнение профилей политики. Результаты сравнения параметров профилей политик можно свернуть. Чтобы свернуть блок, нажмите на треугольный значок ▲ рядом с названием блока.

Удаление политики

► Чтобы удалить политику, выполните следующие действия:

1. В рабочей области группы администрирования на закладке **Политики** выберите политику, которую нужно удалить.
2. Удалите политику одним из следующих способов:
 - В контекстном меню политики выберите пункт **Удалить**.
 - По ссылке **Удалить политику**, расположенной в рабочей области, в блоке работы с выбранной политикой.

Копирование политики

► Чтобы скопировать политику, выполните следующие действия:

1. В рабочей области нужной вам группы на закладке **Политики** выберите политику.
2. В контекстном меню политики выберите пункт **Копировать**.
3. Выберите в дереве консоли группу, в которую требуется добавить политику.

Политику можно добавить в ту же группу, из которой она скопирована.

4. В контекстном меню списка политик для выбранной группы на закладке **Политики** выберите пункт **Вставить**.

В результате политика копируется с сохранением всех параметров и распространяется на устройства группы, в которую она перенесена. Если вы вставляете политику в ту же группу, из которой она была скопирована, к имени политики автоматически добавляется окончание вида (<порядковый номер>), например: **(1)**, **(2)**.

Активная политика при копировании становится неактивной. В случае необходимости вы можете сделать ее активной.

Экспорт политики

► Чтобы экспортировать политику, выполните следующие действия:

1. Экспортируйте политику одним из следующих способов:
 - В контекстном меню политики выберите пункт **Все задачи** → **Экспортировать**.
 - По ссылке **Экспортировать политику в файл**, расположенной в рабочей области, в блоке работы с выбранной политикой.
2. В открывшемся окне **Сохранить как** укажите имя файла политики и путь для его сохранения. Нажмите на кнопку **Сохранить**.

Импорт политики

► Чтобы импортировать политику, выполните следующие действия:

1. В рабочей области нужной вам группы на закладке **Политики** выберите один из следующих способов импорта политики:
 - В контекстном меню списка политик выберите пункт **Все задачи** → **Импортировать**.
 - По ссылке **Импортировать политику из файла** в блоке управления списком политик.
2. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать политику. Нажмите на кнопку **Открыть**.

В результате добавленная политика отображается в списке политик.

Если в выбранном списке политик уже существует политика с именем, аналогичным имени импортируемой политики, к имени импортируемой политики будет добавлено окончание вида (<порядковый номер>), например: (1), (2).

Конвертация политик

Kaspersky Security Center может конвертировать политики предыдущих версий программ "Лаборатории Касперского" в политики текущих версий этих программ.

Конвертация возможна для политик следующих программ:

- Антивирус Касперского 6.0 для Windows Workstations MP4;
- Kaspersky Endpoint Security 8 для Windows;
- Kaspersky Endpoint Security 10 для Windows.

► *Чтобы конвертировать политики, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию политик.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

В результате запускается мастер массовой конвертации политик и задач. Следуйте его указаниям.

В результате работы мастера формируются новые политики, использующие параметры политик предыдущих версий программ "Лаборатории Касперского".

Управление профилями политик

Этот раздел содержит информацию о профилях политик, которые используются для эффективного управления группами клиентских устройств. Описаны преимущества профилей политик, способы их применения. В разделе также приведены инструкции по созданию, настройке и удалению профилей политик.

В этом разделе

О профиле политики	73
Создание профиля политики	77
Изменение профиля политики.....	78
Удаление профиля политики.....	79
Создание правила активации профиля политики	80

О профиле политики

Профиль политики – это именованный набор параметров политики, который активируется на клиентском устройстве (компьютере, мобильном устройстве), если устройство удовлетворяет заданным правилам активации (см. раздел "Создание правила активации профиля политики" на стр. [80](#)). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики. Например, возможна ситуация, когда в группе администрирования для некоторых устройств параметры политики должны быть изменены. В этом случае для такой политики можно настроить профили политики, использование которых позволяет изменять параметры политики не для всех устройств группы администрирования. Например, политика запрещает запуск программ городской навигации для всех устройств группы администрирования "Пользователи". Программы городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". На этом устройстве можно установить тег "Курьер" и настроить профиль политики таким образом, чтобы был разрешен запуск программ городской навигации только на устройстве с тегом "Курьер", с сохранением всех остальных параметров политики. В этом случае если в группе администрирования "Пользователи" появляется устройство с тегом "Курьер", на нем будет разрешен запуск программ городской навигации. Запуск программ городской

навигации на других устройствах в группе администрирования "Пользователи", у которых тег "Курьер" отсутствует, будет запрещен.

Профили поддерживаются только для следующих политик:

- политики программы Kaspersky Endpoint Security 10 Service Pack 1 для Windows и выше;
- политики программы Kaspersky Endpoint Security 10 Service Pack 1 для Mac;
- политики плагина Kaspersky Mobile Device Management версий от 10 Service Pack 1 до 10 Service Pack 3 Maintenance Release 1;
- политики плагина Kaspersky Device Management для iOS.

Преимущества профилей политик

Профили политик облегчают управление клиентскими устройствами, на которых применены политики:

- Параметры профиля политики могут отличаться от параметров самой политики.
- Не требуется поддерживать и применять вручную несколько копий одной политики, которые различаются только небольшим количеством параметров.
- Не требуется отдельная политика для автономных пользователей.
- Вы можете экспортировать и импортировать профили политики, а также создавать новые профили на основе существующих.
- Для одной политики несколько профилей политики могут быть активными. К устройству будут применены те из профилей, которые удовлетворяют правилам активации на этом устройстве.
- Профили подчиняются иерархии политик. Унаследованная политика содержит все профили политики верхнего уровня.

Приоритеты профилей

Профили, созданные для политики, упорядочены в порядке убывания приоритета. Например, если профиль X находится выше профиля Y в списке профилей, то профиль X

имеет более высокий приоритет, чем Y. К одному устройству одновременно могут быть применены несколько профилей. Если значение какого-то параметра различается в профилях, на устройстве применится значение параметра из того профиля, который имеет более высокий приоритет.

Правила активации профиля

Профиль политики активируется на клиентском устройстве при выполнении правила активации. *Правила активации* – набор условий, при выполнении которых профиль политики начинает работать на устройстве. Правило активации может содержать следующие условия:

- Агент администрирования на клиентском устройстве подключается к Серверу с определенным набором параметров подключения, например, адрес Сервера, номер порта и так далее.
- Клиентское устройство находится в автономном режиме.
- Клиентскому устройству назначены определенные теги.
- Клиентское устройство явно (устройство находится непосредственно в указанном подразделении) или неявно (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности) размещено в определенном подразделении Active Directory®, устройство или его владелец находятся в группе безопасности Active Directory.
- Клиентское устройство принадлежит определенному владельцу или владелец устройства находится во внутренней группе безопасности Kaspersky Security Center.

Политики в иерархии групп администрирования

Если вы создаете политику в группе администрирования нижнего уровня, то новая политика наследует профили активной политики для группы верхнего уровня. Профили с одинаковыми именами объединяются. Профили политики для группы более высокого уровня имеют более высокий приоритет. Например, в группе администрирования A политика P(A) имеет профили X1, X2, и X3, в порядке убывания приоритета. В группе администрирования B, которая является подгруппой группы A, создана политика P(B), с профилями X2, X4, X5. Тогда политика P(B) будет изменена политикой P(A), так, что в политике P(B) список профилей в порядке убывания приоритета будет X1, X2, X3, X4, X5.

Приоритет профиля X2 будет зависеть от начального состояния X2 политики P(B) и X2 политики P(A). После создания политики P(B) политика P(A) не будет отображаться в подгруппе B.

Активная политика вычисляется каждый раз заново при запуске Агента администрирования, при включении и выключении автономного режима, а также при изменении списка тегов, назначенных клиентскому устройству. Например, устройству увеличили объем оперативной памяти, в результате активировался профиль политики, который применяется для устройств с большим объемом оперативной памяти.

Свойства и ограничения профиля политики

Профили имеют следующие свойства:

- Профили неактивной политики не влияют на клиентские устройства.
- Если политика активна в автономном режиме, то и профили этой политики применяются только в автономном режиме.
- Профили не поддерживают статический анализ доступа к исполняемым файлам (см. раздел "Просмотр результатов статического анализа правил запуска исполняемых файлов" на стр. [258](#)).
- Профиль политики не может содержать параметры оповещений о событиях.
- Если используется UDP-порт 15000 для подключения устройства к Серверу администрирования, то при назначении тега устройству соответствующий профиль политики активируется в течение одной минуты.
- Вы можете использовать правила подключения Агента администрирования к Серверу администрирования (см. раздел "Создание правила переключения Агента администрирования по сетевому местоположению" на стр. [59](#)), когда вы создаете правила активации профиля политики.

Создание профиля политики

Создание профиля доступно только для политик Kaspersky Endpoint Security 10 Service Pack 1 для Windows и выше, для политик программы Kaspersky Endpoint Security 10 Service Pack 1 для Mac, для политик плагина Kaspersky Mobile Device Management версий от 10 Service Pack 1 до 10 Service Pack 3 Maintenance Release 1, для политики плагина Kaspersky Device Management для iOS.

► Чтобы создать профиль политики, выполните следующие действия:

1. В дереве консоли выберите группу администрирования, для политики которой нужно создать профиль политики.
2. В рабочей области группы администрирования выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики и нажмите на кнопку **Добавить**.

Запустится мастер создания профиля политики.

5. В окне мастера **Имя профиля политики** укажите:

- a. Имя профиля политики.

Имя профиля не может превышать 100 символов.

- b. Состояние профиля политики (*Включен, Выключен*).

Рекомендуется создавать неактивные профили политики и включать их только после полного завершения настройки параметров и условий активации профилей политики.

6. Установите флажок **После закрытия мастера создания профиля политики перейти к настройке правила активации профиля политики**, чтобы запустить мастер создания правила активации профиля политики (см. раздел "Создание правила активации профиля политики" на стр. [80](#)). Следуйте шагам мастера.

7. Измените параметры профиля политики в окне свойств профиля политики (см. раздел "Изменение профиля политики" на стр. [78](#)), как вам необходимо.

8. Сохраните изменения, нажав на кнопку **ОК**.

Профиль будет сохранен. Профиль будет активирован на устройствах, удовлетворяющих правилам активации.

Для одной политики можно создать несколько профилей политики. Профили, созданные для политики, отображаются в свойствах политики в разделе **Профили политики**. Вы можете изменить профиль политики и приоритет профиля (см. раздел "Изменение профиля политики" на стр. [78](#)), а также удалить профиль (см. раздел "Удаление профиля политики" на стр. [79](#)).

Изменение профиля политики

Изменение параметров профиля политики

Изменение профиля доступно только для политик Kaspersky Endpoint Security 10 Service Pack 1 для Windows.

► *Чтобы изменить профиль политики, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно изменить профиль политики.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профиль политики** в свойствах политики.

В разделе содержится список профилей, созданных для политики. Профили в списке отображаются в соответствии с их приоритетом.

5. Выберите профиль политики и нажмите на кнопку **Свойства**.

6. В окне свойств настройте параметры профиля:

- Если необходимо, в разделе **Общие** измените имя профиля и включите или выключите профиль с помощью флажка **Включить профиль**.
- В разделе **Правила активации** измените правила активации профиля.
- Измените параметры политики в соответствующих разделах.

7. Нажмите на кнопку **ОК**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

Изменение приоритета профиля политики

Приоритет профилей политик определяет порядок активации профилей на клиентском устройстве. Приоритет используется, если для разных профилей политики заданы одинаковые правила активации.

Например, созданы два профиля политики: *Профиль 1* и *Профиль 2*, отличающиеся друг от друга значениями одного параметра (*Значение 1* и *Значение 2*). Приоритет *Профиля 1* выше, чем приоритет *Профиля 2*. Кроме того, существуют профили с более низким приоритетом, чем *Профиль 2*. Правила активации профилей совпадают.

При выполнении правила активации будет активирован *Профиль 1*. Параметр на устройстве примет *Значение 1*. Если удалить *Профиль 1*, то *Профиль 2*, будет иметь самый высокий приоритет, и параметр примет *Значение 2*.

В списке профилей политики профили отображаются в соответствии с их приоритетом. На первом месте в списке стоит профиль с самым высоким приоритетом. Приоритет профиля

можно изменять с помощью кнопок  и .

Удаление профиля политики

► Чтобы удалить профиль политики, выполните следующие действия:

1. Выберите в дереве консоли группу администрирования, для которой нужно удалить профиль политики.

2. В рабочей области группы администрирования выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профиль политики** в свойствах политики Kaspersky Endpoint Security.
5. Выберите профиль политики, который нужно удалить, и нажмите на кнопку **Удалить**.

В результате профиль политики будет удален. Активным станет либо другой профиль политики, правила активации которого выполняются на устройстве, либо политика.

Создание правила активации профиля политики

► *Чтобы создать правило активации профиля политики, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать правило активации профиля политики.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики.
5. Выберите профиль политики, для которого нужно создать правило активации, и нажмите на кнопку **Свойства**.

В результате откроется окно свойств профиля политики.

Если список профилей политики пуст, вы можете создать профиль политики (см. раздел "Создание профиля политики" на стр. [77](#)).

6. Выберите раздел **Правила активации** и нажмите на кнопку **Добавить**.

В результате запустится мастер создания правила активации профиля политики.

7. В окне **Правила активации профиля политики** установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

a. Общие правила активации профиля политики

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

b. Правила для использования Active Directory

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

c. Правила для определенного владельца устройства

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от того, кто является владельцем устройства, и от членства устройства во внутренней группе безопасности Kaspersky Security Center.

d. Правила для характеристик оборудования

Установите флажок, чтобы настроить условие активации на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.

8. В окне **Общие условия** настройте следующие параметры:

a. В поле **Устройство в автономном режиме** в раскрывающемся списке укажите условие нахождения устройства в сети:

- **Да**

Устройство находится во внешней сети, то есть Сервер

администрирования недоступен.

- **Нет**

Устройство находится в сети, Сервер администрирования доступен.

- **Значение не выбрано**

Критерий не применяется.

- b. В поле **Устройство находится в указанном сетевом местоположении** с помощью раскрывающихся списков настройте активацию профиля политики при выполнении / невыполнении на устройстве правила подключения к Серверу администрирования:

- **Выполняется / Не выполняется**

Условие активации профиля политики (правило выполняется или не выполняется).

- **Имя правила**

Описание сетевого местоположения устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

Окно **Общие условия** отображается, если был установлен флажок **Общие правила активации профиля политики**.

9. В окне **Условия с использованием тегов** настройте следующие параметры:

a. **Список тегов**

В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не

применяется. По умолчанию флажки сняты.

b. Применять к устройствам без выбранных тегов

Установите флажок, если необходимо инвертировать выбор тегов.

Если флажок установлен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если флажок снят, критерий не применяется. По умолчанию флажок снят.

Окно **Условия с использованием тегов** отображается, если был установлен флажок **Общие правила активации профиля политики**.

10. В окне **Условия с использованием Active Directory** настройте следующие параметры:

a. Членство владельца устройства в группе безопасности Active Directory

Если флажок установлен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности или членом групп безопасности, входящих в указанную группу. Вы можете указать группу безопасности Active Directory, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

b. Членство устройства в группе безопасности Active Directory

Если флажок установлен, профиль политики активируется на устройстве, которое является членом указанной группы безопасности или членом групп безопасности, входящих в указанную группу. Вы можете указать группу безопасности Active Directory, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

a. Размещение устройства в подразделении Active Directory

Если флажок установлен, профиль политики активируется на устройстве, которое явно или неявно входит в указанное подразделение Active Directory. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

Окно **Условия с использованием Active Directory** отображается, если был установлен флажок **Правила для использования Active Directory**.

1. В окне **Условия с использованием владельца устройства** настройте следующие параметры:

- а. Владелец устройства**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- устройство принадлежит указанному владельцу (знак "=");
- устройство не принадлежит указанному владельцу (знак "≠").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

- а. Владелец устройства входит во внутреннюю группу безопасности**

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- владелец устройства является членом указанной группы безопасности (знак "=");
- владелец устройства не является членом указанной группы безопасности (знак "≠").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

Окно **Условия с использованием владельца устройства** отображается, если был установлен флажок **Правила для определенного владельца устройства**.

1. В окне **Условия с использованием характеристик оборудования** настройте следующие параметры:

а. Объем оперативной памяти (МБ)

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- объем оперативной памяти устройства меньше указанного значения (знак "<");
- объем оперативной памяти устройства больше указанного значения (знак ">").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не применяется. По умолчанию флажок снят.

б. Количество логических процессоров

Установите флажок, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- количество логических процессоров устройства меньше или равно указанному значению (знак "<=");
- количество логических процессоров устройства больше или равно указанному значению (знак ">=").

Если флажок установлен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства, когда флажок установлен. Если флажок снят, критерий активации профиля не

применяется. По умолчанию флажок снят.

Окно **Условия с использованием характеристик оборудования** отображается, если был установлен флажок **Правила для характеристик оборудования**.

2. В окне **Имя правила активации профиля политики** в поле **Имя условия** укажите имя правила.

В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики в разделе **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Управление задачами

Kaspersky Security Center управляет работой программ, установленных на устройствах, путем создания и запуска задач. С помощью задач выполняются установка, запуск и остановка программ, проверка файлов, обновление баз и модулей программ, другие действия с программами.

Задачи делятся на следующие типы:

- *Групповые задачи.* Задачи, которые выполняются на устройствах выбранной группы администрирования.
- *Задачи Сервера администрирования.* Задачи, которые выполняются на Сервере администрирования.
- *Задачи для наборов устройств.* Задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.
- *Локальные задачи.* Задачи, которые выполняются на конкретном устройстве.

Создание задач для программы возможно только в случае, если на рабочее место администратора установлен плагин управления этой программой.

Список устройств, для которых будет создана задача, можно сформировать одним из следующих способов:

- Выбрать устройства, обнаруженные в сети Сервером администрирования.
- Задать список устройств вручную. В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.
- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования при подключении устройств или в результате опроса сети.

Для каждой программы вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Обмен информацией о задачах между программой, установленной на устройстве, и информационной базой Kaspersky Security Center происходит в момент соединения Агента администрирования с Сервером администрирования.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи. При остановке программы выполнение всех запущенных задач прекращается.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, пароль доменного администратора.

В этом разделе

Создание задачи	90
Создание задачи Сервера администрирования.....	90
Создание задачи для набора устройств	92
Создание локальной задачи.....	93
Отображение унаследованной групповой задачи в рабочей области вложенной группы	94
Автоматическое включение устройств перед запуском задачи.....	94
Автоматическое выключение устройства после выполнения задачи	95
Ограничение времени выполнения задачи	95
Экспорт задачи.....	96
Импорт задачи.....	96
Конвертация задач.....	97
Запуск и остановка задачи вручную.....	98
Приостановка и возобновление задачи вручную	99
Наблюдение за ходом выполнения задачи	99
Просмотр результатов выполнения задач, хранящихся на Сервере администрирования	99
Настройка фильтра информации о результатах выполнения задачи	100
Изменение задачи. Откат изменений.....	100
Сравнение задач	101
Учетные записи для запуска задач	103
Установка программы с помощью групповых политик Active Directory	103

Создание задачи

В Консоли администрирования можно создавать задачи непосредственно в папке группы администрирования, для которой создается групповая задача, и в рабочей области папки **Задачи**.

► *Чтобы создать групповую задачу в папке группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой требуется создать задачу.
2. В рабочей области группы выберите закладку **Задачи**.
3. Запустите создание задачи по кнопке **Создать задачу**.

В результате запускается мастер создания задачи. Следуйте его указаниям.

► *Чтобы создать задачу в рабочей области папки **Задачи**, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите создание задачи по кнопке **Создать задачу**.

В результате запускается мастер создания задачи. Следуйте его указаниям.

Не используйте в параметрах задач конфиденциальные данные. Например, пароль доменного администратора.

Создание задачи Сервера администрирования

Сервер администрирования выполняет следующие задачи:

- автоматическую рассылку отчетов;

- загрузку обновлений в хранилище;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На виртуальном Сервере администрирования доступна только задача автоматической рассылки отчетов и задача создания инсталляционного пакета на основе образа операционной системы эталонного устройства. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования. Резервное копирование данных виртуального Сервера осуществляется в рамках резервного копирования данных главного Сервера администрирования.

► *Чтобы создать задачу Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи одним из следующих способов:
 - В дереве консоли в контекстном меню папки **Задачи** выберите пункт **Создать** → **Задачу**.
 - По кнопке **Создать задачу** в рабочей области папки **Задачи**.

В результате запускается мастер создания задачи. Следуйте его указаниям.

Задачи **Загрузка обновлений в хранилище**, **Синхронизация обновлений Windows Update**, **Обслуживание базы данных** и **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задачи **Загрузка обновлений в хранилище**, **Обслуживание базы данных**, **Резервное копирование данных Сервера администрирования** и **Синхронизация обновлений Windows Update** уже созданы для Сервера администрирования, то они не отображаются в окне выбора типа задачи мастера создания задачи.

Создание задачи для набора устройств

В Kaspersky Security Center можно создавать задачи для произвольно выбранного набора устройств. Устройства в наборе могут входить в разные группы администрирования или не входить ни в одну группу администрирования. Kaspersky Security Center позволяет выполнять следующие основные задачи для набора устройств:

- удаленную установку программы;
- сообщение для пользователя (см. раздел "Отправка сообщения пользователям устройств" на стр. [128](#));
- смену Сервера администрирования (см. раздел "Смена Сервера администрирования для клиентских устройств" на стр. [123](#));
- управление устройством (см. раздел "Удаленное включение, выключение и перезагрузка клиентских устройств" на стр. [125](#));
- проверку обновлений (см. раздел "Проверка полученных обновлений" на стр. [377](#));
- распространение инсталляционного пакета;
- удаленную установку программы на подчиненные Серверы администрирования;
- удаленную деинсталляцию программы.

► *Чтобы создать задачу для набора устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.

2. Запустите процесс создания задачи одним из следующих способов:

- В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.
- По кнопке **Создать задачу** в рабочей области папки **Задачи**.

В результате запускается мастер создания задачи. Следуйте его указаниям.

Создание локальной задачи

► *Чтобы создать локальную задачу для устройства, выполните следующие действия:*

1. В рабочей области группы, в состав которой входит устройство, выберите закладку **Устройства**.
2. В списке устройств на закладке **Устройства** выберите устройство, для которого нужно создать локальную задачу.
3. Запустите процесс создания задачи для выбранного устройства одним из следующих способов:
 - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите **Создать задачу**.
 - По ссылке **Создать задачу** в блоке работы с устройством.
 - Из окна свойств устройства следующим образом:
 - а. В контекстном меню устройства выберите пункт **Свойства**.
 - б. В открывшемся окне свойств устройства выберите раздел **Задачи** и нажмите на кнопку **Добавить**.

В результате запускается мастер создания задачи. Следуйте его указаниям.

Подробные описания создания и настройки локальных задач приводятся в Руководствах к соответствующим программам "Лаборатории Касперского".

Отображение унаследованной групповой задачи в рабочей области вложенной группы

► Чтобы включить отображение унаследованных задач вложенной группы в рабочей области, выполните следующие действия:

1. Выберите в рабочей области вложенной группы закладку **Задачи**.
2. В рабочей области закладки **Задачи** нажмите на кнопку **Показывать унаследованные задачи**.

В результате унаследованные задачи отображаются в списке задач со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования редактирование унаследованных задач доступно только в той группе, в которой они были созданы. Редактирование унаследованных задач недоступно в той группе, которая наследует задачи.

Автоматическое включение устройств перед запуском задачи

Kaspersky Security Center позволяет настроить параметры задачи так, чтобы перед выполнением задачи на выключенных устройствах загружалась операционная система.

► Чтобы настроить автоматическое включение устройств перед запуском задачи, выполните следующие действия:

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с устройствами по ссылке **Дополнительно**.

3. В открывшемся окне **Дополнительно** установите флажок **Активировать устройство перед запуском задачи функцией Wake On Lan за (мин)** и укажите время в минутах.

В результате выключенные устройства будут автоматически включены за указанное количество минут до запуска задачи, и на них будет загружена операционная система.

Автоматическая загрузка операционной системы доступна только на устройствах с поддержкой функции Wake On LAN.

Автоматическое выключение устройства после выполнения задачи

Kaspersky Security Center позволяет настроить параметры задачи таким образом, чтобы после ее выполнения устройства, на которые она распространяется, автоматически выключались.

- ▶ *Чтобы устройства автоматически выключались после выполнения задачи, выполните следующие действия:*
 1. В окне свойств задачи выберите раздел **Расписание**.
 2. Откройте окно настройки действий с устройствами по ссылке **Дополнительно**.
 3. В открывшемся окне **Дополнительно** установите флажок **Выключать устройство после выполнения задачи**.

Ограничение времени выполнения задачи

- ▶ *Чтобы ограничить время выполнения задачи на устройствах, выполните следующие действия:*
 1. В окне свойств задачи выберите раздел **Расписание**.
 2. Откройте окно настройки действий с клиентскими устройствами по ссылке **Дополнительно**.

3. В открывшемся окне **Дополнительно** установите флажок **Остановить, если задача выполняется дольше (мин)** и укажите время в минутах.

В результате, если по истечении указанного времени выполнение задачи на устройстве не будет завершено, Kaspersky Security Center автоматически остановит выполнение задачи.

Экспорт задачи

Вы можете экспортировать групповые задачи и задачи для наборов устройств в файл. Задачи Сервера администрирования и локальные задачи недоступны для экспорта.

► *Чтобы экспортировать задачу, выполните следующие действия:*

1. В контекстном меню задачи выберите пункт **Все задачи** → **Экспортировать**.
2. В открывшемся окне **Сохранить как** укажите имя файла и путь для сохранения.
3. Нажмите на кнопку **Сохранить**.

Права локальных пользователей не экспортируются.

Импорт задачи

Вы можете импортировать групповые задачи и задачи для наборов устройств. Задачи Сервера администрирования и локальные задачи недоступны для импорта.

► *Чтобы импортировать задачу, выполните следующие действия:*

1. Выберите список задач, в который требуется импортировать задачу:
 - Если вы хотите импортировать задачу в список групповых задач, в рабочей области нужной вам группы администрирования выберите закладку **Задачи**.
 - Если вы хотите импортировать задачу в список задач для наборов устройств, в дереве консоли выберите папку **Задачи**.
2. Выберите один из следующих способов импорта задачи:

- В контекстном меню списка задач выберите пункт **Все задачи** → **Импортировать**.
 - По ссылке **Импортировать задачу из файла** в блоке управления списком задач.
3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать задачу.
 4. Нажмите на кнопку **Открыть**.

В результате импортированная задача отобразится в списке задач.

Если в выбранном списке уже существует задача с именем, аналогичным имени импортируемой задачи, к имени импортируемой задачи будет добавлено окончание вида (<порядковый номер>), например: (1), (2).

Конвертация задач

С помощью Kaspersky Security Center можно конвертировать задачи предыдущих версий программ "Лаборатории Касперского" в задачи текущих версий программ.

Конвертация возможна для задач следующих программ:

- Антивирус Касперского 6.0 для Windows Workstations MP4;
- Kaspersky Endpoint Security 8 для Windows;
- Kaspersky Endpoint Security 10 для Windows.

► *Чтобы конвертировать задачи, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию задач.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

В результате запускается мастер массовой конвертации политик и задач. Следуйте его указаниям.

В результате работы мастера формируются новые задачи, использующие параметры задач предыдущих версий программ.

Запуск и остановка задачи вручную

Задачи можно запускать и останавливать двумя способами: из контекстного меню задачи и в окне свойств клиентского устройства, которому назначена эта задача.

Запускать групповые задачи из контекстного меню устройства могут пользователи, входящие в группу **KLAdmins** (см. раздел "**Права доступа к Серверу администрирования и его объектам**" на стр. [23](#)).

► *Чтобы запустить или остановить задачу из контекстного меню или окна свойств задачи, выполните следующие действия:*

1. В списке задач выберите задачу.
2. Запустите или остановите задачу одним из следующих способов:
 - В контекстном меню задачи выберите пункт **Запустить** или **Остановить**.
 - В разделе **Общие** окна свойств задачи нажмите на кнопку **Запустить** или **Остановить**.

► *Чтобы запустить или остановить задачу из контекстного меню или окна свойств клиентского устройства, выполните следующие действия:*

1. В списке устройств выберите устройство.
2. Запустите или остановите задачу одним из следующих способов:
 - В контекстном меню устройства выберите пункт **Все задачи** → **Запустить задачу**. Из списка задач выберите требуемую.

Список устройств, для которых назначена задача, будет замещен выбранным устройством. Задача будет запущена.

- В окне свойств устройства в разделе **Задачи** нажмите на кнопку  или .

Приостановка и возобновление задачи вручную

► Чтобы приостановить или возобновить выполнение запущенной задачи, выполните следующие действия:

1. В списке задач выберите задачу.
2. Приостановите или возобновите выполнение задачи из следующих способов:
 - В контекстном меню задачи выберите пункт **Приостановить** или **Возобновить**.
 - В разделе **Общие** окна свойств задачи нажмите на кнопку **Приостановить** или **Возобновить**.

Наблюдение за ходом выполнения задачи

► Чтобы наблюдать за ходом выполнения задачи,

в окне свойств задачи выберите раздел **Общие**.

В средней части окна раздела **Общие** содержится информация о текущем состоянии задачи.

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky Security Center позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Просмотр результатов выполнения локальных задач недоступен.

► Чтобы просмотреть результаты выполнения задачи, выполните следующие действия:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

Настройка фильтра информации о результатах выполнения задачи

Kaspersky Security Center позволяет фильтровать информацию о результатах выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Для локальных задач фильтрация недоступна.

► *Чтобы настроить фильтр для информации о результатах выполнения задачи, выполните следующие действия:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

Таблица в верхней части окна содержит список всех устройств, для которых назначена задача. Таблица в нижней части окна содержит результаты выполнения задачи на выбранном устройстве.

3. В интересующей вас таблице по правой клавише мыши откройте контекстное меню и выберите в нем пункт **Фильтр**.
4. В открывшемся окне **Применить фильтр** настройте параметры фильтра в разделах окна **События**, **Устройства** и **Время**. Нажмите на кнопку **ОК**.

В результате в окне **Результаты выполнения задачи** будет отображаться информация, удовлетворяющая параметрам, заданным в фильтре.

Изменение задачи. Откат изменений

► *Чтобы изменить задачу, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** выберите задачу и с помощью контекстного меню перейдите в окно свойств задачи.
3. Внесите необходимые изменения.

В разделе **Исключения из области действия задачи** можно настроить список вложенных групп, на которые не будет распространяться задача.

4. Нажмите на кнопку **Применить**.

Изменения задачи будут сохранены в окне свойств задачи, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения задачи.

► *Чтобы откатить изменения задачи, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Выберите задачу, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств задачи.
3. В окне свойств задачи выберите раздел **История ревизий**.
4. В списке ревизий задачи выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Сравнение задач

Вы можете сравнивать задачи одного типа, например, можно сравнить две задачи поиска вирусов, но нельзя сравнить задачу поиска вирусов с задачей установки обновлений. В результате сравнения задач вы получаете отчет, показывающий, какие параметры задач совпадают, а какие различаются. Вы можете распечатать отчет сравнения задач или сохранить его в файле. Сравнение задач может потребоваться в случае, когда для разных подразделений одной компании есть различные задачи одного типа. Например, для бухгалтерии есть задача проверять на вирусы только локальные диски компьютера, а для отдела продаж, сотрудники которого переписываются с клиентами, есть задача проверять и локальные диски, и почту. Чтобы быстро увидеть такие различия, нет необходимости просматривать все параметры задачи, достаточно выполнить сравнение задач.

Сравнение можно выполнить только для задач одного типа.

Задачи можно сравнивать только попарно.

Вы можете сравнить задачи двумя способами: выбрать одну задачу и сравнить ее с другой или сравнить две задачи из списка задач.

► *Чтобы выбрать одну задачу и сравнить ее с другой, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** выберите задачу, которую нужно сравнить с другой задачей.
3. В контекстном меню задачи выберите пункт **Все задачи** → **Сравнить с другой задачей**.
4. В окне **Выбор задачи** выберите задачу для сравнения.
5. Нажмите на кнопку **ОК**.

Отобразится отчет сравнения двух задач в формате HTML.

► *Чтобы сравнить две задачи из списка задач, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** в списке задач с помощью клавиши **SHIFT** или **CTRL** выберите две задачи одного типа.
3. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения выбранных задач в формате HTML.

При сравнении задач, в случае если используемые пароли отличаются, в отчете сравнения задач будут отображаться символы *********.

Если в свойствах задачи был изменен пароль, в отчете сравнения ревизий задачи будут отображаться символы *********.

Учетные записи для запуска задач

Вы можете задавать учетную запись, под которой должна запускаться задача.

Например, для выполнения задач проверки по требованию необходимы права на доступ к проверяемому объекту, а для выполнения задач обновления – права авторизованного пользователя прокси-сервера. Возможность задать учетную запись для запуска задачи позволяет избежать ошибки при выполнении задач проверки по требованию и задач обновления, если у пользователя, запустившего задачу, нет необходимых прав доступа.

В задачах удаленной установки и деинсталляции программы учетная запись используется для загрузки на клиентские устройства файлов, необходимых для установки (удаления), если на устройстве не установлен или недоступен Агент администрирования. При установленном и доступном Агенте администрирования учетная запись используется, если согласно параметрам задачи доставка файлов выполняется только средствами Microsoft Windows из папки общего доступа. В этом случае учетная запись должна обладать следующими правами на устройстве:

- правом на удаленный запуск программ;
- правами на ресурс Admin\$;
- правом *Вход в качестве службы*.

Если доставку файлов на устройства выполняет Агент администрирования, учетная запись использоваться не будет. Все операции по копированию и установке файлов будет выполнять Агент администрирования под учетной записью **Локальная система (Local System Account)**.

Установка программы с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать программы "Лаборатории Касперского" с помощью групповых политик Active Directory.

Установка программ с помощью групповых политик Active Directory возможна только при использовании инсталляционных пакетов, в состав которых входит Агент администрирования.

► *Чтобы установить программу с помощью групповых политик Active Directory, выполните следующие действия:*

1. Запустите процесс создания групповой задачи удаленной установки или задачи удаленной установки для набора устройств.
2. В окне мастера создания задачи **Параметры** установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.
3. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:
 - Групповая политика с именем **Kaspersky_AK{GUID}**.
 - Связанная с групповой политикой группа безопасности **Kaspersky_AK{GUID}**. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область действия групповой политики.
2. Установка программ на клиентские устройства осуществляется непосредственно из сетевой папки общего доступа программы Share. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msі для устанавливаемой программы.
3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи установлен флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.

4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.
5. При удалении задачи из Active Directory будут удалены политика, ссылка на политику и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной безопасности прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением `msi`, расположенный во вложенной папке `exes` в папке инсталляционного пакета нужной программы.
- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки `exes`, так как помимо файла с расширением `msi` в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы ключ был установлен вместе с программой, в эту папку следует также скопировать файл ключа.

Просмотр и изменение локальных параметров программы

Система администрирования Kaspersky Security Center позволяет удаленно управлять локальными параметрами программ на устройствах через Консоль администрирования.

Локальные параметры программы – это параметры программы, индивидуальные для устройства. С помощью Kaspersky Security Center вы можете устанавливать локальные параметры программ для устройств, входящих в группы администрирования.

Подробные описания параметров программ "Лаборатории Касперского" приводятся в Руководствах для этих программ.

► *Чтобы просмотреть или изменить локальные параметры программы, выполните следующие действия:*

1. В рабочей области группы, в которую входит нужное вам устройство, выберите закладку **Устройства**.
2. В окне свойств устройства в разделе **Программы** выберите нужную вам программу.
3. Откройте окно свойств программы двойным щелчком мыши по названию программы или нажатием на кнопку **Свойства**.

В результате откроется окно локальных параметров выбранной программы, которые можно просмотреть и изменить.

Вы можете изменять значения тех параметров, изменение которых не запрещено групповой политикой (параметр не закрыт "замком" в политике).

Управление клиентскими устройствами

Этот раздел содержит информацию о работе с клиентскими устройствами.

В этом разделе

Подключение клиентских устройств к Серверу администрирования	108
Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover	110
Туннелирование соединения клиентского устройства с Сервером администрирования .	112
Удаленное подключение к рабочему столу клиентского устройства	113
Подключение к устройствам с помощью Windows Desktop Sharing	115
Настройка перезагрузки клиентского устройства	116
Аудит действий на удаленном клиентском устройстве	117
Проверка соединения клиентского устройства с Сервером администрирования	119
Идентификация клиентских устройств на Сервере администрирования	122
Перемещение устройств в состав группы администрирования	122
Смена Сервера администрирования для клиентских устройств	123
Кластеры и массивы серверов	124
Удаленное включение, выключение и перезагрузка клиентских устройств	125
Доступ к локальным задачам и статистике, флажок "Не разрывать соединение с Сервером администрирования"	126
Форсирование синхронизации	127
О менеджере соединений	127
Отправка сообщения пользователям устройств	128
Работа с программой Kaspersky Security для виртуальных сред	128
Контроль изменения состояния виртуальных машин	129
Настройка переключения статусов устройств	130

Отслеживание состояния антивирусной защиты с помощью информации в системном реестре	136
Назначение тегов устройствам и просмотр назначенных тегов	138
Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center	143
Устройства с защитой на уровне UEFI	149
Параметры управляемого устройства	150
Параметры политики Агента администрирования	158

Подключение клиентских устройств к Серверу администрирования

Подключение клиентского устройства к Серверу администрирования осуществляет Агент администрирования, установленный на клиентском устройстве.

При подключении клиентского устройства к Серверу администрирования выполняются следующие операции:

- Автоматическая синхронизация данных:
 - синхронизация списка программ, установленных на клиентском устройстве;
 - синхронизация политик, параметров программ, задач и параметров задач.
- Получение Сервером текущей информации о состоянии программ, выполнении задач и статистики работы программ.
- Доставка на Сервер информации о событиях, которые требуется обработать.

Автоматическая синхронизация данных производится периодически, в соответствии с параметрами Агента администрирования (например, один раз в 15 минут). Вы можете вручную задать интервал между соединениями.

Информация о событии доставляется на Сервер администрирования сразу после того, как событие произошло.

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления программами и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 100 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования на порт 15000, не дожидаясь синхронизации с устройством.

Kaspersky Security Center позволяет настроить соединение клиентского устройства с Сервером администрирования таким образом, чтобы соединение не завершалось по окончании выполнения операций. Непрерывное соединение необходимо в том случае, если требуется постоянный контроль состояния программ, а Сервер администрирования не может инициировать соединение с клиентским устройством (например, соединение

защищено межсетевым экраном, запрещено открывать порты на клиентском устройстве, неизвестен IP-адрес клиентского устройства). Установить неразрывное соединение клиентского устройства с Сервером администрирования можно в окне свойств устройства, в разделе **Общие**.

Рекомендуется устанавливать непрерывное соединение с наиболее важными устройствами. Общее количество соединений, поддерживаемых Сервером администрирования одновременно, ограничено (несколько сотен).

При синхронизации вручную используется вспомогательный способ подключения, при котором соединение инициирует Сервер администрирования. Перед подключением на клиентском устройстве требуется открыть UDP-порт. Сервер администрирования посылает на UDP-порт клиентского устройства запрос на соединение. В ответ на него производится проверка сертификата Сервера администрирования. Если сертификат Сервера совпадает с копией сертификата на клиентском устройстве, соединение осуществляется.

Запуск процесса синхронизации вручную используется также для получения текущей информации о состоянии программ, выполнении задач и статистике работы программ.

Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover

Если вам требуется подключить клиентское устройство к Серверу администрирования вручную, вы можете воспользоваться утилитой klmover на клиентском устройстве.

При установке на клиентское устройство Агента администрирования утилита автоматически копируется в папку установки Агента администрирования.

- *Чтобы подключить клиентское устройство к Серверу администрирования вручную с помощью утилиты klmover,*

на устройстве запустите утилиту klmover из командной строки.

При запуске из командной строки утилита klmover в зависимости от используемых ключей выполняет следующие действия:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

Синтаксис утилиты:

```
klmover [-logfile <имя файла>] [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-noss1] [-cert <путь к файлу сертификата>] [-silent] [-dupfix]
```

Описание ключей:

- `-logfile <имя файла>` – записать результаты выполнения утилиты в файл журнала.

По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, результаты и сообщения об ошибках выводятся на экран.

- `-address <адрес сервера>` – адрес Сервера администрирования для подключения.

В качестве адреса можно указать IP-адрес, NetBIOS- или DNS-имя устройства.

- `-pn <номер порта>` – номер порта, по которому будет осуществляться незащищенное подключение к Серверу администрирования.

По умолчанию используется порт 14000.

- `-ps <номер SSL-порта>` – номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.

По умолчанию используется порт 13000.

- `-noss1` – использовать незащищенное подключение к Серверу администрирования.

Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.

- `-cert` <путь к файлу сертификата> – использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.

Если ключ не используется, Агент администрирования получает сертификат при первом подключении к Серверу администрирования.

- `-silent` – запустить утилиту на выполнение в неинтерактивном режиме.

Использование ключа может быть полезно, например, при запуске утилиты из сценария входа при регистрации пользователя.

- `-dupfix` – ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.

Туннелирование соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

В частности, туннелирование используется для подключения к удаленному рабочему столу: как для подключения к существующей сессии, так и для создания новой удаленной сессии.

Также туннелирование может быть использовано при помощи механизма внешних инструментов. В частности, администратор может запускать таким образом утилиту `putty`, VNC-клиент и прочие инструменты.

Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с

Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

- Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
- Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт брандмауэром.

► *Чтобы произвести туннелирование соединения клиентского устройства с Сервером администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку группы, в которую входит клиентское устройство.
2. На закладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Все задачи** → **Туннелирование соединения**.
4. Создайте туннель в открывшемся окне **Туннелирование соединения**.

Удаленное подключение к рабочему столу клиентского устройства

Администратор может получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять программами, установленными на нем.

Удаленное подключение к клиентскому устройству можно осуществить двумя способами:

- С помощью стандартного компонента Microsoft Windows "Подключение к удаленному рабочему столу". Подключение к удаленному рабочему столу выполняется с помощью штатной утилиты Windows `mstsc.exe` в соответствии с параметрами работы этой утилиты.

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. После подключения администратора к сеансу пользователь устройства будет отключен от сеанса без предварительного уведомления.

- С помощью технологии Windows Desktop Sharing. При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center.

Администратор может подключиться к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве будет совместный доступ к рабочему столу.

Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита программа сохраняет информацию о файлах на клиентском устройстве, которые открывал и / или изменял администратор (см. раздел "Аудит действий на удаленном клиентском устройстве" на стр. [117](#)).

Для подключения к рабочему столу клиентского устройства с помощью Windows Desktop Sharing требуется выполнение следующих условий:

- На устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
 - На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью Windows Desktop Sharing.
 - Kaspersky Security Center использует лицензию на Системное администрирование.
- *Чтобы подключиться к рабочему столу клиентского устройства с помощью компонента "Подключение к удаленному рабочему столу", выполните следующие действия:*
1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.

2. В контекстном меню устройства выберите пункт **Все задачи** → **Подключиться к устройству** → **Создать новую сессию RDP**.

В результате будет запущена штатная утилита Windows mstsc.exe для подключения к удаленному рабочему столу.

3. Следуйте указаниям в открывающихся окнах утилиты.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью технологии Windows Desktop Sharing, выполните следующие действия:*

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи** → **Подключиться к устройству** → **Совместный доступ к рабочему столу**.
3. В открывшемся окне **Выбор сессии рабочего стола** выберите сеанс на клиентском устройстве, к которому требуется подключиться.

В случае успешного подключения к клиентскому устройству рабочий стол этого устройства будет доступен в окне **Kaspersky Remote desktop session viewer**.

4. Для начала взаимодействия с устройством в главном меню окна **Kaspersky Remote desktop session viewer** выберите пункт **Действия** → **Интерактивный режим**.

Подключение к устройствам с помощью Windows Desktop Sharing

► *Чтобы подключиться к устройству с помощью технологии Windows Desktop Sharing, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства** на закладке **Устройства**.

В рабочей области папки отображается список устройств.

2. В контекстном меню устройства, к которому вы хотите подключиться, выберите пункт **Подключиться к устройству** → **Windows Desktop Sharing**.

Откроется окно **Выбор сессии рабочего стола**.

3. В окне **Выбор сессии рабочего стола** выберите сессию рабочего стола, которая будет использоваться для подключения к устройству.
4. Нажмите на кнопку **ОК**.

Будет выполнено подключение к устройству.

Настройка перезагрузки клиентского устройства

В ходе работы, установки или удаления Kaspersky Security Center может потребоваться перезагрузка клиентского устройства. Программа позволяет настроить параметры перезагрузки устройств.

► *Чтобы настроить перезагрузку клиентского устройства, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно настроить перезагрузку.
2. В рабочей области группы выберите закладку **Политики**.
3. В списке политик выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Управление перезагрузкой**.
5. Выберите действие, которое нужно выполнять, если потребуется перезагрузка устройства:
 - Выберите **Не перезагружать операционную систему**, чтобы запретить автоматическую перезагрузку.

- Выберите **При необходимости перезагрузить операционную систему автоматически**, чтобы разрешить автоматическую перезагрузку.
- Выберите **Запрашивать у пользователя**, чтобы включить запрос на перезагрузку у пользователя.

Вы можете указать периодичность запроса на перезагрузку, включить принудительную перезагрузку и принудительное закрытие программ в заблокированных сессиях на устройстве, установив соответствующие флажки.

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате перезагрузка операционной системы устройства будет настроена.

Аудит действий на удаленном клиентском устройстве

Программа позволяет выполнять аудит действий администратора на удаленном клиентском устройстве. В ходе аудита программа сохраняет информацию о файлах на устройстве, которые открывал и / или изменял администратор. Аудит действий администратора доступен при выполнении следующих условий:

- есть в наличии действующая лицензия на Системное администрирование;
- у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

► *Чтобы включить аудит действий на удаленном клиентском устройстве, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой нужно настроить аудит действий администратора.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Общий доступ к рабочему столу**.

5. Установите флажок **Включить аудит**.
6. В списках **Маски файлов, чтение которых нужно отслеживать** и **Маски файлов, изменение которых нужно отслеживать** добавьте маски файлов, действия с которыми нужно отслеживать в ходе аудита.

По умолчанию программа отслеживает действия с файлами с расширениями txt, rtf, doc, xls, docx, xlsx, odt, pdf.

7. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу будет настроен.

Записи о действиях администратора на удаленном устройстве сохраняются:

- в журнале событий на удаленном устройстве;
- в файле с расширением syslog, который находится в папке Агента администрирования на удаленном устройстве (например, C:\ProgramData\KasperskyLab\adminkit\1103\logs);
- в базе событий Kaspersky Security Center.

Проверка соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет проверять соединение клиентского устройства с Сервером администрирования автоматически или вручную.

Автоматическая проверка соединения осуществляется на Сервере администрирования. Проверка соединения вручную осуществляется на устройстве.

В этом разделе

Автоматическая проверка соединения клиентского устройства с Сервером администрирования	119
Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk	120
Проверка времени соединения устройства с Сервером администрирования	121

Автоматическая проверка соединения клиентского устройства с Сервером администрирования

- ▶ *Чтобы запустить автоматическую проверку соединения клиентского устройства с Сервером администрирования, выполните следующие действия:*
 1. В дереве консоли выберите группу администрирования, в которую входит устройство.
 2. В рабочей области группы администрирования на закладке **Устройства** выберите устройство.
 3. В контекстном меню устройства выберите пункт **Проверить доступность устройства**.

В результате открывается окно, содержащее информацию о доступности устройства.

Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита `klagchk`

Вы можете проверять соединение и получать подробную информацию о параметрах подключения клиентского устройства к Серверу администрирования с помощью утилиты `klagchk`.

При установке на устройство Агента администрирования утилита `klagchk` автоматически копируется в папку установки Агента администрирования.

При запуске из командной строки утилита `klagchk` в зависимости от используемых ключей выполняет следующие действия:

- Выводит на экран или заносит в файл журнала событий значения параметров подключения Агента администрирования, установленного на устройстве, к Серверу администрирования.
- Записывает в файл журнала событий статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты, либо выводит информацию на экран.
- Предпринимает попытку установить соединение Агента администрирования с Сервером администрирования.

Если соединение установить не удалось, утилита посылает ICMP-пакет для проверки статуса устройства, на котором установлен Сервер администрирования.

► *Чтобы проверить соединение клиентского устройства с Сервером администрирования с помощью утилиты `klagchk`,*

на устройстве запустите утилиту `klagchk` из командной строки.

Синтаксис утилиты:

```
klagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>] [-restart]
```

Описание ключей:

- `-logfile <имя файла>` – записать значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала.

По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.

- `-sp` – вывести пароль для аутентификации пользователя на прокси-сервере.

Параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.

- `-savecert <имя файла>` – сохранить сертификат для аутентификации доступа к Серверу администрирования в указанном файле.

- `-restart` – перезапустить Агент администрирования после завершения утилиты.

Проверка времени соединения устройства с Сервером администрирования

При выключении устройства Агент администрирования уведомляет о выключении Сервер администрирования. В Консоли администрирования такое устройство отображается как выключенное. Однако Агенту удастся уведомить Сервер администрирования не во всех случаях. Поэтому Сервер администрирования для каждого устройства периодически анализирует атрибут **Время последнего соединения** (значение атрибута отображается в Консоли администрирования в свойствах устройства в разделе **Общие**) и сопоставляет его с периодом синхронизации из действующих параметров Агента администрирования. Если устройство не выходило на связь более чем три периода синхронизации, то такое устройство отмечается как выключенное.

Идентификация клиентских устройств на Сервере администрирования

Идентификация клиентских устройств осуществляется на основании их имен. Имя устройства является уникальным среди всех имен устройств, подключенных к Серверу администрирования.

Имя устройства передается на Сервер администрирования либо при опросе сети Windows и обнаружении в ней нового устройства, либо при первом подключении к Серверу администрирования установленного на устройство Агента администрирования. По умолчанию имя совпадает с именем устройства в сети Windows (NetBIOS-имя). Если на Сервере администрирования уже зарегистрировано устройство с таким именем, то к имени нового устройства будет добавлено окончание с порядковым номером, например: <Имя>-1, <Имя>-2. Под этим именем устройство включается в состав группы администрирования.

Перемещение устройств в состав группы администрирования

► *Чтобы включить одно или несколько устройств в состав выбранной группы администрирования, выполните следующие действия:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой будут включены клиентские устройства.

Если вы хотите включить устройства в состав группы **Управляемые устройства**, этот шаг можно пропустить.

3. В рабочей области выбранной группы администрирования на закладке **Устройства** запустите процесс включения устройств в группу одним из следующих способов:
 - Добавьте устройства в группу по кнопке **Переместить устройства в группу** в блоке управления списком устройств.
 - В контекстном меню списка устройств выберите пункт **Создать** → **Устройство**.

В результате запустится мастер перемещения устройств. Следуя его указаниям, определите способ перемещения устройств в группу и сформируйте список устройств, включаемых в состав группы.

Если вы формируете список устройств вручную, в качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя. Вручную в список устройств могут быть перемещены только те устройства, информация о которых уже была ранее занесена в базу данных Сервера администрирования при подключении устройства или в результате опроса сети.

Для импорта списка устройств из файла требуется указать файл в формате TXT с перечнем адресов добавляемых устройств. Каждый адрес должен располагаться в отдельной строке.

После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Можно переместить устройство в выбранную группу администрирования, перетащив его мышью из папки **Нераспределенные устройства** в папку группы администрирования.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи **Смена Сервера администрирования**.

► *Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу смены Сервера администрирования одним из следующих способов:

- Если требуется сменить Сервер администрирования для устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. [90](#)).
- Если требуется сменить Сервер администрирования для устройств, входящих в разные группы администрирования или не входящих в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. [92](#)).

В результате запустится мастер создания задачи. Следуйте его указаниям. В окне **Тип задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Смена Сервера администрирования**.

3. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает функциональность управления шифрованием и защитой данных, то при создании задачи **Смена Сервера администрирования** отображается предупреждение о том, что при наличии на устройствах зашифрованных данных, после переключения устройств под управление другого сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в онлайн-справке Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>.

Кластеры и массивы серверов

Kaspersky Security Center поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что программа, установленная на клиентском устройстве, является частью массива сервера, то

клиентское устройство становится узлом кластера. Кластер будет добавлен как отдельный объект в папке **Управляемые устройства** в дереве консоли со значком .

Можно выделить несколько типичных свойств кластера:

- Кластер и любой из его узлов всегда располагаются в одной группе администрирования.
- Если администратор попытается переместить какой-либо узел кластера, то узел вернется в исходное местоположение.
- Если администратор попытается переместить кластер в другую группу, то все его узлы также переместятся вместе с ним.

Удаленное включение, выключение и перезагрузка клиентских устройств

Kaspersky Security Center позволяет удаленно управлять клиентскими устройствами: включать, выключать и перезагружать их.

► *Чтобы удаленно управлять клиентскими устройствами, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу управления устройствами одним из следующих способов:
 - Если требуется включить, выключить или перезагрузить устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. [90](#)).
 - Если требуется включить, выключить или перезагрузить устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. [92](#)).

В результате запустится мастер создания задачи. Следуйте его указаниям. В окне **Тип задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Управление устройствами**.

3. Запустите созданную задачу.

После завершения работы задачи команда (включение, выключение или перезагрузка) будет выполнена на выбранных устройствах.

Доступ к локальным задачам и статистике, флажок "Не разрывать соединение с Сервером администрирования"

По умолчанию в Kaspersky Security Center нет постоянных соединений между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Продолжительность периода такой синхронизации (по умолчанию 15 минут) задается в политике Агента администрирования. Если необходима досрочная синхронизация (например, для ускорения применения политики), то Сервер администрирования посылает Агенту администрирования подписанный сетевой пакет на порт UDP 15000. Если подключение по UDP от Сервера администрирования к управляемому устройству по какой-то причине невозможно, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Некоторые операции не могут быть выполнены без досрочного подключения Агента администрирования к Серверу: запуск и остановка локальных задач, получение статистики управляемой программы (программы защиты или Агента администрирования), создание туннеля и прочее. Для решения этой проблемы в свойствах управляемого устройства (раздел **Общие**) нужно установить флажок **Не разрывать соединение с Сервером администрирования**. Общее количество устройств с установленным флажком **Не разрывать соединение с Сервером администрирования** не может превышать 300.

Форсирование синхронизации

Несмотря на то, что Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в данный момент времени для данного устройства синхронизация выполнена.

В контекстном меню управляемых устройств в Консоли администрирования устройства в пункте меню **Все задачи** имеется команда **Синхронизировать принудительно**. В Kaspersky Security Center 10 Service Pack 3 при выполнении этой команды в свойствах устройства устанавливается флажок **Назначена принудительная синхронизация**, затем Сервер администрирования пытается связаться с устройством. Если это удастся, то выполняется принудительная синхронизация, и флажок снимается. В противном случае принудительная синхронизация и снятие флажка произойдет лишь после очередного выхода Агента администрирования на связь с Сервером. Исчезновение флажка является сигналом для администратора о том, что синхронизация выполнена.

О менеджере соединений

В окне свойств политики Агента администрирования в разделе **Сеть** во вложенном разделе **Менеджер соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования.

Подключаться при необходимости. Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

Подключаться в указанные периоды времени. Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Отправка сообщения пользователям устройств

► Чтобы отправить сообщение пользователям устройств, выполните следующие действия:

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу отправки сообщения пользователям устройств одним из следующих способов:
 - Если требуется отправить сообщение пользователям устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. [90](#)).
 - Если требуется отправить сообщение пользователям устройств, входящих в разные группы администрирования или не входящих в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. [92](#)).

В результате запустится мастер создания задачи. Следуйте его указаниям. В окне **Тип задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Сообщение для пользователя**.

3. Запустите созданную задачу.

После завершения работы задачи созданное сообщение будет отправлено пользователям выбранных устройств.

Работа с программой Kaspersky Security для виртуальных сред

Kaspersky Security Center поддерживает возможность подключения виртуальных машин к Серверу администрирования. Управление виртуальными машинами осуществляется с помощью программы Kaspersky Security для виртуальных сред 4.0. Подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 4.0*.

Контроль изменения состояния виртуальных машин

Сервер администрирования хранит информацию о состоянии управляемых устройств, например, реестр оборудования и список установленных программ, параметры управляемых программ, задач и политик. Если управляемым устройством является виртуальная машина, пользователь может в любой момент восстановить ее состояние из образа виртуальной машины (snapshot), сделанного ранее. В результате информация о состоянии виртуальной машины на Сервере администрирования может стать неактуальной.

Например, в 12:00 администратор создал на Сервере администрирования политику защиты, которая в 12:01 начала действовать на виртуальной машине VM_1. В 12:30 пользователь виртуальной машины VM_1 изменил ее состояние, выполнив восстановление из образа, сделанного в 11:00. В результате этого политика защиты на виртуальной машине перестанет действовать. Однако на Сервере администрирования сохранится неактуальная информация о том, что политика защиты на виртуальной машине VM_1 продолжает действовать.

Kaspersky Security Center позволяет контролировать изменение состояния виртуальных машин.

После каждой синхронизации с устройством Сервер администрирования формирует уникальный идентификатор, который хранится как на устройстве, так и на Сервере администрирования. Перед началом следующей синхронизации Сервер администрирования сравнивает значения идентификаторов на обеих сторонах. Если значения идентификаторов не совпадают, Сервер администрирования считает виртуальную машину восстановленной из образа. Сервер администрирования сбрасывает действующие для этой виртуальной машины параметры политик и задач и отправляет на нее актуальные политики и список групповых задач.

Настройка переключения статусов устройств

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*.

► *Чтобы настроить изменение статуса устройства на Критический, выполните следующие действия:*

1. Откройте окно свойств одним из следующих способов:
 - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
 - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств перейдите в раздел **Статус устройства**.
3. В блоке **Условия для статуса Критический** установите флажок для условия из списка.
4. Для выбранного условия установите необходимое вам значение.

Не для все условий можно задать значения.
5. Нажмите на кнопку **ОК**.

► *Чтобы настроить изменение статуса устройства на Предупреждение, выполните следующие действия:*

1. Откройте окно свойств одним из следующих способов:
 - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
 - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств перейдите в раздел **Статус устройства**.

3. В блоке **Условия для статуса Предупреждение** установите флажок для условия из списка.

4. Для выбранного условия установите необходимое вам значение.

Не для все условий можно задать значения.

5. Нажмите на кнопку **ОК**.

Разным значениям одного условия могут соответствовать разные статусы. Например, при соблюдении условия **Базы устарели** со значением *Более 7 дней* клиентскому устройству присваивается статус *Предупреждение*, а со значением *Более 14 дней* – статус *Критический*.

В таблице приведены условия для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения

Таблица 1. Условия присвоения статусов устройству

Условие	Описание условия	Возможные значения
Не установлена программа защиты	На устройстве не установлена программа защиты.	<ul style="list-style-type: none"> • Флажок установлен. • Флажок снят.
Найдено много вирусов	На устройстве в результате работы задач поиска вирусов, например, задачи Поиск вирусов , найдены вирусы.	Более чем 0
Уровень постоянной защиты отличается от уровня, установленного администратором	Уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	<ul style="list-style-type: none"> • Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вирусов	Задача Поиск вирусов не выполнялась больше указанного времени.	Более чем 1 дней
Базы устарели	Антивирусные базы на устройстве не обновлялись больше указанного времени	Более чем 1 дней
Давно не подключался	Устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более чем 1 дней

Условие	Описание условия	Возможные значения
Есть необработанные объекты	Количество необработанных объектов в папке Необработанные файлы превышает указанное значение.	Более чем 0 штук
Требуется перезагрузка	В результате установки программ или обновлений на устройство, для его корректной работы требуется перезагрузка устройства.	Более чем 0 минут
Установлены несовместимые программы	В результате инвентаризации программного обеспечения Агентом администрирования на устройстве обнаружены установленные несовместимые программы.	<ul style="list-style-type: none"> • Флажок снят. • Флажок установлен.
Обнаружены уязвимости в программах	В результате выполнения задачи Поиск уязвимостей и требуемых обновлений на устройстве обнаружены уязвимости в программах с заданным уровнем критичности.	<ul style="list-style-type: none"> • Предельный. • Высокий. • Средний. • Игнорировать, если нельзя закрыть уязвимость. • Игнорировать, если обновление назначено к установке.

Условие	Описание условия	Возможные значения
Срок действия лицензии истек	Срок действия лицензии на устройстве истек более чем на указанное количество дней.	Более чем 0 дней
Давно не выполнялся поиск обновлений Windows	Не выполнялась задача Синхронизация обновлений Windows Update больше указанного времени.	Более чем 1 дней
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	<ul style="list-style-type: none"> • Флажок снят. • Флажок установлен.
Есть необработанные инциденты	На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.	<ul style="list-style-type: none"> • Флажок снят. • Флажок установлен.

Условие	Описание условия	Возможные значения
Определяемый программой	Статус устройства определяется управляемой программой.	<ul style="list-style-type: none"> • Флажок снят. • Флажок установлен.
Контроль над устройством потерян	При опросе сети устройство определяется видимым в сети, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	<ul style="list-style-type: none"> • Флажок снят. • Флажок установлен.
Не включена защита	Программа защиты на устройстве отключена больше указанного времени.	Более чем 0 минут
Не запущена программа защиты	Программа защиты установлена на устройстве, но не запущена.	<ul style="list-style-type: none"> • Флажок снят. • Флажок установлен.



См. также

Настройка общих параметров Сервера администрирования..... [40](#)

Отслеживание состояния антивирусной защиты с помощью информации в системном реестре

► Чтобы отследить состояние антивирусной защиты на клиентском устройстве с помощью информации, записанной Агентом администрирования в системный реестр, выполните следующие действия:

1. Откройте системный реестр клиентского устройства (например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**).
2. Перейдите в раздел:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103  
\1.0.0.0\Statistics\AVState
```

В результате в системном реестре отобразится информация о состоянии антивирусной защиты клиентского устройства.

Состояние антивирусной защиты соответствует значениям ключей, описанных в таблице ниже.

Таблица 2. Ключи реестра и их возможные значения

Ключ (тип данных)	Значение	Описание
Protection_AdmServer (REG_SZ)	<Имя Сервера администрирования>	Имя Сервера администрирования, который управляет устройством.
Protection_AvInstalled (REG_DWORD)	отлично от 0	На устройстве установлена программа защиты.
Protection_AvRunning (REG_DWORD)	отлично от 0	Постоянная защита устройства включена.
Protection_HasRtp (REG_DWORD)	отлично от 0	Установлен компонент постоянной защиты.
	Состояние постоянной защиты:	
	0	Неизвестно.
	2	Не включена.
	3	Приостановлена.
	4	Запускается.
	5	Включена.
	6	Включена, высокий уровень (максимальная защита).
7	Включена, используются параметры по умолчанию (рекомендуемые).	

Ключ (тип данных)	Значение	Описание
	8	Включена, используются параметры, настроенные пользователем.
	9	Сбой в работе.
Protection_LastFscan (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последней полной проверки.
Protection_BasesDate (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) выпуска баз программы.
Protection_LastConnected (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последнего соединения с Сервером администрирования.

Назначение тегов устройствам и просмотр назначенных тегов

Kaspersky Security Center позволяет назначать теги устройствам. *Тег* представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Ручное назначение тегов устройству выполняется в свойствах устройства и может понадобиться, когда необходимо отметить отдельное устройство. Автоматическое назначение тегов выполняется Сервером администрирования в соответствии с заданными правилами назначения тегов.

В свойствах Сервера администрирования вы можете настроить автоматическое назначение тегов устройствам, управляемым этим Сервером администрирования. Автоматическое

назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве программам и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы Windows, назначается тег *Win*. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать устройства, работающие под управлением операционной системы Windows, и назначить им задачу.

Вы также можете использовать теги в качестве условия для активации профиля политики на управляемом устройстве, чтобы определенные профили политик применялись только на устройствах, имеющих определенные теги. Например, если в группе администрирования *Пользователи* появляется устройство с тегом *Курьер* и по тегу *Курьер* настроена активация соответствующего профиля политики, то к этому устройству будет применяться не сама политика, созданная для группы *Пользователи*, а ее профиль. Профиль политики может разрешить на этом устройстве запуск отдельных программ, которые запрещено запускать в рамках политики.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов в свойствах устройства. Каждое правило назначения тегов можно включить или выключить. Если правило включено, оно применяется к устройствам, управляемым Сервером администрирования. Если правило не нужно, но может понадобиться в дальнейшем, то нет необходимости его удалять; достаточно снять флажок **Включить правило**. При этом правило выключается и не выполняется до тех пор, пока флажок **Включить правило** не будет установлен. Отключение правила без удаления может потребоваться, если это правило необходимо временно исключить из списка правил назначения тегов, а потом опять включить.

В этом разделе

Автоматическое назначение тегов устройствам	140
Просмотр и настройка тегов, назначенных устройству.....	142

Автоматическое назначение тегов устройствам

Вы можете создавать и изменять правила автоматического назначения тегов в окне свойств Сервера администрирования.

► *Чтобы автоматически назначить теги устройствам, выполните следующие действия:*

1. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется задать правила назначения тегов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Правила назначения тегов**.
4. В разделе **Правила назначения тегов** нажмите на кнопку **Добавить**.

Откроется окно **Новое правило**.

5. В окне **Новое правило** настройте общие свойства правила:

- Укажите имя правила.

Имя правила не может превышать 255 символов и содержать специальные символы (" * < > ? \ : |).

- Включите или выключите правило с помощью флажка **Включить правило**.

По умолчанию флажок **Включить правило** установлен.

- В поле **Тег** введите название тега.

Название тега не может превышать 255 символов и содержать специальные символы (" * < > ? \ : |).

6. В разделе **Условия** нажмите на кнопку **Добавить**, чтобы добавить новое условие, или нажмите на кнопку **Свойства**, чтобы изменить существующее условие.

Откроется окно мастера создания условия для правила автоматического назначения тегов.

7. В окне **Условия назначения тега** установите флажки для тех условий, которые должны влиять на назначения тега. Можно выбрать несколько условий.

8. В зависимости от того, какие условия назначения тега вы выбрали, мастер покажет окна для настройки соответствующих условий. Настройте срабатывание правила по следующим условиям:

- **Сеть** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену, к IP-диапазону).
- **Active Directory** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.
- **Программы** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
- **Виртуальные машины** – принадлежность устройства к разным типам виртуальных машин.
- **Реестр программ** – наличие на устройстве программ различных производителей.

9. После настройки условия введите название условия и завершите работу мастера.

При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий. Добавленные условия отображаются в разделе **Условия** окна свойств правила.

10. Нажмите на кнопку **ОК** в окне **Новое правило** и на кнопку **ОК** в окне свойств Сервера администрирования.

Созданные правила выполняются на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

Просмотр и настройка тегов, назначенных устройству

Вы можете просмотреть список всех тегов, назначенных устройству, а также перейти к настройке правил автоматического назначения тегов в окне свойств устройства.

► *Чтобы просмотреть и настроить назначенные устройству теги, выполните следующие действия:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В рабочей области папки **Управляемые устройства** выберите устройство, для которого вы хотите посмотреть назначенные теги.
3. В контекстном меню выбранного устройства выберите пункт **Свойства**.
4. В окне свойств устройства выберите раздел **Теги**.

Отобразится список тегов, назначенных выбранному устройству, а также способ назначения тега: вручную или по правилу.

5. При необходимости выполните одно из следующих действий:
 - Чтобы перейти к настройке правил назначения тегов, нажмите на ссылку **Настроить правила автоматического назначения тегов**.
 - Чтобы переименовать тег, выделите тег и нажмите на кнопку **Переименовать**.
 - Чтобы удалить тег, выделите тег и нажмите на кнопку **Удалить**.
 - Чтобы добавить тег вручную, введите тег в поле в нижней части раздела **Теги** и нажмите на кнопку **Добавить**.

6. Нажмите на кнопку **Применить**, если вы делали какие-либо изменения в разделе **Теги**, чтобы ваши изменения вступили в силу.

7. Нажмите на кнопку **ОК**.

Если вы удалили или переименовали тег в свойствах устройства, это изменение не распространится на правила назначения тегов, заданные в свойствах Сервера администрирования. Изменение будет применено только к тому устройству, в свойства которого вы внесли изменения.

Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center

Утилита удаленной диагностики Kaspersky Security Center (далее – утилита удаленной диагностики) предназначена для удаленного выполнения на клиентских устройствах следующих операций:

- включения и выключения трассировки, изменения уровня трассировки, загрузки файла трассировки;
- загрузки параметров программ;
- загрузки журналов событий;
- запуска диагностики и скачивания результатов диагностики;
- запуска и остановки программ.

Утилита удаленной диагностики автоматически устанавливается на устройство совместно с Консолью администрирования.

В этом разделе

Подключение утилиты удаленной диагностики к клиентскому устройству	144
Включение и выключение трассировки, загрузка файла трассировки.....	146
Загрузка параметров программ.....	147
Загрузка журналов событий.....	148
Запуск диагностики и загрузка ее результатов.....	148
Запуск, остановка и перезапуск программ.....	149

Подключение утилиты удаленной диагностики к клиентскому устройству

► Чтобы подключить утилиту удаленной диагностики к клиентскому устройству, выполните следующие действия:

1. В дереве консоли выберите любую группу администрирования.
2. В рабочей области на закладке **Устройства** в контекстном меню любого устройства выберите пункт **Внешние инструменты** → **Удаленная диагностика**.

В результате открывается главное окно утилиты удаленной диагностики.

3. В первом поле главного окна утилиты удаленной диагностики определите, какими средствами требуется подключиться к устройству:
 - **Доступ средствами сети Microsoft Windows.**
 - **Доступ средствами Сервера администрирования.**
4. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами сети Microsoft Windows**, выполните следующие действия:

- В поле **Устройство** укажите адрес устройства, к которому требуется подключиться.

В качестве адреса устройства можно использовать IP-адрес, NetBIOS- или DNS-имя.

По умолчанию указан адрес устройства, из контекстного меню которого запущена утилита.

- Укажите учетную запись для подключения к устройству:
 - **Подключиться от имени текущего пользователя** (выбрано по умолчанию). Подключение под учетной записью текущего пользователя.
 - **При подключении использовать предоставленное имя пользователя и пароль.** Подключение под указанной учетной записью. Укажите **Имя пользователя** и **Пароль** нужной учетной записи.

Подключение к устройству возможно только под учетной записью локального администратора устройства.

5. Если в первом поле вы выбрали вариант **Доступ средствами Сервера администрирования**, выполните следующие действия:

- В поле **Сервер администрирования** укажите адрес Сервера администрирования, с которого следует подключиться к устройству.

В качестве адреса Сервера можно использовать IP-адрес, NetBIOS- или DNS-имя.

По умолчанию указан адрес Сервера, с которого запущена утилита.

- Если требуется, установите флажки **Использовать SSL**, **Сжимать трафик** и **Устройство принадлежит подчиненному Серверу администрирования**.

Если установлен флажок **Устройство принадлежит подчиненному Серверу администрирования**, в поле **Подчиненный Сервер** вы можете выбрать подчиненный Сервер администрирования, под управлением которого находится устройство, нажав на кнопку **Обзор**.

6. Для подключения к устройству нажмите на кнопку **Войти**.

В результате откроется окно удаленной диагностики устройства (см. рис. ниже). В левой части окна расположены ссылки для выполнения операций по диагностике устройства. В правой части окна расположено дерево объектов устройства, с которыми может работать утилита. В нижней части окна отображается процесс выполнения операций утилиты.

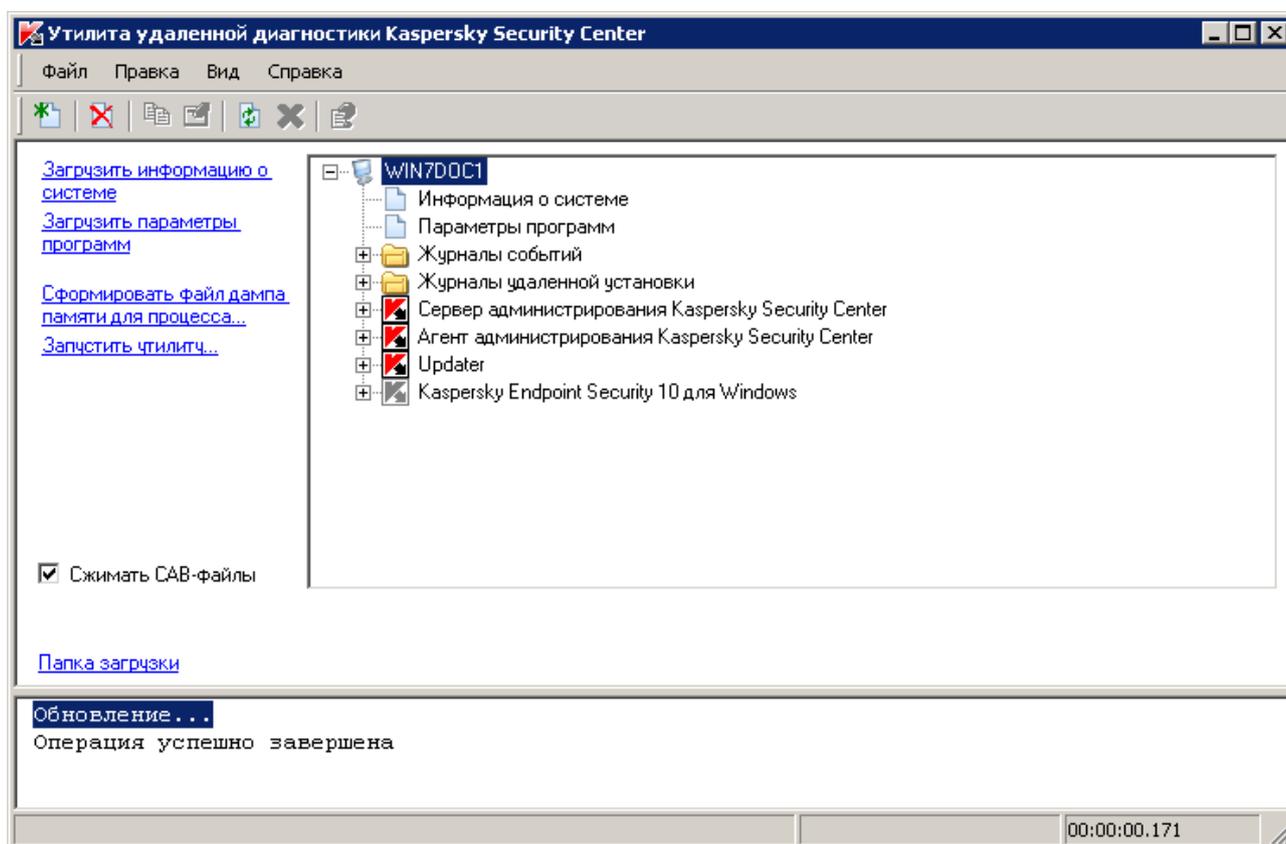


Рисунок 3. Утилита удаленной диагностики. Окно удаленной диагностики клиентского компьютера

Утилита удаленной диагностики сохраняет загруженные с устройств файлы на рабочем столе устройства, с которого она запущена.

Включение и выключение трассировки, загрузка файла трассировки

► Чтобы включить трассировку на удаленном устройстве, загрузить файл трассировки и выключить трассировку, выполните следующие действия:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству.

2. В дереве объектов устройства выберите программу, трассировку для которой требуется получить, и включите трассировку по ссылке **Включить трассировку** в левой части окна утилиты удаленной диагностики.

Включение и выключение трассировки у программ с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

В некоторых случаях для включения трассировки программы защиты требуется перезапустить эту программу и ее задачу.

3. В узле программы, для которой включена трассировка, в папке **Файлы трассировки** выберите нужный вам файл и скачайте его по ссылке **Скачать файл**. Для файлов большого объема есть возможность скачать только последние части трассировки.

Вы можете удалить выделенный файл трассировки. Удаление файла возможно после выключения трассировки.

4. Выключите трассировку для выбранной программы по ссылке **Выключить трассировку**.

Загрузка параметров программ

► Чтобы загрузить с удаленного устройства параметры программ, выполните следующие действия:

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству.
2. В дереве объектов окна удаленной диагностики устройства выберите верхний узел с именем устройства и в левой части окна выберите нужное вам действие:
 - **Загрузить информацию о системе.**
 - **Загрузить параметры программ.**
 - **Сформировать файл дампа для процесса.**

В окне, открывшемся по этой ссылке, укажите исполняемый файл выбранной программы, для которого нужно сформировать файл дампа памяти.

- **Запустить утилиту.**

В окне, открывшемся по этой ссылке, укажите исполняемый файл выбранной утилиты и параметры ее запуска.

В результате выбранная утилита будет загружена на устройство и запущена на нем.

Загрузка журналов событий

- ▶ *Чтобы загрузить с удаленного устройства журнал событий, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству.
2. В папке **Журналы событий** дерева объектов устройства выберите нужный вам журнал и загрузите его по ссылке **Загрузить журнал событий Kaspersky Event Log** в левой части окна утилиты удаленной диагностики.

Запуск диагностики и загрузка ее результатов

- ▶ *Чтобы запустить диагностику программы на удаленном устройстве и загрузить ее результаты, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству.
2. В дереве объектов устройства выберите нужную вам программу и запустите диагностику по ссылке **Выполнить диагностику**.

В результате в узле выбранной программы в дереве объектов появится отчет диагностики.

3. Выберите сформированный отчет диагностики в дереве объектов и скачайте его по ссылке **Скачать файл**.

Запуск, остановка и перезапуск программ

Запуск, остановка и перезапуск программ возможны только при подключении к устройству средствами Сервера администрирования.

► *Чтобы запустить, остановить или перезапустить программу, выполните следующие действия:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству.
2. В дереве объектов устройства выберите нужную вам программу и в левой части окна выберите действие:
 - **Остановить программу.**
 - **Перезапустить программу.**
 - **Запустить программу.**

В зависимости от выбранного вами действия программа будет запущена, остановлена или перезапущена.

Устройства с защитой на уровне UEFI

Устройство с защитой на уровне UEFI – это устройство с программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска программы защиты. Kaspersky Security Center поддерживает управление такими устройствами.

► *Чтобы изменить параметры подключения устройств с защитой на уровне UEFI, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Параметры подключения к Серверу** → **Дополнительные порты**.

4. В разделе **Дополнительные порты** измените необходимые вам параметры:

- **Открыть порт для устройств с защитой на уровне UEFI**

Если флажок установлен, то устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

По умолчанию флажок установлен.

- **Порт для устройств с защитой на уровне UEFI**

Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию используется порт 13294.

5. Нажмите на кнопку **ОК**.

Параметры управляемого устройства

Общие

Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:

- **Имя**

В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.

- **Описание**

В поле можно ввести дополнительное описание клиентского устройства.

- **Windows-домен**

Windows-домен или рабочая группа, в которую входит устройство.

- **NetBIOS-имя**

Имя клиентского устройства в сети Windows.

- **DNS-имя**

Имя DNS-домена устройства.

- **IP-адрес**

IP-адрес устройства.

- **Группа**

Группа администрирования, в состав которой входит клиентское устройство.

- **Последнее обновление**

Дата последнего обновления баз или программ на устройстве.

- **Видим в сети**

Дата и время, когда устройство последний раз было видимо в сети.

- **Соединение с Сервером**

Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

- **Не разрывать соединение с Сервером администрирования**

Если флажок установлен, поддерживается непрерывное соединение между Сервером администрирования и клиентским устройством.

Если флажок снят, клиентское устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

По умолчанию флажок установлен, если на устройстве установлен Сервер администрирования.

Если на устройстве установлен только Агент администрирования, по умолчанию флажок снят.

Защита

В разделе **Защита** представлена информация о состоянии антивирусной защиты на клиентском устройстве:

- **Статус устройства**

Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на устройстве и активности устройства в сети.

- **Статус постоянной защиты**

Статус текущего состояния постоянной защиты клиентского устройства.

- **Последняя проверка по требованию**

Дата и время последнего поиска вирусов на клиентском устройстве.

- **Обнаружено вирусов**

Общее количество обнаруженных на клиентском устройстве вирусов (счетчик обнаруженных вирусов) со времени установки программы защиты (первой проверки устройства), либо со времени последнего обнуления значения этой величины.

- **Необработанных файлов**

Количество необработанных файлов на клиентском устройстве.

В поле не учитывается количество необработанных файлов для мобильных устройств.

Программы

В разделе **Программы** отображается список программ "Лаборатории Касперского", установленных на клиентском устройстве.

- **События**

При нажатии на кнопку можно просмотреть список событий,

произошедших на клиентском устройстве при работе программы, а также результаты выполнения задач для этой программы.

- **Статистика**

При нажатии на кнопку можно просмотреть текущую статистическую информацию о работе программы.

- **Свойства**

При нажатии на кнопку можно получить информацию о программе и выполнить настройку программы.

Задачи

В разделе **Задачи** можно управлять задачами клиентского устройства: просматривать список существующих, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры, просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. В случае отсутствия связи статус не отображается.

События

В разделе **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

Теги

В разделе **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые и переименовывать старые теги, удалять теги.

Информация о системе

В разделе **Общая информация о системе** представлена информация о программе, установленной на клиентском устройстве.

Реестр программ

В разделе **Реестр программ** можно просмотреть реестр установленных на клиентском устройстве программ и обновлений для них, а также настроить отображение реестра программ.

Информация об установленных программах предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**.

Агент администрирования предоставляет информацию о программах на основе данных системного реестра.

- **Показывать только несовместимые программы безопасности**

Если флажок установлен, в списке программ отображаются только те программы безопасности, которые несовместимы с программами "Лаборатории Касперского".

По умолчанию флажок снят.

- **Показывать обновления**

Если флажок установлен, в списке программ отображаются не только программы, но и установленные для них пакеты обновлений.

По умолчанию флажок снят.

Исполняемые файлы

В разделе **Исполняемые файлы** отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

Реестр оборудования

В этом разделе можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

Сеансы

В разделе **Сеансы** представлена информация о владельце клиентского устройства, а также об учетных записях пользователей, которые работали с выбранным клиентским устройством.

Информация о доменных пользователях формируется на основе данных Active Directory. Информация о локальных пользователях предоставляется Диспетчером учетных записей безопасности (Security Account Manager), установленным на клиентском устройстве.

- **Владелец устройства**

В поле **Владелец устройства** отображается имя пользователя, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с клиентским устройством.

По кнопкам **Назначить** и **Свойства** можно выбрать владельца устройства и просмотреть информацию о пользователе, назначенном владельцем устройства.

По кнопке с красным крестом можно удалить текущего владельца устройства.

В списке содержатся учетные записи пользователей, которые работают с клиентским устройством.

- **Имя**

Имя устройства в сети.

- **Имя участника**

Имя пользователя (доменное или локальное), который выполнил вход в систему на этом устройстве.

- **Учетная запись**

Учетная запись пользователя, который выполнил вход в систему на этом устройстве.

- **Электронная почта**

Адрес электронной почты пользователя.

- **Телефон**

Номер телефона пользователя.

Инциденты

В разделе **Инциденты** можно просматривать, редактировать и создавать инциденты для клиентского устройства. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные программы с личного съемного диска, администратор может создать по этому поводу инцидент. В тексте инцидента администратор может кратко описать ситуацию и рекомендуемые действия, например, административные меры в отношении пользователя, а также добавить ссылку на пользователя.

Инцидент, для которого выполнены необходимые действия, называется обработанным. Наличие необработанных инцидентов может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список инцидентов, созданных для устройства. Инциденты классифицируются по уровню важности и типу. Тип инцидента определяется программой "Лаборатории Касперского", которая создает инцидент. Обработанные инциденты можно отметить в списке, установив флажок в графе **Обработан**.

Уязвимости в программах

В разделе **Уязвимости в программах** можно просмотреть список с информацией об уязвимостях сторонних программ, установленных на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке уязвимости по имени уязвимости.

- **Экспортировать в файл**

По кнопке **Экспортировать в файл** вы можете сохранить список уязвимостей в файле. По умолчанию программа экспортирует список уязвимостей в файл формата CSV.

- **Показывать только те уязвимости, которые можно закрыть**

Если флажок установлен, в разделе отображаются уязвимости, которые можно закрыть патчем.

Если флажок снят, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

По умолчанию флажок установлен.

Неустановленные обновления

В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Показывать установленные обновления**

Если флажок установлен, в списке обновлений отображаются и не установленные обновления, и обновления, которые уже установлены на клиентском устройстве.

По умолчанию флажок снят.

Действующие профили политик

- **Список профилей политик**

В списке можно просмотреть информацию о действующих профилях политики, которые активны на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке действующие профили политик по имени политики или по имени профиля политики.

- **Экспортировать в файл**

По кнопке **Экспортировать в файл** вы можете сохранить список активных профилей политики в файле. По умолчанию программа экспортирует список профилей политики в файл формата CSV.

Агенты обновлений

В этом разделе представлен список агентов обновлений, с которыми взаимодействует устройство.

- **Экспортировать в файл**

По кнопке **Экспортировать в файл** вы можете сохранить в файле список агентов обновлений, с которыми взаимодействует устройство. По умолчанию программа экспортирует список устройств в файл формата CSV.

Свойства По кнопке **Свойства** вы можете посмотреть и настроить параметры агента обновлений, с которым взаимодействует устройство.

См. также

| Настройка общих параметров Сервера администрирования..... [40](#)

Параметры политики Агента администрирования

► *Чтобы настроить параметры политики Агента администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки выберите политику Агента администрирования.
3. В контекстном меню политики выберите пункт **Свойства**.

Откроется окно свойств политики Агента администрирования.

Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики.

В блоке **Состояние политики** можно выбрать один из вариантов действия политики:

- **Активная политика**

Если выбран этот вариант, политика становится активной.

По умолчанию выбран этот вариант.

- **Политика для автономных пользователей**

Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. Политика для автономных пользователей доступна только для Антивируса Касперского для Windows Workstations версии 6.0 MP3 и выше.

- **Неактивная политика**

Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

В блоке **Наследование параметров** можно настроить параметры наследования политики:

- **Наследовать параметры из политики верхнего уровня**

Если флажок установлен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

По умолчанию флажок установлен.

- **Форсировать наследование параметров дочерними политиками**

Если флажок установлен, после применения изменений в политике будут выполнены следующие действия:

- значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
- в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически установлен флажок **Наследовать параметры политики верхнего уровня**.

Когда флажок установлен, значения параметров дочерних политик недоступны для изменения.

По умолчанию флажок снят.

Настройка событий

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

В списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке.

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Передавать файлы только через агенты обновлений**

Если флажок установлен, клиентские устройства получают обновления только через агенты обновлений, а не напрямую с серверов обновлений.

Если флажок снят, клиентские устройства могут получать обновления из разных источников: напрямую с серверов обновлений, от главного Сервера администрирования, из локальной или сетевой папки.

По умолчанию флажок снят.

- **Включить NAP**

Если флажок установлен, для проверки работоспособности системы клиентского устройства используется Kaspersky Security Center SHV (SHV). Флажок доступен, если на устройстве установлена программа Kaspersky Security Center SHV.

По умолчанию флажок снят.

- **Максимальный размер очереди событий (МБ)**

В поле можно указать максимальное место на диске, которое может

занимать очередь событий.

По умолчанию указано значение 2 МБ.

- **Использовать пароль деинсталляции**

Если флажок установлен, при нажатии на кнопку **Изменить** можно указать пароль для задачи удаленной деинсталляции Агента администрирования.

По умолчанию флажок снят.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, параметры недоступны для изменения.

- **Информация об установленных программах**

Если флажок установлен, на Сервер администрирования отправляется информация о программах, установленных на клиентских устройствах.

По умолчанию флажок установлен.

- **Информация об обновлениях Microsoft Windows**

Если флажок установлен, на Сервер администрирования отправляется информация об обновлениях Microsoft Windows, которые необходимо установить на клиентских устройствах.

По умолчанию флажок установлен.

- **Информация об уязвимостях ПО**

Если флажок установлен, на Сервер администрирования отправляется информация об уязвимостях программного обеспечения, обнаруженных на клиентских устройствах.

По умолчанию флажок установлен.

- **Информация о реестре оборудования**

Обновления и уязвимости в программах

В разделе **Обновления и уязвимости в программах** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей:

- **Использовать Сервер администрирования в роли WSUS-сервера**

Если флажок установлен, обновления Windows загружаются на Сервер администрирования. Загруженные обновления Сервер администрирования централизованно предоставляет службам Windows Update на клиентских устройствах с помощью Агентов администрирования.

Если флажок снят, Сервер администрирования не используется для загрузки обновлений Windows. В этом случае клиентские устройства получают обновления Windows самостоятельно.

По умолчанию флажок снят.

В блоке параметров **Режим поиска обновлений Windows Update** можно выбрать режим поиска обновлений:

- **Активный**

Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от агента обновлений Windows.

По умолчанию выбран этот вариант.

- **Пассивный**

Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента

обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

- **Выключен**

Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

Если флажок установлен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

По умолчанию флажок установлен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если в ходе работы, установки или удаления программы требуется перезагрузка операционной системы:

- **Не перезагружать операционную систему**

Перезагрузка операционной системы не выполняется.

Этот вариант выбран по умолчанию.

- **При необходимости перезагрузить операционную систему автоматически**

При необходимости перезагрузка операционной системы выполняется автоматически.

- **Запрашивать у пользователя**

Программа запрашивает у пользователя разрешение перезагрузить операционную систему.

- **Повторять запрос периодически через (мин)**

Если флажок установлен, программа запрашивает у пользователя разрешение на перезагрузку операционной системы с

периодичностью, указанной в поле рядом с флажком. По умолчанию периодичность повторных запросов составляет 5 минут.

Если флажок снят, программа не запрашивает разрешение на перезагрузку повторно.

По умолчанию флажок установлен.

- **Принудительно перезагружать через (мин)**

Если флажок установлен, после запроса у пользователя операционная система перезагружается принудительно по истечении времени, указанного в поле рядом с флажком.

Если флажок снят, принудительная перезагрузка не выполняется.

По умолчанию флажок снят.

- **Принудительно закрывать программы в заблокированных сессиях через (мин)**

Принудительное завершение работы программ, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

Если флажок установлен, работа программ на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

Если флажок снят, работа программ на заблокированном устройстве не прекращается.

По умолчанию флажок снят.

Общий доступ к рабочему столу

В разделе **Общий доступ к рабочему столу** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу:

- **Включить аудит**

Если флажок установлен, аудит действий администратора на удаленном устройстве включен. Записи о действиях администратора на удаленном устройстве сохраняются:

- в журнале событий на удаленном устройстве;
- в файле с расширением syslog, который находится в папке установки Агента администрирования на удаленном устройстве;
- в базе событий Kaspersky Security Center.

Аудит действий администратора доступен при выполнении следующих условий:

- есть в наличии действующая лицензия на Системное администрирование;
- у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

Если флажок снят, аудит действий администратора на удаленном устройстве выключен.

По умолчанию флажок снят.

- **Маски файлов, чтение которых нужно отслеживать**

В списке содержатся маски файлов. Когда аудит включен, программа отслеживает чтение администратором файлов, соответствующих маскам, и сохраняет информацию о чтении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Маски файлов, изменение которых нужно отслеживать**

В списке содержатся маски файлов на удаленном устройстве. Когда аудит включен, программа отслеживает изменение администратором файлов, соответствующих маскам, и сохраняет информацию об изменении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx,

*.xlsx, *.odt, *.pdf.

Управление патчами и обновлениями

В разделе **Управление патчами и обновлениями** можно настроить получение и распространение обновлений и установку патчей на управляемые устройства.

- **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center 10 со статусом "Не определено"**

Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Автоматическая установка патчей со статусом *Не определено* доступна для версий Kaspersky Security Center Service Pack 2 и выше.

Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того как администратор изменит их статус на *Одобрен*.

По умолчанию флажок установлен.

- **Загружать обновления и антивирусные базы с Сервера администрирования заранее**

Если флажок установлен, включена офлайн-модель получения обновлений. В этом случае, когда Сервер администрирования получает обновления, он оповещает Агенты администрирования о том, какие обновления потребуются для программ на клиентских устройствах. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загружает все обновления, обновления становятся доступными для программ на клиентском устройстве.

Когда управляемая программа на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть

ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемой программы, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемой программе обновления из локального кеша. Соединение с Сервером администрирования при этом может отсутствовать, но оно и не требуется для обновления.

Если флажок снят, офлайн-модель получения обновлений выключена. Обновления распределяются по расписанию задачи обновления.

По умолчанию флажок установлен.

Сеть

Раздел **Сеть** включает три вложенных раздела:

- **Сеть,**
- **Подключение,**
- **Менеджер соединений.**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

В блоке **Подключение к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования.

- **Сжимать сетевой трафик**

Если флажок установлен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

Нагрузка на центральный процессор клиентского компьютера может возрасти.

По умолчанию флажок установлен.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

Если флажок установлен, UDP-порт, необходимый для работы Агента администрирования, будет добавлен в список исключений сетевого экрана Microsoft Windows.

По умолчанию флажок установлен.

- **Использовать SSL-соединение**

Если флажок установлен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

По умолчанию флажок установлен.

- **Использовать шлюз соединений агента обновлений (при наличии) в параметрах подключения по умолчанию**

Если флажок установлен, то используется шлюз соединений агента обновлений, параметры которого заданы в свойствах группы администрирования.

По умолчанию флажок установлен.

В блоке **Порт Агента администрирования** можно разрешить подключение Сервера администрирования к клиентским устройствам через UDP-порт и указать номер порта.

- **Использовать UDP-порт**

Если флажок установлен, соединение клиентского устройства с Сервером администрирования будет устанавливаться через UDP-порт.

По умолчанию флажок установлен.

- **Номер UDP-порта**

В поле можно ввести номер UDP-порта. По умолчанию используется порт 15000.

Используется десятичная форма записи.

Если клиентское устройство работает под управлением операционной системы Windows XP Service Pack 2, встроенный межсетевой экран блокирует UDP-порт с номером 15000. Этот порт требуется открыть вручную.

В разделе **Подключение** можно задать параметры сетевого местоположения, настроить профили подключения к Серверу администрирования, включить автономный режим, когда Сервер администрирования недоступен.

- **Параметры сетевого местоположения**

Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

- подключении клиентского устройства к другой локальной сети;
- отключении устройства от локальной сети организации;
- изменении адреса шлюза соединения или изменении адреса DNS-сервера.

- **Включить автономный режим, когда Сервер администрирования недоступен**

Если флажок установлен, при подключении через этот профиль программы, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. раздел "Автономные пользователи" на стр. [52](#)). В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

Если флажок снят, программы будут использовать активные политики.

По умолчанию флажок снят.

В разделе **Менеджер соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

Этот вариант выбран по умолчанию.

- **Подключаться в указанные периоды**

Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Агенты обновлений

В блоке **Опрос сети** можно включить автоматический опрос сети и настроить периодичность опроса.

- **Разрешить опрос сети**

Если флажок установлен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить период быстрого опроса** и **Настроить период полного опроса**.

Если флажок снят, Сервер администрирования не выполняет опрос сети.

Периодичность опроса сети для версий Агента администрирования версий ниже 10.2 можно настроить в полях **Период запроса информации с доменов, мин** и **Период опроса компьютерной сети, мин**. Поля доступны, если флажок установлен.

По умолчанию флажок установлен.

В блоке **Опрос IP-подсети** можно включить автоматический опрос IP-диапазонов и настроить периодичность опроса.

- **Разрешить опрос IP-диапазонов**

Если флажок установлен, Сервер администрирования автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

Если флажок снят, Сервер администрирования не выполняет опрос IP-диапазонов.

Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если флажок установлен.

По умолчанию флажок снят.

В блоке **Опрос Active Directory** можно включить автоматический опрос сети в соответствии со структурой Active Directory и настроить периодичность опроса.

- **Разрешить опрос Active Directory**

Если флажок установлен, Сервер администрирования автоматически выполняет опрос Active Directory в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

Если флажок снят, Сервер администрирования не выполняет опрос Active Directory.

Периодичность опроса Active Directory для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если флажок установлен.

По умолчанию флажок установлен.

Параметры подключения к интернету

В разделе **Параметры подключения к интернету** можно настроить параметры доступа к сети интернет:

- **Использовать прокси сервер**

Если флажок установлен, в полях ввода можно настроить параметры подключения к прокси-серверу.

По умолчанию флажок снят.

- **Адрес**

Адрес прокси-сервера.

- **Номер порта**

Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

Если флажок установлен, то при подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

По умолчанию флажок снят.

- **Авторизация на прокси-сервере**

Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

По умолчанию флажок снят.

- **Имя пользователя**

Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

История ревизий

В этом разделе можно посмотреть историю ревизий Агента администрирования (см. раздел "Работа с ревизиями объектов" на стр. [225](#)). Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Управление учетными записями пользователей

Этот раздел содержит информацию об учетных записях пользователей управляемых устройств и учетных записях внутренних пользователей Kaspersky Security Center (администраторов, управляющих устройствами пользователей). В разделе приведены инструкции по созданию учетных записей и ролей пользователей Kaspersky Security Center. Раздел также содержит инструкции по работе со списками сертификатов и мобильных устройств пользователя, по рассылке сообщений пользователям.

В этом разделе

Работа с учетными записями пользователей.....	174
Добавление учетной записи пользователя.....	175
Настройка проверки уникальности имени внутреннего пользователя.....	176
Добавление группы пользователей	178
Добавление пользователя в группу	179
Назначение пользователя владельцем устройства.....	179
Рассылка сообщений пользователям	180
Просмотр списка мобильных устройств пользователя	181
Установка сертификата пользователю	182
Просмотр списка сертификатов, выписанных пользователю	183
Об администраторе виртуального Сервера	183

Работа с учетными записями пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Программа поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей (см. раздел "Работа с внутренними пользователями" на стр. [44](#)). Учетные записи внутренних пользователей создаются (см. раздел "Добавление учетной записи пользователя" на стр. [175](#)) и используются только внутри Kaspersky Security Center.

Все учетные записи пользователей можно просмотреть в папке **Учетные записи пользователей** в дереве консоли. Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

Вы можете выполнять с учетными записями пользователей и группами учетных записей следующие действия:

- настраивать права доступа пользователей к функциям программы с помощью ролей (см. раздел "Настройка прав. Роли пользователей" на стр. [20](#));
- рассылать сообщения пользователям с помощью электронной почты и SMS (см. раздел "Рассылка сообщений пользователям" на стр. [180](#));
- просматривать список мобильных устройств пользователя (см. раздел "Просмотр списка мобильных устройств пользователя" на стр. [181](#));
- выписывать и устанавливать сертификаты на мобильные устройства пользователя (см. раздел "Установка сертификата пользователю" на стр. [182](#));
- просматривать список сертификатов, выписанных пользователю (см. раздел "Просмотр списка сертификатов, выписанных пользователю" на стр. [183](#)).

Добавление учетной записи пользователя

► Чтобы добавить новую учетную запись пользователя Kaspersky Security Center, выполните следующие действия:

1. В дереве консоли откройте папку **Учетные записи пользователей**.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В рабочей области по кнопке **Добавить пользователя** откройте окно **Свойства**.

3. В окне **Свойства** укажите:

- **Основная электронная почта.** Администратор может указать вручную основной адрес электронной почты внутреннего пользователя. Для учетных записей, загруженных из Active Directory, основной адрес электронной почты изменить нельзя.
- **Основной телефон.** Администратор может указать вручную основной номер телефона внутреннего пользователя. Для учетных записей, загруженных из Active Directory, основной номер телефона изменить нельзя.
- Параметры учетной записи и пароль для подключения пользователя к Kaspersky Security Center.

Пароль должен содержать латинские буквы в верхнем и нижнем регистре, цифры или спецсимволы (@#\$%^&*~_!+=[\]|\\:'.?/~()\"). Длина пароля должна быть не меньше 8 и не больше 16 символов.

Пароль не должен содержать последовательность символов .@.

После того как вы начали вводить пароль, отображается кнопка **Показать пароль**. Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать пароль** и удерживайте ее необходимое вам время.

Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Количество попыток ввода пароля можно изменить в реестре с помощью ключа SrvSpIPpcLogonAttempts.

Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. Администратор может разблокировать учетную запись, только сменив пароль.

Если установить флажок **Отключить учетную запись**, внутренний пользователь (например, пользователь с правами администратора или оператора), не сможет подключиться к программе. Вы можете установить флажок, например, в случае увольнения сотрудника. По умолчанию флажок снят.

4. Нажмите на кнопку **ОК**.

Созданная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

Настройка проверки уникальности имени внутреннего пользователя

Вы можете настроить проверку уникальности имени внутреннего пользователя Kaspersky Security Center при его добавлении в программу. Проверка на уникальность имени внутреннего пользователя может выполняться только на виртуальном Сервере или главном Сервере, для которого создается учетная запись пользователя, или на всех виртуальных Серверах и главном Сервере. По умолчанию проверка на уникальность имени внутреннего пользователя выполняется на всех виртуальных Серверах и на главном Сервере администрирования.

► *Чтобы включить проверку уникальности имени внутреннего пользователя в рамках виртуального Сервера или главного Севера, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.

2. Перейдите в раздел:

- для 64-разрядной системы:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34
\.core\independent\KLLIM

- для 32-разрядной системы:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\independ
ent\KLLIM

3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000001.

По умолчанию для этого ключа указано значение 0.

4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена только на том виртуальном Сервере, на котором был создан внутренний пользователь, или на главном Сервере, если пользователь был создан на главном Сервере.

► *Чтобы включить проверку уникальности имени внутреннего пользователя на всех виртуальных Серверах и главном Сервере, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.

2. Перейдите в раздел:

- для 64-разрядной системы:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34
\.core\independent\KLLIM

- для 32-разрядной системы:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\independ
ent\KLLIM

3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000000.

По умолчанию для этого ключа указано значение 0.

4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена на всех виртуальных Серверах и на главном Сервере администрирования.

Добавление группы пользователей

Вы можете добавлять группы пользователей, гибко настраивать состав групп и доступ группы пользователей к разным функциям программы. Группам пользователей можно давать названия, соответствующие их назначению. Например, название может соответствовать расположению пользователей в офисе или названию структурного подразделения компании, к которому относятся пользователи.

Один пользователь может входить в состав нескольких групп пользователей. Учетная запись пользователя под управлением виртуального Сервера администрирования может входить только в группы пользователей этого виртуального Сервера и иметь права доступа только в рамках этого виртуального Сервера.

► *Чтобы добавить группу пользователей, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Добавить группу безопасности**.

Откроется окно **Новая группа безопасности**.

3. В окне **Новая группа безопасности** в разделе **Общие** укажите имя группы.

Имя группы не может превышать 255 символов и не может содержать символы *, <, >, ?, \, :, |. Имя группы должно быть уникальным.

Вы можете ввести описание группы в поле ввода **Описание**. Заполнение поля **Описание** не является обязательным.

4. Нажмите на кнопку **ОК**.

Добавленная группа пользователей отобразится в папке **Учетные записи пользователей** в дереве консоли. Вы можете добавить пользователей (см. раздел "Добавление пользователя в группу" на стр. [179](#)) в созданную группу.

Добавление пользователя в группу

► *Чтобы добавить пользователя в группу, выполните следующие действия:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В списке учетных записей пользователей и групп выберите группу, в которую нужно добавить пользователя.

3. В контекстном меню группы выберите пункт **Свойства**.

4. В окне свойств группы выберите раздел **Пользователи группы**, затем нажмите на кнопку **Добавить**.

В результате откроется окно со списком пользователей.

5. В списке выберите пользователя или пользователей, которых нужно включить в состав группы.

6. Нажмите на кнопку **ОК**.

В результате пользователь или пользователи будут включены в состав группы.

Назначение пользователя владельцем устройства

Вы можете назначить пользователя владельцем устройства, чтобы "закрепить" устройство за этим пользователем. При необходимости выполнить какие-либо действия с устройством

(например, обновить аппаратное обеспечение) администратор может проинформировать владельца устройства и согласовать действия с ним.

► *Чтобы назначить пользователя владельцем устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки на закладке **Устройства** выберите устройство, для которого нужно назначить владельца.
3. В контекстном меню устройства выберите пункт **Свойства**.
4. В окне свойств устройства выберите раздел **Информация о системе** → **Сеансы**.
5. Нажмите на кнопку **Назначить** рядом с полем **Владелец устройства**.
6. В окне **Выбор пользователя** выберите пользователя, которого нужно назначить владельцем устройства и нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК**.

В результате владелец устройства будет назначен. По умолчанию поле **Владелец устройства** заполнено значением из Active Directory и обновляется при каждом опросе Active Directory (см. раздел "Просмотр и изменение параметров опроса групп Active Directory" на стр. [236](#)). Вы можете просмотреть список владельцев устройств в отчете **Отчет о владельцах устройств**. Отчет можно создать с помощью мастера создания отчетов (см. раздел "Создание шаблона отчета" на стр. [185](#)).

Рассылка сообщений пользователям

► *Чтобы отправить сообщение пользователю по электронной почте, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню пользователя выберите **Отправить сообщение по электронной почте**.
3. Заполните необходимые поля в окне **Сообщение для пользователя** и нажмите на кнопку **ОК**.

В результате сообщение будет отправлено на электронную почту, указанную в свойствах пользователя.

► *Чтобы отправить SMS-сообщение пользователю, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.
2. В контекстном меню пользователя выберите **Отправить SMS-сообщение**.
3. Заполните необходимые поля в окне **Текст SMS** и нажмите на кнопку **ОК**.

В результате сообщение будет отправлено на мобильное устройство, номер которого указан в свойствах пользователя.

Просмотр списка мобильных устройств пользователя

► *Чтобы просмотреть список мобильных устройств пользователя, выполните следующие действия:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.
3. В окне свойств учетной записи пользователя выберите раздел **Мобильные устройства**.

В разделе **Мобильные устройства** можно просмотреть список мобильных устройств пользователя и информацию о мобильных устройствах. По кнопке **Экспортировать в файл** можно сохранить список мобильных устройств в файле.

Установка сертификата пользователю

Вы можете установить пользователю сертификаты трех типов:

- общий сертификат, необходим для идентификации мобильного устройства пользователя;
- почтовый сертификат, необходим для настройки корпоративной почты на мобильном устройстве пользователя;
- VPN сертификат, необходим для настройки виртуальной частной сети на мобильном устройстве пользователя.

► *Чтобы выписать сертификат пользователю и установить его, выполните следующие действия:*

1. В дереве консоли откройте папку **Учетные записи пользователей** и выберите учетную запись пользователя.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

Будет запущен мастер установки сертификата. Следуйте его указаниям.

В результате работы мастера установки сертификата сертификат будет создан и установлен пользователю. Список установленных сертификатов пользователя можно просмотреть и экспортировать в файл (см. раздел "Просмотр списка сертификатов, выписанных пользователю" на стр. [183](#)).

Просмотр списка сертификатов, выписанных пользователю

► Чтобы просмотреть список всех сертификатов, выписанных пользователю, выполните следующие действия:

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.

3. В окне свойств учетной записи пользователя выберите раздел **Сертификаты**.

В разделе **Сертификаты** можно просмотреть список сертификатов пользователя и информацию о сертификатах. По кнопке **Экспортировать в файл** можно сохранить список сертификатов в файле.

Об администраторе виртуального Сервера

При необходимости можно создать несколько учетных записей администраторов виртуального Сервера.

Администратор виртуального Сервера администрирования является внутренним пользователем Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Работа с отчетами, статистикой и уведомлениями

В этом разделе представлена информация о работе с отчетами, статистикой и выборками событий и устройств в Kaspersky Security Center, а также о настройке параметров уведомлений Сервера администрирования.

В этом разделе

Работа с отчетами.....	184
Работа со статистической информацией.....	196
Настройка параметров уведомлений о событиях	197
Создание сертификата для SMTP-сервера.....	199
Выборки событий	200
Настройка экспорта событий в SIEM-систему	203
Выборки устройств.....	205
Политики.....	224
Задачи.....	225

Работа с отчетами

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования. Вы можете создавать отчеты для следующих объектов:

- для выборок устройств, созданных по определенным параметрам;

- для групп администрирования;
- для наборов устройств из разных групп администрирования;
- для всех устройств в сети (в отчете о развертывании).

В программе есть набор стандартных шаблонов отчетов. Предусмотрена также возможность создавать пользовательские шаблоны отчетов. Отчеты отображаются в главном окне программы, в папке дерева консоли **Сервер администрирования**.

В этом разделе

Создание шаблона отчета	185
Создание и просмотр отчета	186
Сохранение отчета.....	186
Создание задачи рассылки отчета.....	187

Создание шаблона отчета

► *Чтобы создать шаблон отчета, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Нажмите на кнопку **Создать шаблон отчета**.

В результате запустится мастер создания шаблона отчета. Следуйте его указаниям.

После окончания работы мастера сформированный шаблон отчета будет добавлен в состав выбранной папки **Сервер администрирования** дерева консоли. Этот шаблон можно использовать для создания и просмотра отчетов.

Создание и просмотр отчета

► *Чтобы сформировать и просмотреть отчет, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.

В результате в рабочей области отображается отчет, сформированный по выбранному шаблону.

В отчете отображаются следующие данные:

- тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
- графическая диаграмма с наиболее характерными данными отчета;
- сводная таблица с вычисляемыми показателями отчета;
- таблица с детальными данными отчета.

Сохранение отчета

► *Чтобы сохранить сформированный отчет, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Сохранить**.

В результате запустится мастер сохранения отчета. Следуйте его указаниям.

После завершения работы мастера откроется папка, в которую вы сохранили файл отчета.

Создание задачи рассылки отчета

Отчеты можно рассылать по электронной почте. Рассылка отчетов в Kaspersky Security Center осуществляется с помощью задачи рассылки отчета.

► *Чтобы создать задачу рассылки одного отчета, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке отчетов.
4. В контекстном меню шаблона отчета выберите пункт **Рассылка отчетов**.

В результате запускается мастер создания задачи рассылки выбранного отчета. Следуйте его указаниям.

► *Чтобы создать задачу рассылки нескольких отчетов, выполните следующие действия:*

1. В дереве консоли в узле с именем нужного вам Сервера администрирования выберите папку **Задачи**.
2. В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

В результате запускается мастер создания задачи. Следуйте его указаниям.

Созданная задача рассылки отчета отображается в папке дерева консоли **Задачи**.

Задача рассылки отчета создается автоматически в случае, если при установке Kaspersky Security Center были заданы параметры электронной почты.

В этом разделе

Шаг 1. Выбор типа задачи.....	188
Шаг 2. Выбор типа отчета.....	188
Шаг 3. Действия с отчетом.....	188
Шаг 4. Выбор учетной записи для запуска задачи	190
Шаг 5. Настройка расписания задачи	190
Шаг 6. Определение названия задачи	195
Шаг 7. Завершение создания задачи	196

Шаг 1. Выбор типа задачи

В окне **Выбор типа задачи** в списке задач выберите тип задачи **Рассылка отчета**.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 2. Выбор типа отчета

В окне **Выбор типа отчета** в списке шаблонов для создания задачи выберите тип отчета.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 3. Действия с отчетом

В окне **Действия с отчетом** настройте следующие параметры:

- **Посылать отчет по электронной почте**

Если флажок установлен, программа отправляет сформированные отчеты по электронной почте.

Параметры отправки отчета по электронной почте можно настроить по

ссылке **Параметры отправки по электронной почте**. Ссылка доступна, когда флажок установлен.

Если флажок снят, программа сохраняет отчеты в указанной папке для хранения отчетов.

По умолчанию флажок снят.

- **Сохранять отчет в папке**

Если флажок установлен, программа сохраняет отчеты в папке, указанной в поле под флажком. Чтобы сохранять отчеты в папке общего доступа, укажите UNC-путь к этой папке. В таком случае в окне **Выбор учетной записи для запуска задачи** необходимо задать учетную запись и пароль пользователя для доступа к этой папке.

Если флажок снят, программа не сохраняет отчеты в папке, а отправляет их по электронной почте.

По умолчанию флажок снят.

- **Замещать предыдущие отчеты того же типа**

Если флажок установлен, при каждом запуске задачи новый файл отчета замещает в папке для хранения отчетов файл, сохраненный при предыдущем запуске задачи.

Если флажок снят, файлы отчетов не перезаписываются. При каждом запуске задачи в папке сохраняется отдельный файл отчета.

Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

По умолчанию флажок снят.

- **Задать учетную запись для доступа к папке**

Если флажок установлен, можно указать учетную запись, от имени которой отчет записывается в папку. Если в окне **Действия с отчетом** в качестве параметра **Сохранять отчет в папке** указан UNC-путь к папке общего доступа, необходимо указать учетную запись и пароль для доступа к этой папке.

Если флажок снят, отчет записывается в папку от имени учетной записи Сервера администрирования.

Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

По умолчанию флажок снят.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 4. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Автоматически созданная учетная запись**

Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись:**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

- **Учетная запись**

Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 5. Настройка расписания задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрываемом списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждый N час**, под раскрываемым списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждые N минут**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрываемым списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрываемым списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Один раз**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Один раз**, под раскрываемым списком отображаются поля **Дата запуска** и **Время запуска**. В поле **Дата запуска** можно указать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Значения этих полей проставляются автоматически и соответствуют текущим системной дате и времени устройства.

- **Вручную**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна программы Kaspersky Security Center при помощи команды **Запустить**

контекстного меню или аналогичного пункта в меню **Действие**.

- **После обновления программы**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **После обновления программы**, задача будет запускаться после каждого обновления программы "Лаборатории Касперского", установленной на клиентском устройстве.

- **При запуске программы**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При запуске программы**, задача будет запускаться при запуске программы "Лаборатории Касперского". В поле ввода **Задержка запуска задачи (мин)** можно указать время, которое должно пройти с момента запуска программы до начала выполнения задачи.

- **При загрузке обновлений в хранилище**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При загрузке обновлений в хранилище**, задача будет запускаться после загрузки обновлений в хранилище.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать программы, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.
- **Запускать пропущенные задачи** (по умолчанию флажок снят)

Если флажок установлен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Автоматически определять интервал для распределения запуска задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при

создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка программы, Исправление уязвимостей).

Распределять запуск задачи случайным образом в интервале (мин)

Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка программы, Исправление уязвимостей).

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 6. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?:\|).

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Шаг 7. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Работа со статистической информацией

Статистическая информация о состоянии системы защиты и управляемых устройств отображается в рабочей области узла **Сервер администрирования** на закладке **Статистика**. Закладка **Статистика** содержит несколько закладок второго уровня (страниц). На каждой странице отображаются информационные панели со статистической информацией, а также ссылки на корпоративные новости и другие материалы "Лаборатории Касперского". Статистическая информация представлена на информационных панелях в виде круговых или столбчатых диаграмм или таблиц. Данные в информационных панелях обновляются в процессе работы программы и отражают текущее состояние программы защиты.

Вы можете изменять набор страниц, содержащихся на закладке **Статистика**, набор информационных панелей на каждой странице, а также способ представления данных на информационных панелях.

► *Чтобы добавить новую страницу с информационными панелями на закладке **Статистика**, выполните следующие действия:*

1. Нажмите на кнопку **Настроить вид** в правом верхнем углу закладки **Статистика**.

Откроется окно **Свойства: Статистика**. В окне содержится список страниц, которые содержатся на закладке **Статистика** в настоящее время. В окне можно изменять порядок отображения страниц на закладке, добавлять и удалять страницы, переходить к настройке свойств страниц по кнопке **Свойства**.

2. Нажмите на кнопку **Добавить**.

Откроется окно свойств новой страницы.

3. Настройте новую страницу:

- В разделе **Общие** укажите название страницы.
- В разделе **Информационные панели** по кнопке **Добавить** добавьте информационные панели, которые должны отображаться на странице.

По кнопке **Свойства** в разделе **Информационные панели** можно настраивать свойства добавленных информационных панелей: название, тип и вид диаграммы на панели, данные, по которым строится диаграмма.

4. Нажмите на кнопку **ОК**.

Добавленная страница с информационными панелями отобразится на закладке **Статистика**. По кнопке  можно быстро перейти к настройке страницы или выбранной информационной панели на странице.

Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений:

- Электронная почта. При возникновении события программа посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события программа посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS через почтовый шлюз или с помощью утилиты Kaspersky SMS Broadcasting.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события.

► *Чтобы настроить параметры уведомлений о событиях на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

В результате откроется окно **Свойства: События**.

4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений.
5. В поле **Текст уведомления** введите текст, который программа будет отправлять при возникновении события.

Из раскрывающего списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

6. По кнопке **Отправить пробное сообщение** проверьте, правильно ли настроены уведомления.

Программа отправляет тестовое уведомление указанному получателю.

7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Вы также можете быстро настроить уведомления о событии в окне свойств события по ссылкам **Настроить параметры событий Kaspersky Endpoint Security** и **Настроить параметры событий Сервера администрирования**.

См. также

| Обработка и хранение событий на Сервере администрирования [41](#)

Создание сертификата для SMTP-сервера

Сертификат для SMTP-сервера необходим для идентификации и верификации почтового сервера, к которому производится подключение. Сертификат используется для защиты пересылаемых писем от перехвата, например, в процессе передачи писем от почтового клиента к серверу и обратно.

► *Чтобы создать сертификат для SMTP-сервера, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

Откроется окно свойств событий.

4. На закладке **Электронная почта** по ссылке **Параметры** откройте окно **Параметры**.
5. В окне **Параметры** по ссылке **Задать сертификат** откройте окно **Сертификат для подписи**.
6. В окне **Сертификат для подписи** нажмите на кнопку **Задать**.

В результате откроется окно **Сертификат**.

7. В раскрывающемся списке **Тип сертификата** выберите открытый или закрытый тип сертификата:

- Если выбран сертификат закрытого типа (**Контейнер PKCS#12**), укажите файл сертификата и пароль.
- Если выбран сертификат открытого типа (**X.509-сертификат**):
 - a. укажите файл закрытого ключа (файл с расширением prk или pem);
 - b. укажите пароль закрытого ключа;
 - c. укажите файл открытого ключа (файл с расширением cer).

8. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат для SMTP-сервера.

Выборки событий

Информация о событиях в работе Kaspersky Security Center и управляемых программ сохраняется как в системном журнале Microsoft Windows, так и в журнале событий Kaspersky Security Center. Вы можете просматривать информацию из журнала событий Kaspersky Security Center в рабочей области узла **Сервер администрирования** на закладке **События**.

Информация на закладке **События** представлена в виде списка выборок событий. Каждая выборка включает в себя только события определенного типа. Например, выборка "Статус устройства – Критический" содержит только записи об изменении статусов устройств на "Критический". После установки программы на закладке **События** содержится ряд стандартных выборок событий. Вы можете создавать дополнительные (пользовательские) выборки событий, а также экспортировать информацию о событиях в файл.

В этом разделе

Просмотр выборки событий.....	201
Настройка параметров выборки событий.....	201
Создание выборки событий.....	202
Экспорт выборки событий в текстовый файл.....	202
Удаление событий из выборки.....	203

Просмотр выборки событий

► *Чтобы просмотреть выборку событий, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. В раскрывающемся списке **События выборки** выберите нужную вам выборку событий.

Если вы хотите, чтобы события этой выборки отображались в рабочей области постоянно, нажмите на кнопку  рядом с выборкой.

В результате в рабочей области будет представлен список событий выбранного типа, хранящихся на Сервере администрирования.

Вы можете сортировать информацию в списке событий по возрастанию или убыванию данных в любой графе списка.

Настройка параметров выборки событий

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

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.

2. В рабочей области узла выберите закладку **События**.
3. Откройте нужную вам выборку событий на закладке **События**.
4. Нажмите на кнопку **Свойства выборки**.

В открывшемся окне свойств выборки событий вы можете настроить параметры выборки.

Создание выборки событий

► *Чтобы создать выборку событий, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Нажмите на кнопку **Создать выборку**.
4. В открывшемся окне **Новая выборка событий** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в раскрывающемся списке **Выборки событий** будет создана выборка с указанным вами именем.

По умолчанию созданная выборка событий содержит все события, хранящиеся на Сервере администрирования. Чтобы в выборке отображались только интересующие вас события, нужно настроить параметры выборки.

Экспорт выборки событий в текстовый файл

► *Чтобы экспортировать выборку событий в текстовый файл, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Нажмите на кнопку **Импорт/Экспорт**.

4. В раскрывающемся списке выберите **Экспортировать события в файл**.

В результате запустится мастер экспорта событий. Следуйте его указаниям.

Удаление событий из выборки

► *Чтобы удалить события из выборки, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Выберите события, которые требуется удалить, с помощью мыши и клавиш **Shift** или **Ctrl**.
4. Удалите выбранные события одним из следующих способов:

- В контекстном меню любого из выделенных событий выберите пункт **Удалить**.

При выборе пункта контекстного меню **Удалить все** из выборки будут удалены все отображаемые события, независимо от того, какие из них вы предварительно выбрали для удаления.

- По ссылке **Удалить событие**, если выбрано одно событие, или по ссылке **Удалить события**, если выбрано несколько событий, в блоке работы с выбранными событиями.

В результате выбранные события будут удалены.

Настройка экспорта событий в SIEM-систему

Программа позволяет экспортировать события в работе Сервера администрирования и других программ "Лаборатории Касперского", установленных на клиентских устройствах, в SIEM-систему (SIEM – Security Information and Event Management).

► Чтобы настроить экспорт событий в SIEM-систему, выполните следующие действия:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить экспорт в SIEM-систему**.

Откроется окно свойств событий на разделе **Экспорт событий**.

4. Установите флажок **Автоматически экспортировать события в базу SIEM-системы**.
5. В раскрывающемся списке **SIEM-система** выберите систему, в которую нужно экспортировать события.

Доступен экспорт событий в SIEM-системы QRadar® (LEEF-формат), ArcSight (CEF-формат), Splunk® (CEF-формат) и формат Syslog (RFC 5424). По умолчанию выбрана система ArcSight (CEF-формат).

6. Укажите адрес сервера SIEM-системы и порт для подключения к серверу в соответствующих полях.

По кнопке **Экспортировать архив** программа экспортирует уже созданные события в базу SIEM-системы с указанной даты. По умолчанию программа экспортирует события с текущей даты.

7. Нажмите на кнопку **ОК**.

В результате после установки флажка **Автоматически экспортировать события в базу SIEM-системы** и настройки соединения с сервером программа будет автоматически экспортировать все события в работе Сервера администрирования и других программ "Лаборатории Касперского" в SIEM-систему.

Более подробную информацию об экспорте событий см. в разделе "Экспорт событий в SIEM-системы (на стр. [416](#))".

Выборки устройств

Информация о состоянии устройств содержится в дереве консоли в папке **Выборки устройств**.

Информация в папке **Выборки устройств** представлена в виде списка выборок устройств. Каждая выборка включает в себя устройства, отвечающие определенным условиям. Например, выборка **Устройства со статусом "Критический"** содержит только устройства со статусом *Критический*. После установки программы папка **Выборки устройств** содержит ряд стандартных выборок. Вы можете создавать дополнительные (пользовательские) выборки устройств, экспортировать параметры выборок в файл, а также создавать выборки с параметрами, импортированными из файла.

В этом разделе

Просмотр выборки устройств	205
Настройка параметров выборки устройств.....	206
Экспорт параметров выборки устройств в файл.....	206
Создание выборки устройств	207
Создание выборки устройств по импортированным параметрам	207
Удаление устройств из групп администрирования в выборке	208
Параметры условий выборки устройств	209

Просмотр выборки устройств

► *Чтобы просмотреть выборку устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки в раскрывающемся списке **Устройства выборки** выберите нужную вам выборку устройств.

Если вы хотите, чтобы устройства этой выборки отображались в рабочей области постоянно, нажмите на кнопку ☆ рядом с выборкой.

В результате в рабочей области отобразится список устройств, отвечающих параметрам выборки.

Вы можете сортировать информацию в списке устройств по возрастанию или убыванию данных в любой из граф.

Настройка параметров выборки устройств

► Чтобы настроить параметры выборки устройств, выполните следующие действия:

1. В дереве консоли выберите папку **Выборки устройств**.
2. Выберите нужную вам выборку устройств.
3. Нажмите на кнопку **Свойства выборки**.
4. В открывшемся окне свойств настройте общие свойства выборки и критерии попадания устройств в выборку.
5. Нажмите на кнопку **ОК**.

См. также

| Параметры условий выборки устройств [209](#)

Экспорт параметров выборки устройств в файл

► Чтобы экспортировать параметры выборки устройств в текстовый файл, выполните следующие действия:

1. В дереве консоли выберите папку **Выборки устройств**.

2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Экспортировать параметры**.
3. В открывшемся окне **Сохранить как** задайте имя файла для экспорта параметров выборки, укажите папку, в которую будет сохранен файл, и нажмите на кнопку **Сохранить**.

Параметры выборки устройств будут сохранены в указанный файл.

Создание выборки устройств

► *Чтобы создать выборку устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Создать выборку**.
3. В открывшемся окне **Новая выборка устройств** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в дереве консоли в папке **Выборки устройств** будет создана новая папка с указанным вами именем. По умолчанию созданная выборка устройств содержит все устройства, входящие в группы администрирования того Сервера, под управлением которого создана выборка. Чтобы в выборке отображались только интересующие вас устройства, нужно настроить параметры выборки по кнопке **Свойства выборки**.

Создание выборки устройств по импортированным параметрам

► *Чтобы создать выборку устройств по импортированным параметрам, выполните следующие действия:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Импортировать**.

3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать параметры выборки. Нажмите на кнопку **Открыть**.

В результате в папке **Выборки устройств** будет создана выборка **Новая выборка**, параметры которой импортированы из указанного файла.

Если в папке **Выборки устройств** уже существует выборка с названием **Новая выборка**, к имени созданной выборки будет добавлено окончание вида (**<порядковый номер>**), например: **(1)**, **(2)**.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

► *Чтобы удалить устройства из групп администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. Выберите устройства, которые требуется удалить, с помощью клавиш **Shift** или **Ctrl**.
3. Удалите выбранные устройства из групп администрирования одним из следующих способов:
 - В контекстном меню любого из выделенных устройств выберите пункт **Удалить**.
 - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите **Удалить из группы**.

В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Параметры условий выборки устройств

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

- **Инвертировать условие выборки**

Если флажок установлен, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

По умолчанию флажок снят.

Сеть

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства**

Имя устройства в сети Windows (NetBIOS-имя).

- **Windows-домен**

Будут отображаться все устройства, входящие в указанный домен Windows.

- **Группа администрирования**

Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие** или в разделе **Заметки**.

Для описания текста в поле **Комментарий** допустимо использовать следующие символы:

- Внутри одного слова:
 - *. Заменяет любую строку длиной 0 и более символов.

Пример:

Для описания слов **Сервер**, **Серверный** или **Серверная** можно использовать строку **Сервер***

- ?. Заменяет любой один символ.

Пример:

Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

Символ * или ? не может использоваться как первый символ в описании текста.

- Для связи нескольких слов:
 - Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами.

Пример:

Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

- +. При написании перед словом обозначает обязательное наличие слова в тексте.

Пример:

Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- -. При написании перед словом обозначает обязательное отсутствие слова в тексте.

Пример:

Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**,

можно использовать строку **+Подчиненный-Виртуальный**.

- **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

Пример:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-интервал**

Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

По умолчанию флажок снят.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

- **Применять, если есть хотя бы один из выбранных тегов**

Если флажок установлен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если флажок снят, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию флажок снят.

- **Тег должен присутствовать**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Active Directory

В разделе **Active Directory** можно настроить критерии включения устройств в выборку на основании их данных Active Directory:

- **Устройство находится в подразделении Active Directory**

Если флажок установлен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

По умолчанию флажок снят.

- **Включая дочерние подразделения**

Если флажок установлен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

По умолчанию флажок снят.

- **Устройство является членом группы Active Directory**

Если флажок установлен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

По умолчанию флажок снят.

Сетевая активность

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Является агентом обновлений**

В раскрывающемся списке можно выбрать критерий включения

устройств в состав выборки при поиске:

- **Да.** В выборку будут включены устройства, являющиеся агентами обновлений.
- **Нет.** Устройства, являющиеся агентами обновлений, не будут включены в выборку.
- **Значение не выбрано.** Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Включен.** В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
- **Выключен.** В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
- **Значение не выбрано.** Критерий не применяется.

- **Переключение профиля подключения**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Нет.** В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Значение не выбрано.** Критерий не применяется.

- **Время последнего соединения с Сервером администрирования**

С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

Если флажок установлен, то в выборку попадают только новые устройства, обнаруженные при опросе сети за количество дней, которое указано в поле **Период обнаружения (сут)**.

Если флажок снят, то в выборку попадают все устройства, обнаруженные при опросе сети.

По умолчанию флажок снят.

- **Устройство видимо в сети**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** Программа включает в выборку устройства, которые видимы в сети в настоящий момент.
- **Нет.** Программа включает в выборку устройства, которые не видимы в сети в настоящий момент.
- **Значение не выбрано.** Критерий не применяется.

Программа

В разделе **Программа** можно настроить критерии включения устройств в выборку на основании выбранной управляемой программы:

- **Название программы**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию программы "Лаборатории Касперского".

В списке представлены названия только тех программ, для которых на рабочем месте администратора установлены плагины управления.

Если программа не выбрана, то критерий не применяется.

- **Версия программы**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии программы "Лаборатории Касперского".

Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для программы наименованию или номеру пакета обновления.

Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей программы**

С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей программ, установленных на устройствах.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей программ, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Устройство под управлением Kaspersky Security Center 10**

В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security

Center:

- **Да.** Программа включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
- **Нет.** Программа включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
- **Значение не выбрано.** Критерий не применяется.

- **Установлена программа защиты**

В раскрываемом списке можно включить в состав выборки устройства, на которых установлена программа защиты:

- **Да.** Программа включает в выборку устройства, на которых установлена программа защиты.
- **Нет.** Программа включает в выборку устройства, на которых не установлена программа защиты.
- **Значение не выбрано.** Критерий не применяется.

Операционная система

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы:

- **Версия операционной системы**

Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Архитектура операционной системы**

В раскрываемом списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Неизвестно, x86, AMD64, IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы (X.Y.)**

В поле можно указать версию пакета установленной операционной системы (в формате X.Y), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

Статус устройства

В разделе **Статус устройства** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемой программы:

- **Статус устройства**

Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК*, *Критический*, *Предупреждение*.

- **Описание статуса устройства**

В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *ОК*, *Критический*, *Предупреждение*.

- **Статус постоянной защиты**

Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Компоненты защиты

В разделе **Компоненты защиты** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

Если флажок установлен, поиск клиентских устройств выполняется по дате выпуска баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

По умолчанию флажок снят.

- **Количество записей в базах**

Если флажок установлен, поиск клиентских устройств выполняется по количеству записей в базах. В полях ввода можно задать нижнее и верхнее значения количества записей.

По умолчанию флажок снят.

- **Время последнего поиска вирусов**

Если флажок установлен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого поиск вирусов выполнялся в последний раз.

По умолчанию флажок снят.

- **Количество найденных вирусов**

Если флажок установлен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию флажок снят.

Реестр программ

В разделе **Реестр программ** можно настроить критерии включения устройств в выборку в зависимости от того, какие программы на них установлены:

- **Название программы**

Раскрывающийся список, в котором можно выбрать программу. Устройства, на которых установлена указанная программа, будут включены в выборку.

- **Версия программы**

Поле ввода, в котором указывается версия выбранной программы.

- **Производитель**

Раскрывающийся список, в котором можно выбрать производителя

установленной на устройстве программы.

- **Статус программы**

Раскрывающийся список, в котором можно выбрать статус программы (*Установлена, Не установлена*). Устройства, на которых указанная программа установлена или не установлена, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

Если флажок установлен, поиск будет выполняться по данным об обновлении программ, установленных на искомым устройствах. После установки флажка названия полей ввода **Название программы** и **Версия программы** меняются на **Имя обновления** и **Версия обновления**.

По умолчанию флажок снят.

- **Название несовместимой программы безопасности**

Раскрывающийся список, в котором можно выбрать программы защиты сторонних производителей. Во время поиска устройства, на которых установлена выбранная программа, будут включены в выборку.

- **Тег программы**

В раскрывающемся списке можно выбрать тег программы. Все устройства, на которых установлены программы, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применять к устройствам без выбранных тегов**

Если флажок установлен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

Если флажок снят, критерий не применяется.

По умолчанию флажок снят.

Реестр оборудования

В разделе **Оборудование** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

- **Устройство**

В раскрываемся списке можно выбрать тип оборудования, которое должно быть установлено на клиентском устройстве, чтобы оно отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Производитель**

В раскрываемся списке можно выбрать производителя оборудования, которое должно быть установлено на устройстве, чтобы устройство отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

Имя устройства в Windows-сети. Устройство с указанным именем будет включено в выборку.

- **Описание**

Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Производитель устройства**

Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц)**

Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

Виртуальные машины

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

В раскрываемом списке можно выбрать следующие элементы:

- **Да.** Искомые устройства должны являться виртуальными машинами.
- **Нет.** Искомые устройства не должны являться виртуальными машинами.

- **Тип виртуальной машины**

В раскрываемом списке можно выбрать производителя виртуальной машины.

Раскрывающийся список доступен, если в раскрываемом списке **Является виртуальной машиной** указано значение **Да**.

- **Часть Virtual Desktop Infrastructure**

В раскрываемом списке можно выбрать следующие элементы:

- **Да.** Искомые устройства должны являться частью Virtual Desktop Infrastructure.
- **Нет.** Искомые устройства не должны являться частью Virtual Desktop Infrastructure.

Уязвимости и обновления

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Windows Update:

- **WUA переключен на Сервер администрирования**

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да.** Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Windows Update с Сервера администрирования.
- **Нет.** Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Windows Update из другого источника.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Описания статусов от управляемой программы

В разделе **Описания статусов от управляемой программы** можно настроить критерии включения устройств в выборку по описаниям статусов устройств от управляемой программы:

- **Описание статуса устройства**

Вы можете установить флажки для описаний статусов от управляемой

программы, при получении которых устройства будут включаться в выборку.

Статусы компонентов управляемых программ

В разделе **Статусы компонентов управляемых программ** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых программ:

- **Статус защиты данных от утечек**

Поиск устройств по статусу компонента защиты от утечки данных (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу компонента защиты для серверов совместной работы (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу компонента антивирусной защиты почтовых серверов (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

Политики

Информация о политиках содержится в папке **Политики**.

В папке **Политики** отображается список политик, созданных в группах администрирования. После установки программы папка содержит список политик, созданных автоматически. Вы можете обновлять список политик, создавать политики, а также просматривать свойства политики, выбранной в списке.

Диаграмма показывает прогресс применения политики на клиентских устройствах, которым она назначена. Когда цвет диаграммы полностью изменяется на зеленый, это означает, что политика применена на всех клиентских устройствах.

Задачи

Информация о задачах содержится в папке **Задачи**.

В папке **Задачи** отображается список задач, назначенных клиентским устройствам в группах администрирования и Серверу администрирования. После установки программы папка содержит список задач, созданных автоматически. Вы можете обновлять список задач, создавать задачи, а также просматривать свойства задач, запускать и останавливать задачи.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия*. Каждая ревизия имеет номер.

Объекты программы, которые поддерживают работу с ревизиями:

- Серверы администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта;
- просматривать выбранную ревизию;
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в файле формата TXT.

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- Номер ревизии объекта.
- Дата и время изменения объекта.
- Имя пользователя, изменившего объект.
- Выполненное действие с объектом.
- Описание ревизии изменения параметров объекта.

По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Описание**. В окне **Описание ревизии объекта** введите текст описания ревизии.

В этом разделе

О ревизиях объектов.....	228
Просмотр раздела История ревизий.....	228
Сравнение ревизий объекта.....	229
Просмотр ревизии объекта.....	231
Сохранение ревизии объекта в файле	232
Откат изменений	232
Добавление описания ревизии.....	233

О ревизиях объектов

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта (см. раздел "Сравнение ревизий объекта" на стр. [229](#));
- просматривать выбранную ревизию (см. раздел "Просмотр раздела История ревизий" на стр. [228](#));
- откатывать изменения объекта к выбранной ревизии (см. раздел "Откат изменений" на стр. [232](#));
- сохранять ревизии в файле формата TXT (см. раздел "Сохранение ревизии объекта в файле" на стр. [232](#)).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- Номер ревизии объекта.
- Дата и время изменения объекта.
- Имя пользователя, изменившего объект.
- Выполненное действие с объектом.
- Описание ревизии изменения параметров объекта (см. раздел "Добавление описания ревизии" на стр. [233](#)).

Просмотр раздела История ревизий

► Чтобы просмотреть раздел **История ревизий** объекта, выполните следующие действия:

1. В дереве консоли выберите один из объектов:

- узел **Сервер администрирования**;
- папку **Политики**;
- папку **Задачи**;
- папку группы администрирования;
- папку **Учетные записи пользователей**;
- папку **Инсталляционные пакеты**, вложенную в папку **Удаленная установка**.

2. Если нужный вам объект находится:

- В узле **Сервера администрирования** или группы администрирования:

В контекстном меню папки группы администрирования или узла **Сервер администрирования** выберите пункт **Свойства**.

- В папках **Политики**, **Задачи**, **Учетные записи пользователей** или **Инсталляционные пакеты**:

В рабочей области папок **Политики**, **Задачи**, **Учетные записи пользователей** или **Инсталляционные пакеты** выберите объект, для которого нужно перейти в раздел **История ревизий**, и с помощью контекстного меню перейдите в окно свойств объекта.

3. В окне свойств объекта выберите раздел **История ревизий**.

Сравнение ревизий объекта

Вы можете сравнить ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

► *Чтобы сравнить ревизии объекта, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [228](#)) объекта.
2. В списке ревизий объекта выберите ревизию для сравнения.

Для выбора двух ревизий объекта используйте клавиши **SHIFT** и **CTRL**.

3. Выполните одно из следующих действий:

- Нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите одно из значений:

- **Сравнить с текущей ревизией**

Выберите этот вариант, чтобы сравнить выбранную ревизию с текущей.

- **Сравнить выбранные ревизии**

Выберите этот вариант, чтобы сравнить две выбранные ревизии.

- **Сравнить с другим объектом**

При работе с ревизиями задач выберите вариант **Сравнить с другой задачей**, чтобы сравнить выбранную ревизию с ревизией другой задачи.

При работе с ревизиями политик выберите вариант **Сравнить с другой политикой**, чтобы сравнить выбранную ревизию с ревизией другой политики

- Откройте окно свойств ревизии двойным щелчком мыши по названию ревизии и нажмите на одну из кнопок:

- **Сравнить с текущей**

Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с текущей.

- **Сравнить с предыдущей**

Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с предыдущей.

Отобразится отчет сравнения ревизий в формате HTML. В отчете можно свернуть некоторые блоки параметров ревизии. Чтобы свернуть блок параметров ревизии, нажмите на значок  рядом с названием блока.

В ревизии Сервера администрирования попадает информация об изменениях, кроме информации:

- из раздела **Трафик**;
- из раздела **Правила назначения тегов**;
- из раздела **Параметры доставки уведомлений**;
- из раздела **Агенты обновлений**;
- из раздела **Вирусная атака**.

Из раздела **Вирусная атака** не будет записана информация о настройке активации политик по событию Вирусная атака.

Просмотр ревизии объекта

Если вам понадобилось узнать, какие изменения проводились с объектом в определенный период, вы можете просмотреть ревизии объекта.

► *Чтобы просмотреть ревизии объекта, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [228](#)) объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно посмотреть.
3. Выполните одно из следующих действий:
 - Нажмите на кнопку **Посмотреть ревизию**.
 - Откройте окно свойств ревизии двойным щелчком мыши по названию ревизии и нажмите на кнопку **Посмотреть ревизию**.

Отобразится отчет с параметрами выбранной ревизии объекта в формате HTML. В отчете можно свернуть некоторые блоки параметров ревизии объекта. Чтобы свернуть блок параметров ревизии, нажмите на значок  рядом с названием блока.

Сохранение ревизии объекта в файле

Вы можете сохранить ревизию объекта в текстовом файле, например, чтобы отправить файл по электронной почте.

► *Чтобы сохранить ревизию объекта в файле, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [228](#)) объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно сохранить.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Сохранить в файл**.

Ревизия будет сохранена в файле формата TXT.

Откат изменений

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

► *Чтобы откатить изменения объекта, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [228](#)) объекта.
2. В списке ревизий объекта выберите номер ревизии, к которой нужно откатить изменения.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Добавление описания ревизии

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

► *Чтобы добавить описание ревизии, выполните следующие действия:*

1. Перейдите к разделу **История ревизий** (см. раздел "**Просмотр раздела История ревизий**" на стр. [228](#)) объекта.
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Описание**.
4. В окне **Описание ревизии объекта** введите текст описания ревизии.

По умолчанию описание ревизии объекта не заполнено.

5. Нажмите на кнопку **ОК**.

Нераспределенные устройства

В этом разделе представлена информация о работе с устройствами сети организации, не входящими в группы администрирования.

В этом разделе

Опрос сети.....	234
Работа с доменами Windows. Просмотр и изменение параметров домена	237
Работа с IP-диапазонами.....	237
Работа с группами Active Directory. Просмотр и изменение параметров группы	238
Создание правил автоматического перемещения устройств в группы администрирования	239
Использование динамического режима VDI на клиентских устройствах	239

Опрос сети

Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования получает в ходе регулярных опросов сети Windows, IP-диапазонов и Active Directory, сформированных в компьютерной сети организации. По результатам этих опросов содержание папки **Нераспределенные устройства** обновляется.

Сервер администрирования может проводить следующие виды опросов сети:

- **Опрос сети Windows.** Существуют два вида опроса сети Windows: быстрый и полный. При быстром опросе Сервер получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация: имя операционной системы, IP-адрес, DNS-имя, NetBIOS-имя.
- **Опрос IP-диапазонов.** Сервер администрирования опрашивает сформированные IP-диапазоны с помощью ICMP-пакетов и получает полную информацию об устройствах, входящих в IP-диапазоны.
- **Опрос Active Directory.** В базу данных Сервера администрирования записывается информация о структуре групп Active Directory, а также информация о DNS-именах устройств, входящих в группы Active Directory.

На основании полученной информации и данных о структуре сети организации Kaspersky Security Center обновляет состав и содержимое папок **Нераспределенные устройства** и **Управляемые устройства**. Если в сети организации настроено автоматическое перемещение устройств в группы администрирования, обнаруженные в сети устройства включаются в состав групп администрирования.

В этом разделе

Просмотр и изменение параметров опроса сети Windows	235
Просмотр и изменение параметров опроса групп Active Directory	236
Просмотр и изменение параметров опроса IP-диапазонов	236

Просмотр и изменение параметров опроса сети Windows

► *Чтобы изменить параметры опроса сети Windows, выполните следующие действия:*

1. В дереве консоли в папке **Опрос сети** выберите вложенную папку **Домены**.

Вы можете перейти в папку **Опрос сети** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

2. Нажмите на кнопку **Настроить параметры опроса** в рабочей области папки **Домены**.

В результате откроется окно **Свойства: Домены**, в котором вы можете просмотреть и изменить параметры опроса сети Windows.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса сети Windows осуществляются в окне свойств агента обновлений, в разделе **Опрос сети**.

Просмотр и изменение параметров опроса групп Active Directory

- ▶ *Чтобы изменить параметры опроса групп Active Directory, выполните следующие действия:*

1. В дереве консоли в папке **Опрос сети** выберите вложенную папку **Active Directory**.

Вы можете перейти в папку **Опрос сети** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

2. По ссылке **Настроить параметры опроса** откройте окно **Свойства: Active Directory**.

В окне **Свойства: Active Directory** вы можете просмотреть и изменить параметры опроса групп Active Directory.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса групп Active Directory осуществляются в окне свойств агента обновлений, в разделе **Опрос сети**.

Просмотр и изменение параметров опроса IP-диапазонов

- ▶ *Чтобы изменить параметры опроса IP-диапазонов, выполните следующие действия:*

1. В дереве консоли в папке **Опрос сети** выберите вложенную папку **IP-диапазоны**.

Вы можете перейти в папку **Опрос сети** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

2. По ссылке **Настроить параметры опроса** откройте окно **Свойства: IP-диапазоны**.

В окне **Свойства: IP-диапазоны** вы можете просмотреть и изменить параметры опроса IP-диапазонов.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса IP-диапазонов осуществляются в окне свойств агента обновлений, в разделе **Опрос сети**. Клиентские устройства, найденные в результате опроса IP-диапазонов, отображаются в папке **Домены** виртуального Сервера.

Работа с доменами Windows. Просмотр и изменение параметров домена

► Чтобы изменить параметры домена, выполните следующие действия:

1. В дереве консоли в папке **Опрос сети** выберите вложенную папку **Домены**.
2. Выберите домен и откройте окно его свойств одним из следующих способов:
 - В контекстном меню домена выберите пункт **Свойства**.
 - По ссылке **Показать свойства группы**.

В результате открывается окно **Свойства: <Имя домена>**, в котором можно настроить параметры выбранного домена.

Работа с IP-диапазонами

Вы можете настраивать параметры существующих IP-диапазонов, а также создавать новые IP-диапазоны.

В этом разделе

Создание IP-диапазона.....	238
Просмотр и изменение параметров IP-диапазона	238

Создание IP-диапазона

► Чтобы создать IP-диапазон, выполните следующие действия:

1. В дереве консоли в папке **Опрос сети** выберите вложенную папку **IP-диапазоны**.
2. В контекстном меню папки выберите пункт **Создать** → **IP-диапазон**.
3. В открывшемся окне **Новый IP-диапазон** настройте параметры создаваемого IP-диапазона.

В результате созданный IP-диапазон появится в составе папки **IP-диапазоны**.

Просмотр и изменение параметров IP-диапазона

► Чтобы изменить параметры IP-диапазона, выполните следующие действия:

1. В дереве консоли в папке **Опрос сети** выберите вложенную папку **IP-диапазоны**.
2. Выберите IP-диапазон и откройте окно его свойств одним из следующих способов:
 - В контекстном меню IP-диапазона выберите пункт **Свойства**.
 - По ссылке **Показать свойства группы**.

В результате открывается окно **Свойства: <Название IP-диапазона>**, в котором можно настроить параметры выбранного IP-диапазона.

Работа с группами Active Directory. Просмотр и изменение параметров группы

► Чтобы изменить параметры группы Active Directory, выполните следующие действия:

1. В дереве консоли в папке **Опрос сети** выберите вложенную папку **Active Directory**.

2. Выберите группу Active Directory и откройте окно ее свойств одним из следующих способов:

- В контекстном меню группы выберите пункт **Свойства**.
- По ссылке **Показать свойства группы**.

В результате открывается окно **Свойства: <Название группы Active Directory>**, в котором можно настроить параметры выбранной группы Active Directory.

Создание правил автоматического перемещения устройств в группы администрирования

Вы можете настроить автоматическое перемещение устройств, обнаруживаемых при опросе сети организации, в группы администрирования.

► *Чтобы настроить правила автоматического перемещения устройств в группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В рабочей области папки нажмите на кнопку **Настроить правила**.

В результате откроется окно **Свойства: Нераспределенные устройства**. Настройте правила автоматического перемещения устройств в группы администрирования в разделе **Перемещение устройств**.

Использование динамического режима VDI на клиентских устройствах

В сети организации может быть развернута виртуальная инфраструктура с использованием временных виртуальных машин. Kaspersky Security Center обнаруживает временные виртуальные машины и добавляет данные о них в базу данных Сервера администрирования. После завершения работы пользователя с временной виртуальной машиной машина удаляется из виртуальной инфраструктуры. Однако запись об удаленной

виртуальной машине может сохраниться в базе данных Сервера администрирования. Кроме того, несуществующие виртуальные машины могут отображаться в Консоли администрирования.

Чтобы избежать сохранения данных о несуществующих виртуальных машинах, в Kaspersky Security Center реализована поддержка динамического режима для Virtual Desktop Infrastructure (VDI). Администратор может включить поддержку динамического режима для VDI (см. раздел "Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования" на стр. [241](#)) в свойствах инсталляционного пакета Агента администрирования, который будет установлен на временной виртуальной машине.

Во время выключения временной виртуальной машины Агент администрирования информирует Сервер администрирования о выключении. В случае успешного выключения виртуальной машины, она удаляется из списка устройств, подключенных к Серверу администрирования. Если выключение виртуальной машины выполнено некорректно и Агент администрирования не послал Серверу уведомление о выключении, используется дублирующий сценарий. Согласно этому сценарию виртуальная машина удаляется из списка устройств, подключенных к Серверу администрирования, после трех неудачных попыток синхронизации с Сервером.

В этом разделе

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования	241
Поиск устройств, являющихся частью VDI	241
Перемещение в группу администрирования устройств, являющихся частью VDI	242

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

► Чтобы включить динамический режим VDI, выполните следующие действия:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

Откроется окно **Свойства: Агент администрирования Kaspersky Security Center**.

3. В окне **Свойства: Агент администрирования Kaspersky Security Center** выберите раздел **Дополнительно**.
4. В разделе **Дополнительно** установите флажок **Включить динамический режим для VDI**.

Устройство, на которое устанавливается Агент администрирования, будет являться частью Virtual Desktop Infrastructure.

Поиск устройств, являющихся частью VDI

► Чтобы найти устройства, являющиеся частью VDI, выполните следующие действия:

1. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
2. В окне **Поиск** на закладке **Виртуальные машины** в раскрывающемся списке **Часть Virtual Desktop Infrastructure** выберите вариант **Да**.
3. Нажмите на кнопку **Найти**.

Будет выполнен поиск устройств, являющихся частью Virtual Desktop Infrastructure.

Перемещение в группу администрирования устройств, являющихся частью VDI

► Чтобы переместить устройства, являющиеся частью VDI, в группу администрирования, выполните следующие действия:

1. В рабочей области папки **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.

В результате откроется окно свойств папки **Нераспределенные устройства**.

2. В окне свойств папки **Нераспределенные устройства** в разделе **Перемещение устройств** нажмите на кнопку **Добавить**.

Откроется окно **Новое правило**.

3. В окне **Новое правило** выберите раздел **Виртуальные машины**.

4. В раскрывающемся списке **Часть Virtual Desktop Infrastructure** выберите вариант **Да**.

Будет создано правило перемещения устройств в группу администрирования.

Управление программами на клиентских устройствах

Kaspersky Security Center позволяет управлять программами "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах.

Администратор может выполнять следующие действия:

- создавать категории программ на основании заданных критериев;
- управлять категориями программ с помощью специально созданных правил;
- управлять запуском программ на устройствах;

- выполнять инвентаризацию и вести реестр программного обеспечения, установленного на устройствах;
- закрывать уязвимости программного обеспечения, установленного на устройствах;
- устанавливать обновления Windows Update и других производителей программного обеспечения на устройствах;
- отслеживать использование ключей для групп лицензионных программ.

В этом разделе

Группы программ.....	243
Уязвимости в программах.....	265
Обновления программного обеспечения	269

Группы программ

В этом разделе описана работа с группами программ, установленных на устройствах.

Создание категорий программ

Kaspersky Security Center позволяет создавать категории программ, установленных на устройствах.

Категории программ можно создавать следующими способами:

- Администратор указывает папку, исполняемые файлы в которой попадают в выбранную категорию.
- Администратор указывает устройство, исполняемые файлы с которого попадают в выбранную категорию.
- Администратор задает критерии, по которым программы попадают в выбранную категорию.

Когда категория программ создана, администратор может задать правила для этой категории программ. Правила определяют поведение программ, входящих в указанную категорию. Например, можно запретить или разрешить запуск программ, входящих в категорию.

Управление запуском программ на устройствах

Kaspersky Security Center позволяет управлять запуском программ на устройствах в режиме "Белый список". Подробное описание приведено в онлайн-справке Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>. В режиме "Белый список" на выбранных устройствах разрешен запуск только тех программ, которые входят в указанные категории. Администратор может просматривать результаты статического анализа правил запуска программ на устройствах по каждому пользователю.

Инвентаризация программного обеспечения, установленного на устройствах

Kaspersky Security Center позволяет выполнять инвентаризацию программного обеспечения на устройствах. Агент администрирования получает информацию обо всех программах, установленных на устройствах. Информация, полученная в результате инвентаризации, отображается в рабочей области папки **Реестр программ**. Администратор может просматривать подробную информацию о каждой программе, в том числе версию и производителя.

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Управление группами лицензионных программ

Kaspersky Security Center позволяет создавать группы лицензионных программ. В группу лицензионных программ входят программы, отвечающие критериям, заданным администратором. Администратор может указывать следующие критерии для групп лицензионных программ:

- название программы;
- версия программы;

- производитель;
- тег программы.

Программы, соответствующие одному или нескольким критериям, автоматически попадают в группу. Для создания группы лицензионных программ должен быть задан хотя бы один критерий включения программ в эту группу.

Каждая группа лицензионных программ имеет свой ключ. Ключ группы лицензионных программ определяет допустимое количество установок для программ, входящих в группу. Если количество установок превысило заданное в ключе ограничение, на Сервере администрирования регистрируется информационное событие. Администратор может указать дату окончания действия ключа. При наступлении этой даты на Сервере администрирования регистрируется информационное событие.

Просмотр информации об исполняемых файлах

Kaspersky Security Center получает всю информацию об исполняемых файлах, которые запускались на устройствах с момента установки на них операционной системы. Полученная информация об исполняемых файлах отображается в главном окне программы в рабочей области папки **Исполняемые файлы**.

В этом разделе

Создание категорий программ	246
Добавление событий в категорию программ	254
Настройка управления запуском программ на клиентских устройствах	256
Просмотр результатов статического анализа правил запуска исполняемых файлов	258
Просмотр реестра программ	259
Создание групп лицензионных программ	260
Управление ключами для групп лицензионных программ	261
Инвентаризация программного обеспечения Kaspersky Security Center	262
Инвентаризация исполняемых файлов	263
Просмотр информации об исполняемых файлах.....	264

Создание категорий программ

► *Чтобы создать категорию программ, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Категории программ**.
2. По кнопке **Создать категорию** запустите мастер создания пользовательской категории.
3. В окне мастера выберите тип пользовательской категории:
 - **Пополняемая вручную категория.** Задайте критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
 - **Автоматически пополняемая категория.** Укажите папку, исполняемые файлы из которой будут автоматически попадать в создаваемую категорию.

При создании автоматически пополняемой категории программа выполняет инвентаризацию следующих форматов файлов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

- **Категория, в которую входят исполняемые файлы с выбранных устройств.**
Укажите устройство., исполняемые файлы которого должны попадать в категорию автоматически.

4. Следуйте указаниям мастера.

В результате работы мастера создается пользовательская категория программ. Просмотреть созданные категории можно в списке категорий в рабочей области папки **Категории программ.**

Категории программ используются компонентом Контроль программ, который входит в состав программы защиты Kaspersky Endpoint Security для Windows. Компонент Контроль программ позволяет администратору установить ограничения на запуск программ на клиентских устройствах, например, на основании программ, которые входят в выбранную категорию.

В этом разделе

Создание пополняемой вручную категории программ.....	247
Создание автоматически пополняемой категории программ	250

Создание пополняемой вручную категории программ

- ▶ *Чтобы создать пополняемую вручную категорию программ, выполните следующие действия:*
 1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ.**

2. По ссылке **Создать категорию** запустите мастер создания пользовательской категории.
3. В окне мастера выберите тип пользовательской категории **Пополняемая вручную категория**.
4. В окне **Настройка условий для включения программ в категорию** нажмите на кнопку **Добавить**.
5. В раскрывающемся списке задайте необходимые вам параметры:

- **Из списка исполняемых файлов**

Если выбран этот вариант, программы для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

- **Из свойств файла**

Если выбран этот вариант, можно вручную указать детальные данные исполняемых файлов, которые будут добавлены в пользовательскую категорию программ.

- **Метаданные файлов папки**

Укажите папку на клиентском устройстве, которая содержит исполняемые файлы. Метаданные исполняемых файлов, входящих в указанную папку, будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию программ.

- **Хеши файлов папки**

Если выбран этот вариант, можно выбрать или создать папку на клиентском устройстве. Хеш файлов, содержащихся в указанной папке, будет передаваться на Сервер администрирования. Программы, имеющие такой же хеш, как и файлы в указанной папке, будут добавлены в пользовательскую категорию программ.

- **Сертификаты файлов из папки**

Если выбран этот вариант, можно указать папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Сертификаты исполняемых файлов считываются и добавляются в условия категории. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Метаданные файлов установщика MSI**

Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика программы будут передаваться на Сервер администрирования. Программы, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию программ.

- **Контрольные суммы файлов msi-инсталлятора программы**

Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать файл установщика MSI. Хеш файлов установщика программы будет передаваться на Сервер администрирования. Программы, у которых хеш файлов установщика MSI совпадает с указанным, будут добавлены в пользовательскую категорию программ.

- **KL-категория**

Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать категорию программ "Лаборатории Касперского". Программы, входящие в указанную KL-катеорию, будут добавлены в пользовательскую категорию программ.

- **Папка программы**

Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию программ.

- **Сертификаты из хранилища сертификатов**

Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Тип носителя**

Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск программы. Программы, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию программ.

6. Следуйте указаниям мастера.

Kaspersky Security Center работает с метаданными только из тех файлов, которые содержат цифровую подпись. Невозможно создать категорию на основе метаданных файлов, не содержащих цифровой подписи.

В результате работы мастера будет создана пользовательская категория программ, пополняемая вручную. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории программ**.

Создание автоматически пополняемой категории программ

► *Чтобы создать автоматически пополняемую категорию программ, выполните следующие действия:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ**.

2. По кнопке **Создать категорию** запустите мастер создания пользовательской категории.

В окне мастера выберите тип пользовательской категории **Автоматически пополняемая категория**.

3. В окне **Папка хранилища** задайте необходимые вам параметры:

- **Путь к папке автоматического пополнения категории**

В поле укажите путь к папке, в которой Сервер администрирования будет периодически искать исполняемые файлы. Путь к папке задается в момент создания категории. Изменить путь к папке нельзя.

- **Включать в категорию динамически подключаемые библиотеки (DLL)**

В категорию программ включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль программ регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

По умолчанию флажок снят.

- **Включать в категорию данные о скриптах**

В категорию программ включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

По умолчанию флажок снят.

- **Алгоритм вычисления хеш-функции**

В зависимости от версии программы защиты, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции программой Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

- Если в вашей сети установлены версии программ защиты Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий программ ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою программы защиты. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
- Если в вашей сети установлены версии программ защиты ниже версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**. Добавить категорию, созданную по критерию MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.
- Если на разных устройствах в вашей сети используются новые и ранние версии программы защиты Kaspersky Endpoint Security 10, установите оба флажка, и **Вычислять SHA-256 для файлов в категории**, и **Вычислять MD5 для файлов в категории**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории**

(поддерживается для **Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше**) установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории** (поддерживается для версий ниже **Kaspersky Endpoint Security 10 Service Pack 2 для Windows**) снят.

- **Принудительно проверять папку на наличие изменений**

Если флажок установлен, программа периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

Если флажок снят, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

По умолчанию флажок снят.

- **Период проверки (ч)**

В поле можно указать период времени в часах, по истечении которого программа принудительно проверяет на наличие изменений папку автоматического пополнения категории. По умолчанию период принудительной проверки равен 24 часам. Поле доступно, если установлен флажок **Принудительно проверять папку на наличие изменений**.

По умолчанию флажок снят.

4. Следуйте указаниям мастера.

В результате работы мастера будет создана автоматически пополняемая категория программ. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории программ**.

Добавление событий в категорию программ

События типа **Запуск программы запрещен** и **Запуск программы запрещен в тестовом режиме** можно добавлять в существующую категорию программ, пополняемую вручную, или в новую категорию программ.

► *Чтобы добавить события в категорию, пополняемую вручную, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. На закладке **События** выберите нужное вам событие.

Можно выбрать несколько событий одновременно.

4. В контекстном меню события выберите пункт **Добавить в категорию**.
5. В окне **Выберите пользовательскую категорию** настройте необходимые вам параметры:

- **Создать категорию программ**

Выберите этот вариант, если необходимо создать новую категорию программ.

Нажмите на кнопку **ОК**, чтобы запустить мастер создания пользовательской категории. В результате работы мастера будет создана категория с указанными параметрами.

По умолчанию вариант не выбран.

- **Добавить правила в указанную категорию**

Выберите этот вариант, если необходимо добавить правила в существующую категорию программ. Выберите необходимую категорию в списке категорий программ.

По умолчанию этот вариант выбран.

В блоке **Тип правила** выберите параметры:

- **Добавить в правила включения**

Выберите этот вариант, если необходимо добавить правила в условия категории программ.

По умолчанию этот вариант выбран.

- **Добавить в правила исключения**

Выберите этот вариант, если необходимо добавить правила в исключения категории программ.

В блоке **Тип информации о файле** выберите один из параметров:

- **Данные сертификата или SHA-256 для файлов без сертификата**

Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA-256 для файлов без сертификата.

По умолчанию этот вариант выбран.

- **Данные сертификата (файлы без сертификата пропускаются)**

Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата

в категорию может попасть несколько версий программы или несколько программ одного производителя.

Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

- **Только SHA-256 (файлы без SHA-256 пропускаются)**

Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA-256 исполняемого файла.

- **MD5 (устаревший режим, только для версий Kaspersky Endpoint Security 10 Service Pack 1)**

Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия программы.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции MD5 исполняемого файла. Вычисление хеш-функции MD5 поддерживается для версий Kaspersky Endpoint Security 10 Service Pack 1 для Windows и ниже.

6. Нажмите на кнопку **OK**.

Настройка управления запуском программ на клиентских устройствах

Категоризация программ позволяет оптимизировать процесс управления запуском программ на устройствах. Вы можете создать категорию программ и настроить компонент Контроль программ политики так, что на устройствах, на которых применена эта политика, будут запускаться только программы из указанной категории. Например, вы создали категорию, которая содержит программы *Программа_1* и *Программа_2*. После добавления этой

категории в политику, на устройствах, к которым применена эта политика, будет разрешен запуск только двух программ, *Программа_1* и *Программа_2*. Если пользователь попытается запустить программу, которая не входит в категорию, например, *Программа_3*, то запуск такой программы будет заблокирован. Пользователю будет отображено сообщение о том, что запуск *Программа_3* запрещен в соответствии с правилом Контроля программ. Вы можете создать автоматически пополняемую категорию на основе различных критериев, входящих в указанную папку. В этом случае файлы будут автоматически добавляться в категорию из указанной папки. Исполняемые файлы программ копируются в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию.

► *Чтобы настроить управление запуском программ на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Категории программ**.
2. В рабочей области папки **Категории программ** создайте категорию программ (см. раздел "Создание категорий программ" на стр. [246](#)), запуском которых вы хотите управлять.
3. В папке **Управляемые устройства** на закладке **Политики** по ссылке **Создать политику Kaspersky Endpoint Security 10 для Windows** запустите мастер создания политики для программы Kaspersky Endpoint Security 10 для Windows и следуйте указаниям мастера.

Если такая политика уже существует, этот шаг можно пропустить. Управление запуском программ в указанной категории можно настроить в параметрах этой политики. Созданная политика отображается в папке **Управляемые устройства** на закладке **Политики**.

4. В контекстном меню политики для программы Kaspersky Endpoint Security 10 для Windows выберите пункт **Свойства**.

Откроется окно свойств политики Kaspersky Endpoint Security 10 для Windows.

5. В окне свойств политики Kaspersky Endpoint Security 10 для Windows в разделе **Контроль программ** нажмите на кнопку **Добавить**.

Откроется окно **Правило Контроля программ**.

6. В окне **Правило Контроля программ** в раскрывающемся списке **Категория** выберите категорию программ, на которую будет распространяться правило запуска. Настройте параметры правила запуска для выбранной категории программ.

Для программ версий Kaspersky Endpoint Security 10 Service Pack 2 и выше категории, созданные по критерию MD5-хеша исполняемого файла программы не отображаются.

Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для программ версий ниже Kaspersky Endpoint Security 10 Service Pack 2. Это может привести к сбою программы.

Подробные инструкции по настройке правил контроля приведены в онлайн-справке Kaspersky Endpoint Security для Windows <https://help.kaspersky.com/KESWin/11/ru-RU/127968.htm>.

7. Нажмите на кнопку **ОК**.

Запуск программ на устройствах, входящих в указанную категорию, будет выполняться согласно созданному правилу. Созданное правило отображается в окне свойств политики Kaspersky Endpoint Security 10 для Windows в разделе **Контроль программ**.

Просмотр результатов статического анализа правил запуска исполняемых файлов

- Чтобы просмотреть информацию о том, запуск каких исполняемых файлов запрещен пользователям, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите закладку **Политики**.
2. В контекстном меню **Политики защиты** выберите пункт **Свойства**.

Откроется окно свойств политики защиты.

3. В окне свойств политики защиты выберите раздел **Контроль программ** и нажмите на кнопку **Статический анализ**.

Откроется окно **Анализ списка прав доступа**.

4. В левой части окна **Анализ списка прав доступа** отображается список пользователей, составленный на основе данных Active Directory.

5. Выберите в списке пользователя.

В правой части окна отобразятся категории программ, назначенные этому пользователю.

6. Чтобы просмотреть исполняемые файлы, запуск которых запрещен пользователю, в окне **Анализ списка прав доступа** нажмите на кнопку **Просмотреть файлы**.

Откроется окно, в котором отображается список исполняемых файлов, запуск которых запрещен пользователю.

7. Чтобы просмотреть список исполняемых файлов, входящих в категорию, выберите категорию программ и нажмите на кнопку **Просмотреть файлы категории**.

Откроется окно, в котором отображается список исполняемых файлов, входящих в категорию программ.

Просмотр реестра программ

Функциональность получения информации об установленных программах поддерживается только для операционных систем Microsoft Windows.

► *Чтобы просмотреть реестр установленных на клиентских устройствах программ,*

в дереве консоли в папке **Управление программами** выберите вложенную папку **Реестр программ**.

В рабочей области папки **Реестр программ** отображается список программ, которые обнаружил на устройствах установленный на них Агент администрирования.

Вы можете просмотреть подробную информацию о любой программе, выбрав в контекстном меню этой программы пункт **Свойства**. В окне свойств программы отображается общая информация о программе и информация об исполняемых файлах программы, а также список устройств, на которых установлена программа.

Для просмотра программ, удовлетворяющих определенным критериям, вы можете воспользоваться полями фильтрации в рабочей области папки **Реестр программ**.

Информация о программах "Лаборатории Касперского" и других производителей на устройствах, подключенных к подчиненным и виртуальным Серверам администрирования, также хранится в реестре программ главного Сервера администрирования. Просмотреть эту информацию можно с помощью отчета о реестре программ, включив в отчет данные от подчиненных и виртуальных Серверов администрирования.

► *Чтобы включить в отчет о реестре программ информацию с подчиненных Серверов администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. В рабочей области закладки **Отчеты** выберите **Отчет о версиях программ "Лаборатории Касперского"**.
4. В контекстном меню отчета выберите пункт **Свойства**.

Откроется окно **Свойства: Отчет о версиях программ "Лаборатории Касперского"**.

5. В разделе **Иерархия Серверов администрирования** установите флажок **Использовать данные с подчиненных и виртуальных Серверов администрирования**.
6. Нажмите на кнопку **ОК**.

В результате информация с подчиненных и виртуальных Серверов администрирования будет включена в отчет **Отчет о версиях программ "Лаборатории Касперского"**.

Создание групп лицензионных программ

► *Чтобы создать группу лицензионных программ, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Учет сторонних лицензий**.

2. По ссылке **Добавить группу лицензионных программ** запустите **Мастер добавления группы лицензионных программ**.

3. Следуйте указаниям мастера.

В результате работы мастера создается группа лицензионных программ, которая отображается в папке **Учет сторонних лицензий**.

Управление ключами для групп лицензионных программ

► *Чтобы создать ключ для группы лицензионных программ, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Учет сторонних лицензий**.

2. В рабочей области папки **Учет сторонних лицензий** нажмите на кнопку **Управлять ключами лицензионных программ**

Откроется окно **Управление ключами лицензионных программ**.

3. В окне **Управление ключами лицензионных программ** нажмите на кнопку **Добавить**.

Откроется окно **Ключ**.

4. В окне **Ключ** укажите свойства ключа и ограничения, которые этот ключ накладывает на группу лицензионных программ.

- **Название.** Название ключа.
- **Комментарий.** Примечания к выбранному ключу.
- **Ограничение.** Количество устройств, на которых может быть установлена программа, использующая этот ключ.
- **Дата окончания.** Дата окончания срока действия ключа.

Созданные ключи отображаются в окне **Управление ключами лицензионных программ**.

► *Чтобы применить ключ к группе лицензионных программ, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Учет сторонних лицензий**.
2. В папке **Учет сторонних лицензий** выберите группу лицензионных программ, к которой вы хотите применить ключ.
3. В контекстном меню группы лицензионных программ выберите пункт **Свойства**.

Откроется окно свойств группы лицензионных программ.

4. В окне свойств группы лицензионных программ в разделе **Ключи** выберите вариант **Контролировать нарушение заданных лицензионных ограничений**.

5. Нажмите на кнопку **Добавить**.

Откроется окно **Выбор ключа**.

6. В окне **Выбор ключа** выберите ключ, который вы хотите применить к группе лицензионных программ.

7. Нажмите на кнопку **ОК**.

Ограничения для группы лицензионных программ, указанные в ключе, будут распространены на выбранную группу лицензионных программ.

Инвентаризация программного обеспечения Kaspersky Security Center

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах.

Агент администрирования составляет список программ, установленных на устройстве, и передает список Серверу администрирования. Агент администрирования автоматически получает информацию об установленных программах из реестра Windows.

Чтобы сохранить ресурсы устройства, по умолчанию Агент администрирования начинает получать информацию об установленных программах через 10 минут после запуска службы Агента администрирования.

► *Чтобы изменить время начала инвентаризации программного обеспечения устройства после запуска службы Агента администрирования, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Агент администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.

2. Перейдите в раздел:

- для 64-разрядной системы:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\1103\1.0.0.0\NagentFlags
```

- для 32-разрядной системы:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\N  
agentFlags
```

3. Для ключа `KLINV_INV_COLLECTOR_START_DELAY_SEC` установите нужное вам значение в секундах.

По умолчанию указано значение 600 секунд.

4. Перезапустите службу Агента администрирования.

В результате время начала инвентаризации программного обеспечения после запуска службы Агента администрирования будет изменено.

Инвентаризация исполняемых файлов

Инвентаризацию исполняемых файлов на клиентских устройствах можно выполнить с помощью задачи инвентаризации. Функциональность инвентаризации исполняемых файлов реализована в программе Kaspersky Endpoint Security 10 для Windows.

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

► *Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

В результате запустится мастер создания задачи

3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Инвентаризация** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате работы мастера создается задача инвентаризации для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.

Список исполняемых файлов, обнаруженных на устройствах в результате выполнения инвентаризации, отображается в рабочей области папки **Исполняемые файлы**.

При выполнении инвентаризации программа обнаруживает исполняемые файлы следующих форматов: mz, com, pe, ne, sys, cmd, bat, ps1, js, vbs, reg, msi, cpl, dll, jar, а также HTML-файлы.

Просмотр информации об исполняемых файлах

► *Чтобы просмотреть список всех исполняемых файлов, обнаруженных на клиентских устройствах,*

в дереве консоли в папке **Управление программами** выберите вложенную папку **Исполняемые файлы**.

В рабочей области папки **Исполняемые файлы** отображается список исполняемых файлов, которые запускались на устройствах с момента установки операционной системы или были обнаружены в процессе работы задачи инвентаризации Kaspersky Endpoint Security 10 для Windows.

Для просмотра данных об исполняемых файлах, удовлетворяющих определенным критериям, вы можете воспользоваться фильтрацией.

► *Чтобы просмотреть свойства исполняемого файла,*

в контекстном меню файла выберите пункт **Свойства**.

Откроется окно, содержащее информацию об исполняемом файле, а также список устройств, на которых присутствует исполняемый файл.

Уязвимости в программах

Папка **Уязвимости в программах**, входящая в состав папки **Управление программами**, содержит список уязвимостей в программах, которые обнаружил на клиентских устройствах установленный на них Агент администрирования. Агент администрирования выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях.

Функциональность анализа информации об уязвимостях в программах поддерживается только для операционных систем Microsoft Windows.

Открыв окно свойств выбранной программы в папке **Уязвимости в программах**, вы можете получить общую информацию об уязвимости, о программе, в которой она обнаружена, просмотреть список устройств, на которых обнаружена уязвимость, а также информацию о закрытии уязвимости.

Вы можете получить сведения об уязвимостях в программах на сайте "Лаборатории Касперского" (<https://threats.kaspersky.com/ru/>).

В этом разделе

Просмотр информации об уязвимостях в программах	266
Поиск уязвимостей в программах.....	267
Заккрытие уязвимостей в программах.....	268

Просмотр информации об уязвимостях в программах

- ▶ *Чтобы просмотреть список уязвимостей, обнаруженных на клиентских устройствах,*

в дереве консоли в папке **Управление программами** выберите вложенную папку **Уязвимости в программах**.

В рабочей области папки отображается список уязвимостей в программах, которые обнаружил на устройствах установленный на них Агент администрирования.

- ▶ *Чтобы получить информацию о выбранной уязвимости,*

в контекстном меню уязвимости выберите пункт **Свойства**.

Откроется окно свойств уязвимости, в котором отображается следующая информация:

- программа, в которой обнаружена уязвимость;
- список устройств, на которых обнаружена уязвимость;
- информация о закрытии уязвимости.

- ▶ *Чтобы просмотреть отчет обо всех обнаруженных уязвимостях,*

в папке **Уязвимости в программах** воспользуйтесь ссылкой **Просмотреть отчет об уязвимостях в программах**.

Будет создан отчет об уязвимостях в программах, установленных на устройствах. Отчет можно просмотреть в узле с именем нужного вам Сервера администрирования на закладке **Отчеты**.

Функциональность получения информации об уязвимостях в программах поддерживается только для операционных систем Microsoft Windows.

Поиск уязвимостей в программах

Если вы выполнили настройку программы с помощью мастера первоначальной настройки, задача поиска уязвимостей создается автоматически. Просмотреть задачу можно в папке **Управляемые устройства** на закладке **Задачи**.

► *Чтобы создать задачу поиска уязвимостей в программах, установленных на клиентских устройствах, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Уязвимости в программах**.
2. По ссылке **Настроить поиск уязвимостей** в рабочей области запустите мастер создания задачи поиска уязвимостей и требуемых обновлений.

Откроется окно мастера создания задачи.

3. Следуйте указаниям мастера.

В результате работы мастера создается задача **Поиск уязвимостей и требуемых обновлений**, которая отображается в списке задач в папке **Управляемые устройства** на закладке **Задачи**.

В результате выполнения задачи **Поиск уязвимостей и требуемых обновлений** на Сервере администрирования появится список найденных уязвимостей в программном обеспечении, установленном на устройстве, и необходимые обновления для закрытия обнаруженных уязвимостей.

Агент администрирования получает информацию о доступных обновлениях Windows и программного обеспечения Microsoft от службы Центра обновлений Windows или от Сервера администрирования, в случае если Сервер администрирования используется в роли

WSUS-сервера. Информация передается в момент запуска программ (если это настроено в политике) и периодического запуска задачи **Поиск уязвимостей и требуемых обновлений** на клиентских устройствах.

Вы можете получить сведения о программном обеспечении сторонних производителей, которое можно обновлять с помощью Kaspersky Security Center, на веб-сайте Службы технической поддержки на странице Kaspersky Security Center в разделе Управление Сервером (<http://support.kaspersky.ru/9327>).

Заккрытие уязвимостей в программах

Если в мастере первоначальной настройки в окне **Параметры управления обновлениями** вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача **Установка требуемых обновлений и закрытие уязвимостей** создается автоматически. Задача отображается в папке **Управляемые устройства** на закладке **Задачи**.

► *Чтобы создать задачу закрытия уязвимостей с помощью доступных обновлений для программ, выполните следующие действия:*

1. В дереве консоли выберите папку **Управляемые устройства** на закладке **Задачи**.
2. По ссылке **Создать задачу** запустите мастер создания задачи.
3. В окне мастера **Выбор типа задачи** укажите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.
4. Следуйте указаниям мастера.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

► *Чтобы закрыть выбранную уязвимость с помощью доступных обновлений для программы, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Уязвимости в программах**.
2. В папке **Обновления программного обеспечения** нажмите на кнопку **Запустить мастер закрытия уязвимости**.

Откроется мастер закрытия уязвимости.

Функционал мастера закрытия уязвимости доступен при наличии лицензии на функциональность Системное администрирование.

3. Следуйте указаниям мастера.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**, или правило для закрытия уязвимости будет добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

Обновления программного обеспечения

Kaspersky Security Center позволяет управлять обновлениями программного обеспечения, установленного на клиентских устройствах, и закрывать уязвимости в программах Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи поиска обновлений и загружает обновления в хранилище обновлений. После завершения поиска обновлений программа предоставляет администратору информацию о доступных обновлениях и об уязвимостях в программах, которые можно закрыть с помощью этих обновлений.

Информация о доступных обновлениях Microsoft Windows передается из центра обновлений Windows. Сервер администрирования может использоваться в роли сервера Windows Update (WSUS). Для использования Сервера администрирования в роли сервера Windows Update необходимо настроить синхронизацию обновлений с центром обновлений Windows. После настройки синхронизации данных с центром обновлений Windows Сервер администрирования с заданной периодичностью централизованно предоставляет обновления службам Windows Update на устройствах.

Управлять обновлениями программного обеспечения можно также с помощью политики Агента администрирования. Для этого необходимо создать политику Агента

администрирования и настроить параметры обновлений программного обеспечения в соответствующих окнах мастера создания политики.

Администратор может просматривать список доступных обновлений в папке **Обновления программного обеспечения**, входящей в состав папки **Управление программами**. Эта папка содержит список полученных Сервером администрирования обновлений программ Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства. После просмотра информации о доступных обновлениях администратор может выполнить установку обновлений на устройства.

Обновление некоторых программ Kaspersky Security Center выполняется путем удаления предыдущей версии программы и установки новой версии.

Перед установкой обновлений на все устройства можно выполнить проверочную установку, чтобы убедиться, что установленные обновления не вызовут сбоев в работе программ на устройствах.

Вы можете получить сведения о программном обеспечении сторонних производителей, которое можно обновлять с помощью Kaspersky Security Center, на веб-сайте Службы технической поддержки на странице Kaspersky Security Center в разделе Управление Сервером (<http://support.kaspersky.ru/9327>).

В этом разделе

Просмотр информации о доступных обновлениях.....	271
Синхронизация обновлений Windows Update с Сервером администрирования	272
Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства..	282
Офлайн-модель получения обновлений.....	284
Включение и выключение офлайн-модели получения обновлений.....	286
Установка обновлений на устройства вручную	288
Настройка обновлений Windows в политике Агента администрирования	291
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center.....	293
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	295
Отмена обновлений программного обеспечения	296

Просмотр информации о доступных обновлениях

- *Чтобы просмотреть список доступных обновлений для программ, установленных на клиентских устройствах,*

в дереве консоли в папке **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.

В рабочей области папки вы можете просматривать список имеющихся обновлений для программ, установленных на устройствах.

► *Чтобы просмотреть свойства обновления,*

в рабочей области папки **Обновления программного обеспечения** в контекстном меню обновления выберите пункт **Свойства**.

В окне свойств обновления для просмотра доступна следующая информация:

- список клиентских устройств, для которых применимо обновление;
- список общесистемных компонентов (прerequisites), которые требуется установить перед установкой обновления (если такие компоненты есть);
- уязвимости в программах, которые закрывает это обновление.

Синхронизация обновлений Windows Update с Сервером администрирования

Если в мастере первоначальной настройки в окне **Параметры управления обновлениями** вы выбрали вариант **Использовать Сервер администрирования в роли WSUS-сервера**, задача синхронизации обновлений Windows Update создается автоматически. Запустить задачу можно в папке **Задачи**. Функциональность обновления программного обеспечения Microsoft доступна только после успешного завершения задачи **Синхронизация обновлений Windows Update**.

Задача **Синхронизация обновлений Windows Update** загружает с серверов Microsoft только метаданные. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

► *Чтобы создать задачу синхронизации обновлений Windows Update с Сервером администрирования, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить синхронизацию обновлений Windows Update**.

В результате работы мастера создается задача **Синхронизация обновлений Windows Update**, которая отображается в папке **Задачи**.

Запустится мастер создания задачи получения данных из центра обновлений Windows. Следуйте указаниям мастера.

Задачу синхронизации обновлений Windows Update также можно создать в папке **Задачи** по кнопке **Создать задачу**.

Microsoft периодически удаляет со своих серверов устаревшие обновления так, что число актуальных обновлений составляет от 200 000 до 300 000. В Kaspersky Security Center 10 версии Service Pack 2 Maintenance Release 1 и ниже сохранялись все обновления, устаревшие обновления не удалялись. Это приводило к постоянному росту размера базы данных. Для уменьшения используемого дискового пространства и размера базы данных в Kaspersky Security Center 10 Service Pack 3 реализовано удаление устаревших обновлений, которые отсутствуют на серверах обновления Microsoft.

Во время выполнения задачи **Синхронизация обновлений Windows Update**, программа получает список актуальных обновлений с сервера обновления Microsoft. После чего Kaspersky Security Center определяет список устаревших обновлений. При следующем запуске задачи **Поиск уязвимостей и требуемых обновлений** Kaspersky Security Center отмечает устаревшие обновления и устанавливает время на удаление. При следующем запуске задачи **Синхронизация обновлений Windows Update** удаляются обновления, которые были отмечены на удаление 30 дней назад. Kaspersky Security Center также выполняет дополнительную проверку для удаления устаревших обновлений, которые были отмечены на удаление более 180 дней назад.

После завершения работы задачи **Синхронизация обновлений Windows Update** и удаления устаревших обновлений в базе данных могут оставаться хеш-коды файлов удаленных обновлений, а также соответствующие им файлы в папке %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\working\wusfiles, в случае если они были загружены ранее. С помощью задачи **Обслуживание базы данных** (см. раздел "**Обслуживание базы данных Сервера администрирования**" на стр. [490](#)) можно удалить такие устаревшие записи из базы данных и соответствующих им файлов.

В этом разделе

Шаг 1. Параметры	274
Шаг 2. Программы	275
Шаг 3. Категории обновлений.....	275
Шаг 4. Языки локализации обновлений	275
Шаг 5. Выбор учетной записи для запуска задачи	276
Шаг 6. Настройка расписания запуска задачи	276
Шаг 7. Определение названия задачи	281
Шаг 8. Завершение создания задачи	281

Шаг 1. Параметры

Когда Kaspersky Security Center синхронизирует обновления с серверами Microsoft Windows Update Servers, информация обо всех файлах сохраняется в базе данных Сервера администрирования. Также на диск загружаются все файлы, необходимые для обновления, при взаимодействии с Агентом обновления Windows. В частности, Kaspersky Security Center сохраняет информацию о файлах экспресс-установки в базу данных и загружает их по мере необходимости. Загрузка файлов экспресс-установки приводит к сокращению свободного места на диске.

Чтобы уменьшить сокращение объема дискового пространства и снизить трафик, снимите флажок **Загружать файлы экспресс-установки**.

Если флажок установлен, в процессе выполнения задачи загружаются файлы экспресс-установки.

По умолчанию флажок снят.

Шаг 2. Программы

В этом разделе можно выбрать программы, для которых будут загружаться обновления.

Если установлен флажок **Все программы**, то обновления будут загружаться для всех имеющихся программ, а также для тех программ, которые могут быть выпущены в будущем.

По умолчанию флажок **Все программы** установлен.

Шаг 3. Категории обновлений

В этом разделе можно выбрать категории обновлений, которые будут загружаться на Сервер администрирования.

Если установлен флажок **Все категории**, то обновления будут загружаться для всех имеющихся категорий обновлений, а также для тех категорий, которые могут появиться в будущем.

По умолчанию флажок **Все категории** установлен.

Шаг 4. Языки локализации обновлений

В этом окне можно выбрать языки локализации обновлений, которые будут загружаться на Сервер администрирования. Выберите один из следующих вариантов загрузки языков локализации обновлений:

- **Загружать все языки, включая новые**

Если выбран этот вариант, на Сервер администрирования будут загружаться все доступные языки локализации обновлений. По умолчанию выбран этот вариант.

- **Загружать выбранные языки**

Если выбран этот вариант, в списке можно выбрать языки локализации обновлений, которые должны загружаться на Сервер администрирования.

Шаг 5. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Автоматически созданная учетная запись**

Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

По умолчанию выбран этот вариант.

- **Задать учетную запись:**

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

- **Учетная запись**

Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

Пароль учетной записи, от имени которой будет запускаться задача.

Шаг 6. Настройка расписания запуска задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

В раскрывающемся списке можно выбрать режим запуска задачи. Отображаемые в окне параметры зависят от выбранного режима запуска задачи.

- **Каждый N час**

Если в раскрывающемся списке **Запуск по расписанию** выбран

режим **Каждый N час**, под раскрывающимся списком отображаются поля **Каждый** и **Начать с**. В поле **Каждый** можно задать периодичность запуска задачи в часах, а в поле **Начать с** – дату и время первого запуска задачи.

Например, если в поле **Каждый** установлено значение 2, а в поле **Начать с** – 3 августа 2008 г. 15:00:00, то задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2008 года.

По умолчанию в поле **Каждый** устанавливается значение 1, а в поле **Начать с** устанавливаются текущие системная дата и время устройства.

- **Каждый N день**

Задайте интервал, с которым повторяется запуск (в сутках), и время начала каждого запуска.

- **Каждую N неделю**

Задайте интервал, с которым повторяется запуск (в неделях), а также день и время начала каждого запуска.

- **Каждые N минут**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Каждые N минут**, под раскрывающимся списком отображаются поля **Каждые N минут** и **Начать с**. В поле **Каждые N минут** можно задать периодичность запуска задачи в минутах, а в поле **Начать с** – время первого запуска задачи.

- **Ежедневно**

Если в раскрывающемся списке **Запуск по расписанию** выбран режим **Ежедневно**, под раскрывающимся списком отображаются поля **Каждый N день** и **Время запуска**. В поле **Каждый N день** можно задать периодичность запуска задачи в часах, а в поле **Время запуска** – время первого запуска задачи.

- **Еженедельно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Еженедельно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно указать день недели, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день недели.

Например, если в поле **Каждый** установлено значение Воскресенье, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- **По дням недели**

Установите флажки у тех дней недели, в которые должна запускаться задача, и укажите время начала запуска.

- **Ежемесячно**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Ежемесячно**, под раскрываемым списком отображаются поля **Каждый** и **Время запуска**. В поле **Каждый** можно задать день месяца, в который должна запускаться задача, а в поле **Время запуска** – время запуска задачи в указанный день месяца.

Например, если в поле **Каждый** установлено значение 20, а в поле **Время запуска** – 15:00:00, задача будет запускаться двадцатого числа каждого месяца в 15 часов.

По умолчанию в поле **Каждый** установлено значение 1, а в поле **Время запуска** – текущее системное время устройства.

- **Вручную**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **Вручную**, можно запустить задачу вручную из главного окна программы Kaspersky Security Center при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.

- **Ежемесячно, в указанные дни выбранных недель**

Если в раскрываемом списке **Запуск по расписанию** выбран этот вариант, отображается таблица для настройки расписания запуска

задачи. В таблице можно указать недели и дни месяца, в которые нужно запускать задачу.

Например, если в таблице установлен флажок **Вторая неделя, вторник**, программа будет ежемесячно запускать проверку во второй вторник месяца. В поле **Время запуска** можно указать точное время запуска задачи в выбранные дни.

По умолчанию все флажки сняты.

- **При обнаружении вирусной атаки**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **При обнаружении вирусной атаки**, выполнение задачи начнется при возникновении события Вирусная атака. Под раскрываемым списком можно выбрать программы, которые должны отвечать за обнаружение вирусной атаки. Доступны следующие варианты выбора:

- Антивирусами для рабочих станций и файловых серверов;
- Антивирусами защиты периметра;
- Антивирусами для почтовых систем.

По умолчанию установлены все флажки.

- **По завершении другой задачи**

Если в раскрываемом списке **Запуск по расписанию** выбран режим **По завершении другой задачи**, текущая задача будет запущена после завершения другой задачи. Под раскрываемым списком отображаются следующие параметры запуска задачи:

- **Имя задачи.** В поле можно указать задачу, после завершения которой будет запускаться текущая задача.
- **Результат выполнения.** В раскрываемом списке можно выбрать варианты завершения задачи, указанной в поле **Имя задачи**. Доступны следующие варианты выбора: **Завершена успешно** и **Завершена с ошибкой**.

- **Запускать пропущенные задачи**

Если флажок установлен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Для режимов **Вручную**, **Один раз** и **Немедленно** задача будет запущена сразу после появления устройства в сети.

Если флажок снят, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах.

- **Автоматически определять интервал для распределения запуска задачи**

Если флажок установлен, задача запускается на клиентских устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени. Интервал времени можно изменить в поле **Распределять запуск задачи случайным образом в интервале (мин)**. По умолчанию интервал времени равен одной минуте. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Рассчитанное значение периода запуска задачи изменяется только при изменении параметров задачи или при запуске задачи вручную.

Если флажок снят, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию флажок установлен.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка программы, Исправление уязвимостей).

Распределять запуск задачи случайным образом в интервале (мин) Если флажок установлен, в поле ввода можно указать максимальное время задержки запуска задачи. Распределенный запуск помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования.

По умолчанию флажок снят.

Флажок не активен для задач Сервера администрирования (Загрузка обновлений в хранилище, Обслуживание базы данных, Резервное копирование данных Сервера администрирования, Синхронизация обновлений Windows Update, Рассылка отчета, Удаленная установка программы, Исправление уязвимостей).

Шаг 7. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы (" * < > ? \ : |). По умолчанию задано значение *Синхронизация обновлений Windows Update*.

Шаг 8. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Созданная задача синхронизации обновлений Windows Update отобразится в списке задач в папке **Задачи** дерева консоли.

Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства

Вы можете настроить автоматическое обновление баз и модулей программы Kaspersky Endpoint Security на клиентских устройствах.

► *Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security на устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Создайте задачу с типом **Обновление** одним из следующих способов:
 - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.
 - В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

В результате запускается мастер создания задачи.

3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Обновление** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате работы мастера создается задача обновления для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.

5. В рабочей области папки **Задачи** выберите созданную задачу обновления.
6. В контекстном меню задачи выберите пункт **Свойства**.
7. В окне свойств задачи выберите раздел **Параметры**.

В разделе **Параметры** можно настроить параметры задачи обновления в локальном и автономном режимах:

- **Параметры обновления в локальном режиме:** между устройством и Сервером администрирования установлена связь.

- **Параметры обновления в автономном режиме:** между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).

8. По кнопке **Настройка** выберите источник обновлений.

9. Установите флажок **Загружать обновления модулей программы**, чтобы одновременно с базами программы загружать и устанавливать обновления модулей программы.

Если флажок установлен, то Kaspersky Endpoint Security уведомляет пользователя о доступных обновлениях модулей программы и во время выполнения задачи обновления включает обновления модулей программы в пакет обновлений. Настройте применение модулей обновлений:

- **Устанавливать критические и одобренные обновления.** При наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает обновления со статусом *Предельный* автоматически, а остальные обновления модулей программы – после одобрения их установки администратором.

Чтобы одобрить обновления программного обеспечения, выполните следующие действия:

- а. В дереве консоли откройте папку **Обновления программного обеспечения**.
- б. В окне свойств обновления в разделе **Общие** в поле **Одобрение обновления** установите значение **Одобрено**.

По умолчанию установлено значение **Не определено**.

Если при настройке свойств обновления для программ "Лаборатории Касперского", которое нельзя деинсталлировать, в поле **Одобрение обновления** вы установите значение **Отклонено**, Kaspersky Security Center не будет деинсталлировать такое обновление с устройств, на которые оно было ранее установлено.

Невозможность удаления обновления для программ "Лаборатории Касперского" отображается в окне свойств обновления на закладке **Общие** в поле **Требования при установке**.

- **Устанавливать только утвержденные обновления.** При наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.

Если обновление модулей программы предполагает ознакомление и согласие с положениями Лицензионного соглашения, то программа устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения.

10. Установите флажок **Копировать обновления в папку**, чтобы программа сохраняла загруженные обновления в папку, указанную по кнопке **Обзор**.

11. Нажмите на кнопку **ОК**.

При выполнении задачи **Обновление** программа отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых программ.

Офлайн-модель получения обновлений

Агенты администрирования на управляемых устройствах не всегда могут подключиться к Серверу администрирования для получения обновлений. Например, Агент администрирования может быть установлен на ноутбук, который иногда не подключен к интернету и локальной сети. Также администратор может ограничить время подключения устройств к сети. В таких случаях Агенты администрирования не смогут получить обновления от Сервера администрирования в соответствии с расписанием. Если настроено обновление управляемых программ (например, Kaspersky Endpoint Security) с помощью Агента администрирования, для обновления требуется соединение с Сервером

администрирования. Когда соединение между Агентом администрирования и Сервером администрирования отсутствует, обновление невозможно. Соединение Агента администрирования с Сервером может быть настроено так, чтобы Агент подключался к Серверу только в определенные периоды времени. В худшем случае, если настроенные периоды подключения "пересекаются" с периодами, когда связь отсутствует, базы никогда не будут обновлены. Также возможны ситуации, когда много управляемых программ одновременно обращаются к Серверу администрирования за обновлениями. В этом случае Сервер администрирования может перестать отвечать на запросы (как во время DDoS-атаки).

Во избежание описанных проблем в Kaspersky Security Center реализована офлайн-модель получения обновления баз и модулей управляемых программ. Эта модель обеспечивает надежность механизма распространения обновлений вне зависимости от временных проблем недоступности каналов связи сервера администрирования, а также снижает нагрузку на Сервер администрирования.

Как работает офлайн-модель получения обновлений

Каждый раз, когда Сервер администрирования получает обновления, он оповещает Агенты администрирования о том, какие обновления потребуются для управляемых программ. Когда Агенты администрирования получают информацию о том, какие обновления скоро потребуют управляемые программы, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. Чтобы распределить нагрузку на Сервер администрирования, Агенты администрирования начинают подключаться к Серверу и загружать обновления случайным образом в течение интервала времени, определенного Сервером. Интервал времени зависит от количества Агентов администрирования, которые загружают обновления, и от размера обновлений. После того как Агент администрирования на устройстве загрузит все обновления, обновления становятся доступными для программ на устройстве.

Для снижения нагрузки на Сервер администрирования вы можете использовать Агенты администрирования в качестве агентов обновлений.

Когда управляемая программа на устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемой программы, Агент администрирования не подключается к Серверу

администрирования и предоставляет управляемой программе обновления из локального кеша. Соединение с Сервером администрирования при этом может отсутствовать, но оно и не требуется для обновления. В противном случае установка обновлений осуществляется в обычном режиме, согласно расписанию задачи получения обновлений.

По умолчанию офлайн-модель получения обновлений включена.

Офлайн-модель получения обновлений используется только для тех управляемых устройств, на которых задача получения обновлений управляемыми программами имеет расписание "По завершении серверной задачи получения обновлений". Для остальных управляемых устройств используется традиционная система получения обновлений с Сервера администрирования в реальном времени.

Рекомендуется выключить офлайн-модель получения обновлений через настройки политик Агента администрирования соответствующих групп администрирования, если в управляемых программах настроено получение обновлений не с Сервера администрирования, а с серверов "Лаборатории Касперского" либо из сетевой папки и при этом задача получения обновлений имеет расписание "По завершении серверной задачи получения обновлений".

Включение и выключение офлайн-модели получения обновлений

Не рекомендуется выключать офлайн-модель получения обновлений. Выключение может привести к сбоям в доставке обновлений на устройства. В некоторых случаях специалист технической поддержки "Лаборатории Касперского" может посоветовать вам снять флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее**; тогда необходимо будет убедиться, что настроена задача получения обновлений для программ "Лаборатории Касперского".

► *Чтобы включить или выключить офлайн-модель получения обновлений для группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить офлайн-модель получения обновлений.
2. В рабочей области группы откройте закладку **Политики**.

3. На закладке **Политики** выберите политику Агента администрирования.

4. В контекстном меню политики выберите пункт **Свойства**.

Откроется окно свойств политики Агента администрирования.

5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.

6. Установите или снимите флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее**, чтобы включить или выключить офлайн-модель получения обновлений соответственно.

По умолчанию офлайн-модель получения обновлений включена.

В результате офлайн-модель получения обновлений будет включена или выключена.

► *Чтобы включить или выключить офлайн-модель получения обновлений одновременно для всех групп администрирования, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.

2. Перейдите в раздел:

- для 64-разрядной системы:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\1093\1.0.0.0\ServerFlags
```

- для 32-разрядной системы:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Components\34\1093\1.0.0.0\ServerFlags
```

3. Для ключа SrvDisableOfflineUpdates (DWORD) установите одно из значений: 0 – чтобы включить офлайн-модель получения обновлений; 1 – чтобы выключить офлайн-модель получения обновления.

По умолчанию для этого ключа указано значение 0 (офлайн-модель получения обновлений включена).

4. Перезапустите службу Сервера администрирования.

В результате офлайн-модель получения обновлений будет включена или выключена для всех групп администрирования.

Установка обновлений на устройства вручную

Если в мастере первоначальной настройки в окне **Параметры управления обновлениями** вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача **Установка требуемых обновлений и закрытие уязвимостей** создается автоматически. Остановить или запустить задачу можно в папке **Управляемые устройства** на закладке **Задачи**.

Если в мастере первоначальной настройки вы выбрали вариант **Искать требующиеся для установки обновления**, вы можете установить обновления программного обеспечения на клиентские устройства с помощью задачи **Установка требуемых обновлений и закрытие уязвимостей**.

► *Чтобы создать задачу установки обновлений, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В папке **Обновления программного обеспечения** откройте контекстное меню обновления и выберите пункт **Установить обновление** → **Новая задача**, или воспользуйтесь ссылкой **Установить обновление (создать задачу)** в блоке работы с выделенными обновлениями.

Откроется мастер создания задачи установки обновлений и закрытия уязвимостей.

3. Следуйте указаниям мастера.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

В параметрах задачи установки обновлений и закрытия уязвимостей вы можете разрешить автоматическую установку общесистемных компонентов (пререквизитов), которые

необходимо установить перед установкой обновлений. В этом случае перед установкой обновления будет выполнена установка всех необходимых общесистемных компонентов. Список этих компонентов можно посмотреть в свойствах обновления.

В параметрах задачи установки обновлений и закрытия уязвимостей вы можете разрешить установку таких обновлений, в результате которых будет установлена новая версия программы.

Если в параметрах задачи настроены правила установки обновлений сторонних производителей, Сервер администрирования загружает с сайта производителей требуемые обновления. Обновления сохраняются в хранилище Сервера администрирования и далее распространяются и устанавливаются на устройства, где они применимы.

Если в параметрах задачи настроены правила установки обновлений Microsoft и Сервер администрирования используется в качестве WSUS-сервера, Сервер администрирования загружает необходимые обновления в хранилище и далее распространяет на управляемые устройства. Если в сети не используется WSUS-сервер, каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

► *Чтобы создать задачу установки выбранного обновления, выполните следующие действия:*

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В папке **Обновления программного обеспечения** нажмите на кнопку **Запустить мастер установки обновления**.

Откроется мастер установки обновления.

Функционал мастера установки обновлений доступен при наличии лицензии на функциональность Системное администрирование.

3. Следуйте указаниям мастера.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**, или новое правило для установки обновления будет добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

После установки новой версии программы может быть нарушена работа других программ, установленных на устройствах и зависящих от работы обновляемой программы.

В параметрах задачи установки обновлений вы можете настроить проверочную установку обновлений.

► *Чтобы настроить проверочную установку обновлений, выполните следующие действия:*

1. В дереве консоли в папке **Управляемые устройства** на закладке **Задачи** выберите задачу **Установка требуемых обновлений и закрытие уязвимостей**.
2. В контекстном меню задачи выберите пункт **Свойства**.

Откроется окно свойств задачи **Установка требуемых обновлений и закрытие уязвимостей**.

3. В окне свойств задачи в разделе **Проверочная установка** выберите один из доступных вариантов проверочной установки:
 - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.
 - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.
 - **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.
 - **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

4. При выборе всех вариантов кроме первого в поле **Время для принятия решения о продолжении установки (ч.)** укажите количество часов, которое должно пройти после проверочной установки обновлений до начала установки обновлений на все устройства.

Настройка обновлений Windows в политике Агента администрирования

► *Чтобы настроить обновления Windows в политике Агента администрирования, выполните следующие действия:*

1. В папке **Управляемые устройства** на закладке **Политики** выберите политику Агента администрирования.
2. В контекстном меню политики выберите пункт **Свойства**.

Откроется окно свойств политики Агента администрирования.

3. В окне свойств политики выберите раздел **Обновления и уязвимости в программах**.
4. Установите флажок **Использовать Сервер администрирования в роли WSUS-сервера**, чтобы загружать обновления Windows на Сервер администрирования и затем распространять обновления на клиентские устройства с помощью Агентов администрирования.

Если флажок снят, обновления Windows не загружаются на Сервер администрирования. В этом случае клиентские устройства получают обновления Windows самостоятельно.

5. Выберите режим поиска обновлений Windows Update:
 - **Активный.** Сервер администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от агента обновлений Windows.
 - **Пассивный.** В этом режиме Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при

последней синхронизации агента обновлений Windows с источником обновлений. Если синхронизация агента обновлений Windows с источником обновлений не выполняется, данные об обновлениях на Сервере администрирования устаревают.

- **Выключен.** Сервер администрирования не получает информацию об обновлениях.
6. Установите флажок **Проверять исполняемые файлы на наличие уязвимостей при запуске**, чтобы при запуске исполняемых файлов выполнять их проверку на наличие уязвимостей.
 7. Нажмите на кнопку **Применить**.

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Автоматическая установка обновлений для компонентов Kaspersky Security Center включена по умолчанию при установке Агента администрирования на устройство. Вы можете выключить ее при установке Агента администрирования или же выключить позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при локальной установке Агента администрирования на устройство, выполните следующие действия:*

1. Запустите локальную установку Агента администрирования на устройство.
2. На шаге **Дополнительные параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.
3. Следуйте далее указаниям мастера.

На устройстве будет установлен Агент администрирования с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при установке Агента администрирования на устройство с помощью инсталляционного пакета, выполните следующие действия:*

1. В дереве консоли выберите папку **Удаленная установка** → **Инсталляционные пакеты**.
2. В контекстном меню пакета **Агент администрирования Kaspersky Security Center <номер версии>** выберите пункт **Свойства**.
3. В свойствах инсталляционного пакета в разделе **Параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center 10 со статусом "Не определено"**.

Агент администрирования будет устанавливаться из этого пакета с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят), впоследствии вы можете выключить (включить) автоматическую установку с помощью политики Агента администрирования.

► *Чтобы включить или выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center с помощью политики Агента администрирования, выполните следующие действия:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить или выключить автоматическую установку обновлений и патчей.
2. В рабочей области группы откройте закладку **Политики**.
3. На закладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

Откроется окно свойств политики Агента администрирования.

5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center 10 со статусом "Не определено"**, чтобы соответственно включить или выключить автоматическую установку.
7. Установите "замок" при этом флажке.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center будет включена (выключена) на этих устройствах.

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center

По умолчанию автоматически устанавливаются загруженные обновления и патчи для следующих компонентов программы (начиная с версии Kaspersky Security Center 10 Service Pack 2):

- Сервер администрирования.
- Агент администрирования.
- Консоль администрирования.
- Сервер мобильных устройств Exchange ActiveSync.
- Сервер iOS MDM.

Вы можете выключить автоматическую установку обновлений и патчей для этих компонентов. В этом случае загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

► *Чтобы одобрить обновления программного обеспечения, выполните следующие действия:*

1. В дереве консоли выберите узел **Дополнительно** → **Управление программами** → **Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** нажмите на ссылку **Обновить** вверху справа и дождитесь загрузки списка обновлений.
3. Выберите необходимые обновления.
4. В раскрывающемся списке **Одобрение обновления** выберите значение **Одобрено**.

Обновление будет поставлено в очередь на установку.

Отмена обновлений программного обеспечения

► *Чтобы отменить установленное обновление, выполните следующие действия:*

1. В дереве консоли выберите узел **Дополнительно** → **Управление программами** → **Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** нажмите на ссылку **Обновить** вверху справа и дождитесь загрузки списка обновлений.
3. Выберите необходимые обновления.
4. В раскрывающемся списке **Одобрение обновления** выберите значение **Отклонено**.

Обновления, для которых вы установили статус **Отклонено**, будут деинсталлированы (если это возможно) на устройствах, на которые они были установлены ранее, и не будут установлены на те устройства, на которые они еще не были установлены.

Некоторые обновления для программ "Лаборатории Касперского" невозможно деинсталлировать. Если вы установите для них статус **Отклонено**, Kaspersky Security Center не будет деинсталлировать такие обновления с устройств, на которые они были ранее установлены, но обновления не будут установлены на те устройства, на которые они не были ранее установлены.

Если вы устанавливаете статус **Отклонено** для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить их, вы можете сделать это вручную локально.

Удаленная установка приложений на устройства с установленным Агентом администрирования

Если на устройстве установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом устройстве можно обновлять версию Агента администрирования, а также устанавливать, обновлять или удалять с помощью Агента администрирования любые поддерживаемые приложения.

Эта функция включается флажком **С помощью Агента администрирования** в свойствах задачи удаленной установки приложений.

Если флажок установлен, то передача на устройства инсталляционных пакетов с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентом администрирования и Сервером администрирования.

Для оптимизации нагрузки на Сервер администрирования и минимизации трафика между Сервером администрирования и устройствами целесообразно назначать в каждой удаленной сети или в каждом ширококонтентном домене агенты обновлений (см. разделы "Роль агентов обновлений" и "Построение структуры групп администрирования и назначение агентов обновлений"). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на устройства через агенты обновлений.

Также с использованием агентов обновлений можно выполнять ширококонтентную (многоадресную) рассылку инсталляционных пакетов, что позволяет многократно снизить сетевой трафик в ходе развертывания приложений.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования, подготовленные к передаче инсталляционные пакеты дополнительно кешируются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\working\FTServer. При использовании большого числа различных инсталляционных пакетов большого размера, и

при большом количестве агентов обновлений размер этой папки может существенно увеличиваться.

Удалять файлы из папки FTServer вручную нельзя. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые агентами обновлений, сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\FTCITmp.

Удалять файлы из папки \$FTCITmp вручную нельзя. По мере завершения задач, использующих данные из папки, содержимое этой папки будет удаляться автоматически.

Поскольку инсталляционные пакеты распространяются по каналам связи между Сервером администрирования и Агентами администрирования из промежуточного хранилища в оптимизированном для передачи по сети формате, нельзя вносить изменения в инсталляционные пакеты в исходной папке инсталляционного пакета. Такие изменения не будут автоматически учтены Сервером администрирования. Если необходимо изменить вручную файлы инсталляционных пакетов (хотя делать это не рекомендуется), нужно обязательно изменить какие-либо параметры инсталляционного пакета в Консоли администрирования. Изменение параметров инсталляционного пакета в Консоли администрирования заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

Управление мобильными устройствами

В этом разделе описано управление мобильными устройствами, подключенными к Серверу администрирования.

В этом разделе

О групповой политике управления EAS и iOS MDM-устройствами	299
Поддержка мобильных устройств	301
Работа с командами для мобильных устройств	307
Работа с сертификатами	315
Добавление мобильных устройств в список управляемых устройств.....	324
Управление мобильными устройствами Exchange ActiveSync	334
Управление iOS MDM-устройствами.....	343
Управление KES-устройствами.....	364

О групповой политике управления EAS и iOS MDM-устройствами

Для управления iOS MDM и EAS-устройствами вы можете использовать плагин управления Kaspersky Device Management для iOS, входящий в комплект поставки Kaspersky Security Center. Kaspersky Device Management для iOS позволяет создавать групповые политики для настройки конфигурационных параметров iOS MDM и EAS-устройств без использования iPhone® Configuration Utility и профиля управления Exchange Active Sync.

Групповая политика управления EAS и iOS MDM-устройствами предоставляет администратору следующие возможности:

- для управления EAS-устройствами:
 - настраивать параметры пароля для разблокирования устройства;
 - настраивать хранение данных на устройстве в зашифрованном виде;
 - настраивать параметры синхронизации корпоративной почты;

- настраивать аппаратные функции мобильных устройств, например, использование съемных дисков, использование камеры, использование Bluetooth;
- настраивать ограничения для использования мобильных приложений на устройстве.
- для управления iOS MDM-устройствами:
 - настраивать параметры безопасности использования пароля на устройстве;
 - настраивать ограничения для использования аппаратных функций устройства, а также ограничения на установку, удаление мобильных приложений;
 - настраивать ограничения для использования на устройстве встроенных мобильных приложений, например, YouTube™, iTunes® Store, Safari;
 - настраивать ограничения просмотра медиаконтента (например, фильмов и тв-шоу) по региону местоположения устройства;
 - настраивать параметры подключения устройства к интернету через прокси-сервер (Глобальный HTTP-прокси);
 - настраивать параметры единой учетной записи, с помощью которой пользователь может получить доступ к корпоративным приложениям и сервисам (технология единого входа);
 - контролировать использование интернета (посещение веб-сайтов) на мобильных устройствах;
 - настраивать параметры беспроводных сетей (Wi-Fi), точек доступа (APN), виртуальных частных сетей (VPN) с использованием различных механизмов аутентификации и сетевых протоколов;
 - настраивать параметры подключения к устройствам AirPlay® для потоковой передачи фотографий, музыки и видео;
 - настраивать параметры подключения к принтерам AirPrint™ для печати документов с устройства беспроводным способом;

- настраивать параметры синхронизации с сервером Microsoft Exchange, а также учетные записи пользователей для использования корпоративной почты на устройствах;
- настраивать учетные данные пользователя для синхронизации со службой каталогов LDAP;
- настраивать учетные данные пользователя для подключения к сервисам CalDAV и CardDAV, что позволяет пользователю использовать корпоративные календари и списки контактов;
- настраивать параметры интерфейса iOS на устройстве пользователя, например, шрифты или иконки для избранных веб-сайтов;
- добавлять новые сертификаты безопасности на устройство;
- настраивать параметры SCEP-сервера для автоматического получения устройством сертификатов из Центра сертификации;
- добавление собственных параметров для работы мобильных приложений.

Особенностью политики управления EAS и iOS MDM-устройствами является то, что она назначается на группу администрирования, в которую входят Сервер мобильных устройств iOS MDM и Сервер мобильных устройств Exchange ActiveSync (далее серверы мобильных устройств). Все параметры, заданные в этой политике, вначале распространяются на серверы мобильных устройств, затем на мобильные устройства, которыми они управляют. В случае использования иерархической структуры групп администрирования подчиненные серверы мобильных устройств получают параметры политики с главных серверов мобильных устройств и распространяют их на мобильные устройства.

Подробные сведения о работе групповой политики управления EAS и iOS MDM-устройствами в Консоли администрирования Kaspersky Security Center приведены в онлайн-справке Kaspersky Security 10 для мобильных устройств <https://help.kaspersky.com/KESMob/10SP3MR1/ru-RU/141410.htm>.

Поддержка мобильных устройств

Управление защитой мобильными устройствами через Kaspersky Security Center

выполняется с помощью компонента Поддержка мобильных устройств. Поддержка мобильных устройств добавляет компоненты, необходимые для управления мобильными устройствами через Kaspersky Security Center.

Включать поддержку мобильных устройств необходимо, если вы планируете управлять мобильными устройствами сотрудников вашей организации. Если вы не используете защиту мобильных устройств в вашей организации, выключите поддержку мобильных устройств.

Раздел содержит инструкции по включению и выключению поддержки мобильных устройств, а также по настройке параметров поддержки мобильных устройств.



В этом разделе

Включение поддержки мобильных устройств.....	302
Изменение параметров поддержки мобильных устройств	304
Выключение поддержки мобильных устройств	306

Включение поддержки мобильных устройств

Для управления мобильными устройствами необходимо включить поддержку мобильных устройств. Если поддержка мобильных устройств не была включена в мастере первоначальной настройки, вы можете включить ее позже. Для управления мобильными устройствами необходима лицензия на функциональность Управления мобильными устройствами.

Включение поддержки мобильных устройств доступно только на главном Сервере администрирования.

► *Чтобы включить поддержку мобильных устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Управление мобильными устройствами**.

2. В рабочей области папки нажмите на кнопку **Включить управление мобильными устройствами**.

Отобразится окно **Дополнительные компоненты** мастера первоначальной настройки Сервера администрирования.

3. Выберите пункт **Включить поддержку мобильных устройств**, чтобы управлять мобильными устройствами.

4. В окне **Выбор способа активации программы** произведите активацию программы с помощью файла ключа или кода активации.

Управление мобильными устройствами будет недоступно без активации функциональности Управление мобильными устройствами.

5. В окне **Параметры прокси-сервера для доступа к сети Интернет** установите флажок **Использовать прокси-сервер**, если вы хотите включить возможность использования прокси-сервера для подключения к интернету. Если флажок установлен, доступны поля ввода параметров. Настройте параметры подключения к прокси-серверу.

6. В окне **Проверка обновлений для плагинов и инсталляционных пакетов** выберите один из следующих вариантов:

- **Проверить актуальность плагинов и инсталляционных пакетов**

Запуск проверки на актуальность. Если проверка обнаружит использование устаревших версий плагинов или инсталляционных пакетов, мастер предложит загрузить актуальные версии вместо устаревших.

- **Пропустить проверку**

Продолжение работы без проверки плагинов и инсталляционных пакетов на актуальность. Этот вариант можно выбрать, например, если у вас нет доступа в интернет или вы по какой-то причине хотите продолжить пользоваться устаревшей версией программы.

Пропуск проверки актуальности плагинов может привести к некорректной работе программы.

7. В окне **Доступные последние версии плагинов** загрузите и установите последние версии плагинов на необходимом вам языке. Обновление версий плагинов не требует наличия лицензии.

После установки плагинов и пакетов программа проверяет, все ли необходимые плагины для корректной работы мобильных устройств были установлены. Если проверка обнаружит использование устаревших версий плагинов, мастер предложит загрузить актуальные версии вместо устаревших.

8. В окне **Параметры подключения мобильных устройств** настройте порты Сервера администрирования.

После завершения работы мастера будут выполнены следующие изменения:

- создана политика Kaspersky Endpoint Security для Android;
- создана политика Kaspersky Device Management для iOS;
- открыты порты для подключения мобильных устройств.

Изменение параметров поддержки мобильных устройств

- *Чтобы изменить параметры поддержки мобильных устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки нажмите на ссылку **Порты подключения для мобильных устройств**.

Отобразится раздел **Дополнительные порты** окна свойств Сервера администрирования.

3. В разделе **Дополнительные порты** измените необходимые вам параметры.

- **SSL-порт для прокси-сервера активации**

Номер SSL-порта для подключения Kaspersky Endpoint Security 10 для Windows к серверам активации "Лаборатории Касперского".

По умолчанию используется порт 17000.

- **Открыть порт для мобильных устройств**

Если флажок установлен, на Сервере администрирования будет открыт порт для мобильных устройств.

Использование порта для мобильных устройств возможно только в случае, если установлен компонент Поддержка мобильных устройств.

Если флажок снят, порт для мобильных устройств на Сервере администрирования не используется.

По умолчанию флажок снят.

- **Порт для мобильных устройств**

Номер порта, по которому осуществляется подключение мобильных устройств к Серверу администрирования. По умолчанию используется порт 13292.

Используется десятичная форма записи.

- **Порт активации мобильных клиентов**

Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

По умолчанию используется порт 17100.

4. Нажмите на кнопку **ОК**.

Выключение поддержки мобильных устройств

Выключение поддержки мобильных устройств доступно только на главном Сервере администрирования.

► *Чтобы выключить поддержку мобильных устройств, выполните следующие действия:*

1. В дереве консоли выберите папку **Управление мобильными устройствами**.
2. В рабочей области папки нажмите на ссылку **Настроить дополнительные компоненты**.

Отобразится окно **Дополнительные компоненты** мастера первоначальной настройки Сервера администрирования.

3. Выберите пункт **Поддержка мобильных устройств не требуется**, если вы больше не хотите управлять мобильными устройствами.
4. Нажмите на кнопку **ОК**.

Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования. Порт подключения мобильных устройств и порт активации мобильных клиентов будут закрыты автоматически.

Созданные политики Kaspersky Endpoint Security для Android и Kaspersky Device Management для iOS не удаляются. Правила выпуска сертификатов не изменяются. Установленные плагины не удаляются. Правило перемещения мобильных устройств не удаляется.

После повторного включения поддержки мобильных устройств на управляемых мобильных устройствах может потребоваться переустановка мобильных приложений, которые необходимы для управления мобильными устройствами.

Работа с командами для мобильных устройств

Этот раздел содержит информацию о командах для управления мобильными устройствами, которые поддерживает программа. В разделе приведены инструкции по отправке команд на мобильные устройства, а также по просмотру статуса выполнения команд в журнале команд.

В этом разделе

Команды для управления мобильными устройствами.....	307
Использование Google Firebase Cloud Messaging	311
Отправка команд	313
Просмотр статусов команд в журнале команд	314

Команды для управления мобильными устройствами

Kaspersky Security Center поддерживает команды для управления мобильными устройствами.

Команды используются для дистанционного управления мобильными устройствами. Например, в случае потери мобильного устройства с помощью команды можно удалить корпоративные данные с устройства.

Вы можете использовать команды для следующих типов управляемых мобильных устройств:

- iOS MDM-устройства;
- KES-устройства;
- EAS-устройства.

Каждый тип устройства поддерживает свой набор команд.

Особенности некоторых команд

- Для всех типов устройств в случае успешного выполнения команды **Сбросить настройки до заводских** все данные будут удалены с устройства, настройки устройства будут сброшены до заводских.
- Для iOS MDM-устройства в случае успешного выполнения команды **Удалить корпоративные данные** с устройства будут удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.
- Для KES-устройства в случае успешного выполнения команды **Удалить корпоративные данные** с устройства будут удалены корпоративные данные, записи в Kontakтах, история SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google™. Для KES-устройства дополнительно будут удалены данные с карты памяти.
- Перед отправкой команды **Определить местоположение** на KES-устройство вам потребуется подтвердить, что вы используете эту команду для санкционированного поиска потерянного устройства, принадлежащего вашей организации или одному из сотрудников. При использовании Kaspersky Security Center версии Service Pack 2 Maintenance Release 1 и более ранних версий мобильное устройство, на которое отправлена команда **Определить местоположение**, блокируется. В Kaspersky Security Center 10 Service Pack 3 блокировка устройства не происходит.

Список команд для мобильных устройств

В таблице ниже приведен список команд для каждого типа устройства.

Таблица 3. Список поддерживаемых команд

Тип мобильного устройства	Команды	Результат выполнения команды
iOS MDM-устройство	Заблокировать	Мобильное устройство заблокировано.
	Разблокировать	Выключена блокировка мобильного устройства PIN-кодом. Установленный ранее PIN-код сброшен.
	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки устройства сброшены до заводских.
	Удалить корпоративные данные	Удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок Удалять вместе с iOS MDM-профилем .
	Синхронизировать устройство	Данные мобильного устройства синхронизированы с Сервером администрирования.
	Установить профиль	Конфигурационный профиль установлен на мобильное устройство.
	Удалить профиль	Конфигурационный профиль удален с мобильного устройства.
	Установить provisioning-профиль	Provisioning-профиль установлен на мобильное устройство.
	Удалить provisioning-профиль	Provisioning-профиль удален с мобильного устройства.

Тип мобильного устройства	Команды	Результат выполнения команды
	Установить приложение	Приложение установлено на мобильное устройство.
	Удалить приложение	Приложение удалено с мобильного устройства.
	Вести код погашения	Введен код погашения для платного приложения.
	Настроить роуминг	Включен или выключен роуминг данных и голосовой роуминг.
	Установить Kaspersky Safe Browser	Приложение Kaspersky Safe Browser установлено на мобильное устройство.
KES-устройство	Заблокировать	Мобильное устройство заблокировано.
	Разблокировать	Выключена блокировка мобильного устройства PIN-кодом. Установленный ранее PIN-код сброшен.
	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских.
	Удалить корпоративные данные	Удалены корпоративные данные, записи в Kontakтах, история SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google. Удалены данные с карты памяти.

Тип мобильного устройства	Команды	Результат выполнения команды
	Синхронизировать устройство	Данные мобильного устройства синхронизированы с Сервером администрирования.
	Определить местоположение	Местоположение мобильного устройства определено и показано на Google Картах™. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
	Сфотографировать	Мобильное устройство заблокировано. Фотография выполнена фронтальной камерой устройства и сохранена на Сервере администрирования. Фотографии доступны для просмотра в журнале команд. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
	Воспроизвести звуковой сигнал	Мобильное устройство воспроизводит звуковой сигнал.
EAS-устройство	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки устройства сброшены до заводских.

Использование Google Firebase Cloud Messaging

Для своевременной доставки команд на KES-устройства под управлением операционной системы Android в Kaspersky Security Center используется механизм push-нотификаций.

Push-нотификации между KES-устройствами и Сервером администрирования осуществляются с помощью сервиса Google Firebase Cloud Messaging. В Консоли администрирования Kaspersky Security Center вы можете указать параметры сервиса Google Cloud Messaging, чтобы подключить KES-устройства к этому сервису.

Для получения параметров Google Firebase Cloud Messaging администратору необходимо иметь учетную запись Google. Более подробную информацию о получении параметров Google Firebase Cloud Messaging см. в статье Базы знаний на веб-сайте Службы технической поддержки <http://support.kaspersky.ru/11770>.

► *Чтобы настроить параметры Google Firebase Cloud Messaging, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
В результате откроется окно свойств папки **Мобильные устройства**.
3. Выберите раздел **Параметры Google Firebase Cloud Messaging**.
4. В поле **Идентификатор отправителя** укажите номер проекта Google API, полученный вами при создании проекта в консоли разработчика Google.
5. В поле **Ключ сервера** введите обычный ключ сервера, который вы создали в консоли разработчика Google.

При следующей синхронизации с Сервером администрирования KES-устройства под управлением операционной системы Android будут подключены к службе Google Firebase Cloud Messaging.

Вы можете изменить параметры Google Firebase Cloud Messaging по кнопке **Сбросить параметры**.

Отправка команд

► Чтобы отправить команду на мобильное устройство пользователя, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. Выберите мобильное устройство пользователя, на которое нужно отправить команду.
3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
4. В окне **Команды для управления мобильным устройством** перейдите в раздел с названием команды, которую нужно отправить на мобильное устройство, и нажмите на кнопку **Отправить команду**.

В зависимости от выбранной команды после нажатия на кнопку **Отправить команду** может открыться окно настройки дополнительных параметров команды. Например, при отправке команды на удаление с мобильного устройства provisioning-профиля программа предлагает выбрать provisioning-профиль, который нужно удалить с мобильного устройства. Укажите в окне дополнительные параметры команды и подтвердите свой выбор. После этого команда будет отправлена на мобильное устройство.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

5. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Просмотр статусов команд в журнале команд

Программа сохраняет информацию о всех командах, отправленных на мобильные устройства, в журнале команд. В журнале команд сохраняется информация о времени и дате отправления команд на мобильное устройство, статусы команд, а также подробные описания результатов выполнения команд. Например, в случае неудачного выполнения команды в журнале отображается причина ошибки. Записи в журнале команд хранятся не более 30 дней.

Команды, отправленные на мобильные устройства, могут иметь следующие статусы:

- *Выполняется* – команда отправлена на мобильное устройство.
- *Завершена* – выполнение команды успешно завершено.
- *Завершена с ошибкой* – выполнить команду не удалось.
- *Удаляется* – команда удаляется из очереди команд, отправленных на мобильное устройство.
- *Удалена* – команда успешно удалена из очереди команд, отправленных на мобильное устройство.
- *Удаление завершено с ошибкой* – команду не удалось удалить из очереди команд, отправленных на мобильное устройство.

Программа ведет журнал команд для каждого мобильного устройства.

► *Чтобы просмотреть журнал команд, отправленных на мобильное устройство, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. Выберите в списке мобильное устройство, для которого вы хотите просмотреть журнал команд.

3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

Откроется окно **Команды для управления мобильным устройством**. Разделы окна **Команды для управления мобильным устройством** соответствуют командам, которые можно отправить на мобильное устройство.

4. Выбирайте разделы с нужными вам командами и просматривайте информацию об отправке и выполнении команд в блоке **Журнал команд**.

В блоке **Журнал команд** можно просмотреть список команд, отправленных на мобильное устройство, и информацию о командах. С помощью фильтра **Показать команды** можно показывать в списке только команды с выбранным статусом.

Работа с сертификатами

Этот раздел содержит информацию о работе с сертификатами мобильных устройств. В разделе приведены инструкции по установке сертификатов на мобильные устройства пользователей и по настройке правил выдачи сертификатов. Раздел также содержит инструкции по интеграции программы с инфраструктурой открытых ключей и по настройке поддержки Kerberos.

В этом разделе

Установка сертификата	316
Настройка правил выпуска сертификатов	321
Интеграция с инфраструктурой открытых ключей.....	322
Включение поддержки Kerberos Constrained Delegation	324

Установка сертификата

Вы можете устанавливать на мобильное устройство пользователя сертификаты трех типов:

- общие сертификаты для идентификации мобильного устройства;
- почтовые сертификаты для настройки на мобильном устройстве корпоративной почты;
- VPN-сертификат для настройки на мобильном устройстве доступа к виртуальной частной сети.

► *Чтобы установить сертификат на мобильное устройство пользователя, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
2. В рабочей области папки **Сертификаты** по ссылке **Добавить сертификат** запустите мастер установки сертификата.

Следуйте указаниям мастера.

В результате работы мастера сертификат будет создан, добавлен в список сертификатов пользователя, кроме того будет отправлено уведомление пользователю со ссылкой для загрузки и установки сертификата на мобильное устройство. Список всех сертификатов можно просмотреть и экспортировать в файл (см. раздел "Просмотр списка сертификатов, выписанных пользователю" на стр. [183](#)). Можно удалять и перевыпускать сертификаты, а также просматривать их свойства.

В этом разделе

Шаг 1. Тип сертификата	317
Шаг 2. Тип устройства	317
Шаг 3. Выбор пользователя.....	318
Шаг 4. Источник сертификата.....	318
Шаг 5. Тег сертификата.....	319
Шаг 6. Способ уведомления пользователей	320

Шаг 1. Тип сертификата

Укажите тип сертификата, который необходимо установить на мобильное устройство пользователя:

- **Общий сертификат** – для идентификации мобильного устройства;
- **Почтовый сертификат** – для настройки на мобильном устройстве корпоративной почты;
- **VPN-сертификат** – для настройки на мобильном устройстве доступа к виртуальной частной сети.

Шаг 2. Тип устройства

Укажите тип операционной системы устройства:

- **iOS MDM-устройство.** Выберите этот вариант, если необходимо установить сертификат на мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM.
- **KES-устройство под управлением Kaspersky Security для мобильных устройств.** Выберите этот вариант, если необходимо установить сертификат на

KES-устройство. В этом случае сертификат будет использоваться при подключении к Серверу администрирования для идентификации пользователя.

- **KES-устройство, которое подключается к Серверу администрирования без аутентификации по сертификату пользователя.** Выберите этот вариант, если необходимо установить сертификат на KES-устройство без аутентификации по сертификату. В этом случае на последнем шаге мастера в окне **Способ уведомления пользователей** администратор должен выбрать тип авторизации пользователя при подключении к Серверу администрирования.

Шаг **Тип устройства** отображается, если ранее был выбран тип сертификата **Почтовый сертификат** или **VPN-сертификат**.

Шаг 3. Выбор пользователя

Выберите в списке пользователей, группы пользователей или группы Active Directory пользователей, для которых вы хотите установить сертификат.

В окне **Выбор пользователя** можно выполнить поиск внутренних пользователей Kaspersky Security Center.

По кнопке **Добавить** вы можете добавить внутреннего пользователя.

Шаг 4. Источник сертификата

В окне можно выбрать источник сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Можно задать сертификат одним из следующих способов:

- Автоматически создать сертификат средствами Сервера администрирования и доставить сертификат на устройство.
- Указать файл ранее созданного сертификата. Этот способ недоступен, если на предыдущем шаге было выбрано несколько пользователей.

Установите флажок **Опубликовать сертификат**, если необходимо отправить уведомление пользователю о создании сертификата для его мобильного устройства.

Если мобильное устройство пользователя уже было авторизовано по сертификату ранее и нет необходимости указывать имя учетной записи и пароль для получения нового сертификата, снимите флажок **Опубликовать сертификат**. В этом случае окно **Способ уведомления пользователя** отображаться не будет.

Шаг 5. Тег сертификата

В выпадающем списке вы можете назначить тег для сертификата iOS MDM-устройства пользователя. Сертификат с назначенным тегом может иметь специальные параметры, установленные для этого тега в свойствах политики Kaspersky Device Management для iOS.

Для выбора в выпадающем списке доступны теги *Шаблон сертификата 1*, *Шаблон сертификата 2* и *Шаблон сертификата 3*, параметры которых могут быть настроены в следующих разделах:

- Если в окне **Тип сертификата** был выбран тип **Почтовый сертификат**, параметры тегов для него настраиваются в свойствах учетной записи Exchange ActiveSync для мобильных устройств (**Управляемые устройства** → **Политики** → Свойства политики Kaspersky Device Management для iOS → Раздел **Exchange ActiveSync** → **Добавить** → **Дополнительно**).
- Если в окне **Тип сертификата** был выбран тип **VPN-сертификат**, параметры тегов для него настраиваются в свойствах сети VPN для мобильных устройств (**Управляемые устройства** → **Политики** → Свойства политики Kaspersky Device Management для iOS → Раздел **VPN** → **Добавить** → **Дополнительно**). Настройка тегов, используемых для VPN-сертификатов, недоступна, если для сети VPN выбран тип соединения L2TP, PPTP, или IPSec (Cisco).

Окно **Тег сертификата** отображается, если в окне **Тип устройства** был выбран вариант **iOS MDM-устройство**.

См. также

| Установка сертификата пользователю [182](#)

Шаг 6. Способ уведомления пользователей

В окне **Способ уведомления пользователя** можно настроить параметры уведомления пользователя об установке сертификата на мобильное устройство:

- **Показать пароль после завершения работы мастера.** При выборе этого варианта пароль для получения сертификата будет отображен на последнем шаге работы мастера установки сертификата. Настройка параметров уведомления пользователя об установленном сертификате будет недоступна.
- **Сообщить пользователю о новом сертификате.** При выборе этого варианта вы можете настроить параметры уведомления пользователя о новом сертификате.

В блоке параметров **По электронной почте** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ оповещения доступен только если настроен SMTP-сервер.

В блоке параметров **С помощью SMS** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен только если настроено SMS-оповещение.

По ссылке **Редактировать сообщение** в блоках параметров **По электронной почте** и **С помощью SMS** просмотрите и при необходимости отредактируйте текст уведомления.

В поле **Пароль пользователя** укажите тип аутентификации пользователя:

- **Доменный пароль или внутреннего пользователя.** В этом случае пользователь использует доменный пароль или пароль внутреннего пользователя Kaspersky Security Center, для того чтобы получить новый сертификат.
- **Одноразовый пароль.** В этом случае пользователь получит одноразовый пароль, который будет выслан на электронную почту или с помощью SMS. Этот пароль необходимо будет указать для получения нового сертификата.

Поле отображается, если ранее был выбран тип устройства **KES-устройство, которое подключается к Серверу администрирования без аутентификации по сертификату пользователя.**

Окно **Способ уведомления пользователей** не отображается, если в окне **Тип устройства** был выбран вариант **iOS MDM-устройство**.

См. также

Установка сертификата пользователю [182](#)

Настройка правил выпуска сертификатов

► *Чтобы настроить правила выпуска сертификатов, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выпуска сертификатов** откройте окно **Правила выпуска сертификатов**.
3. Перейдите в раздел с названием типа сертификата:

Выпуск сертификатов общего типа – для настройки выпуска сертификатов общего типа;

Выпуск почтовых сертификатов – для настройки выпуска почтовых сертификатов;

Выпуск VPN-сертификатов – для настройки выпуска VPN-сертификатов.

4. В блоке **Параметры выпуска** настройте выпуск сертификата:
 - Укажите срок действия сертификата в днях.
 - Выберите источник сертификатов (**Сервер администрирования** или **Сертификаты задаются вручную**).

По умолчанию источником сертификатов выбран Сервер администрирования.

 - Задайте шаблон сертификатов (**Шаблон по умолчанию**, **Другой шаблон**).

Настройка шаблонов доступна, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей (на стр. [322](#)).

5. В блоке **Параметры автоматического обновления** настройте автоматическое обновление сертификата:

- В поле **Обновлять, когда до истечения срока действия осталось (сут)** укажите, за какое количество дней до истечения срока действия нужно обновлять сертификат.
- Чтобы включить автоматическое обновление сертификатов, установите флажок **Автоматически перевыпускать сертификат, если это возможно**.

Сертификат общего типа можно перевыпускать только вручную.

6. В блоке **Защита паролем** включите и настройте использование пароля при расшифровке сертификатов.

Защита паролем доступна только для сертификатов общего типа.

- а. Установите флажок **Запрашивать пароль при установке сертификата**.
- б. С помощью ползунка настройте максимальное количество символов в пароле для шифрования.

7. Нажмите на кнопку **ОК**.

Интеграция с инфраструктурой открытых ключей

Интеграция программы с инфраструктурой открытых ключей (Public Key Infrastructure, PKI) необходима для упрощения выдачи доменных сертификатов пользователей. В результате интеграции выдачи сертификатов происходит автоматически.

Минимально поддерживаемая версия сервера PKI – Windows Server 2008.

Для интеграции с PKI необходимо настроить учетную запись. Учетная запись должна

соответствовать следующим требованиям:

- быть доменным пользователем и администратором устройства, на котором установлен Сервер администрирования;
- иметь привилегию SeServiceLogonRight на устройстве с установленным Сервером администрирования.

Под настроенной учетной записью нужно хотя бы один раз выполнить вход на устройстве с установленным Сервером администрирования для того, чтобы создать постоянный профиль пользователя. В хранилище сертификатов этого пользователя, на устройстве с Сервером администрирования, необходимо установить сертификат агента регистрации, предоставленный администраторами домена.

► *Чтобы настроить интеграцию с инфраструктурой открытых ключей, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.
2. В рабочей области по кнопке **Интегрировать с инфраструктурой открытых ключей** откройте раздел **Интеграция с PKI** окна **Правила выпуска сертификатов**.

В результате откроется раздел **Интеграция с PKI** окна **Правила выпуска сертификатов**.

3. Установите флажок **Интегрировать выписку сертификатов с PKI**.
4. В поле **Учетная запись** укажите имя учетной записи пользователя, которая будет использоваться для интеграции с инфраструктурой открытых ключей.
5. В поле **Пароль** укажите доменный пароль учетной записи.
6. В списке **Укажите имя шаблона сертификата в системе PKI** выберите шаблон сертификатов, на основании которого будут выпускаться сертификаты для пользователей домена.

Под указанной учетной записью в Kaspersky Security Center запускается специализированная служба, ответственная за выпуск доменных сертификатов пользователей. Служба запускается, когда происходит загрузка списка шаблонов сертификатов по кнопке **Обновить список**, или при выпуске сертификата.

7. Нажмите на кнопку **ОК**, чтобы сохранить параметры.

В результате интеграции выписки сертификатов происходит автоматически.

Включение поддержки Kerberos Constrained Delegation

Программа поддерживает использование Kerberos Constrained Delegation.

- ▶ *Чтобы включить поддержку Kerberos Constrained Delegation, выполните следующие действия:*
 1. В дереве консоли откройте папку **Управление мобильными устройствами**.
 2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
 3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
 4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.
 5. В окне свойств Сервера iOS MDM выберите раздел **Параметры**.
 6. В разделе **Параметры** установите флажок **Обеспечить совместимость с Kerberos Constrained Delegation**.
 7. Нажмите на кнопку **ОК**.

Добавление мобильных устройств в список управляемых устройств

Чтобы добавить мобильное устройство пользователя в список управляемых устройств, на устройство нужно доставить и установить общий сертификат (см. раздел "Работа с сертификатами" на стр. [315](#)). Общие сертификаты используются для идентификации мобильных устройств Сервером администрирования. После доставки и установки общего сертификата на мобильном устройстве оно отображается в списке управляемых устройств.

Добавление мобильных устройств пользователей в список управляемых устройств выполняется с помощью мастера.

Запуск мастера добавления нового устройства

► *Чтобы запустить мастер добавления нового мобильного устройства пользователю, выполните одно из следующих действий:*

- Запустите мастер с помощью контекстного меню в папке **Учетные записи пользователей**:

1. В дереве консоли выберите папку **Учетные записи пользователей**.

По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. Выберите учетную запись пользователя, мобильное устройство которого вы хотите добавить в список управляемых устройств.

3. В контекстном меню учетной записи пользователя выберите пункт **Добавить мобильное устройство**.

Запустится мастер добавления мобильных устройств.

- Запустите мастер по кнопке **Добавить мобильное устройство** в папке **Мобильные устройства**:

1. В дереве консоли выберите папку **Мобильные устройства**, вложенную в папку **Управление мобильными устройствами**.

2. В рабочей области папки **Мобильные устройства** нажмите на кнопку **Добавить мобильное устройство**.

3. Запустится мастер добавления мобильных устройств.

4. В окне **Операционная система** выберите тип операционной системы мобильного устройства (Android, iOS).

Ваши дальнейшие действия в мастере добавления мобильных устройств зависят от того, какой тип операционной системы мобильного устройства вы выбрали (см. инструкции ниже).

Если был выбран способ добавления мобильного устройства с помощью кнопки **Добавить мобильное устройство** в папке **Мобильные устройства**, в мастере отображается окно **Выбор пользователей**. В окне **Выбор пользователей** выберите пользователей, группы пользователей или группы Active Directory пользователей, для которых вы хотите добавить мобильные устройства в список управляемых устройств.

Добавление мобильного устройства в случае, если общий сертификат доставляется с помощью ссылки App Store

► *Чтобы установить на iOS-устройство приложение Kaspersky Safe Browser из App Store и затем подключить устройство к Серверу администрирования, выполните следующие действия:*

1. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **iOS**.
2. В окне мастера **Способ защиты iOS MDM-устройства** выберите вариант **Установить Kaspersky Safe Browser по ссылке на App Store**.
3. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

- **Выписать сертификат средствами Сервера администрирования**

Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

Этот вариант выбран по умолчанию.

- **Указать файл сертификата**

Укажите файл ранее созданного сертификата. Этот способ не доступен, если на предыдущем шаге было выбрано несколько пользователей.

4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

- **Показать ссылку на инсталляционный пакет**

При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

- **Отправить ссылку на Kaspersky Safe Browser**

При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS оповещение, отправка SMS-сообщений пользователям невозможна.

1. В окне мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате работы мастера на мобильное устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Safe Browser с App Store. Пользователь переходит по ссылке или сканирует QR-код. После этого операционная система мобильного устройства запрашивает у пользователя согласие на установку Kaspersky Safe Browser. Пользователь устанавливает Kaspersky Safe Browser на мобильное устройство. После установки Kaspersky Safe Browser пользователь повторно сканирует QR-код для получения параметров подключения к Серверу администрирования. В результате повторного сканирования QR-кода в Safe Browser пользователь получает параметры подключения к Серверу администрирования и общий сертификат. Мобильное

устройство подключается к Серверу администрирования и загружает себе общий сертификат. Сертификат, установленный на мобильное устройство, будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Если Kaspersky Safe Browser был установлен ранее на мобильное устройство, параметры подключения к Серверу администрирования нужно вводить самостоятельно. После этого необходимо установить на мобильное устройство общий сертификат (см. раздел "Установка сертификата" на стр. [316](#)). Загрузка и установка Kaspersky Safe Browser в этом случае не выполняется.

Добавление мобильного устройства в случае, если общий сертификат доставляется в составе iOS MDM-профиля

► *Чтобы подключить к Серверу администрирования iOS-устройство по протоколу iOS MDM, выполните следующие действия:*

1. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **iOS**.
2. В окне мастера **Способ защиты iOS MDM-устройства** выберите вариант **Использовать iOS MDM-профиль Сервера iOS MDM**.

В появившемся поле ниже выберите Сервер iOS MDM.

3. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

- **Выписать сертификат средствами Сервера администрирования**

Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

Этот вариант выбран по умолчанию.

- **Указать файл сертификата**

Укажите файл ранее созданного сертификата. Этот способ не доступен, если на предыдущем шаге было выбрано несколько пользователей.

4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

- **Показать ссылку на инсталляционный пакет**

При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

- **Отправить ссылку на Kaspersky Safe Browser**

При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS оповещение, отправка SMS-сообщений пользователям невозможна.

1. В окне мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате iOS MDM-профиль автоматически публикуется на Веб-сервере Kaspersky Security Center. Пользователь мобильного устройства получит уведомление со ссылкой для загрузки iOS MDM-профиля с Веб-сервера. Пользователь самостоятельно переходит по полученной ссылке. После этого операционная система мобильного устройства запрашивает у пользователя согласие на установку iOS MDM-профиля. Чтобы iOS

MDM-профиль загрузился на мобильное устройство, пользователь должен согласиться на установку iOS MDM-профиля. После загрузки iOS MDM-профиля и синхронизации с Сервером администрирования мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Для перехода пользователем по полученной ссылке на Веб-сервере Kaspersky Security Center необходимо, чтобы с его мобильного устройства было доступно соединение с Сервером администрирования по порту 8061.

Добавление мобильного устройства в случае, если общий сертификат доставляется с помощью ссылки Google Play

► *Чтобы установить на KES-устройство приложение Kaspersky Endpoint Security для Android из Google Play и затем подключить устройство к Серверу администрирования, выполните следующие действия:*

1. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **Android**.
2. В окне мастера **Способ установки Kaspersky Endpoint Security для Android** выберите вариант **По ссылке на Google Play**.
3. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

- **Выписать сертификат средствами Сервера администрирования**

Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

Этот вариант выбран по умолчанию.

- **Указать файл сертификата**

Укажите файл ранее созданного сертификата. Этот способ не доступен, если на предыдущем шаге было выбрано несколько

пользователей.

4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

- **Показать ссылку на инсталляционный пакет**

При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

- **Отправить ссылку на Kaspersky Safe Browser**

При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS оповещение, отправка SMS-сообщений пользователям невозможна.

1. В окне мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате работы мастера на мобильное устройство пользователя будет отправлена ссылка и QR-код для загрузки Kaspersky Endpoint Security для Android. Пользователь переходит по ссылке или сканирует QR-код. После этого операционная система мобильного устройства запрашивает у пользователя согласие на установку Kaspersky Endpoint Security для Android. После загрузки и установки Kaspersky Endpoint Security для Android мобильное устройство подключается к Серверу администрирования и загружает общий сертификат. После установки сертификата на мобильное устройство, мобильное

устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Добавление мобильного устройства в случае, если общий сертификат доставляется в составе мобильного приложения

- ▶ *Чтобы установить на Android-устройство приложение Kaspersky Endpoint Security для Android и затем подключить устройство к Серверу администрирования, выполните следующие действия:*

Для установки используется приложение Kaspersky Endpoint Security для Android, опубликованное на Сервере администрирования.

1. В окне мастера **Операционная система** выберите тип операционной системы мобильного устройства **Android**.
2. В окне мастера **Способ установки Kaspersky Endpoint Security для Android** выберите вариант **По ссылке на Веб-сервер**.

В появившемся поле ниже выберите инсталляционный пакет или создайте новый инсталляционный пакет по кнопке **Новый**.

3. В окне мастера **Источник сертификата** требуется указать способ создания общего сертификата, с помощью которого Сервер администрирования идентифицирует мобильное устройство. Вы можете задать общий сертификат одним из двух способов:

- **Выписать сертификат средствами Сервера администрирования**

Если выбран этот вариант, то iOS MDM-профиль будет подписан сертификатом, автоматически созданным Сервером администрирования.

Этот вариант выбран по умолчанию.

- **Указать файл сертификата**

Укажите файл ранее созданного сертификата. Этот способ не доступен, если на предыдущем шаге было выбрано несколько пользователей.

4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте:

- **Показать ссылку на инсталляционный пакет**

При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.

Этот вариант недоступен, если было выбрано несколько пользователей для подключения устройства.

- **Отправить ссылку на Kaspersky Safe Browser**

При выборе этого варианта можно настроить параметры оповещения пользователя о подключении нового мобильного устройства.

Можно выбрать тип адреса электронной почты, указать дополнительный адрес и отредактировать текст сообщения. Можно также выбрать тип телефона пользователя для отправки SMS-сообщения, указать дополнительный номер телефона и отредактировать текст отправляемого SMS-сообщения.

Если не настроен SMTP-сервер, отправка сообщений электронной почты пользователям невозможна. Если не настроено SMS оповещение, отправка SMS-сообщений пользователям невозможна.

1. В окне мастера **Результат** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате пакет мобильного приложения Kaspersky Endpoint Security для Android автоматически публикуется на Веб-сервере Kaspersky Security Center. Пакет мобильного приложения содержит приложение, параметры подключения мобильного устройства к Серверу администрирования и сертификат. Пользователь мобильного устройства получит уведомление со ссылкой для загрузки пакета с Веб-сервера. Пользователь самостоятельно переходит по полученной ссылке. После этого операционная система устройства запрашивает у пользователя согласие на установку пакета мобильного приложения. Если пользователь соглашается, пакет загружается на мобильное устройство. После загрузки пакета и синхронизации с Сервером администрирования

мобильное устройство будет отображаться в папке **Мобильные устройства**, вложенной в папку **Управление мобильными устройствами** дерева консоли.

Управление мобильными устройствами Exchange ActiveSync

В этом разделе описаны дополнительные возможности управления EAS-устройствами с помощью Kaspersky Security Center.

Кроме управления EAS-устройствами с помощью команд, администратор может использовать следующие возможности:

- Создавать профили управления EAS-устройствами, назначать их почтовым ящикам пользователей (см. стр. [335](#)). *Профиль управления EAS-устройствами* – это политика Exchange ActiveSync, которая используется на сервере Microsoft Exchange для управления EAS-устройствами. В профиле управления EAS-устройствами вы можете настраивать следующие группы параметров:
 - параметры управления паролем пользователя;
 - параметры синхронизации почты;
 - ограничения для использования функций мобильного устройства;
 - ограничения для использования мобильных приложений на мобильном устройстве.

В зависимости от модели мобильного устройства параметры профиля управления могут применяться частично. Статус применения политики Exchange ActiveSync вы можете посмотреть в свойствах мобильного устройства.

- Просматривать информацию о параметрах управления EAS-устройствами (см. стр. [340](#)). Например, в свойствах мобильного устройства администратор может посмотреть время последней синхронизации мобильного устройства с сервером Microsoft Exchange, идентификатор EAS-устройства, название политики Exchange ActiveSync и статус ее применения на мобильном устройстве.

- Отключать неиспользуемые пользователями EAS-устройства от управления (см. стр. [340](#)).
- Настраивать параметры опроса Active Directory Сервером мобильных устройств Exchange ActiveSync, в результате которого обновляется информация о почтовых ящиках пользователей и их мобильных устройствах.

В этом разделе

Добавление профиля управления.....	335
Удаление профиля управления	337
Работа с политиками Exchange ActiveSync	338
Настройка области сканирования	339
Работа с EAS-устройствами	339
Просмотр информации о EAS-устройстве	340
Отключение EAS-устройства от управления	340
Права пользователя для управления мобильными устройствами Exchange ActiveSync .	341

Добавление профиля управления

Для управления EAS-устройствами вы можете создавать профили управления EAS-устройствами и назначать их выбранным почтовым ящикам Microsoft Exchange.

Почтовому ящику Microsoft Exchange может быть назначен только один профиль управления EAS-устройствами.

► *Чтобы добавить профиль управления EAS-устройствами для почтового ящика Microsoft Exchange, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.

2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.

3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер мобильных устройств Exchange ActiveSync.

4. В контекстном меню Сервера мобильных устройств Exchange ActiveSync выберите пункт **Свойства**.

Откроется окно свойств Сервера мобильных устройств.

5. В окне свойств **Сервера мобильных устройств Exchange ActiveSync** выберите раздел **Почтовые ящики**.

6. Выберите почтовый ящик и нажмите на кнопку **Назначить профиль**.

Откроется окно **Профили политики**.

7. В окне **Профили политики** нажмите на кнопку **Добавить**.

Откроется окно **Новый профиль**.

8. Выполните настройку параметров профиля на закладках окна **Новый профиль**:

- Если вы хотите задать имя профиля и период его обновления, выберите закладку **Общие**.
- Если вы хотите настроить параметры пароля пользователя мобильного устройства, выберите закладку **Пароль**.
- Если вы хотите настроить параметры синхронизации с сервером Microsoft Exchange, выберите закладку **Параметры синхронизации**.
- Если вы хотите настроить параметры ограничения функций мобильного устройства, выберите закладку **Устройство**.
- Если вы хотите настроить параметры ограничения использования мобильных приложений на мобильном устройстве, выберите закладку **Ограничения приложений**.

9. Нажмите на кнопку **ОК**.

Новый профиль отобразится в списке профилей в окне **Профили политики**.

Если вы хотите, чтобы этот профиль автоматически присваивался новым почтовым ящикам и почтовым ящикам, профиль которых был удален, выберите его в списке профилей и нажмите на кнопку **Сделать профилем по умолчанию**.

Профиль по умолчанию нельзя удалить. Чтобы удалить текущий профиль по умолчанию, необходимо назначить свойство "профиль по умолчанию" другому профилю.

10. Нажмите на кнопку **ОК** в окне **Профили политики**.

Параметры профиля управления будут применены на EAS-устройстве при следующей синхронизации устройства с Сервером мобильных устройств Exchange ActiveSync.

Удаление профиля управления

► *Чтобы удалить профиль управления EAS-устройствами для почтового ящика Microsoft Exchange, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер мобильных устройств Exchange ActiveSync.
4. В контекстном меню Сервера мобильных устройств Exchange ActiveSync выберите пункт **Свойства**.

Откроется окно свойств Сервера мобильных устройств.

5. В окне свойств Сервера мобильных устройств Exchange ActiveSync выберите раздел **Почтовые ящики**.
6. Выберите почтовый ящик и нажмите на кнопку **Изменить профили**.

Откроется окно **Профили политики**.

7. В окне **Профили политики** выберите профиль, который вы хотите удалить, и нажмите на кнопку удаления с красным крестом.

Выбранный профиль будет удален из списка профилей управления. К EAS-устройствам, находящимся под управлением удаленного профиля, будет применен текущий профиль по умолчанию.

Если вы хотите удалить текущий профиль по умолчанию, назначьте свойство "профиль по умолчанию" другому профилю, затем удалите профиль.

Работа с политиками Exchange ActiveSync

После установки Сервера мобильных устройств Exchange ActiveSync в разделе **Почтовые ящики** окна свойств этого Сервера вы можете посмотреть информацию об учетных записях сервера Microsoft Exchange, полученных в результате опроса текущего домена либо леса доменов.

Кроме того, в окне свойств Сервера мобильных устройств Exchange ActiveSync вы можете использовать следующие кнопки:

- **Изменить профили** – позволяет открыть окно **Профили политики**, содержащее список политик, полученных с сервера Microsoft Exchange. В этом окне можно создавать, изменять или удалять политики Exchange ActiveSync. Окно **Профили политики** почти полностью соответствует окну редактирования политик в консоли Exchange Management Console.
- **Назначить профили мобильным устройствам** – позволяет назначить выбранную политику Exchange ActiveSync одной или нескольким учетным записям.
- **Вкл/выкл ActiveSync** – позволяет включить или выключить HTTP протокол Exchange ActiveSync для одной или нескольких учетных записей.

Настройка области сканирования

В свойствах установленного Сервера мобильных устройств Exchange ActiveSync в разделе **Параметры** вы можете настроить область сканирования. По умолчанию область сканирования – это текущий домен, в котором установлен Сервер мобильных устройств Exchange ActiveSync. При выборе значения **Весь лес доменов** область сканирования расширится на весь лес доменов.

Работа с EAS-устройствами

Устройства, полученные в результате сканирования сервера Microsoft Exchange, попадают в единый список устройств, который находится в узле **Управление мобильными устройствами** в папке **Мобильные устройства**.

Если вы хотите, чтобы в папке **Мобильные устройства** отображались только устройства Exchange ActiveSync (далее EAS-устройства), отфильтруйте список устройств по ссылке **Exchange ActiveSync (EAS)**, расположенной над ним.

Вы можете управлять EAS-устройствами с помощью команд. Например, команда **Сбросить настройки до заводских** позволяет удалить все данные с устройства и сбросить настройки устройства до заводских. Эта команда полезна в случае кражи или потери устройства, когда необходимо избежать попадания корпоративных или персональных данных к третьим лицам.

Если с устройства были удалены все данные, то при следующем подключении этого устройства к серверу Microsoft Exchange с него снова будут удалены все данные. Команда будет повторяться до тех пор, пока устройство не будет удалено из списка устройств. Такое поведение обусловлено особенностями работы сервера Microsoft Exchange.

Чтобы удалить EAS-устройство из списка, в контекстном меню устройства выберите пункт **Удалить**. Если с EAS-устройства не будет удалена учетная запись Exchange ActiveSync, то при последующей синхронизации устройства с сервером Microsoft Exchange оно снова появится в списке устройств.

Просмотр информации о EAS-устройстве

► Чтобы просмотреть информацию о EAS-устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте EAS-устройства по типу протокола управления (EAS).

3. В контекстном меню мобильного устройства выберите пункт **Свойства**.

В результате откроется окно свойств EAS-устройства.

В окне свойств мобильного устройства отображается информация о подключенном EAS-устройстве.

Отключение EAS-устройства от управления

► Чтобы отключить EAS-устройство от управления Сервером мобильных устройств Exchange ActiveSync, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте EAS-устройства по типу протокола управления (EAS).

3. Выберите мобильное устройство, которое вы хотите отключить от управления Сервером мобильных устройств Exchange ActiveSync.

4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

В результате EAS-устройство будет отмечено на удаление значком с красным крестом. Фактическое удаление мобильного устройства из списка управляемых устройств произойдет после его удаления из базы данных Сервера мобильных устройств Exchange

ActiveSync. Для этого администратору необходимо удалить учетную запись пользователя на сервере Microsoft Exchange.

Права пользователя для управления мобильными устройствами Exchange ActiveSync

Для управления мобильными устройствами, которые работают по протоколу Exchange ActiveSync с сервером Microsoft Exchange Server 2010 или Microsoft Exchange Server 2013, необходимо, чтобы пользователь был членом ролевой группы, для которой разрешены выполнения следующих командлетов:

- Get-CASMailbox;
- Set-CASMailbox;
- Remove-ActiveSyncDevice;
- Clear-ActiveSyncDevice;
- Get-ActiveSyncDeviceStatistics;
- Get-AcceptedDomain;
- Set-AdServerSettings;
- Get-ActiveSyncMailboxPolicy;
- New-ActiveSyncMailboxPolicy;
- Set-ActiveSyncMailboxPolicy;
- Remove-ActiveSyncMailboxPolicy.

Для управления мобильными устройствами, которые работают по протоколу Exchange ActiveSync с сервером Microsoft Exchange Server 2007, необходимо, чтобы пользователь обладал административными правами. В случае их отсутствия выполните командлеты для

наделения административными правами пользователя (см. таблицу ниже).

Таблица 4. Административные права для управления мобильными устройствами Exchange ActiveSync для Microsoft Exchange Server 2007

Доступ	Объект	Командлет
Полный	Ветка "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	<pre>Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configu ration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericAll</pre>
Чтение	Ветка "CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	<pre>Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configu ration,DC=<Имя домена>" -InheritanceType All -AccessRight GenericRead</pre>
Чтение и запись	Свойства msExchMobileMailboxPolicyLink и msExchOmaAdminWirelessEnable для объектов в Active Directory	<pre>Add-ADPermission -User <Имя пользователя или группы> -Identity "DC=<Имя домена>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable</pre>

Доступ	Объект	Командлет
Полный	Хранилища почтовых ящиков ms-Exch-Store-Admin для mailboxstorages	Get-MailboxDatabase Add-ADPermission -User <имя пользователя или группы> -ExtendedRights ms-Exch-Store-Admin

Подробную информацию об использовании командлетов в консоли Exchange Management Shell смотрите на веб-сайте технической поддержки Microsoft Exchange Server [http://technet.microsoft.com/en-us/library/bb123778\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/bb123778(v=exchg.150).aspx).

Управление iOS MDM-устройствами

В этом разделе описаны дополнительные возможности управления iOS MDM-устройствами с помощью Kaspersky Security Center. Для управления iOS MDM-устройствами программа поддерживает следующие возможности:

- Централизованно настраивать параметры управляемых iOS MDM-устройств и ограничивать функции устройств с помощью конфигурационных профилей. Вы можете добавлять и изменять конфигурационные профили и устанавливать профили на мобильные устройства.
- Устанавливать приложения на мобильные устройства не через App Store с помощью provisioning-профилей. Например, с помощью provisioning-профилей можно устанавливать на мобильные устройства пользователей корпоративные приложения, разработанные внутри компании. Provisioning-профиль содержит информацию о приложении и мобильном устройстве.
- Устанавливать приложения на iOS MDM-устройство через App Store. Перед установкой приложения на iOS MDM-устройство приложение необходимо добавить на Сервер iOS MDM.

Каждые 24 часа всем подключенным iOS MDM-устройствам отправляется PUSH-нотификация для синхронизации данных с Сервером iOS MDM.

Информацию о конфигурационном профиле и provisioning–профиле, а также о приложениях, установленных на iOS MDM-устройстве, можно просмотреть в окне свойств устройства (см. раздел "Просмотр информации о iOS MDM-устройстве" на стр. [361](#)).

В этом разделе

Выписка сертификата iOS MDM-профиля	345
Добавление конфигурационного профиля	346
Установка конфигурационного профиля на устройство.....	347
Удаление конфигурационного профиля с устройства	349
Добавление нового устройства посредством публикации ссылки на профиль.....	350
Добавление нового устройства посредством установки профиля администратором	351
Добавление provisioning-профиля.....	351
Установка provisioning-профиля на устройство	352
Удаление provisioning-профиля с устройства.....	354
Добавление управляемого приложения	355
Установка приложения на мобильное устройство	356
Удаление приложения с устройства	358
Установка приложения Kaspersky Safe Browser на мобильное устройство	359
Настройка параметров роуминга на мобильном устройстве iOS MDM.....	360
Просмотр информации о iOS MDM-устройстве.....	361
Отключение iOS MDM-устройства от управления.....	362
Отправка команд на устройство	363
Проверка статуса исполнения отправленных команд.....	363

Выписка сертификата iOS MDM-профиля

Вы можете выписать сертификат iOS MDM-профиля для определения его подлинности мобильным устройством.

► *Чтобы создать сертификат iOS MDM-профиля, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки выберите раздел **Параметры подключения iOS-устройств**.
4. Нажмите на кнопку **Задать** ниже поля **Выберите сертификат**.

В результате откроется окно **Сертификат**.

5. В поле **Тип сертификата** укажите выберите открытый или закрытый тип сертификата:
 - Если выбрано значение **Контейнер PKCS#12**, укажите файл сертификата и пароль.
 - Если выбрано значение **X.509-сертификат**:
 - a. укажите файл закрытого ключа (файл с расширением *.p12 или *.pem);
 - b. укажите пароль закрытого ключа;
 - c. укажите файл открытого ключа (файл с расширением *.cer).
6. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат iOS MDM-профиля.

Добавление конфигурационного профиля

Для создания конфигурационного профиля необходимо установить программу iPhone Configuration Utility на том же устройстве, на котором установлена Консоль администрирования. Программу iPhone Configuration Utility нужно предварительно скачать с сайта Apple Inc. и установить штатными средствами операционной системы.

► *Чтобы создать конфигурационный профиль и добавить его на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли выберите папку **Управление мобильными устройствами**.

Папка **Управление мобильными устройствами** по умолчанию вложена в папку **Дополнительно**.

2. В рабочей области папки **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.

3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.

4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

Откроется окно свойств Сервера мобильных устройств.

5. В окне свойств Сервера iOS MDM выберите раздел **Конфигурационные профили**.

6. В разделе **Конфигурационные профили** нажмите на кнопку **Создать**.

Откроется окно **Добавление нового конфигурационного профиля**.

7. В окне **Добавление нового конфигурационного профиля** укажите название профиля и идентификатор профиля.

Идентификатор конфигурационного профиля должен быть уникальным, значение идентификатора следует задавать в формате Reverse-DNS, например, *com.companyname.identifier*.

8. Нажмите на кнопку **ОК**.

Запустится программа iPhone Configuration Utility.

9. Выполните настройку параметров профиля в программе iPhone Configuration Utility.

Описание параметров профиля и инструкции по его настройке приведены в документации для программы iPhone Configuration Utility.

После настройки параметров профиля в программе iPhone Configuration Utility, новый конфигурационный профиль отображается в разделе **Конфигурационные профили** в окне свойств Сервера iOS MDM.

По кнопке **Изменить** конфигурационный профиль можно отредактировать.

По кнопке **Импортировать** можно загрузить конфигурационный профиль в программу.

По кнопке **Экспортировать** конфигурационный профиль можно сохранить в файле.

Созданный профиль следует установить на iOS MDM-устройства (см. раздел "Установка конфигурационного профиля на устройство" на стр. [347](#)).

Установка конфигурационного профиля на устройство

- *Чтобы установить конфигурационный профиль на мобильное устройство, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.
3. Выберите мобильное устройство пользователя, на которое нужно установить конфигурационный профиль

Вы можете выбрать несколько мобильных устройств, чтобы установить на них профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить профиль** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить профиль**.

В результате откроется окно **Выбор профилей** со списком профилей. Выберите в списке профиль, который нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько профилей одновременно. Чтобы выбрать диапазон профилей, используйте клавишу **SHIFT**. Для объединения отдельных профилей в группу используйте клавишу **CTRL**.

6. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

В результате выполнения команды выбранный конфигурационный профиль будет установлен на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд примет значение *Выполнено*.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

7. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Установленный профиль можно просмотреть и при необходимости удалить (см. раздел "Удаление конфигурационного профиля с устройства" на стр. [349](#)).

Удаление конфигурационного профиля с устройства

► Чтобы удалить конфигурационный профиль с мобильного устройства, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по ссылке **iOS MDM**.

3. Выберите мобильное устройство пользователя, с которого нужно удалить конфигурационный профиль.

Вы можете выбрать несколько мобильных устройств, чтобы удалить с них профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить профиль** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды**, затем **Удалить профиль**.

В результате откроется окно **Удаление профилей** со списком профилей.

6. Выберите в списке профиль, который нужно удалить с мобильного устройства. Вы можете выбрать и удалить с мобильного устройства несколько профилей одновременно. Чтобы выбрать диапазон профилей, используйте клавишу **SHIFT**. Для объединения отдельных профилей в группу используйте клавишу **CTRL**.

7. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

В результате выполнения команды выбранный конфигурационный профиль будет удален с мобильного устройства пользователя. В случае успешного выполнения команды текущий статус команды примет значение *Завершено*.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Добавление нового устройства посредством публикации ссылки на профиль

В Консоли администрирования с помощью мастера подключения нового мобильного устройства администратор создает новый iOS MDM-профиль. В результате работы мастера будут выполнены следующие действия:

- iOS MDM-профиль автоматически опубликуется на веб-сервере.
- Пользователю будет отправлена ссылка на iOS MDM-профиль в SMS-сообщении или по электронной почте. После получения ссылки пользователь установит iOS MDM-профиль на мобильном устройстве.
- Мобильное устройство будет подключено к Серверу iOS MDM.

В связи с введенным компанией Apple ужесточением политики безопасности, для подключения мобильного устройства с операционной системой iOS 11 к Серверу администрирования с настроенной интеграцией с Public Key Infrastructure (PKI) необходимо настроить протоколы версий TLS 1.1 и TLS 1.2.

Добавление нового устройства посредством установки профиля администратором

Чтобы подключить мобильное устройство к Серверу iOS MDM с помощью установки iOS MDM-профиля на мобильное устройство, администратор должен выполнить следующие действия:

1. В Консоли администрирования открыть мастер подключения нового устройства.
2. Создать новый iOS MDM-профиль, установив в окне мастера создания профиля флажок **Показать сертификат после завершения работы мастера**.
3. Сохранить iOS MDM-профиль.
4. Установить iOS MDM-профиль на мобильное устройство пользователя с помощью утилиты Apple Configurator.

В результате мобильное устройство будет подключено к Серверу iOS MDM.

В связи с введенным компанией Apple ужесточением политики безопасности, для подключения мобильного устройства с операционной системой iOS 11 к Серверу администрирования с настроенной интеграцией с Public Key Infrastructure (PKI) необходимо настроить протоколы версий TLS 1.1 и TLS 1.2.

Добавление provisioning-профиля

► *Чтобы добавить provisioning-профиль на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

Откроется окно свойств Сервера мобильных устройств.

5. В окне свойств **Сервера iOS MDM** перейдите в раздел **Provisioning-профили**.
6. В разделе **Provisioning-профили** нажмите на кнопку **Импортировать** и укажите путь к файлу provisioning-профиля.

Профиль будет добавлен в параметры Сервера iOS MDM.

По кнопке **Экспортировать** provisioning-профиль можно сохранить в файле.

Импортированный provisioning-профиль можно установить на iOS MDM-устройства (см. раздел "Установка provisioning-профиля на устройство" на стр. [352](#)).

Установка provisioning-профиля на устройство

► *Чтобы установить provisioning-профиль на мобильное устройство, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.
3. Выберите мобильное устройство пользователя, на которое нужно установить provisioning-профиль.

Вы можете выбрать несколько мобильных устройств, чтобы установить на них provisioning-профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить provisioning-профиль** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить provisioning-профиль**.

В результате откроется окно **Выбор provisioning-профилей** со списком provisioning-профилей. Выберите в списке provisioning-профиль, который нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько provisioning-профилей одновременно. Чтобы выбрать диапазон provisioning-профилей, используйте клавишу **SHIFT**. Для объединения отдельных provisioning-профилей в группу используйте клавишу **CTRL**.

6. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

В результате выполнения команды выбранный provisioning-профиль будет установлен на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд примет значение *Завершено*.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

7. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Установленный профиль можно просмотреть и при необходимости удалить (см. раздел "Удаление provisioning-профиля с устройства" на стр. [354](#)).

Удаление provisioning-профиля с устройства

► Чтобы удалить provisioning-профиль с мобильного устройства, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.

3. Выберите мобильное устройство пользователя, с которого нужно удалить provisioning-профиль.

Вы можете выбрать несколько мобильных устройств, чтобы удалить с них provisioning-профиль одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить provisioning-профиль** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды**, затем **Удалить provisioning-профиль**.

В результате откроется окно **Удаление provisioning-профилей** со списком профилей.

6. Выберите в списке provisioning-профиль, который нужно удалить с мобильного устройства. Вы можете выбрать и удалить с мобильного устройства несколько provisioning-профилей одновременно. Чтобы выбрать диапазон provisioning-профилей, используйте клавишу **SHIFT**. Для объединения отдельных provisioning-профилей в группу используйте клавишу **CTRL**.

7. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

В результате выполнения команды выбранный provisioning-профиль будет удален с мобильного устройства пользователя. Приложения, связанные с удаленным

provisioning-профилем, не будут работать. В случае успешного выполнения команды текущий статус команды примет значение *Завершено*.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Добавление управляемого приложения

Перед установкой приложения на iOS MDM-устройство приложение необходимо добавить на Сервер iOS MDM. Приложение является управляемым, если оно было установлено на устройство с помощью Kaspersky Security Center. Управляемым приложением можно дистанционно управлять средствами Kaspersky Security Center.

► *Чтобы добавить управляемое приложение на Сервер iOS MDM, выполните следующие действия:*

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Серверы мобильных устройств**.
3. В рабочей области папки **Серверы мобильных устройств** выберите Сервер iOS MDM.
4. В контекстном меню Сервера iOS MDM выберите пункт **Свойства**.

Откроется окно свойств Сервера iOS MDM.

5. В окне свойств Сервера iOS MDM выберите раздел **Управляемые приложения**.

6. В разделе **Управляемые приложения** нажмите на кнопку **Добавить**.

Откроется окно **Добавление приложения**.

7. В окне **Добавление приложения** в поле **Название приложения** укажите название добавляемого приложения.

8. В поле **Apple ID приложения или ссылка на приложение в App Store** укажите Apple ID добавляемого приложения или ссылку на манифест-файл, по которой можно загрузить приложение.

9. Если вы хотите, чтобы при удалении iOS MDM-профиля одновременно с профилем с мобильного устройства пользователя было удалено и управляемое приложение, установите флажок **Удалять вместе с iOS MDM-профилем**.

10. Если вы хотите запретить резервное копирование данных приложения с помощью iTunes, установите флажок **Запретить создавать резервные копии данных**.

11. Нажмите на кнопку **ОК**.

Добавленное приложение отображается в разделе **Управляемые приложения** окна свойств Сервера iOS MDM.

Установка приложения на мобильное устройство

► *Чтобы установить приложение на мобильное устройство iOS MDM, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. Выберите iOS MDM-устройство, на которое нужно установить приложение.

Вы можете выбрать несколько мобильных устройств, чтобы установить на них приложение одновременно.

3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
4. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить приложение** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить приложение**.

В результате откроется окно **Выбор приложений** со списком приложений. Выберите в списке приложение, которое нужно установить на мобильное устройство. Вы можете выбрать и установить на мобильное устройство несколько приложений одновременно. Чтобы выбрать диапазон приложений, используйте клавишу **SHIFT**. Для объединения отдельных приложений в группу используйте клавишу **CTRL**.

5. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

В результате выполнения команды выбранное приложений будет установлено на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд принимает значение *Завершено*.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз. По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

6. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Информация об установленном приложении отображается в свойствах мобильного устройства iOS MDM (см. раздел "Просмотр информации о iOS MDM-устройстве" на стр. [361](#)). Вы можете удалить приложение с мобильного устройства с помощью журнала команд или из контекстного меню мобильного устройства (см. раздел "Удаление приложения с устройства" на стр. [358](#)).

Удаление приложения с устройства

► Чтобы удалить приложение с мобильного устройства, выполните следующие действия:

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте iOS MDM-устройства по протоколу управления *iOS MDM*.

3. Выберите мобильное устройство пользователя, с которого нужно удалить приложение.

Вы можете выбрать несколько мобильных устройств, чтобы удалить с них приложение одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Удалить приложение** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Удалить приложение**.

В результате откроется окно **Удаление приложений** со списком приложений.

6. Выберите в списке приложение, которое нужно удалить с мобильного устройства. Вы можете выбрать и удалить с устройства несколько приложений одновременно. Чтобы выбрать диапазон приложений, используйте клавишу **SHIFT**. Для объединения отдельных приложений в группу используйте клавишу **CTRL**.

7. Нажмите на кнопку **ОК**, чтобы отправить команду на мобильное устройство.

В результате выполнения команды выбранное приложение будет удалено с мобильного устройства пользователя. В случае успешного выполнения команды текущий статус команды примет значение *Завершено*.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз.

По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

8. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Установка приложения Kaspersky Safe Browser на мобильное устройство

► *Чтобы установить приложение Kaspersky Safe Browser на мобильное устройство iOS MDM, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки **Управление мобильными устройствами** отображается список управляемых мобильных устройств.

2. Выберите iOS MDM-устройство, на которое нужно установить приложение Kaspersky Safe Browser.

Вы можете выбрать несколько мобильных устройств, чтобы установить на них приложение Kaspersky Safe Browser одновременно.

3. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.

4. В окне **Команды для управления мобильным устройством** перейдите в раздел **Установить Kaspersky Safe Browser** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на устройство, выбрав в контекстном меню мобильного устройства пункт **Все команды**, затем **Установить Kaspersky Safe Browser**.

В результате выполнения команды приложение Kaspersky Safe Browser будет установлено на мобильное устройство пользователя. В случае успешного выполнения команды текущий статус команды в журнале команд принимает значение *Завершено*.

По кнопке **Отправить повторно** команду можно отправить на мобильное устройство пользователя еще раз. По кнопке **Удалить из очереди** выполнение отправленной команды можно отменить, если команда еще не выполнена.

В блоке **Журнал команд** отображаются команды, отправленные на мобильное устройство, и статусы выполнения этих команд. По кнопке **Обновить** вы можете обновить список команд.

5. Нажмите на кнопку **ОК**, чтобы закрыть окно **Команды для управления мобильным устройством**.

Информация об установленном приложении Kaspersky Safe Browser отображается в свойствах мобильного устройства iOS MDM (см. раздел "Просмотр информации о iOS MDM-устройстве" на стр. [361](#)). Вы можете удалить приложение с мобильного устройства с помощью журнала команд или из контекстного меню мобильного устройства (см. раздел "Удаление приложения с устройства" на стр. [358](#)).

Настройка параметров роуминга на мобильном устройстве iOS MDM

► Чтобы настроить параметры роуминга, выполните следующие действия:

1. В дереве консоли откройте папку **Управление мобильными устройствами**.
2. В папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

3. Выберите iOS MDM-устройство пользователя, для которого нужно настроить роуминг.

Вы можете выбрать несколько мобильных устройств, чтобы настроить для них роуминг одновременно.

4. В контекстном меню мобильного устройства выберите пункт **Показать журнал команд**.
5. В окне **Команды для управления мобильным устройством** перейдите в раздел **Настроить параметры роуминга** и нажмите на кнопку **Отправить команду**.

Вы также можете отправить команду на мобильное устройство, выбрав в контекстном меню устройства пункт **Все команды** → **Настроить параметры роуминга**.

6. В окне **Параметры роуминга** укажите нужные вам параметры:

- **Включить голосовой роуминг**

Если флажок установлен, на мобильном устройстве iOS MDM включен голосовой роуминг. Пользователь iOS MDM-устройства может звонить и отвечать на звонки в роуминге.

По умолчанию флажок установлен.

- **Включить роуминг данных**

Если флажок установлен, на мобильном устройстве iOS MDM включен роуминг данных. Пользователь iOS MDM-устройства может пользоваться интернетом в роуминге.

По умолчанию флажок снят.

Параметры роуминга будут настроены для выбранных устройств.

Просмотр информации о iOS MDM-устройстве

► *Чтобы просмотреть информацию о iOS MDM-устройстве, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM по ссылке **iOS MDM**.
3. Выберите мобильное устройство, информацию о котором нужно просмотреть.
4. В контекстном меню мобильного устройства выберите пункт **Свойства**.

В результате откроется окно свойств iOS MDM-устройства.

В окне свойств мобильного устройства отображается информация о подключенном iOS MDM-устройстве.

Отключение iOS MDM-устройства от управления

► *Чтобы отключить iOS MDM-устройство от Сервера iOS MDM, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте устройства iOS MDM по ссылке **iOS MDM**.
3. Выберите мобильное устройство, которое необходимо отключить.
4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

В результате iOS MDM-устройство будет отмечено в списке на удаление. Мобильное устройство будет автоматически удалено из списка управляемых устройств после его удаления из базы данных Сервера iOS MDM. Удаление мобильного устройства из базы данных Сервера iOS MDM происходит в течение одной минуты.

В результате отключения iOS MDM-устройства от управления с мобильного устройства будут удалены все установленные конфигурационные профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем** (см. раздел "**Добавление управляемого приложения**" на стр. [355](#)).

Отправка команд на устройство

► Чтобы отправить команду на iOS MDM-устройство, администратор должен выполнить следующие действия:

1. В Консоли администрирования открыть узел **Управление мобильными устройствами**.
2. Выбрать папку **Мобильные устройства**.
3. В папке **Мобильные устройства** выбрать мобильное устройство, на которое необходимо отправить команды.
4. В контекстном меню мобильного устройства выбрать пункт **Показать журнал команд** или **Управление устройством**, во всплывающем списке выбрать необходимую команду для отправки на мобильное устройство.

Проверка статуса исполнения отправленных команд

► Чтобы проверить статус выполнения отправленной команды на мобильном устройстве, администратор должен выполнить следующие действия:

1. В Консоли администрирования открыть узел **Управление мобильными устройствами**.
2. Выбрать папку **Мобильные устройства**.
3. В папке **Мобильные устройства** выбрать мобильное устройство, на котором необходимо проверить статус выполнения отправленных команд.
4. В контекстном меню мобильного устройства выбрать пункт **Показать журнал команд**.

Управление KES-устройствами

Kaspersky Security Center поддерживает следующие возможности для управления мобильными KES-устройствами:

- централизованно управлять KES-устройствами с помощью команд (см. раздел "Команды для управления мобильными устройствами" на стр. [307](#));
- просматривать информацию о параметрах управления KES-устройствами (см. раздел "Просмотр информации о KES-устройстве" на стр. [367](#));
- устанавливать приложения с помощью пакетов мобильных приложений (см. раздел "Создание пакета мобильных приложений для KES-устройств" на стр. [364](#));
- отключать KES-устройства от управления (см. раздел "Отключение KES-устройства от управления" на стр. [367](#)).

В этом разделе

Создание пакета мобильных приложений для KES-устройств.....	364
Включение двухфакторной аутентификации KES-устройств	366
Просмотр информации о KES-устройстве	367
Отключение KES-устройства от управления.....	367

Создание пакета мобильных приложений для KES-устройств

Для создания пакета мобильных приложений для KES-устройств необходима лицензия Kaspersky Endpoint Security для Android.

► *Чтобы создать пакет мобильных приложений, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Управлять пакетами мобильных приложений**.

3. В окне **Управление пакетами мобильных приложений** нажмите на кнопку **Новый**.

4. Запустится мастер создания пакета мобильных приложений. Следуйте указаниям мастера.

5. Если вы хотите поместить программу в контейнер, в окне мастера **Параметры** установите флажок **Создать контейнер с выбранным приложением**.

Если на рабочем месте администратора установлен плагин Kaspersky Endpoint Security для Android Service Pack 3 Maintenance Release 2 или более поздней версии, флажок **Создать контейнер с выбранным приложением** недоступен. Поддержка создания контейнеров для мобильных приложений прекращена. Вы можете доставлять на Android-устройства контейнеры, созданные в более ранних версиях.

Созданный пакет мобильных приложений отобразится в окне **Управление пакетами мобильных приложений**.

Контейнеры используются для контроля активности программ, запускаемых на мобильном устройстве пользователя. К программам, помещенным в контейнер, могут быть применены правила политики безопасности. Правила для программ можно настроить в окне свойств политики программы Kaspersky Endpoint Security для Android в разделе **Контейнеры**. Подробная информация о контейнерах и работе с ними приведена в документации для программы Kaspersky Endpoint Security для Android.

Вы можете поместить в контейнер стороннюю программу. Невозможно поместить в контейнер дистрибутив Kaspersky Endpoint Security 10 для Android.

Включение двухфакторной аутентификации KES-устройств

► Чтобы включить двухфакторную аутентификацию KES-устройства, выполните следующие действия:

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
 - для 64-разрядной системы:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\core\independent\KLLIM`
 - для 32-разрядной системы:
`HKLM\Software\KasperskyLab\Components\34\core\independent\KLLIM`
3. Создайте ключ с именем LP_MobileMustUseTwoWayAuthOnPort13292.
4. Укажите тип ключа REG_DWORD.
5. Установите значение ключа 1.
6. Перезапустите службу Сервера администрирования.

В результате обязательная двухфакторная аутентификация KES-устройства с использованием общего сертификата будет включена после запуска службы Сервера администрирования.

При первом подключении KES-устройства к Серверу администрирования наличие сертификата не обязательно.

По умолчанию двухфакторная аутентификация KES-устройств отключена.

Просмотр информации о KES-устройстве

► *Чтобы просмотреть информацию о KES-устройстве, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте KES-устройства по протоколу управления *KES*.
3. Выберите мобильное устройство, информацию которого нужно просмотреть.
4. В контекстном меню мобильного устройства выберите пункт **Свойства**.

В результате откроется окно свойств KES-устройства.

В окне свойств мобильного устройства отображается информация о подключенном KES-устройстве.

Отключение KES-устройства от управления

Чтобы отключить KES-устройство от управления, пользователь должен удалить Агент администрирования с мобильного устройства. После удаления пользователем Агента администрирования информация о мобильном устройстве удаляется из базы данных Сервера администрирования и администратор может удалить мобильное устройство из списка управляемых устройств.

► *Чтобы удалить KES-устройство из списка управляемых устройств, выполните следующие действия:*

1. В дереве консоли в папке **Управление мобильными устройствами** выберите вложенную папку **Мобильные устройства**.

В рабочей области папки отображается список управляемых мобильных устройств.

2. В рабочей области отфильтруйте KES-устройства по протоколу управления *KES*.
3. Выберите мобильное устройство, которое необходимо отключить от управления.

4. В контекстном меню мобильного устройства выберите пункт **Удалить**.

В результате мобильное устройство будет удалено из списка управляемых устройств.

Если Kaspersky Endpoint Security для Android не удален с мобильного устройства, то после синхронизации с Сервером администрирования мобильное устройство снова появится в списке управляемых устройств.

Инвентаризация оборудования, обнаруженного в сети

Kaspersky Security Center получает информацию об оборудовании, обнаруженном в результате опроса сети. Инвентаризации подвергается любое оборудование, подключенное к сети организации. При каждом последующем опросе сети информация об оборудовании обновляется. В списке обнаруженного оборудования могут присутствовать следующие типы устройств:

- устройства;
- мобильные устройства;
- сетевые устройства;
- виртуальные устройства;
- компьютерные комплектующие;
- компьютерная периферия;
- подключаемые устройства;
- VoIP-телефоны;
- сетевые хранилища.

Обнаруженное в ходе опроса сети оборудование отображается в папке **Хранилища**, вложенной в папку **Оборудование** дерева консоли.

Администратор может добавлять новые устройства в список оборудования вручную или редактировать информацию об уже имеющемся в сети оборудовании. В свойствах устройства можно просматривать и редактировать подробную информацию об устройствах.

Администратор может присваивать обнаруженным устройствам признак "Корпоративное оборудование". Этот признак можно присвоить в свойствах устройства вручную или задать критерии для его автоматического присвоения. В этом случае признак "Корпоративное оборудование" присваивается по типу устройства. По признаку "Корпоративное оборудование" можно разрешать или запрещать подключение оборудования к сети.

Kaspersky Security Center позволяет выполнять списание оборудования. Для этого в свойствах устройства необходимо установить флажок **Устройство списано**. Такое устройство не отображается в списке оборудования.

Администратор может работать со списком программируемых логических контроллеров (ПЛК) в папке **Оборудование**. Подробная информация о работе со списками ПЛК приведена в *Руководстве пользователя Kaspersky Industrial CyberSecurity for Networks*.

В этом разделе

Добавление информации о новых устройствах	369
Настройка критериев определения корпоративных устройств.....	370
Настройка пользовательских полей.....	371

Добавление информации о новых устройствах

► *Чтобы добавить информацию о новых устройствах в сети, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** по кнопке **Добавить устройство** откройте окно **Новое устройство**.

Откроется окно **Новое устройство**.

3. В окне **Новое устройство** в раскрывающемся списке **Тип** выберите тип устройства, которое вы хотите добавить.
4. Нажмите на кнопку **ОК**.

Откроется окно свойств устройства на разделе **Общие**.

5. В разделе **Общие** заполните поля ввода данными об устройстве. В разделе **Общие** доступны следующие параметры:
 - **Корпоративное устройство**. Установите флажок, если вы хотите присвоить устройству признак "Корпоративное". По этому признаку можно выполнять поиск устройств в папке **Оборудование**.
 - **Устройство списано**. Установите флажок, если вы не хотите, чтобы устройство отображалось в списке устройств в папке **Оборудование**.
6. Нажмите на кнопку **Применить**.

Новое устройство отобразится в рабочей области папки **Оборудование**.

Настройка критериев определения корпоративных устройств

► *Чтобы настроить критерии определения корпоративных устройств, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить критерии определения корпоративных устройств**.

Откроется окно свойств оборудования.

3. В окне свойств оборудования в разделе **Корпоративные устройства** выберите способ присвоения устройству признака "Корпоративное":

- **Вручную устанавливать для устройства признак "Корпоративное"**. Признак "Корпоративное оборудование" назначается устройству вручную в окне свойств устройства в разделе **Общие**.
- **Автоматически устанавливать для устройства признак "Корпоративное"**. В блоке параметров **По типу устройства** укажите типы устройств, которым программа будет автоматически присваивать признак "Корпоративное".

4. Нажмите на кнопку **Применить**.

Настройка пользовательских полей

► *Чтобы настроить пользовательские поля устройств, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить пользовательские поля данных**.

Откроется окно свойств оборудования.

3. В окне свойств оборудования в разделе **Пользовательские поля** нажмите на кнопку **Добавить**.

Откроется окно **Добавить поле**.

4. В окне **Добавить поле** укажите название пользовательского поля, которое будет отображаться в свойствах оборудования.

Вы можете создать несколько пользовательских полей с уникальными именами.

5. Нажмите на кнопку **Применить**.

В результате в свойствах оборудования в разделе **Пользовательские поля** будут отображаться добавленные пользовательские поля. Вы можете использовать пользовательские поля для указания специфической информации об устройствах. Например, номер внутренней заявки на приобретение оборудования.

Обновление баз и программных модулей

В этом разделе описаны загрузка и распространение обновлений баз и программных модулей с помощью Kaspersky Security Center.

Для поддержания системы защиты нужно своевременно обновлять базы и модули программ "Лаборатории Касперского", управляемых при помощи Kaspersky Security Center.

Для обновления баз и модулей программ "Лаборатории Касперского", управляемых при помощи Kaspersky Security Center, используется задача Сервера администрирования **Загрузка обновлений в хранилище**. В результате выполнения задачи на Сервер администрирования с источника обновлений загружаются базы и обновления программных модулей.

Задача **Загрузка обновлений в хранилище** недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок перед установкой на клиентские устройства.

При выполнении задачи **Загрузка обновлений в хранилище**, для обеспечения загрузки необходимых версий баз и программных модулей, на серверы обновлений «Лаборатории Касперского» в автоматическом режиме передается следующая информация:

- идентификатор и версия программы,
- идентификатор установки программы;
- идентификатор активного ключа;
- идентификатор запуска задачи **Загрузка обновлений в хранилище**.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

В этом разделе

Создание задачи загрузки обновлений в хранилище.....	373
Создание задачи принудительной загрузки обновлений в хранилища агентов обновлений.....	375
Настройка параметров задачи загрузки обновлений в хранилище.....	377
Проверка полученных обновлений.....	377
Настройка проверочных политик и вспомогательных задач	379
Просмотр полученных обновлений	381
Автоматическое распространение обновлений.....	381
Удаление обновлений программного обеспечения из хранилища.....	391
Алгоритм установки патча для программы "Лаборатории Касперского" в кластерной модели	391

Создание задачи загрузки обновлений в хранилище

Задача загрузки обновлений в хранилище Сервера администрирования создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище может быть создана в одном экземпляре. Поэтому вы можете создать задачу загрузки обновлений в хранилище только в случае, если она была удалена из списка задач Сервера администрирования.

► Чтобы создать задачу загрузки обновлений в хранилище, выполните следующие действия:

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи одним из следующих способов:
 - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.
 - По кнопке **Создать задачу** в рабочей области.

В результате запускается мастер создания задачи. Следуйте его указаниям. В окне мастера **Тип задачи** выберите тип задачи **Загрузка обновлений в хранилище**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилище** появится в списке задач Сервера администрирования.

В результате выполнения задачи **Загрузка обновлений в хранилище** обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского" – серверы "Лаборатории Касперского", на которых размещаются обновленные базы и программные модули.
- Главный Сервер администрирования.
- FTP- / HTTP-сервер или сетевая папка обновлений – FTP-, HTTP-сервер, локальная или сетевая папка, добавленная пользователем и содержащая актуальные обновления. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

Для обновления Сервера администрирования с FTP- / HTTP-сервера или из сетевой папки на эти ресурсы требуется скопировать правильную структуру папок с обновлениями, совпадающую со структурой, формируемой при использовании серверов обновлений "Лаборатории Касперского".

Выбор ресурса зависит от параметров задачи. По умолчанию обновление производится из интернета с серверов обновлений "Лаборатории Касперского".

См. также

| Проверка полученных обновлений..... [377](#)

Создание задачи принудительной загрузки обновлений в хранилища агентов обновлений

Вы можете создать задачу **Принудительная загрузка обновлений в хранилища агентов обновлений** для группы администрирования. Такая задача будет выполняться для агентов обновлений, входящих в указанную группу администрирования. Задача **Принудительная загрузка обновлений в хранилища агентов обновлений** позволяет экономить трафик сети, так как обновления загружаются один раз в папку общего доступа агентов обновлений группы администрирования и задача не распространяется на каждый Агент администрирования группы.

► *Чтобы создать задачу принудительной загрузки обновлений в хранилище агентов обновлений для выбранной группы администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. По кнопке **Создать задачу** в рабочей области папки запустите мастер создания задачи.

3. В окне **Тип задачи** мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center 10**.
4. В узле **Сервер администрирования Kaspersky Security Center 10** раскройте папку **Дополнительно**.
5. В папке **Дополнительно** выберите задачу **Принудительная загрузка обновлений в хранилища агентов обновлений**.
6. Следуйте шагам мастера.

После завершения работы мастера созданная задача **Принудительная загрузка обновлений в хранилища агентов обновлений** появится в списке задач Агента администрирования в соответствующей группе администрирования и в папке **Задачи**.

В результате выполнения задачи **Принудительная загрузка обновлений в хранилища агентов обновлений** обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа. Загруженные обновления будут использоваться только теми агентами обновлений, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

В свойствах каждого агента обновлений в разделе **Источники обновлений** можно указать источники обновлений (*Получать с Сервера администрирования* или *Использовать задачу получения обновлений*). Для агента обновлений, назначенного вручную или автоматически, по умолчанию выбран вариант **Получать с Сервера администрирования**. Такие агенты обновлений будут использовать результаты задачи **Принудительная загрузка обновлений в хранилища агентов обновлений**.

В свойствах каждого агента обновлений указана сетевая папка, настроенная индивидуально для этого агента обновлений. Названия папок могут быть разными для разных агентов обновлений. Поэтому не рекомендуется изменять сетевую папку обновлений в свойствах задачи, если задача создается для группы устройств.

Вы можете изменить сетевую папку обновлений в свойствах задачи **Принудительная загрузка обновлений в хранилища агентов обновлений**, если вы создаете локальную задачу для устройства.

Предыдущие версии программы, Kaspersky Security Center Service Pack 2 и ниже, позволяли создать задачу загрузки обновлений для агентов обновлений только как локальную задачу. Начиная с версии Kaspersky Security Center Service Pack 3 такого ограничения нет, что приводит к уменьшению трафика.

Настройка параметров задачи загрузки обновлений в хранилище

► Чтобы настроить параметры задачи загрузки обновлений в хранилище, выполните следующие действия:

1. В рабочей области папки дерева консоли **Задачи** выберите задачу **Загрузка обновлений в хранилище** в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:
 - В контекстном меню задачи выберите пункт **Свойства**.
 - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.

В результате откроется окно свойств задачи **Загрузка обновлений в хранилище**. В нем вы можете настроить параметры загрузки обновлений в хранилище Сервера администрирования.

Проверка полученных обновлений

► Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства, выполните следующие действия:

1. В рабочей области папки **Задачи** дерева консоли выберите задачу **Загрузка обновлений в хранилище** в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:
 - В контекстном меню задачи выберите пункт **Свойства**.

- По ссылке **Изменить параметры задачи** в блоке работы с выбранной задачей.
3. В открывшемся окне свойств задачи в разделе **Проверка обновлений** установите флажок **Выполнять проверку обновлений перед распространением** и выберите задачу проверки обновлений одним из следующих способов:

- Нажмите на кнопку **Выбрать**, чтобы выбрать уже сформированную задачу проверки обновлений.
- Нажмите на кнопку **Создать**, чтобы создать задачу проверки обновлений.

В результате запустится мастер создания задачи проверки обновлений. Следуйте его указаниям.

Во время создания задачи проверки обновлений необходимо выбрать группу администрирования, на устройствах которой будет выполняться задача. Устройства, входящие в эту группу, называются *тестовыми устройствами*.

В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Это позволяет повысить качество проверки, снизить риск возникновения ложных срабатываний, а также вероятность обнаружения вирусов при проверке (при нахождении вирусов на тестовых устройствах задача проверки обновлений считается завершившейся неудачно).

4. Закройте окно свойств задачи загрузки обновлений в хранилище, нажав на кнопку **ОК**.

В результате в рамках выполнения задачи загрузки обновлений в хранилище будет выполняться задача проверки полученных обновлений. Сервер администрирования будет копировать обновления с источника, сохранять их во временном хранилище и запускать задачу проверки обновлений. В случае успешного выполнения этой задачи обновления будут скопированы из временного хранилища в папку общего доступа Сервера администрирования (<Папка установки Kaspersky Security Center>\Share\Updates) и распространены на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи проверки обновлений размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится и на Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции будут выполнены при следующем запуске задачи загрузки обновлений в хранилище, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты программы защиты;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования программы "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача проверки обновлений считается успешно выполненной.

Настройка проверочных политик и вспомогательных задач

При создании задачи проверки обновлений Сервер администрирования формирует проверочные политики, а также вспомогательные групповые задачи обновления и проверки по требованию.

На выполнение вспомогательных групповых задач обновления и проверки по требованию требуется некоторое время. Эти задачи выполняются в рамках выполнения задачи проверки обновлений. Задача проверки обновлений выполняется в рамках выполнения задачи загрузки обновлений в хранилище. Время выполнения задачи загрузки обновлений в хранилище включает в себя время выполнения вспомогательных групповых задач обновления и проверки по требованию.

Параметры проверочных политик и вспомогательных задач можно изменять.

► *Чтобы изменить параметры проверочной политики или вспомогательной задачи, выполните следующие действия:*

1. В дереве консоли выберите группу, для которой сформирована задача проверки обновлений.
2. В рабочей области группы выберите одну из следующих закладок:
 - **Политики**, если вы хотите изменить параметры проверочной политики.
 - **Задачи**, если вы хотите изменить параметры вспомогательной задачи.
3. В рабочей области закладки выберите политику или задачу, параметры которой вы хотите изменить.
4. Откройте окно свойств этой политики (задачи) одним из следующих способов:
 - В контекстном меню политики (задачи) выберите пункт **Свойства**.
 - По ссылке **Настроить параметры политики (Настроить параметры задачи)** в блоке работы с выбранной политикой (задачей).

Чтобы проверка обновлений выполнялась правильно, необходимо соблюдать следующие ограничения на изменение параметров проверочных политик и вспомогательных задач:

- В параметрах вспомогательных задач:
 - Сохранять на Сервере администрирования все события с уровнями важности **Критическое событие** и **Отказ функционирования**. На основе событий этих типов Сервер администрирования проводит анализ работы программ.

- Использовать в качестве источника обновлений Сервер администрирования.
- Указывать тип расписания задач: **Вручную**.
- В параметрах проверочных политик:
 - Не использовать технологии ускорения проверки iChecker, iSwift и iStream.
 - Выбрать действия над зараженными объектами: **Не запрашивать / Пропускать / Записывать информацию в отчет**.
- В параметрах проверочных политик и вспомогательных задач:

Если после установки обновлений программных модулей потребуется перезагрузка устройства, ее следует выполнить незамедлительно. Если устройство не будет перезагружено, то проверить этот тип обновлений будет невозможно. Для некоторых программ установка обновлений, требующих перезагрузки, может быть запрещена или выполняться только после подтверждения от пользователя. Эти ограничения должны быть отключены в параметрах проверочных политик и вспомогательных задач.

Просмотр полученных обновлений

► Чтобы просмотреть список полученных обновлений,

в дереве консоли в папке **Хранилища** выберите вложенную папку **Обновления и патчи ПО "Лаборатории Касперского"**.

В рабочей области папки **Обновления и патчи ПО "Лаборатории Касперского"** представлен список обновлений, сохраненных на Сервере администрирования.

Автоматическое распространение обновлений

Kaspersky Security Center позволяет автоматически распространять и устанавливать обновления на клиентские устройства и подчиненные Серверы администрирования.

В этом разделе

Автоматическое распространение обновлений на клиентские устройства	382
Автоматическое распространение обновлений на подчиненные Серверы администрирования	383
Автоматическая установка обновлений программных модулей Агентов администрирования	384
Назначение устройства агентом обновлений вручную	385
Удаление устройства из списка агентов обновлений	389
Получение обновлений агентами обновлений	389

Автоматическое распространение обновлений на клиентские устройства

► *Чтобы обновления выбранной вами программы автоматически распространялись на клиентские устройства сразу после загрузки обновлений в хранилище Сервера администрирования, выполните следующие действия:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся клиентские устройства.
2. Создайте задачу распространения обновлений этой программы для выбранных клиентских устройств одним из следующих способов:
 - Если требуется распространять обновления на клиентские устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы (см. раздел "Создание задачи" на стр. [90](#)).
 - Если требуется распространять обновления на клиентские устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств (см. раздел "Создание задачи для набора устройств" на стр. [92](#)).

В результате запустится мастер создания задачи. Следуйте его указаниям, выполнив следующие условия:

- a. В окне мастера **Тип задачи** в узле нужной вам программы выберите задачу распространения обновлений.

Название задачи распространения обновлений, которое отображается в окне **Тип задачи**, зависит от программы, для которой создается задача. Подробнее о названиях задач обновления для выбранных программ "Лаборатории Касперского" см. в Руководствах к этим программам.

- b. В окне мастера **Расписание** в поле **Запуск по расписанию** выберите вариант запуска **При загрузке обновлений в хранилище**.

В результате созданная задача распространения обновлений будет запускаться для выбранных устройств каждый раз при загрузке обновлений в хранилище Сервера администрирования.

Если задача распространения обновлений нужной вам программы уже создана для выбранных устройств, для автоматического распространения обновлений на клиентские устройства в окне свойств задачи в разделе **Расписание** нужно выбрать вариант запуска **При загрузке обновлений в хранилище** в поле **Запуск по расписанию**.

Автоматическое распространение обновлений на подчиненные Серверы администрирования

► Чтобы обновления выбранной вами программы автоматически распространялись на подчиненные Серверы администрирования сразу после загрузки обновлений в хранилище главного Сервера администрирования, выполните следующие действия:

1. В дереве консоли в узле главного Сервера администрирования выберите папку **Задачи**.
2. В списке задач рабочей области выберите задачу загрузки обновлений в хранилище Сервера администрирования.

3. Откройте раздел **Параметры** окна свойств выбранной задачи одним из следующих способов:
 - В контекстном меню задачи выберите пункт **Свойства**.
 - По ссылке **Изменить параметры** в блоке работы с выбранной задачей.
4. В разделе **Параметры** окна свойств задачи откройте окно **Прочие параметры** по ссылке **Настроить** в подразделе **Прочие параметры**.
5. В открывшемся окне **Прочие параметры** установите флажок **Форсировать обновление подчиненных Серверов**.

В параметрах задачи получения обновлений Сервером администрирования на закладке **Параметры** окна свойств задачи установите флажок **Форсировать обновление подчиненных Серверов**.

В результате сразу после получения обновлений главным Сервером администрирования будут автоматически запускаться задачи загрузки обновлений подчиненными Серверами администрирования, независимо от расписания, установленного в параметрах этих задач.

Автоматическая установка обновлений программных модулей Агентов администрирования

- ▶ *Чтобы обновления программных модулей Агентов администрирования автоматически устанавливались после их загрузки в хранилище Сервера администрирования, выполните следующие действия:*
 1. В дереве консоли в узле главного Сервера администрирования выберите папку **Задачи**.
 2. В списке задач в рабочей области выберите задачу загрузки обновлений в хранилище Сервера администрирования.
 3. Откройте окно свойств выбранной задачи одним из следующих способов:
 - В контекстном меню задачи выберите пункт **Свойства**.

- По ссылке **Изменить параметры** в блоке работы с выбранной задачей.
4. В окне свойств задачи выберите раздел **Параметры**.
 5. По ссылке **Настроить** в блоке **Прочие параметры** откройте окно **Прочие параметры**.
 6. В открывшемся окне **Прочие параметры** установите флажок **Обновлять модули Агентов администрирования**.

Если флажок установлен, обновления программных модулей Агента администрирования будут устанавливаться автоматически после их загрузки в хранилище Сервера администрирования. Если флажок снят, автоматическая установка обновлений Агента администрирования не выполняется. Полученные обновления можно устанавливать вручную. По умолчанию флажок установлен.

Автоматическая установка программных модулей Агентов администрирования доступна только для Агентов администрирования версии 10 Service Pack 1 и ниже.

7. Нажмите на кнопку **ОК**.

В результате обновления программных модулей Агентов администрирования будут устанавливаться автоматически.

Назначение устройства агентом обновлений вручную

Kaspersky Security Center позволяет назначать устройства агентами обновлений.

Рекомендуется назначать агенты обновлений автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать агентами обновлений. Однако если вы по какой-то причине хотите отказаться от автоматического назначения агентов обновлений (например, если вы хотите использовать специально выделенные серверы), вы можете назначать агенты обновлений вручную, предварительно рассчитав их количество и конфигурацию.

► Чтобы вручную назначить устройство агентом обновлений, выполните следующие действия:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Агенты обновлений** нажмите на кнопку **Добавить**. Кнопка доступна, если выбран вариант **Вручную назначать агенты обновлений**.

В результате откроется окно **Добавление агента обновлений**.

4. В окне **Добавление агента обновлений** выполните следующие действия:
 - a. Выберите устройство, которое будет выполнять роль агента обновлений (выберите в группе администрирования или укажите IP-адрес устройства). При выборе устройства учитывайте особенности работы агентов обновлений и требования к устройству, которое выполняет роль агента обновлений.
 - b. Укажите набор устройств, на которые агент обновлений будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.
5. Нажмите на кнопку **ОК**.

Добавленный агент обновлений отобразится в списке агентов обновлений в разделе **Агенты обновлений**.

6. Выберите в списке добавленный агент обновлений и по кнопке **Свойства** откройте окно его свойств.
7. В окне свойств настройте параметры агента обновлений:
 - В разделе **Общие** укажите параметры взаимодействия агента обновлений с клиентскими устройствами:
 - **Номер SSL-порта.**

Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к агенту обновлений с

использованием протокола SSL.

По умолчанию номер порта – 13000.

- **Использовать многоадресную IP-рассылку.**

Если флажок установлен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

- **Адрес IP-рассылки.**

IP-адрес, на который будет выполняться многоадресная рассылка.

IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

По умолчанию указан IP-адрес 225.6.7.8.

- **Номер порта IP-рассылки.**

Номер порта многоадресной рассылки.

Номер порта по умолчанию – 15001. Если в качестве агента обновлений указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

- **Распространять обновления.**

Если флажок установлен, обновления распространяются на клиентские устройства с помощью этого агента обновлений.

По умолчанию флажок установлен.

- **Распространять инсталляционные пакеты.**

Если флажок установлен, инсталляционные пакеты обновления распространяются на клиентские устройства с помощью этого агента обновлений.

По умолчанию флажок установлен.

- В разделе **Область действия** укажите область, на которую агент обновлений распространяет обновления (группы администрирования и / или сетевое местоположение).
- В разделе **Опрос сети** настройте параметры опроса агентом обновлений доменов Windows, Active Directory и IP-диапазонов.

- В разделе **Дополнительно** укажите папку, которую агент обновлений должен использовать для хранения распространяемых данных.

- **Использовать папку по умолчанию.**

При выборе этого варианта для сохранения данных будет использоваться папка, в которую на агенте обновлений установлен Агент администрирования.

- **Использовать указанную папку.**

При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на агенте обновлений, так и удаленно, на любом из устройств, входящих в состав сети организации.

Учетная запись, под которой на агенте обновлений запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

В результате выбранные устройства будут выполнять роль агентов обновлений.

Только устройства под управлением операционной системы Windows могут определять свое сетевое местоположение. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

► *Чтобы назначить агенты обновлений автоматически с помощью Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Агенты обновлений** выберите вариант **Автоматически назначать агенты обновлений**.

Если автоматическое назначение устройств агентами обновлений включено, невозможно вручную настраивать параметры агентов обновлений, а также изменять список агентов обновлений.

4. Нажмите на кнопку **ОК**.

В результате Сервер администрирования будет автоматически назначать агенты обновлений и настраивать их параметры.

Удаление устройства из списка агентов обновлений

► *Чтобы удалить устройство из списка агентов обновлений, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Агенты обновлений** выберите устройство, выполняющее функции агента обновлений, и нажмите на кнопку **Удалить**.

В результате устройство будет удалено из списка агентов обновлений и перестанет выполнять функции агента обновлений.

Нельзя удалить устройство из списка агентов обновлений, если оно было назначено Сервером администрирования автоматически (см. раздел "Назначение устройства агентом обновлений вручную" на стр. [385](#)).

Получение обновлений агентами обновлений

Kaspersky Security Center позволяет агентам обновлений получать обновления от Сервера администрирования, серверов "Лаборатории Касперского", из локальной или сетевой папки.

► *Чтобы настроить получение обновлений для агента обновлений, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования**.

2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Агенты обновлений** выберите агент обновлений, через который обновления будут доставляться на клиентские устройства группы.
4. По кнопке **Свойства** откройте окно свойств выбранного агента обновлений.
5. В окне свойств агента выберите раздел **Источник обновлений**.
6. Выберите источник обновлений для агента обновлений:
 - Чтобы агент обновлений получал обновления с Сервера администрирования, выберите вариант **Получать с Сервера администрирования**.
 - Чтобы агент обновлений получал обновления с помощью задачи, выберите вариант **Использовать задачу принудительной загрузки обновлений**:
 - Нажмите на кнопку **Выбрать**, если такая задача уже есть на устройстве, и выберите задачу в появившемся списке.
 - Нажмите на кнопку **Новая задача**, чтобы создать задачу, если такой задачи еще нет на устройстве. Запустится мастер создания задачи. Следуйте его указаниям.

Задача принудительной загрузки обновлений в хранилище обновлений – локальная задача. Для каждого устройства, выполняющего роль агента обновлений, задачу требуется создавать отдельно.

В результате агент обновлений будет получать обновления из указанного источника.

Удаление обновлений программного обеспечения из хранилища

► Чтобы удалить обновления программного обеспечения из хранилища Сервера администрирования, выполните следующие действия:

1. В дереве консоли в папке **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** выберите обновление, которое нужно удалить.
3. В контекстном меню обновления выберите **Удалить файлы обновлений**.

Обновления программного обеспечения будут удалены из хранилища Сервера администрирования.

Алгоритм установки патча для программы "Лаборатории Касперского" в кластерной модели

Kaspersky Security Center поддерживает только ручную установку патчей для программ "Лаборатории Касперского" в кластерной модели.

Чтобы установить патч для программы «Лаборатории Касперского», выполните следующие действия:

1. Загрузите на каждый узел кластера патч.
2. Запустите установку патча на активном узле.

Дождитесь успешной установки патча.

3. Последовательно запустите патч на всех подчиненных узлах кластера.

При запуске патча из командной строки используйте ключ `"-CLUSTER_SECONDARY_NODE"`.

В результате этих действий патч будет установлен на каждом узле кластера.

4. Запустите вручную кластерные службы "Лаборатории Касперского".

Каждый узел кластера будет отображаться в Консоли администрирования как устройство с установленным Агентом администрирования.

Информацию об установленных патчах можно просмотреть в папке **Обновления программного обеспечения** или в отчете о версиях обновлений программных модулей программ "Лаборатории Касперского".

См. также

Настройка общих параметров Сервера администрирования..... [40](#)

Работа с ключами программ

В этом разделе описаны возможности Kaspersky Security Center по работе с ключами управляемых программ "Лаборатории Касперского".

Kaspersky Security Center позволяет централизованно распространять ключи программ "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении ключа с помощью Kaspersky Security Center свойства ключа сохраняются на Сервере администрирования. На основании этой информации программа формирует отчет об использовании ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах ключей. Вы можете настраивать параметры оповещений об использовании ключей в составе параметров Сервера администрирования.

В этом разделе

Просмотр информации об используемых ключах	393
Добавление ключа в хранилище Сервера администрирования.....	394
Удаление ключа Сервера администрирования	394
Распространение ключа на клиентские устройства	395
Автоматическое распространение ключа	396
Создание и просмотр отчета об использовании ключей	397

Просмотр информации об используемых ключах

- Чтобы просмотреть информацию об используемых ключах, выберите в дереве консоли папку **Лицензии Лаборатории Касперского**.

В рабочей области папки отображается перечень ключей, используемых на клиентских устройствах.

Рядом с каждым ключом отображается значок, соответствующий типу его использования:

-  – информация об используемом ключе получена от подключенного к Серверу администрирования клиентского устройства. Файл этого ключа не хранится на Сервере администрирования.
-  – файл ключа находится в хранилище Сервера администрирования. Автоматическое распространение этого ключа отключено.
-  – файл ключа находится в хранилище Сервера администрирования. Включено автоматическое распространение этого ключа.

Вы можете просмотреть информацию о том, какие ключи используются для программы на клиентском устройстве, в разделе **Программы** окна свойств клиентского устройства (см. раздел "Просмотр и изменение локальных параметров программы" на стр. [105](#)).

Для определения актуальных параметров ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки.

Добавление ключа в хранилище Сервера администрирования

► *Чтобы добавить ключ в хранилище Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. Запустите задачу добавления ключа одним из следующих способов:
 - в контекстном меню списка ключей выберите пункт **Добавить код активации или ключ**;
 - по ссылке **Добавить код активации или ключ** в блоке управления списком ключей.

В результате запускается мастер добавления ключа. Следуйте его указаниям.

Удаление ключа Сервера администрирования

► *Чтобы удалить ключ Сервера администрирования, выполните следующие действия:*

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования выберите раздел **Ключи**.

3. Удалите активный или дополнительный ключ по кнопке **Удалить**.

В результате ключ будет удален.

Если добавлен дополнительный ключ, после удаления активного ключа дополнительный ключ автоматически становится активным.

После удаления активного ключа для Сервера администрирования становятся недоступными функции Системное администрирование и Управление мобильными устройствами. Можно добавить (см. раздел "Добавление ключа в хранилище Сервера администрирования" на стр. [394](#)) удаленный ключ повторно или добавить другой ключ.

Распространение ключа на клиентские устройства

Kaspersky Security Center позволяет распространить ключ на клиентские устройства с помощью задачи распространения ключа.

► *Чтобы распространить ключ на клиентские устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Лицензии Лаборатории Касперского**.
2. Нажмите на кнопку **Распространить ключ на управляемые устройства** в блоке управления списком ключей.

В результате запустится мастер создания задачи распространения ключа. Следуйте его указаниям.

Задачи, сформированные при помощи мастера создания задачи распространения ключа, являются задачами для наборов устройств и размещаются в папке **Задачи** дерева консоли.

Вы также можете создать групповую или локальную задачу распространения ключа с помощью мастера создания задачи для группы администрирования и для клиентского устройства.

Автоматическое распространение ключа

Kaspersky Security Center позволяет автоматически распространять на управляемые устройства ключи, размещенные в хранилище ключей на Сервере администрирования.

► *Чтобы автоматически распространять ключ на управляемые устройства, выполните следующие действия:*

1. Выберите в дереве консоли папку **Лицензии Лаборатории Касперского**.
2. В рабочей области папки выберите ключ, который вы хотите автоматически распространять на устройства.
3. Откройте окно свойств выбранного ключа одним из следующих способов:
 - в контекстном меню ключа выберите пункт **Свойства**;
 - по ссылке **Посмотреть свойства ключа** в блоке работы с выбранным ключом.
4. В открывшемся окне свойств ключа установите флажок **Автоматически распространяемый ключ**. Закройте окно свойств ключа.

В результате ключ будет автоматически распространяться в качестве активного или дополнительного ключа на те устройства, для которых он подходит.

Распространение ключа выполняется средствами Агента администрирования. Вспомогательные задачи распространения ключа для программы при этом не создаются.

При автоматическом распространении ключа в качестве активного или дополнительного учитывается лицензионное ограничение на количество устройств, заложенное в свойствах ключа. Если лицензионное ограничение достигнуто, распространение ключа на устройства автоматически прекращается.

Создание и просмотр отчета об использовании ключей

► Чтобы создать отчет об использовании ключей на клиентских устройствах, выполните следующие действия:

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите шаблон отчета **Отчет об использовании ключей** или создайте новый шаблон отчета одноименного типа.

В результате в рабочей области отчета об использовании ключей отображается информация об активных и дополнительных ключах, используемых на клиентских устройствах. Также в отчете содержатся сведения об устройствах, на которых используются ключи, и об ограничениях, заданных в свойствах ключей.

Хранилища данных

Этот раздел содержит информацию о данных, которые хранятся на Сервере администрирования и используются для отслеживания состояния клиентских устройств и для их обслуживания.

Данные, которые используются для отслеживания состояния устройств и их обслуживания, отображаются в папке дерева консоли **Хранилища**.

Папка **Хранилища** содержит следующие объекты:

- полученные Сервером администрирования обновления, которые распространяются на клиентские устройства (см. раздел "Просмотр полученных обновлений" на стр. [381](#));
- список оборудования, обнаруженного в сети;

- ключи, обнаруженные на клиентских устройствах (см. раздел "Работа с ключами программ" на стр. [392](#));
- файлы, помещенные программами защиты в карантинные папки на устройствах;
- файлы, помещенные в резервные хранилища устройств;
- файлы, для которых программы защиты определили необходимость отложенной проверки.

В этом разделе

Экспорт списка объектов, находящихся в хранилище, в текстовый файл.....	398
Инсталляционные пакеты.....	399
Основные статусы файлов в хранилище.....	399
Карантин и резервное хранилище.....	401
Необработанные файлы.....	405

Экспорт списка объектов, находящихся в хранилище, в текстовый файл

Вы можете экспортировать в текстовый файл список объектов, находящихся в хранилище.

► *Чтобы экспортировать в текстовый файл список объектов, находящихся в хранилище, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку нужного вам хранилища.
2. В контекстном меню списка объектов хранилища выберите пункт **Экспортировать список**.

В результате откроется окно **Экспорт списка**, в котором вы можете указать имя текстового файла и адрес папки, в которую он будет помещен.

Инсталляционные пакеты

Kaspersky Security Center помещает в хранилища данных инсталляционные пакеты программ "Лаборатории Касперского" и программ сторонних производителей.

Инсталляционный пакет представляет собой набор файлов, необходимых для установки программы. Инсталляционный пакет содержит параметры процесса установки и первоначальной конфигурации устанавливаемой программы.

Если вы хотите установить какую-либо программу на клиентское устройство, для этой программы необходимо создать инсталляционный пакет или использовать уже созданный инсталляционный пакет. Список созданных инсталляционных пакетов содержится в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

Основные статусы файлов в хранилище

Программы защиты проверяют файлы на устройствах на наличие известных вирусов и других программ, представляющих угрозу, присваивают статусы файлам и помещают некоторые файлы в хранилище.

Например, программы защиты могут

- сохранять в хранилище копию файла перед удалением,
- изолировать в хранилище возможно зараженные файлы.

Основные статусы файлов приведены в таблице ниже. Вы можете получить более подробную информацию о действиях с файлами в справках программ защиты.

Таблица 5. Статусы файлов в хранилище

Название статуса	Описание статуса
Заражен	В файле найден участок кода известного вируса или другой представляющей угрозу программы, информация о которой содержится в антивирусных базах "Лаборатории Касперского".
Не заражен	В файле не обнаружено известных вирусов или других программ, представляющих угрозу.
Предупреждение	В файле содержится участок кода, частично совпадающий с контрольным участком кода известной угрозы.
Возможно зараженный	В файле содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, пока не известный "Лаборатории Касперского".
Помещен в папку пользователем	Пользователь самостоятельно поместил файл в хранилище, например, поведение файла давало основание подозревать в нем наличие угрозы. Пользователь может проверить файл на наличие в нем угроз с помощью обновленных баз.
Ложное срабатывание	Программа "Лаборатории Касперского" присвоила статус незараженному файлу как зараженному ввиду того, что его код напоминает код вируса. После проверки с применением обновленных баз файл определяется как незараженный.
Вылечен	Файл удалось вылечить.
Удален	Файл удален в результате обработки.
Защищен паролем	Файл не может быть обработан по причине того, что он защищен паролем.

См. также

Значки статусов файлов в Консоли администрирования [513](#)

Карантин и резервное хранилище

Антивирусные программы "Лаборатории Касперского", установленные на клиентских устройствах, в процессе проверки устройств могут помещать файлы на карантин или в резервное хранилище.

Карантин – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения.

Резервное хранилище предназначено для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Kaspersky Security Center формирует общий список файлов, помещенных на карантин и в резервное хранилище программами "Лаборатории Касперского" на устройствах. Агенты администрирования клиентских устройств передают информацию о файлах на карантине и в резервных хранилищах на Сервер администрирования. Через Консоль администрирования можно просматривать свойства файлов, находящихся в хранилищах на устройствах, запускать антивирусную проверку хранилищ и удалять из них файлы. Значки статусов файлов описаны в приложении (см. раздел "Значки статусов файлов в Консоли администрирования" на стр. [513](#)).

Работа с карантином и резервным хранилищем доступна для Антивируса Касперского для Windows Workstations и Антивируса Касперского для Windows Servers версий 6.0 и выше, а также для Kaspersky Endpoint Security 10 для Windows и выше.

Kaspersky Security Center не копирует файлы из хранилищ на Сервер администрирования. Все файлы размещаются в хранилищах на устройствах. Восстановление файлов выполняется на устройстве, где установлена программа защиты, поместившая файл в хранилище.

В этом разделе

Включение удаленного управления файлами в хранилищах.....	402
Просмотр свойств файла, помещенного в хранилище	403
Удаление файлов из хранилища.....	403
Восстановление файлов из хранилища.....	404
Сохранение файла из хранилища на диск.....	404
Проверка файлов на карантине	405

Включение удаленного управления файлами в хранилищах

По умолчанию удаленное управление файлами в хранилищах на клиентских устройствах отключено.

- ▶ *Чтобы включить удаленное управление файлами в хранилищах на клиентских устройствах, выполните следующие действия:*
 1. В дереве консоли выберите группу администрирования, для которой требуется включить удаленное управление файлами хранилищ.
 2. В рабочей области группы откройте закладку **Политики**.
 3. На закладке **Политики** выберите политику программы защиты, помещающей файлы в хранилища на устройствах.
 4. В окне свойств политики в блоке **Информировать Сервер администрирования** установите флажки, соответствующие хранилищам, для которых вы хотите включить удаленное управление.

Расположение блока **Информировать Сервер администрирования** в окне свойств политики и названия флажков в блоке индивидуальны для каждой программы защиты.

Просмотр свойств файла, помещенного в хранилище

- ▶ *Чтобы просмотреть свойства файла, помещенного на карантин или в резервное хранилище, выполните следующие действия:*
 1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
 2. В рабочей области папки **Карантин (Резервное хранилище)** выберите файл, параметры которого требуется просмотреть.
 3. В контекстном меню файла выберите пункт **Свойства**.

Удаление файлов из хранилища

- ▶ *Чтобы удалить файл, помещенный на карантин или в резервное хранилище, выполните следующие действия:*
 1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
 2. В рабочей области папки **Карантин (Резервное хранилище)** с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется удалить.
 3. Удалите файлы одним из следующих способов:
 - В контекстном меню файлов выберите пункт **Удалить**.
 - По ссылке **Удалить объекты (Удалить объект** при удалении одного файла) в блоке работы с выбранными файлами.

В результате программы защиты, поместившие выбранные файлы в хранилища на клиентских устройствах, удалят файлы из этих хранилищ.

Восстановление файлов из хранилища

► *Чтобы восстановить файл из карантина или резервного хранилища, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин (Резервное хранилище)** с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется восстановить.
3. Запустите процесс восстановления файлов одним из следующих способов:
 - В контекстном меню файлов выберите пункт **Восстановить**.
 - По ссылке **Восстановить** в блоке работы с выбранными файлами.

В результате программы защиты, поместившие файлы в хранилища на клиентских устройствах, восстановят файлы в исходные папки.

Сохранение файла из хранилища на диск

Kaspersky Security Center позволяет сохранять на диск копии файлов, помещенных программой защиты на карантин или в резервное хранилище на клиентском устройстве. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

► *Чтобы сохранить копию файла из карантина или резервного хранилища на диск, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин (Резервное хранилище)** выберите файл, который требуется скопировать на диск.
3. Запустите процесс копирования файла одним из следующих способов:
 - В контекстном меню файла выберите пункт **Сохранить на диск**.

- По ссылке **Сохранить на диск** в блоке работы с выбранным файлом.

В результате программа защиты, поместившая файл на карантин на устройстве, сохранит копию файла в указанную папку.

Проверка файлов на карантине

► *Чтобы проверить файлы, находящиеся на карантине, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин**.
2. В рабочей области папки **Карантин** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется проверить.
3. Запустите процесс проверки файлов одним из следующих способов:
 - В контекстном меню файла выберите пункт **Проверить объекты на карантине**.
 - По ссылке **Проверить** в блоке работы с выбранными файлами.

В результате для программ защиты, поместивших файлы на карантин, будет запущена задача проверки по требованию на тех устройствах, на которых находятся на карантине выбранные файлы.

Необработанные файлы

Информация о необработанных файлах, обнаруженных на клиентских устройствах, содержится в папке **Хранилища**, во вложенной папке **Необработанные файлы**.

Отложенная обработка и лечение файлов программой защиты осуществляются по требованию или после наступления определенного события. Вы можете настраивать параметры отложенного лечения файлов.

В этом разделе

Лечение необработанного файла	406
Сохранение необработанного файла на диск	407
Удаление файлов из папки "Необработанные файлы"	407

Лечение необработанного файла

► *Чтобы запустить лечение необработанного файла, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Необработанные файлы**.
2. В рабочей области папки **Необработанные файлы** выберите файл, который требуется вылечить.
3. Запустите процесс лечения файла одним из следующих способов:
 - В контекстном меню файла выберите пункт **Лечить**.
 - По ссылке **Лечить** в блоке работы с выбранным файлом.

В результате выполняется попытка лечения файла.

Если файл вылечен, программа защиты, установленная на устройстве, восстанавливает его в исходную папку. Запись о файле удаляется из списка папки **Необработанные файлы**. Если лечение файла невозможно, программа защиты, установленная на устройстве, удаляет файл с устройства. Запись о файле удаляется из списка папки **Необработанные файлы**.

Сохранение необработанного файла на диск

Kaspersky Security Center позволяет сохранять на диск копии необработанных файлов, обнаруженные на клиентских устройствах. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

► *Чтобы сохранить копию необработанного файла на диск, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Необработанные файлы**.
2. В рабочей области папки **Необработанные файлы** выберите файлы, которые требуется скопировать на диск.
3. Запустите процесс копирования файла одним из следующих способов:
 - В контекстном меню файла выберите пункт **Сохранить на диск**.
 - По ссылке **Сохранить на диск** в блоке работы с выбранным файлом.

В результате программа защиты клиентского устройства, на котором обнаружен выбранный необработанный файл, сохранит копию файла в указанную папку.

Удаление файлов из папки "Необработанные файлы"

► *Чтобы удалить файл из папки **Необработанные файлы**, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Необработанные файлы**.
2. В рабочей области папки **Необработанные файлы** с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется удалить.
3. Удалите файлы одним из следующих способов:
 - В контекстном меню файлов выберите пункт **Удалить**.

- По ссылке **Удалить объекты** (**Удалить объект** при удалении одного файла) в блоке работы с выбранными файлами.

В результате программы защиты, поместившие выбранные файлы в хранилища на клиентских устройствах, удаляют файлы из этих хранилищ. Записи о файлах удаляются из списка в папке **Необработанные файлы**.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другой без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных через Консоль администрирования.
- Запустить утилиту `kbackup` на устройстве, где установлен Сервер администрирования. Эта утилита входит в состав дистрибутива Kaspersky Security Center и после установки Сервера администрирования располагается в корне папки назначения, указанной при установке программы.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- информационная база Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;

- хранилище дистрибутивов программ для удаленной установки;
- сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты kbackup.

В этом разделе

Создание задачи резервного копирования данных.....	409
Утилита резервного копирования и восстановления данных (kbackup).....	410
Резервное копирование и восстановление данных в интерактивном режиме	411
Резервное копирование и восстановление данных в неинтерактивном режиме	412
Перенос Сервера администрирования на другое устройство	414

Создание задачи резервного копирования данных

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки. Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

► *Чтобы создать задачу резервного копирования данных Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи одним из следующих способов:
 - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Создать** → **Задачу**.

- По кнопке **Создать задачу** в рабочей области.

В результате запускается мастер создания задачи. Следуйте его указаниям. В окне мастера **Тип задачи** выберите тип задачи **Резервное копирование данных Сервера администрирования**.

Задачу **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задача резервного копирования данных Сервера администрирования уже создана для Сервера администрирования, то она не отображается в окне выбора типа задачи мастера создания задачи.

Утилита резервного копирования и восстановления данных (klbackup)

Вы можете выполнять копирование данных Сервера администрирования для резервного хранения и последующего восстановления с помощью утилиты klbackup, входящей в состав дистрибутива Kaspersky Security Center.

Утилита klbackup может работать в двух режимах:

- интерактивном (см. раздел "Резервное копирование и восстановление данных в интерактивном режиме" на стр. [411](#));
- неинтерактивном (см. раздел "Резервное копирование и восстановление данных в неинтерактивном режиме" на стр. [412](#)).

Резервное копирование и восстановление данных в интерактивном режиме

► *Чтобы создать резервную копию данных Сервера администрирования в интерактивном режиме, выполните следующие действия:*

1. Запустите утилиту kbackup, расположенную в папке установки Kaspersky Security Center.

Будет запущен мастер резервного копирования и восстановления данных.

2. В первом окне мастера выберите пункт **Выполнить резервное копирование данных Сервера администрирования**.

При установке флажка **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будет сохранена только резервная копия сертификата Сервера администрирования.

Нажмите на кнопку **Далее**.

3. В следующем окне мастера укажите пароль и папку назначения для резервного копирования. Нажмите на кнопку **Далее** для выполнения резервного копирования.

► *Чтобы восстановить данные Сервера администрирования в интерактивном режиме, выполните следующие действия:*

1. Деинсталлируйте Сервер администрирования, затем установите его заново.
2. Запустите утилиту kbackup, расположенную в папке установки Kaspersky Security Center.

В результате запустится мастер резервного копирования и восстановления данных.

Запускать утилиту kbackup необходимо под той же учетной записью, под которой был установлен Сервер администрирования

3. В первом окне мастера выберите пункт **Выполнить восстановление данных Сервера администрирования**.

При установке флажка **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будет восстановлен только сертификат Сервера администрирования.

Нажмите на кнопку **Далее**.

4. В окне мастера **Параметры восстановления**:

- Укажите папку, содержащую резервную копию данных Сервера администрирования.
- Укажите пароль, введенный при резервном копировании данных.

5. Нажмите на кнопку **Далее** для восстановления данных.

При восстановлении данных должен быть указан тот же пароль, что и при резервном копировании. Если пароль указан неверно, данные не будут восстановлены. Если после резервного копирования путь к папке общего доступа изменялся, после восстановления данных нужно проверить работу задач, в которых используются восстановленные данные (задачи восстановления, дистанционной установки). При необходимости нужно изменить параметры этих задач.

Во время восстановления данных из файла резервного копирования никто не должен использовать папку общего доступа Сервера администрирования. Учетная запись, под которой запускается утилита k1backup, должна иметь полный доступ к папке общего доступа.

Резервное копирование и восстановление данных в неинтерактивном режиме

- *Чтобы создать резервную копию данных или восстановить данные Сервера администрирования в неинтерактивном режиме,*

в командной строке устройства, на котором установлен Сервер администрирования, запустите утилиту k1backup с необходимым набором ключей.

Синтаксис утилиты:

```
klbackup [-logfile LOGFILE] -path BACKUP_PATH  
[-use_ts][[-restore] -savecert PASSWORD
```

Если не задать пароль в командной строке утилиты klbackup, утилита запросит его ввод интерактивно.

Описание ключей:

- `-logfile LOGFILE` – сохранить отчет о копировании или восстановлении данных Сервера администрирования.
- `-path BACKUP_PATH` – сохранить информацию в папке `BACKUP_PATH` / использовать для восстановления данные из папки `BACKUP_PATH` (обязательный параметр).

Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке `BACKUP_PATH`.

- `-use_ts` – при сохранении данных копировать информацию в папку `BACKUP_PATH`, во вложенную папку с именем, отображающим текущую системную дату и время операции в формате `klbackup ГГГГ-ММ-ДД # ЧЧ-ММ-СС`. Если ключ не задан, информация сохраняется в корне папки `BACKUP_PATH`.

При попытке сохранить информацию в папку, в которой уже есть резервная копия, появится сообщение об ошибке. Обновление информации не произойдет.

Наличие ключа `-use_ts` позволяет вести архив данных Сервера администрирования. Например, если ключом `-path` была задана папка `C:\KLBackups`, то в папке `klbackup 2017-06-19 # 11-30-18` сохранится информация о состоянии Сервера администрирования на дату 19 июня 2017 года, 11 часов 30 минут 18 секунд.

- `-restore` – выполнить восстановление данных Сервера администрирования. Восстановление данных осуществляется на основании информации, представленной

в папке `BACKUP_PATH`. Если ключ отсутствует, производится резервное копирование данных в папку `BACKUP_PATH`.

- `-savecert PASSWORD` – сохранить или восстановить сертификат Сервера администрирования; для шифрования и расшифровки сертификата использовать пароль, заданный параметром `PASSWORD`.

При восстановлении данных должен быть указан тот же пароль, что и при резервном копировании. Если пароль указан неверно, данные не будут восстановлены. Если после резервного копирования путь к папке общего доступа изменялся, после восстановления данных нужно проверить работу задач, в которых используются восстановленные данные (задачи восстановления, дистанционной установки). При необходимости нужно изменить параметры этих задач.

Во время восстановления данных из файла резервного копирования никто не должен использовать папку общего доступа Сервера администрирования. Учетная запись, под которой запускается утилита `kbackup`, должна иметь полный доступ к папке общего доступа.

Перенос Сервера администрирования на другое устройство

- ▶ *Чтобы перенести Сервер администрирования на другое устройство без смены базы данных Сервера администрирования, выполните следующие действия:*
 1. Создайте резервную копию данных Сервера администрирования.
 2. Установите Сервер администрирования на выбранное устройство.

Для упрощения переноса групп администрирования желательно, чтобы адрес нового Сервера администрирования совпадал с адресом предыдущего Сервера. Адрес (имя устройства в сети Windows или IP-адрес) указывается в параметрах подключения Агента администрирования к Серверу.

3. На новом Сервере администрирования выполните восстановление данных Сервера из резервной копии.
4. Если адрес (имя устройства в сети Windows или IP-адрес) нового Сервера администрирования не совпадает с адресом предыдущего Сервера, для подключения клиентских устройств к новому Серверу создайте на предыдущем Сервере задачу смены Сервера администрирования для группы **Управляемые устройства**.

Если адреса совпадают, задачу смены Сервера создавать не нужно, подключение будет выполнено по указанному в параметрах адресу Сервера.

5. Удалите предыдущий Сервер администрирования.

► *Чтобы перенести Сервер администрирования на другое устройство со сменой базы данных Сервера администрирования, выполните следующие действия:*

1. Создайте резервную копию данных Сервера администрирования.
2. Установите новый SQL-сервер.

Для правильного переноса информации база данных на новом SQL-сервере должна иметь те же схемы сопоставления (collation), что и на предыдущем SQL-сервере.

3. Установите новый Сервер администрирования. Название баз данных предыдущего и нового SQL-серверов должны совпадать.

Для упрощения переноса групп администрирования желательно, чтобы адрес нового Сервера администрирования совпадал с адресом предыдущего Сервера. Адрес (имя устройства в сети Windows или IP-адрес) указывается в параметрах подключения Агента администрирования к Серверу.

4. На новом Сервере администрирования выполните восстановление данных предыдущего Сервера из резервной копии.
5. Если адрес (имя устройства в сети Windows или IP-адрес) нового Сервера администрирования не совпадает с адресом предыдущего Сервера, для подключения клиентских устройств к новому Серверу создайте на предыдущем Сервере задачу смены Сервера администрирования для группы **Управляемые устройства**.
6. Если адреса совпадают, задачу смены Сервера создавать не нужно, подключение будет выполнено по указанному в параметрах адресу Сервера.
7. Удалите предыдущий Сервер администрирования.

Экспорт событий в SIEM-системы

В этом разделе описана процедура экспорта событий, зарегистрированных в Kaspersky Security Center, во внешние системы управления событиями информационной безопасности (SIEM-системы, Security Information and Event Management).

Об экспорте событий

Экспорт событий можно использовать в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться на панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В этом разделе

События в Kaspersky Security Center	417
Процедура экспорта событий	420
Настройка экспорта событий в Kaspersky Security Center	421
Настройка экспорта событий в SIEM-системе	446
Просмотр результатов экспорта.....	449
Общие события	449

События в Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования, управляемых устройств и других программ "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Вы можете экспортировать эту информацию во внешние SIEM-системы. Экспорт информации о событиях во внешние SIEM-системы позволяет администраторам SIEM-систем оперативно реагировать на события системы безопасности, произошедшие на управляемых устройствах или группах устройств.

Каждая программа "Лаборатории Касперского" имеет собственный набор событий. *Общие события* – это события, которые произошли на Сервере администрирования или в Агенте

администрирования Kaspersky Security Center. Эти события перечислены в разделе "Общие события".

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на потенциально возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе программы или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

См. также

События Сервера администрирования.....	450
События Агента администрирования.....	454

Процедура экспорта событий

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center – и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе и в Консоли администрирования Kaspersky Security Center. Последовательность настройки не имеет значения: можно либо сначала настроить отправку событий в Консоли администрирования Kaspersky Security Center, а затем получение событий в SIEM-системе, либо наоборот.

Способы отправки событий из Kaspersky Security Center

Существует три способа отправки событий из Kaspersky Security Center во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

По протоколу Syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в программах "Лаборатории Касперского", установленных на управляемых устройствах. При экспорте событий по протоколу Syslog можно выбирать, какие именно события будут переданы в SIEM-систему. Протокол Syslog – это стандартный протокол регистрации сообщений, поэтому вы можете использовать протокол Syslog для экспорта событий в любую SIEM-систему.

- Отправка событий по протоколам CEF и LEEF в системы QRadar, Splunk и ArcSight.

Протоколы CEF и LEEF можно использовать для экспорта общих событий, т. е. событий, произошедших на Сервере администрирования или в Агенте администрирования Kaspersky Security Center. При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий; выполняется экспорт всех общих событий. Протоколы CEF и LEEF не являются универсальными, как протокол Syslog. Они предназначены для соответствующих SIEM-систем (QRadar, Splunk и ArcSight), поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

- Напрямую из базы данных Kaspersky Security Center в любую SIEM-систему.

Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в .xml файл, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center. Для этого необходимо выполнить настройку SIEM-системы. Настройка зависит от конкретной используемой SIEM-системы, однако имеется ряд общих шагов в настройке всех SIEM-систем: настройка приемника и анализатора.

Настройка экспорта событий в Kaspersky Security Center

Для успешного экспорта событий необходимо выполнить настройку в Консоли администрирования Kaspersky Security Center. Настройка Kaspersky Security Center зависит от того, какой способ передачи событий из Kaspersky Security Center в SIEM-систему вы выбрали.

В этом разделе описано, как настроить Kaspersky Security Center, если вы выбрали экспортировать события следующими способами:

- по протоколу Syslog;
- по протоколам CEF и LEEF;
- напрямую из базы данных Security Center.

В этом разделе

Экспорт событий по протоколу Syslog	422
Экспорт событий по протоколам CEF и LEEF	435
Экспорт событий напрямую из базы данных	440

Экспорт событий по протоколу Syslog

По протоколу Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других программах "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Протокол Syslog определяется документами "Рабочее предложение" (Request for Comments, RFC), опубликованными Инженерным советом Интернета (Internet Engineering Task Force). Стандарт RFC 5424 (<https://tools.ietf.org/html/rfc5424>) используется для экспорта событий из Kaspersky Security Center во внешние системы.

В Kaspersky Security Center можно настроить экспорт событий во внешние системы по протоколу Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky Security Center таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center начинается сразу после включения автоматического экспорта.

2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

В этом разделе

Предварительные условия	423
Включение автоматического экспорта	424
Выбор экспортируемых событий	427

Предварительные условия

При настройке автоматического экспорта событий в Консоли администрирования Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

Протокол Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

Включение автоматического экспорта

Первый шаг настройки экспорта событий по протоколу Syslog – это включение автоматического экспорта в Kaspersky Security Center.

► Чтобы включить автоматический экспорт событий по протоколу Syslog, выполните следующие действия:

1. В дереве консоли Kaspersky Security Center выберите узел с именем Сервера администрирования, события которого необходимо экспортировать.
2. В рабочей области выбранного Сервера администрирования перейдите на закладку **События**.
3. Нажмите на стрелку рядом со ссылкой **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить экспорт в SIEM-систему**.

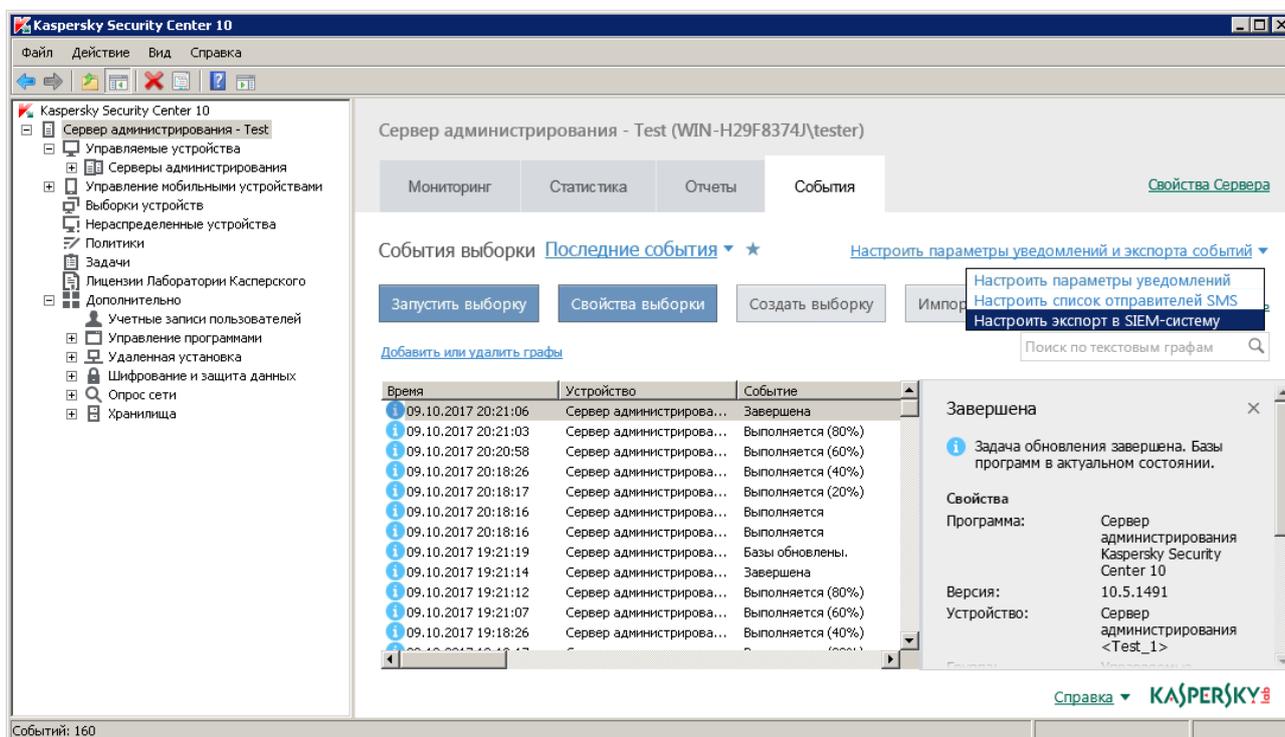


Рисунок 4. Окно свойств событий

Откроется окно свойств событий на разделе **Экспорт событий**.

4. В разделе **Экспорт событий** укажите следующие параметры:

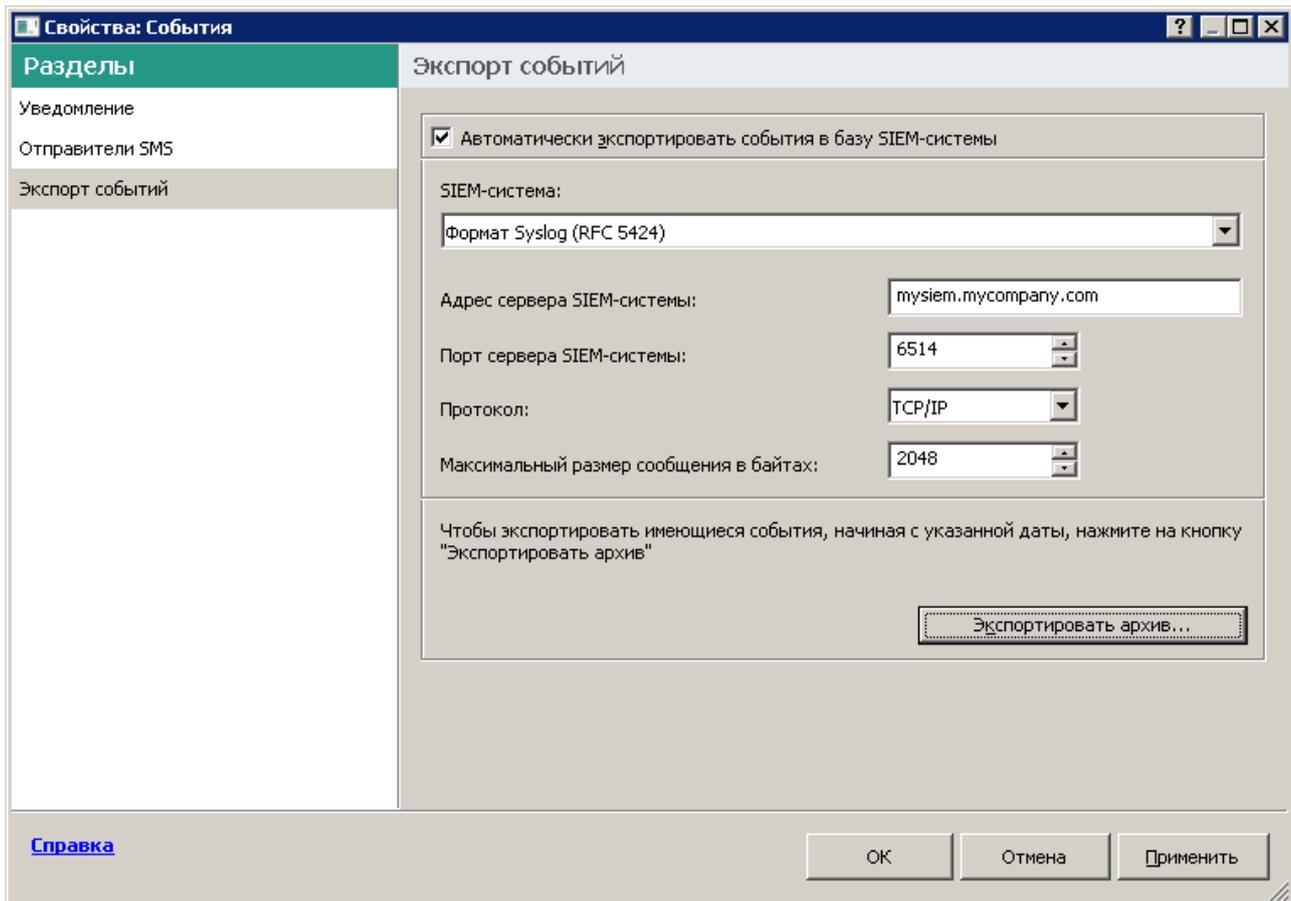


Рисунок 5. Раздел Экспорт событий

- **Автоматически экспортировать события в базу SIEM-системы**

Установите этот флажок, для того чтобы включить автоматический экспорт событий в SIEM-систему. При установке этого флажка все поля в разделе **Экспорт событий** становятся доступными для редактирования.

- **SIEM-система**

Выберите вариант **Формат Syslog (RFC 5424)** для передачи событий по протоколу Syslog.

- **Адрес сервера SIEM-системы**

Укажите адрес сервера SIEM-системы. Адрес сервера можно указать в формате DNS- или NetBIOS-имени или IP-адреса

- **Порт сервера SIEM-системы**

Укажите номер порта для соединения с сервером SIEM-системы. Этот номер порта должен совпадать с номером порта, который вы указываете в настройках приемника SIEM-системы для получения событий (см. раздел Настройка SIEM-системы).

- **Протокол**

Выберите протокол передачи сообщений в SIEM-систему. Можно выбрать протокол TCP/IP или UDP. Протокол TCP/IP является более надежным и поддерживает уведомление о получении сообщений. Протокол UDP является более простым, он применяется в случаях, когда проверка и исправление ошибок передачи сообщений не обязательны или выполняются внутри приложения.

- **Максимальный размер сообщения в байтах**

Укажите максимальный размер в байтах одного сообщения, передаваемого в SIEM-систему. Каждое событие передается одним сообщением. Если реальная длина сообщения превышает указанное значение, сообщение обрезается и данные могут быть утеряны. По умолчанию размер сообщения составляет 2048 байт. Данное поле доступно только в случае, если вы выбрали формат Syslog в поле **SIEM-система**.

5. Если требуется выполнить экспорт в SIEM-систему событий, произошедших после определенной даты в прошлом, нажмите на кнопку **Экспортировать архив** и укажите дату, начиная с которой будет выполнен экспорт событий. По умолчанию экспорт событий начинается сразу после включения.

6. Нажмите на кнопку **ОК**.

Автоматический экспорт событий включен. После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться в SIEM-систему. Эта процедура описана в разделе "Выбор экспортируемых событий".

Выбор экспортируемых событий

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий во внешнюю систему по одному из следующих условий:

- Выбор событий в политике. Если вы выбираете экспортируемые события в политике, то в SIEM-систему будут переданы выбранные события, которые произошли во всех программах, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельной программы, управляемой этой политикой.
- Выбор событий для отдельной программы. Если вы выбираете экспортируемые события для отдельной программы, то в SIEM-систему будут переданы только события, которые произошли в этой программе.

В этом разделе описано, как выбрать экспортируемые события в политике и для отдельной программы.

В этом разделе

Выбор событий в политике	427
Выбор событий для программы.....	431

Выбор событий в политике

Если вы хотите выполнить экспорт событий, произошедших во всех программах, управляемых определенной политикой, выберите экспортируемые события в политике. В этом случае выбор событий для отдельной программы невозможен.

► Чтобы выбрать экспортируемые события в политике, выполните следующие действия:

1. В дереве консоли Kaspersky Security Center выберите узел **Политики**.

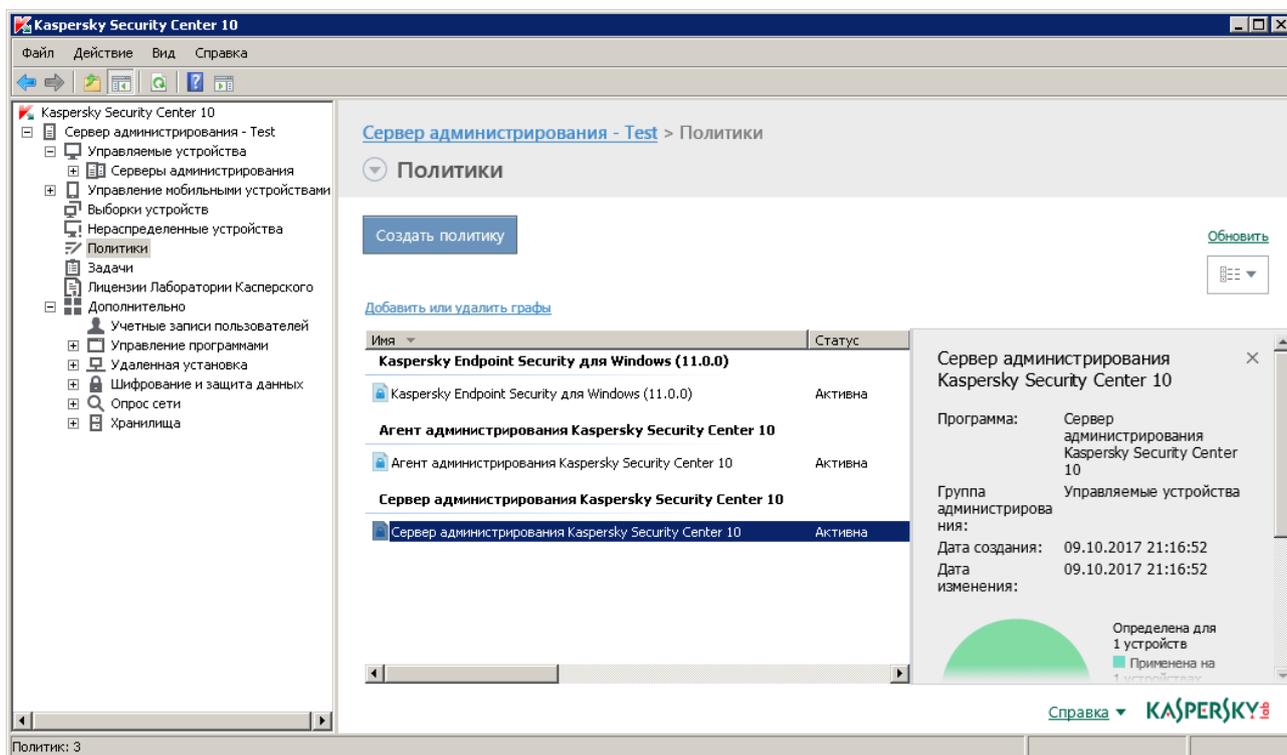
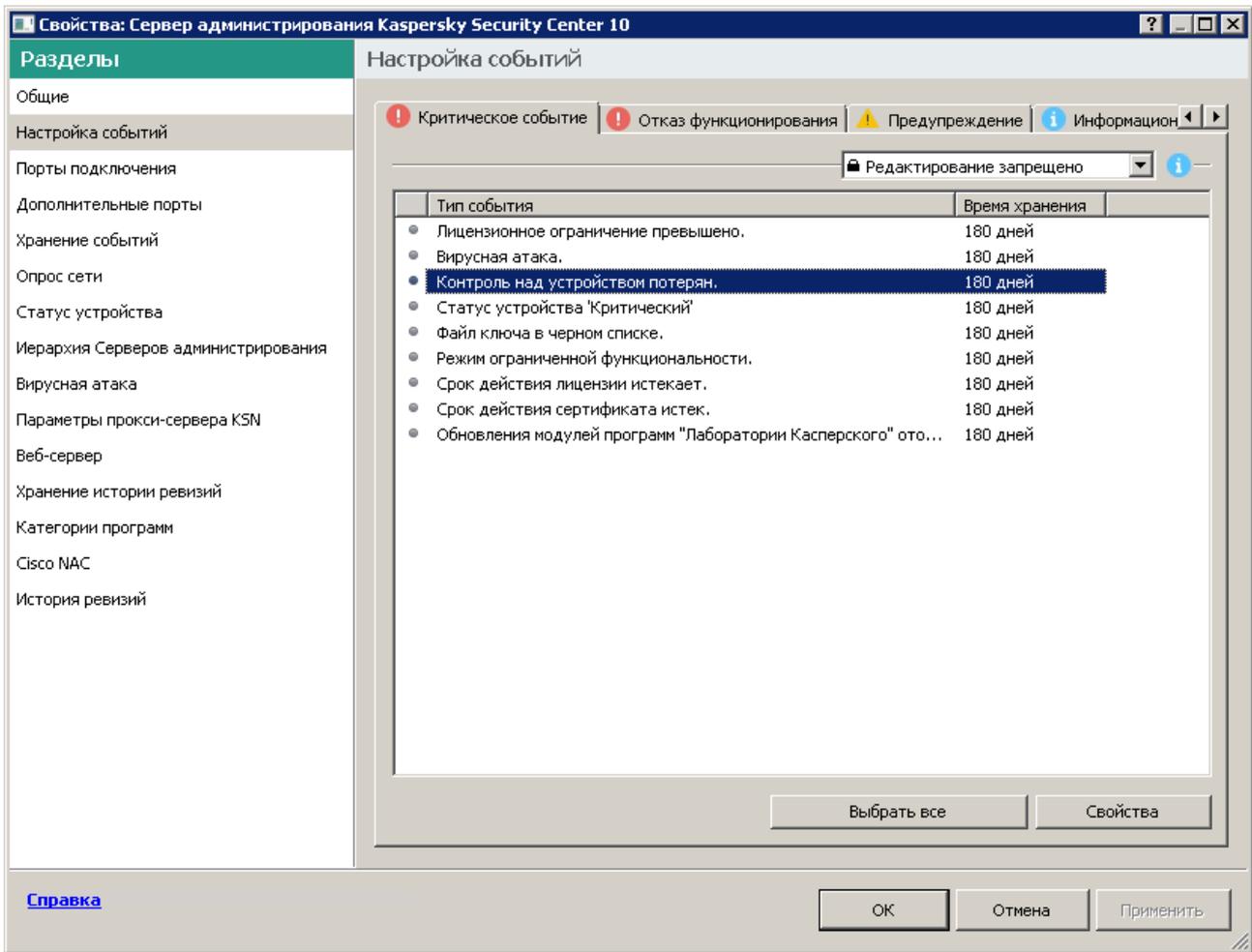


Рисунок 6. Узел Политики

2. Откройте контекстное меню требуемой политики по правой клавише мыши и выберите пункт **Свойства**.

3. В открывшемся окне свойств политики выберите раздел **Настройка событий**.



4. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.

Если требуется выбрать все события, нажмите на кнопку **Выбрать все**.

5. В появившемся окне свойств событий установите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы включить экспорт для выбранных событий.

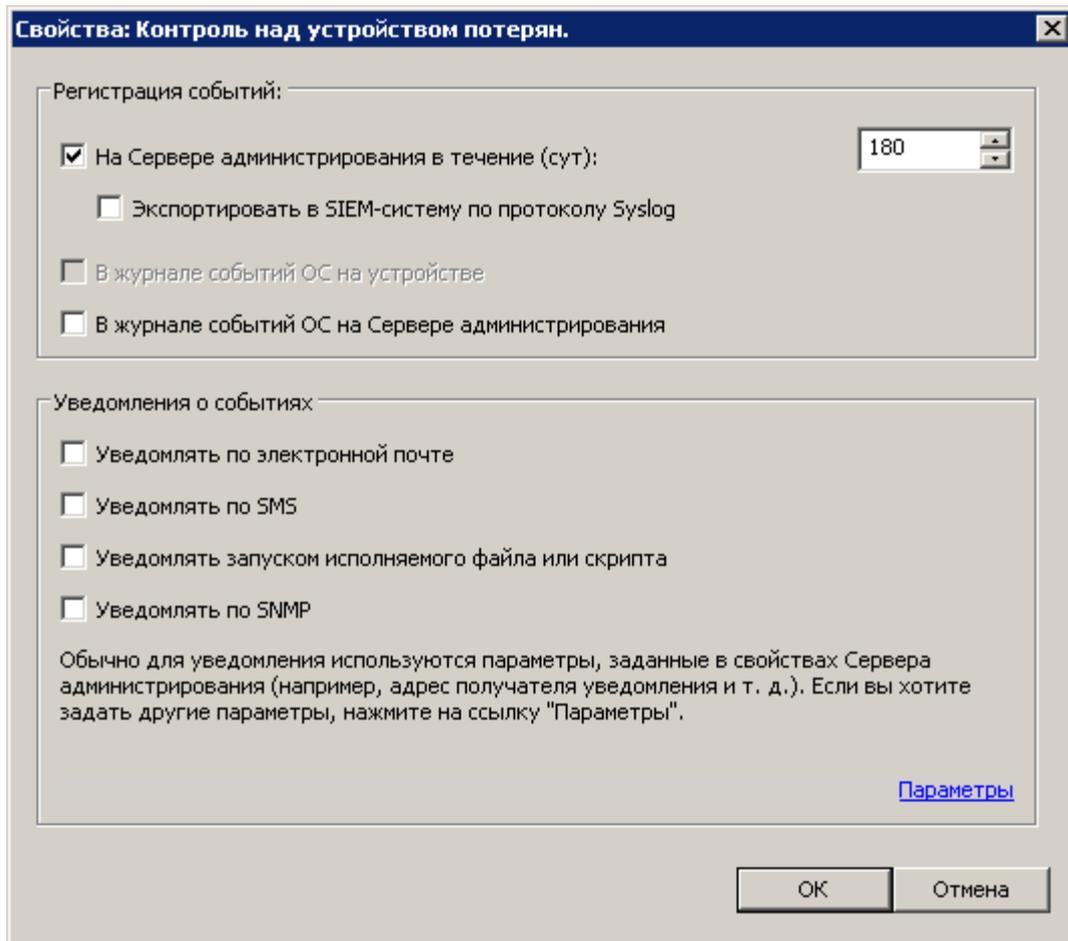


Рисунок 7. Включение экспорта для выбранных событий

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

7. В окне свойств политики нажмите на кнопку **ОК**.

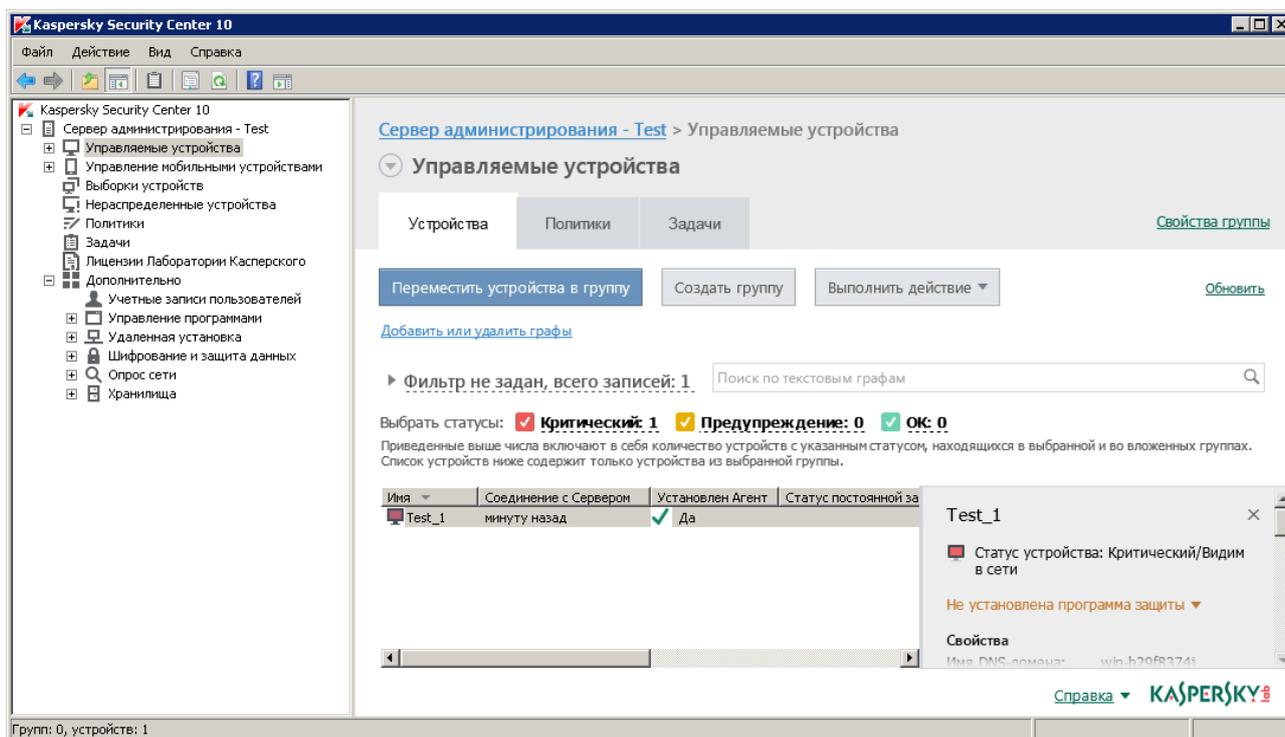
Выбранные события будут отправляться в SIEM-систему по протоколу Syslog. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

Выбор событий для программы

Если вы хотите выполнить экспорт событий, произошедших в отдельной программе, выберите экспортируемые события для программы. В случае, если ранее экспортируемые события были выбраны в политике, вам не удастся переопределить выбранные события для отдельной программы, управляемой этой политикой.

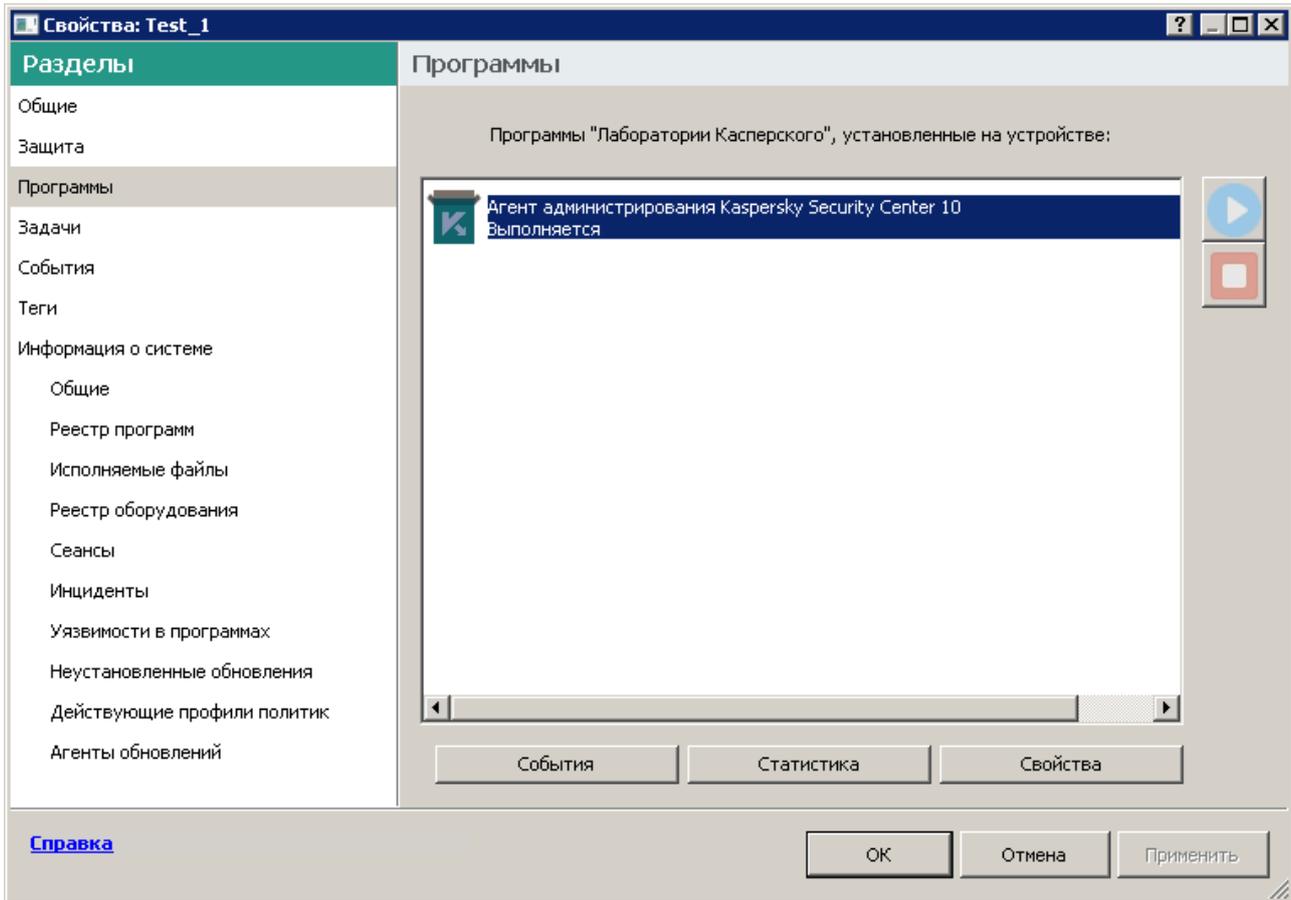
► Чтобы выбрать экспортируемые события для отдельной программы, выполните следующие действия:

1. В дереве консоли Kaspersky Security Center выберите узел **Управляемые устройства** и перейдите на закладку **Устройства**.



2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств устройства выберите раздел **Программы**.

4. В появившемся списке программ выберите программу, события которой требуется экспортировать, и нажмите на кнопку **Свойства**.



5. В окне свойств программы выберите раздел **Настройка событий**.

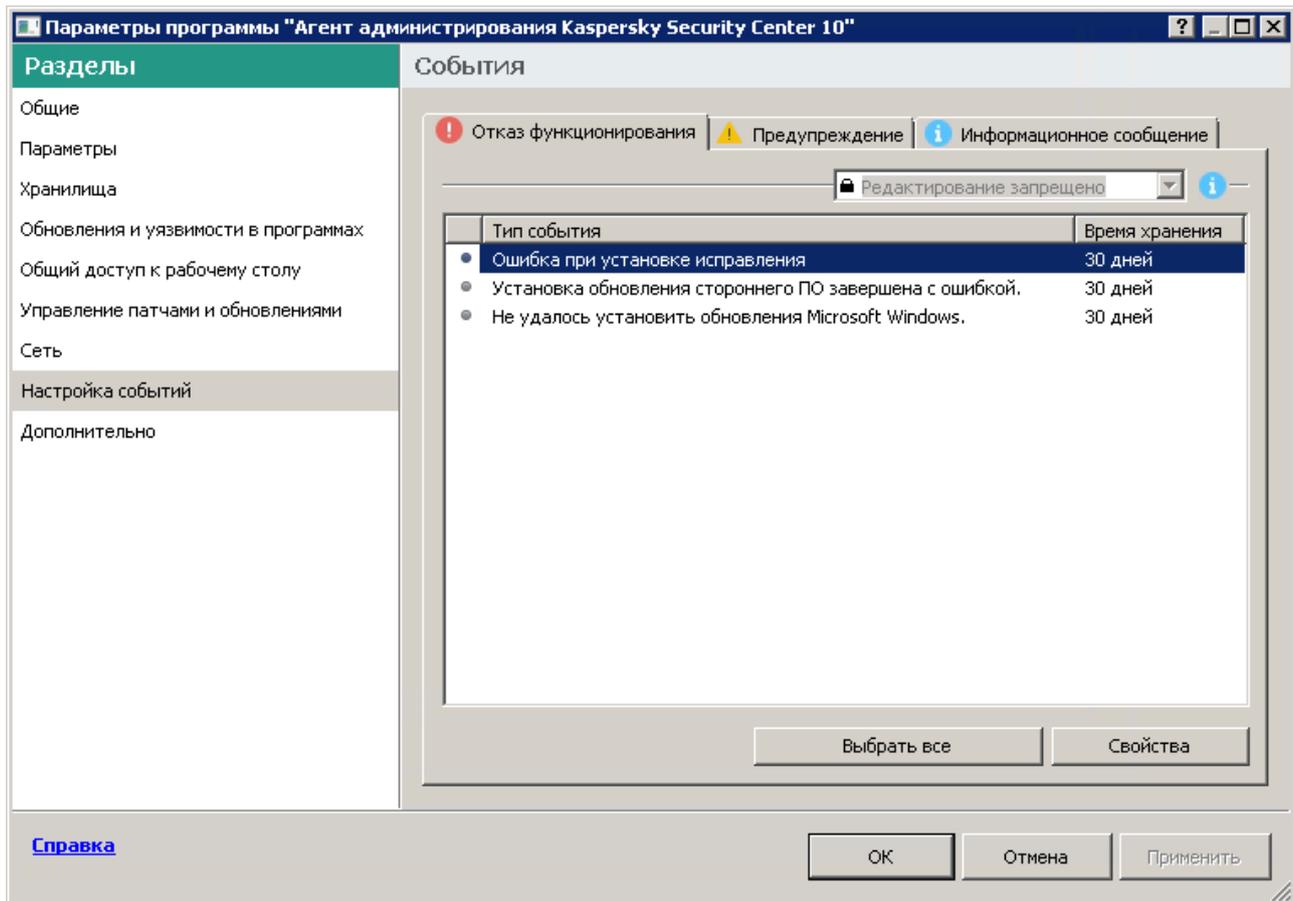


Рисунок 8. Раздел События в окне свойств программы

6. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.
7. В появившемся окне свойств событий установите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы включить экспорт для выбранных событий.

Если свойства события заданы в политике, поля этого окна недоступны для редактирования.

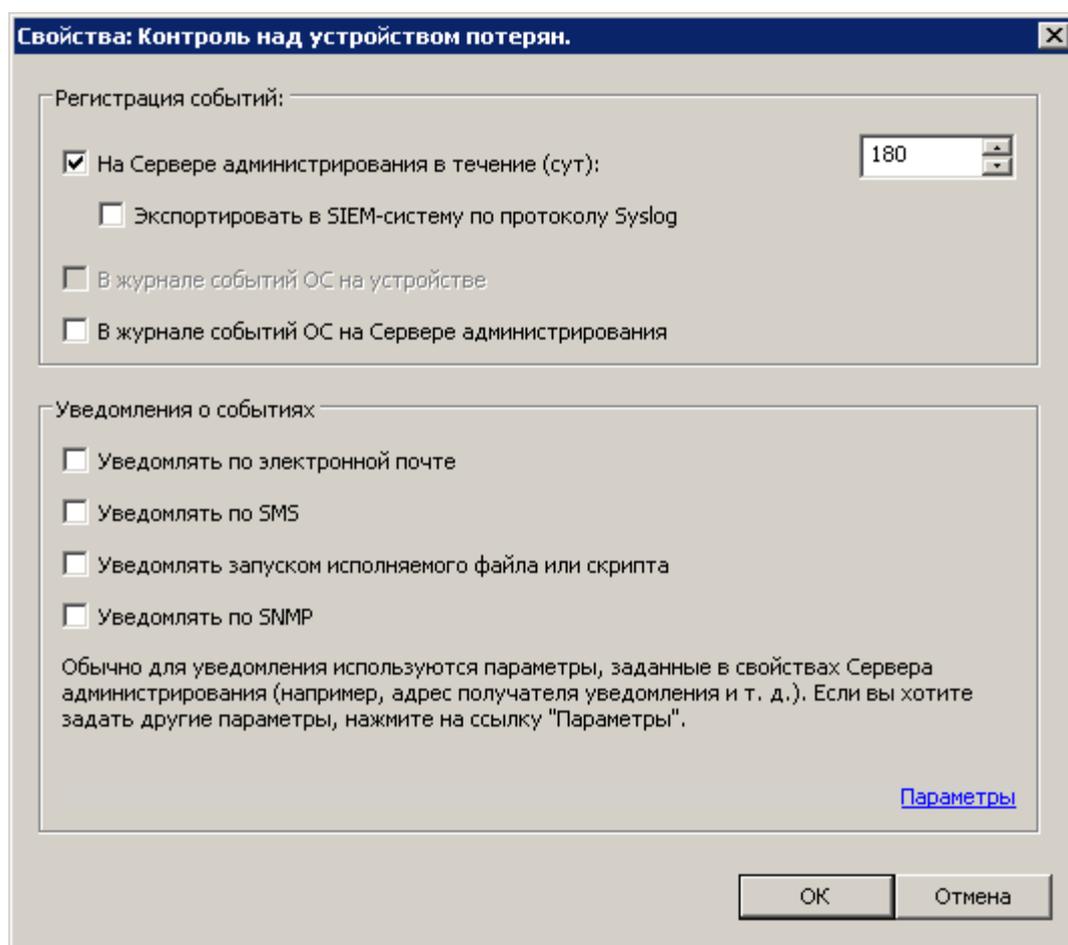


Рисунок 9. Окно свойств событий

8. Нажмите на кнопку **OK**, чтобы сохранить изменения.
9. Нажмите на кнопку **OK** в окне свойств программы и в окне свойств устройства.

Выбранные события будут отправляться в SIEM-систему по протоколу Syslog. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

Экспорт событий по протоколам CEF и LEEF

Протоколы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий (см. раздел "Общие события" на стр. [449](#)) – событий, произошедших на Сервере администрирования или в Агенте администрирования Kaspersky Security Center. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует.

Протокол экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им протоколы экспорта.

Таблица 6. Протоколы экспорта событий в SIEM-систему

SIEM-система	Протокол экспорта
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF – это специализированный формат событий для IBM® Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/_logsource_protocols.html).
- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа.

При автоматическом экспорте Kaspersky Security Center отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

В этом разделе

Предварительные условия	436
Включение автоматического экспорта общих событий.....	437

Предварительные условия

При настройке автоматического экспорта событий в Консоли администрирования Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

- **Протокол**

Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в

SIEM-системе.

Включение автоматического экспорта общих событий

В Kaspersky Security Center можно включить автоматический экспорт общих событий по протоколу LEEF или CEF.

Экспорт событий от управляемых программ недоступен по протоколам CEF и LEEF. Если необходимо экспортировать события управляемых программ или пользовательский набор событий, который настроен с помощью политик управляемых программ, используйте экспорт событий по протоколу Syslog.

- ▶ *Чтобы включить автоматический экспорт событий по протоколу CEF или LEEF, выполните следующие действия:*
 1. В дереве консоли Kaspersky Security Center выберите узел с именем Сервера администрирования, события которого необходимо экспортировать.
 2. В рабочей области выбранного Сервера администрирования перейдите на закладку **События**.

3. Нажмите на стрелку рядом со ссылкой **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить экспорт в SIEM-систему**.

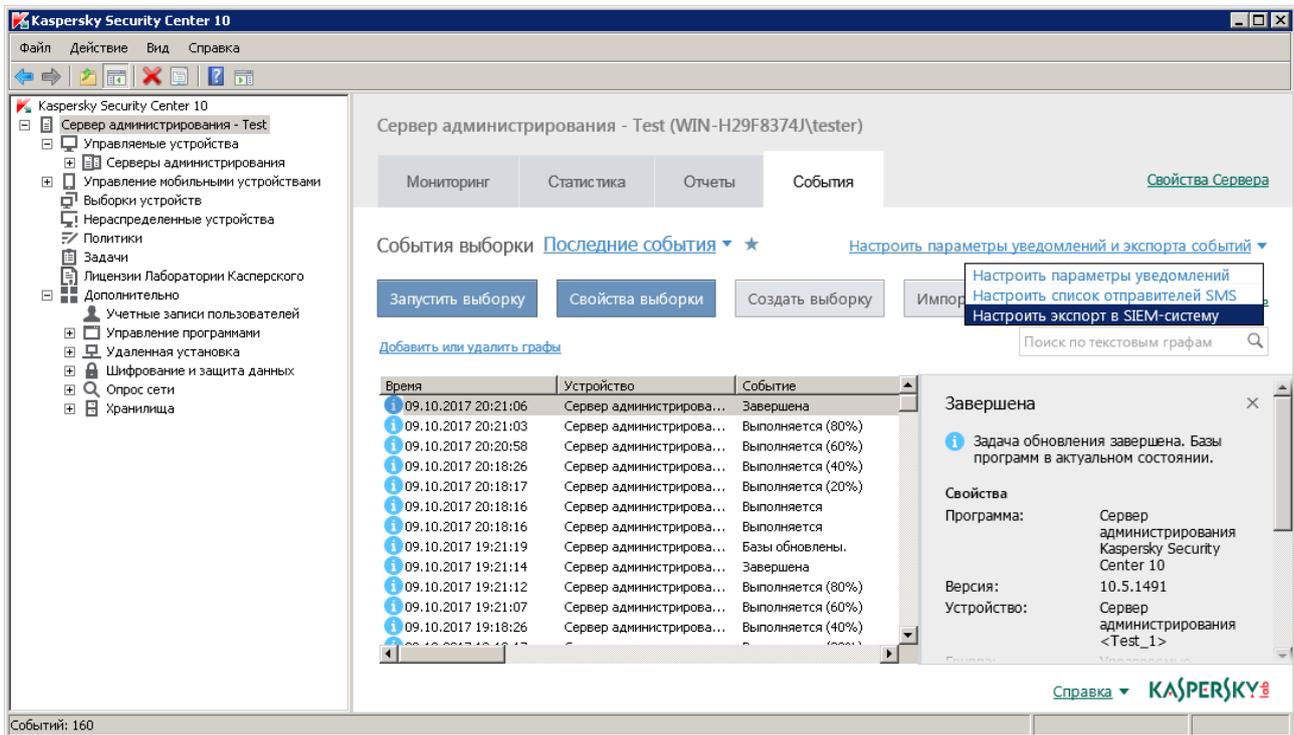


Рисунок 10. Окно свойств событий

Откроется окно свойств событий на разделе **Экспорт событий**.

4. В разделе **Экспорт событий** укажите следующие параметры:

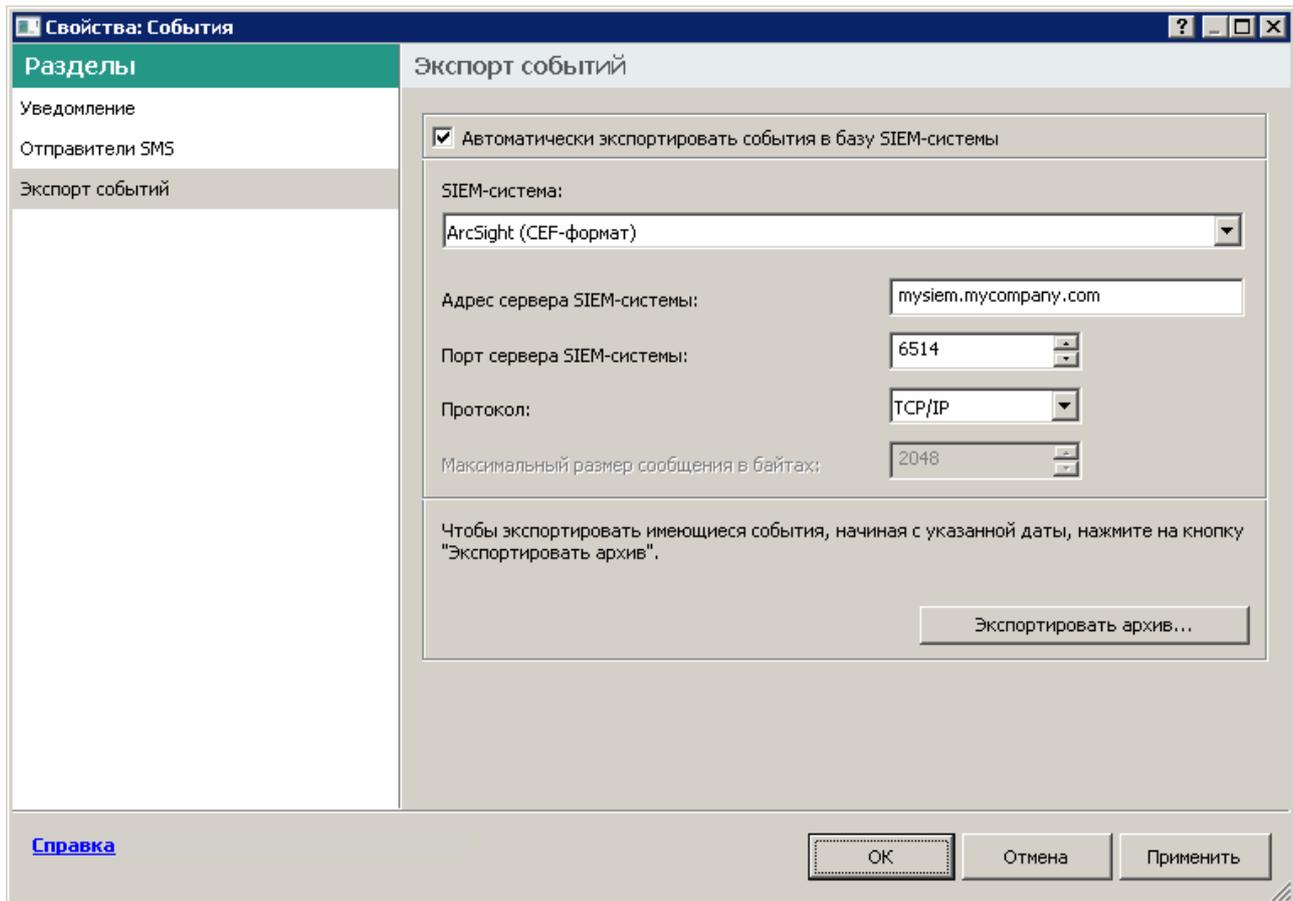


Рисунок 11. Раздел Экспорт событий

- **Автоматически экспортировать события в базу SIEM-системы**

Установите этот флажок, для того чтобы включить автоматический экспорт событий в SIEM-систему. При установке этого флажка все поля в разделе **Экспорт событий** становятся доступными для редактирования.

- **SIEM-система**

Выберите, в какую SIEM-систему будет выполняться экспорт событий: QRadar, Splunk или ArcSight.

- **Адрес сервера SIEM-системы**

Укажите адрес сервера SIEM-системы. Адрес сервера можно указать в формате DNS- или NetBIOS-имени или IP-адреса

- **Порт сервера SIEM-системы**

Укажите номер порта для соединения с сервером SIEM-системы. Этот номер порта должен совпадать с номером порта, который вы указываете в настройках приемника SIEM-системы для получения событий (см. раздел Настройка SIEM-системы).

- **Протокол**

Выберите протокол передачи сообщений в SIEM-систему. Можно выбрать протокол TCP/IP или UDP. Протокол TCP/IP является более надежным и поддерживает уведомление о получении сообщений. Протокол UDP является более простым, он применяется в случаях, когда проверка и исправление ошибок передачи сообщений не обязательны или выполняются внутри приложения.

5. Если требуется выполнить экспорт в SIEM-систему событий, произошедших после определенной даты в прошлом, нажмите на кнопку **Экспортировать архив** и укажите дату, начиная с которой будет выполнен экспорт событий. По умолчанию экспорт событий начинается сразу после включения.
6. Нажмите на кнопку **ОК**.

Автоматический экспорт событий будет включен. Общие события будут автоматически экспортироваться в SIEM-систему.

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center, не используя интерфейс Kaspersky Security Center. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

Публичные представления

Для вашего удобства в базе данных Kaspersky Security Center предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе klakdb.chm (<http://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip>).

Публичное представление v_akpub_ev_event содержит набор полей, соответствующих параметрам событий в базе данных. В документе klakdb.chm также содержится информация о публичных представлениях, относящихся к другим объектам Kaspersky Security Center, например, устройствам, программам, пользователям. Вы можете использовать эту информацию при создании запросов.

Инструменты работы с базой данных

Для работы с публичными представлениями Kaspersky Security Center можно использовать средства управления базами данных SQL Server или MySQL. Для работы с отдельными SQL-запросами вы можете загрузить и использовать утилиту klsql2 (<http://media.kaspersky.com/utilities/CorporateUtilities/klsql2.zip>), доступную на веб-сайте "Лаборатории Касперского". Эта утилита предназначена для создания отдельных SQL-запросов к публичным представлениям Kaspersky Security Center. Утилита доступна в виде zip-архива.

В этом разделе приведены инструкции по созданию SQL-запроса с помощью утилиты klsql2, а также пример такого запроса.

Вы также можете использовать любые другие программы для работы с базами данных для создания SQL-запросов и представлений баз данных. Ниже представлена информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center, такие как имя экземпляра и имя базы данных.

В этом разделе

Создание SQL-запроса с помощью утилиты klsql2	442
Просмотр имени базы данных Kaspersky Security Center	444

Создание SQL-запроса с помощью утилиты klsql2

В этом разделе приведены инструкции по загрузке и использованию утилиты klsql2, а также по созданию SQL-запроса с использованием этой утилиты. При создании SQL-запроса с помощью утилиты klsql2 нет необходимости в явном виде указывать имя и параметры доступа для базы данных Kaspersky Security Center, поскольку запрос обращается напрямую к публичным представлениям Kaspersky Security Center.

► *Чтобы загрузить и использовать утилиту klsql2, выполните следующие действия:*

1. Загрузите утилиту klsql2 (<http://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip>) с веб-сайта "Лаборатории Касперского".
2. Скопируйте и извлеките содержимое архива klsql2.zip в любую папку на устройстве, на котором установлен Сервер администрирования Kaspersky Security Center.

Пакет klsql2.zip содержит следующие файлы:

- klsql2.exe
 - src.sql
 - start.cmd
3. Откройте файл src.sql с помощью любого текстового редактора.
 4. Выполните следующие действия с файлом src.sql:
 - a. Удалите содержимое файла src.sql.
 - b. В файле src.sql введите требуемый SQL-запрос.
 - c. Сохраните файл src.sql.
 5. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для запуска SQL-запроса из файла src.sql и сохранения результатов в файл result.xml:

```
klsql2 -i src.sql -o result.xml
```

6. Откройте созданный файл result.xml и посмотрите результаты выполнения запроса.

Вы можете редактировать файл src.sql и создавать в нем любые запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить запрос и сохранить результаты в файл.

В этом разделе

| Пример SQL-запроса, созданного с помощью утилиты klsql2 [443](#)

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, созданного с помощью утилиты klsql2.

Следующий пример показывает, как получить список событий, произошедших на устройствах пользователей за последние 7 дней, и отсортировать его по времени возникновения событий, самые недавние события отображаются первыми.

Пример:

```
SELECT
e.nId,                               /* идентификатор
события */
e.tmRiseTime,                         /* время
возникновения события */
e.strEventType,                       /* внутреннее имя типа
события */
e.wstrEventTypeDisplayName,          /* отображаемое
имя события */
e.wstrDescription,                   /* отображаемое
описание события */
e.wstrGroupName,                     /* имя группы устройств */
h.wstrDisplayName,                   /* отображаемое имя
устройства, на котором произошло событие */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp      /*
IP-адрес устройства, на котором произошло событие */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Просмотр имени базы данных Kaspersky Security Center

Для доступа к базе данных Kaspersky Security Center с помощью SQL Server или MySQL необходимо знать имя базы данных, чтобы иметь возможность подключиться к ней из редактора скриптов SQL.

► Чтобы просмотреть имя базы данных Kaspersky Security Center, выполните следующие действия:

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В появившемся окне свойств Сервера администрирования выберите пункт **Дополнительно**, а затем **Информация об используемой базе данных**.
3. В разделе **Информация об используемой базе данных** обратите внимание на следующие свойства базы данных:

- **Имя экземпляра**

Имя экземпляра используемой базы данных Kaspersky Security Center.
Значение по умолчанию – `.IKAV_CS_ADMIN_KIT`.

- **Имя базы данных**

Имя базы данных SQL Kaspersky Security Center. Значение по умолчанию – KAV.

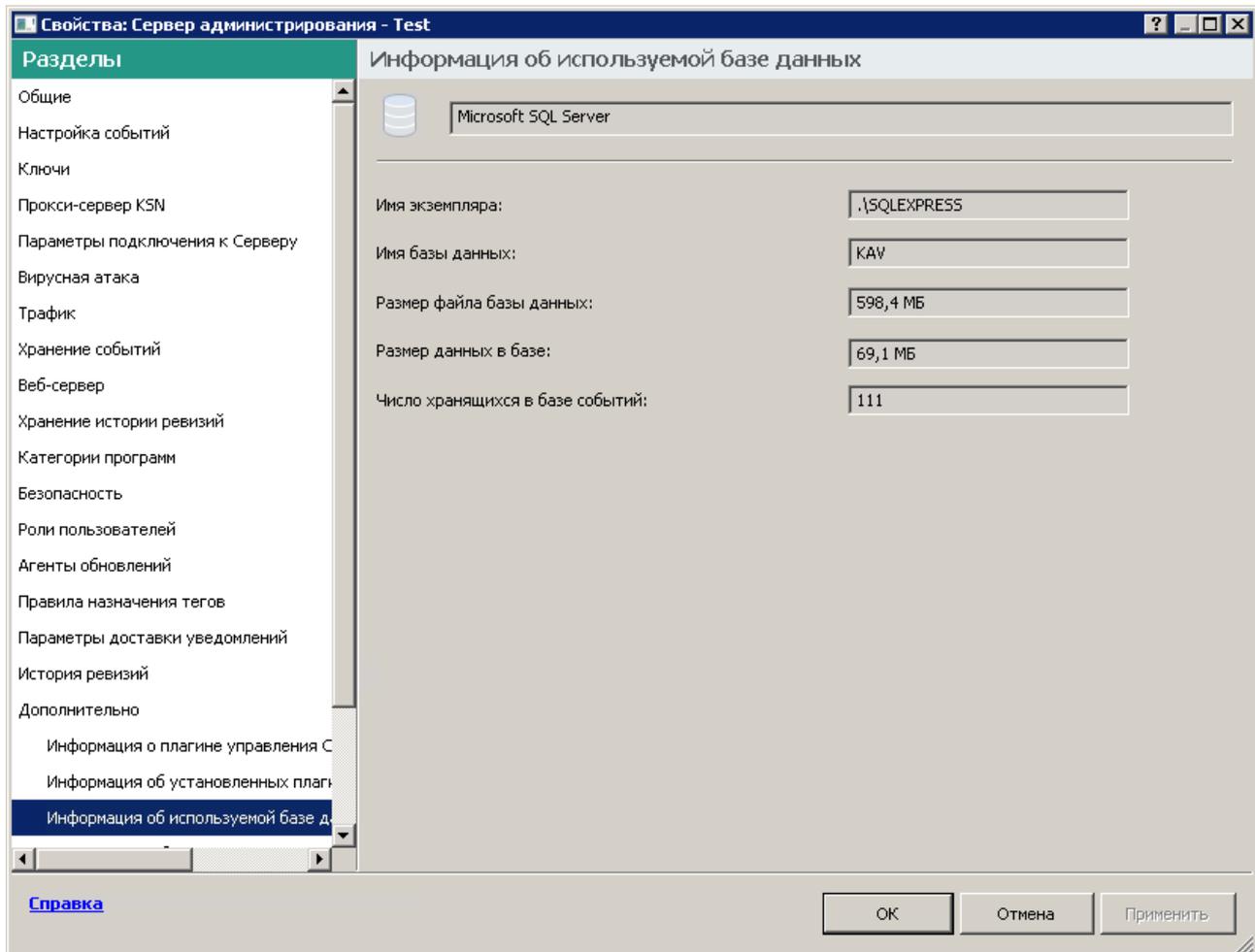


Рисунок 12. Имя базы данных SQL Kaspersky Security Center

4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

Настройка экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center – и получатель

событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Консоли администрирования Kaspersky Security Center.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky Security Center. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта или тип входных данных**

Протокол передачи сообщений, TCP/IP или UDP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

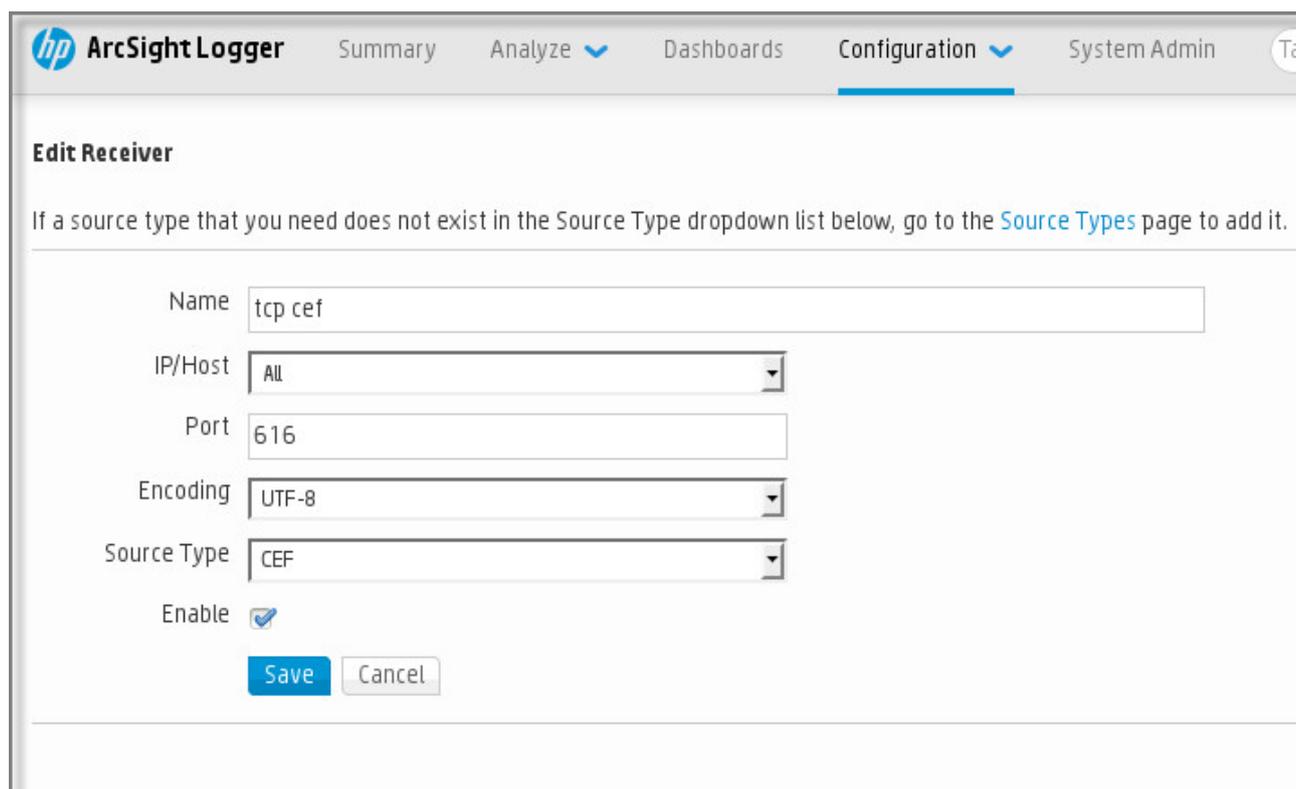
Номер порта для подключения к Kaspersky Security Center. Необходимо указать тот же номер порта, который был выбран в Kaspersky Security Center для передачи событий.

- **Протокол передачи сообщений или тип исходных данных**

Протокол, используемый для экспорта событий в SIEM-систему. Может являться одним из стандартных протоколов: Syslog, CEF или LEEF. SIEM-система выбирает анализатор событий, соответствующий указанному протоколу.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На следующем рисунке приведен пример настройки приемника в ArcSight.



The screenshot shows the 'Edit Receiver' configuration page in the ArcSight Logger interface. The page has a navigation bar at the top with 'hp ArcSight Logger' and tabs for 'Summary', 'Analyze', 'Dashboards', 'Configuration', and 'System Admin'. Below the navigation bar, the title 'Edit Receiver' is displayed. A note states: 'If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.' The configuration fields are: 'Name' (text input: tcp cef), 'IP/Host' (dropdown: All), 'Port' (text input: 616), 'Encoding' (dropdown: UTF-8), 'Source Type' (dropdown: CEF), and 'Enable' (checkbox: checked). At the bottom, there are 'Save' and 'Cancel' buttons.

Рисунок 13. Пример настройки приемника сообщений

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание и прочие параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

В каждой SIEM-системе имеется набор стандартных анализаторов сообщений. "Лаборатория Касперского" также предоставляет анализаторы сообщений для некоторых SIEM-систем, например, для QRadar и ArcSight. Вы можете загрузить эти анализаторы сообщений с веб-страниц соответствующих SIEM-систем. При настройке приемника можно выбрать используемый анализатор сообщений: один из стандартных анализаторов вашей SIEM-системы или анализатор, предоставляемый "Лабораторией Касперского".

Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky Security Center события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky Security Center и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. На рисунке видно, что первое событие относится к критическим событиям Сервера администрирования – *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.

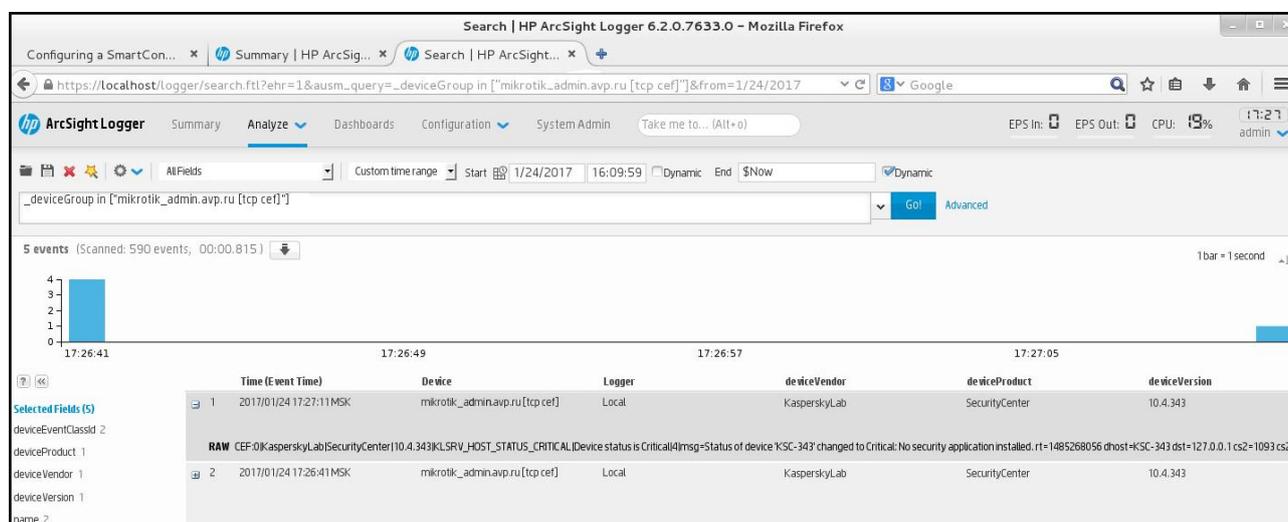


Рисунок 14. Пример событий

Общие события

Каждая программа "Лаборатории Касперского" имеет собственный набор событий. Общие события – это события Сервера администрирования или Агента администрирования Kaspersky Security Center.

В этом разделе приведены списки общих событий, а также их уровни важности и заданное по умолчанию время хранения.

В этом разделе

События Сервера администрирования.....	450
События Агента администрирования.....	454

События Сервера администрирования

В следующей таблице приведены события Сервера администрирования Kaspersky Security Center, объединенные по уровню важности. Для каждого события указано заданное по умолчанию время хранения. Время хранения события можно задать в Kaspersky Security Center.

Таблица 7. События Сервера администрирования

Уровень важности	Событие	Время хранения
Критическое событие	Лицензионное ограничение превышено.	180 дней
	Вирусная атака.	180 дней
	Контроль над устройством потерян.	180 дней
	Статус устройства "Критический".	180 дней
	Файл ключа в черном списке.	180 дней
	Режим ограниченной функциональности.	180 дней
	Срок действия лицензии истекает.	180 дней
	Срок действия сертификата истек.	Не хранится
	Обновления модулей программ "Лаборатории Касперского" отозваны.	180 дней

Уровень важности	Событие	Время хранения
Отказ функционирования	Ошибка времени выполнения.	180 дней
	Для одной из групп лицензионных программ превышено ограничение числа установок.	180 дней
	При копировании обновлений в заданную папку произошла ошибка.	180 дней
	Нет свободного места на диске.	180 дней
	Недоступна папка общего доступа.	180 дней
	Недоступна информационная база Сервера администрирования.	180 дней
	Нет свободного места в информационной базе Сервера администрирования.	180 дней
Предупреждение	Лицензионное ограничение превышено.	90 дней
	Устройство долго не проявляет активности в сети.	90 дней
	Конфликт имен устройств.	90 дней
	Статус устройства "Предупреждение".	90 дней
	Для одной из групп лицензионных программ скоро будет превышено ограничение числа установок.	90 дней
	Сертификат запрошен.	Не хранится
	Сертификат удален.	Не хранится
	Срок действия APNs-сертификата истек.	Не хранится

Уровень важности	Событие	Время хранения
	Срок действия APNs-сертификата истекает.	Не хранится
	Не удалось отправить GCM-сообщение на мобильное устройство.	Не хранится
	HTTP ошибка при отправке GCM-сообщения на GCM сервер.	Не хранится
	Не удалось отправить GCM-сообщение на GCM сервер.	Не хранится
	Мало свободного места на дисках.	90 дней
	Мало свободного места в информационной базе Сервера администрирования.	90 дней
	Разорвано соединение с подчиненным Сервером администрирования.	90 дней
	Разорвано соединение с главным Сервером администрирования.	90 дней
	Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN.	90 дней
	Зарегистрированы новые обновления для модулей программ "Лаборатории Касперского".	90 дней
	Началось удаление событий из базы данных, так как превышено ограничение числа событий.	90 дней

Уровень важности	Событие	Время хранения
	Удалены события из базы данных, так как превышено ограничение числа событий.	90 дней
	Срок действия лицензии истекает.	90 дней
Информационное сообщение	Ключ использован более чем на 90%.	30 дней
	Найдено новое устройство.	30 дней
	Устройство автоматически добавлено в группу.	30 дней
	Устройство удалено из группы: долгое отсутствие активности.	30 дней
	Для одной из групп лицензионных программ скоро будет превышено ограничение числа установок (использовано более 95%).	30 дней
	Появились файлы для отправки на анализ в "Лабораторию Касперского".	30 дней
	Регистрационный GCM-идентификатор мобильного устройства изменен.	Не хранится
	Обновления успешно скопированы в заданную папку.	30 дней
	Установлено соединение с подчиненным Сервером администрирования.	30 дней
	Установлено соединение с главным Сервером администрирования.	30 дней
Базы обновлены.	30 дней	

Уровень важности	Событие	Время хранения
	Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно.	30 дней
	Прокси-сервер KSN был остановлен.	30 дней
	Аудит: Подключение к Серверу администрирования.	30 дней
	Аудит: Изменение объекта.	30 дней
	Аудит: Изменение статуса объекта.	30 дней
	Аудит: Изменение параметров группы.	30 дней

События Агента администрирования

В следующей таблице приведены события Агента администрирования Kaspersky Security Center, объединенные по уровню важности. Для каждого события указано заданное по умолчанию время хранения. Время хранения события можно задать в Kaspersky Security Center.

Таблица 8. События Агента администрирования

Уровень важности	Событие	Время хранения
Отказ функционирования	Ошибка при установке исправления.	30 дней
	Установка обновления стороннего ПО завершена с ошибкой.	30 дней
	Не удалось установить обновления Microsoft Windows.	30 дней

Уровень важности	Событие	Время хранения
Предупреждение	Предупреждение при установке обновления программных модулей.	30 дней
	Установка обновления стороннего ПО завершена с предупреждением.	30 дней
	Установка обновления стороннего ПО отложена.	30 дней
	Произошел инцидент.	30 дней
Информационное сообщение	Обновление программных модулей успешно установлено.	30 дней
	Запущена установка обновления программных модулей.	30 дней
	Установлена программа.	30 дней
	Удалена программа.	30 дней
	Установлена наблюдаемая программа.	30 дней
	Удалена наблюдаемая программа.	30 дней
	Установлена сторонняя программа.	30 дней
	Новое устройство добавлено.	30 дней
	Устройство удалено.	30 дней
	Обнаружено устройство.	30 дней
	Устройство авторизовано.	30 дней
	Доступ к рабочему столу: файл был прочитан.	30 дней

Уровень важности	Событие	Время хранения
	Доступ к рабочему столу: файл был изменен.	30 дней
	Доступ к рабочему столу: программа была запущена.	30 дней
	Доступ к рабочему столу: предоставлен.	30 дней
	Доступ к рабочему столу: завершен.	30 дней
	Установка обновления стороннего ПО завершена успешно.	30 дней
	Запущена установка обновления стороннего ПО.	30 дней

Kaspersky Security Network и Kaspersky Private Security Network

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN). Приведена информация о KSN и KPSN, а также инструкции по включению KPSN, настройке доступа к KPSN, по просмотру статистики использования прокси-сервера KSN.

В этом разделе

О KSN и KPSN	457
О предоставлении данных.....	459
Настройка доступа к KPSN	461
Включение и отключение KPSN	463
Просмотр статистики прокси-сервера KSN.....	464

О KSN и KPSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая 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 программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о программах, установленных на клиентских устройствах.

Участвуя в KSN, вы в соответствии с Положением о KSN соглашаетесь в автоматическом режиме передавать в "Лабораторию Касперского" информацию о работе программ

"Лаборатории Касперского", установленных на клиентских устройствах под управлением Kaspersky Security Center. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN (см. раздел "Настройка доступа к KPSN" на стр. [461](#)).

Программа предлагает присоединиться к KSN во время установки программы и во время работы Мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с программой (см. раздел "Включение и отключение KPSN" на стр. [463](#)).

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Необходимо использовать Kaspersky Private Security Network или отказаться от использования KSN.

Вы можете использовать Kaspersky Private Security Network (далее также KPSN) вместо Kaspersky Security Network, чтобы не использовать отправку данных вашей организации за пределы локальной сети организации.

Kaspersky Private Security Network (KPSN) – это решение, позволяющее получать доступ к данным Kaspersky Security Network через сервер, размещенный внутри сети вашей организации. KPSN позволяет программам "Лаборатории Касперского" получать доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсах и программном обеспечении. KPSN не передает статистику и файлы в "Лабораторию Касперского". Для получения подробной информации см. "Kaspersky Private Security Network. Подготовительные процедуры и руководство по эксплуатации".

Служба Kaspersky Private Security Network разработана для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

- отсутствия подключения серверов к интернету;
- законодательного запрета на отправку любых данных за пределы страны;
- требований корпоративной безопасности на отправку любых данных за пределы локальной сети организации.

Клиентские устройства, находящиеся под управлением Сервера администрирования, для взаимодействия с KSN или KPSN могут использовать службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет и серверам KPSN.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования (см. раздел "Настройка доступа к KPSN" на стр. [461](#)).

О предоставлении данных

Участвуя в программе Kaspersky Security Network, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе программ "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Kaspersky Security Center. Специалисты "Лаборатории Касперского" используют информацию, полученную с клиентских устройств, для устранения проблем в работе программ "Лаборатории Касперского" или изменения их функциональности.

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Необходимо использовать Kaspersky Private Security Network или отказаться от использования KSN.

Принимая условия использования Kaspersky Security Network, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" следующие данные, полученные в результате работы Kaspersky Security Center на устройстве:

- идентификатор устройства и версия используемого на нем Агента администрирования;
- версия операционной системы устройства;
- дату и время принятия/отклонения Положения о Kaspersky Security Network;

- идентификатор Положения о Kaspersky Security Network и версии Положения о Kaspersky Security Network, принятого или отклоненного пользователем;
- информацию об установке/снятии флажка **Я принимаю условия использования Kaspersky Security Network**;
- уникальные идентификаторы устройства и пользователя;
- полную версию программы;
- тип программы.

В случае использования функциональности Системное администрирование и установки обновлений для программного обеспечения сторонних производителей, а также принятия условий использования Kaspersky Security Network вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" следующие данные:

- название, версия, используемый язык программы, для которой устанавливается обновление;
- версия базы данных обновлений, используемой программным обеспечением при установке;
- результат установки обновления;
- параметры программного обеспечения, используемые при установке обновлений (идентификаторы выполненных операций, коды результатов выполнения операций);
- уникальный идентификатор установки программного обеспечения на устройстве, полная версия установленного программного обеспечения и идентификатор типа программного обеспечения.

В случае использования продукта Kaspersky for Managed Service Providers и принятия условий использования Kaspersky Security Network вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" следующие данные:

- Тип платформы Managed Services Providers, версия приложения Правообладателя, которое используется для интеграции ПО с платформой Managed Services Providers.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Предоставление данных является добровольным. Функцию предоставления данных можно в любой момент включить или выключить в окне настройки программы.

Настройка доступа к KPSN

► *Чтобы настроить доступ Сервера администрирования к KPSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить доступ к KPSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Параметры прокси-сервера KSN**.
4. Установите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы включить службу прокси-сервера KSN.

Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в PSN.

5. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**.
6. Установите флажок **Настроить Локальный KSN** и по кнопке **Выбрать файл с параметрами KSN** загрузите параметры Локального KSN (файлы с расширениями pkcs7, pem).

Работу с Локальным KSN поддерживают не все программы "Лаборатории Касперского". Подробная информация приводится в Руководствах к соответствующим программам "Лаборатории Касперского".

Если для работы с Локальным KSN вы используете версии программ ниже Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2 или ниже Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, рекомендуется использовать подчиненные Серверы администрирования, для которых не настроено использование Локального KSN.

7. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

- В поле ввода **TCP-порт** укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через порт 13111.
- Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию флажок снят, подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

8. Установите флажок **Подключать подчиненные Серверы администрирования к KSN через главный Сервер**.

Если флажок установлен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если флажок снят, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Прокси-сервер KSN** также установлен флажок **Использовать Сервер администрирования как прокси-сервер**.

9. Нажмите на кнопку **ОК**.

В результате параметры доступа к KPSN будут сохранены.

Включение и отключение KPSN

► *Чтобы включить KPSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KPSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Установите флажок **Настроить Локальный KSN**.
5. Нажмите на кнопку **Выбрать файл с параметрами KSN** загрузите параметры Локального KSN (файлы с расширениями rkcs7, rem).

В результате KPSN будет включен.

6. Нажмите на кнопку **ОК**.

► *Чтобы выключить KPSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно выключить KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервера KSN**.
4. Снимите флажок **Настроить Локальный KSN**.

В результате KPSN будет выключен.

5. Нажмите на кнопку **ОК**.

Просмотр статистики прокси-сервера KSN

Прокси-сервер KSN – это служба, обеспечивающая взаимодействие между инфраструктурой Kaspersky Security Network и клиентскими устройствами, находящимися под управлением Сервера администрирования.

Использование прокси-сервера KSN предоставляет вам следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

В окне свойств Сервера администрирования вы можете настроить параметры прокси-сервера KSN и просмотреть статистическую информацию об использовании прокси-сервера KSN.

► *Чтобы просмотреть статистику работы прокси-сервера KSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно просмотреть статистику KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Статистика прокси-сервера KSN**.

В разделе отображается статистика работы прокси-сервера KSN. Если необходимо, выполните дополнительные действия:

- по кнопке **Обновить** обновите статистическую информацию об использовании прокси-сервера KSN;
- по кнопке **Экспортировать в файл** экспортируйте данные статистики в файл формата CSV;

- по кнопке **Проверить подключение к KSN** проверьте, подключен ли Сервер администрирования к KSN в настоящий момент.
4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Устранение неисправностей

В этом разделе содержится информация о наиболее распространенных ошибках и проблемах при развертывании и использовании Kaspersky Security Center, а также рекомендации по решению проблем.

В этом разделе

Проблемы при удаленной установке программ	466
Неверно выполнено копирование образа жесткого диска	469
Проблемы с Сервером мобильных устройств Exchange ActiveSync.....	471
Проблемы с Сервером iOS MDM	473
Проблемы с KES-устройствами.....	478

Проблемы при удаленной установке программ

В таблице ниже перечислены проблемы, возникающие при удаленной установке программ, и типовые причины возникновения этих проблем.

Таблица 9. Проблемы при удаленной установке программ

Проблема	Типовая причина проблемы и вариант решения
Недостаточно прав для установки	Учетная запись, под которой запущена установка, не имеет достаточно прав для выполнения операций, необходимых для установки программы.
Недостаточно места на диске	Недостаточно свободного места на диске для завершения установки. Освободите место на диске и повторите операцию.
Произошла незапланированная перезагрузка ОС	Во время установки произошла незапланированная перезагрузка ОС, точный результат установки может быть неизвестен. Проверьте правильность параметров запуска инсталляционного приложения или обратитесь в Службу технической поддержки.
Не найден необходимый файл	В инсталляционном пакете не найден необходимый файл. Проверьте целостность используемого инсталляционного пакета.
Несовместимая платформа	Инсталляционный пакет не предназначен для данной платформы. Используйте соответствующий инсталляционный пакет.
Несовместимая программа	На устройстве установлена программа, несовместимая с устанавливаемой программой. Перед установкой удалите все программы, входящие в список несовместимых.
Недостаточные системные требования	Инсталляционный пакет требует наличия в системе дополнительного программного обеспечения. Проверьте соответствие конфигурации системы системным требованиям устанавливаемой программы.

Проблема	Типовая причина проблемы и вариант решения
Незавершенная установка	Предыдущая установка или удаление программы не было штатно завершено. Для завершения предыдущей установки или удаления программы, выполненного на данном устройстве, необходимо перезагрузить ОС и повторить процесс установки.
Не та версия инсталляционного приложения	Установка данного инсталляционного пакета не поддерживается версией инсталляционного приложения, установленного на устройстве.
Инсталляция уже запущена	На устройстве уже запущена установка другого приложения.
Не удалось открыть инсталляционный пакет	Не удалось открыть инсталляционный пакет. Возможные причины: пакет отсутствует, пакет поврежден, недостаточно прав для доступа к пакету.
Несовместимая локализация	Инсталляционный пакет не предназначен для установки на данную локализацию ОС.
Установка запрещена политикой	Установка программ на данном устройстве запрещена политикой.
Ошибка записи файла	Во время установки программы произошла ошибка записи. Проверьте наличие прав у учетной записи, под которой выполняется установка, и наличие свободного места на диске.
Неверный пароль деинсталляции	Пароль для удаления программы задан неверно.
Недостаточные аппаратные требования	Аппаратные требования системы не удовлетворяют требованиям программы (объем оперативной памяти, свободное место на диске и так далее).

Проблема	Типовая причина проблемы и вариант решения
Недопустимый каталог установки	Установка программы в указанный каталог запрещена политикой инсталляционного приложения.
Требуется повторная попытка установки после перезагрузки устройства	Требуется повторный запуск инсталлятора программы после перезагрузки устройства.
Для продолжения установки требуется перезагрузка устройства	Для продолжения работы инсталлятора программы требуется перезагрузка устройства.

Неверно выполнено копирование образа жесткого диска

Если копирование образа жесткого диска с установленным Агентом администрирования было выполнено без учета правил развертывания, часть устройств в Консоли администрирования может отображаться как один значок устройства, постоянно меняющий имя.

Можно использовать следующие способы решения этой проблемы:

- Удаление Агента администрирования.

Этот способ является самым надежным. На устройствах, которые были скопированы из образа неправильно, нужно при помощи сторонних средств удалить Агент администрирования, а затем установить его заново. Удаление Агента администрирования не может быть выполнено средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

- Запуск утилиты klmover с ключом "-dupfix".

На проблемных устройствах (на всех, которые были скопированы из образа неправильно) необходимо при помощи сторонних средств однократно запустить утилиту klmover с ключом "-dupfix" (klmover -dupfix), расположенную в папке установки Агента администрирования. Запуск утилиты не может быть выполнен средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

Затем следует удалить значок, на который отображались проблемные устройства до запуска утилиты.

- Ужесточение правила обнаружения неправильно скопированных устройств.

Этот способ можно использовать только в случае, если установлены Сервер администрирования и Агенты администрирования версии 10 Service Pack 1 или новее.

Следует ужесточить правило обнаружения неправильно скопированных Агентов администрирования таким образом, чтобы изменение NetBIOS-имени устройства приводило к автоматической "починке" таких Агентов администрирования (предполагается, что скопированные устройства имеют различные NetBIOS-имена).

На устройстве с Сервером администрирования нужно импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

- Если на устройстве с Сервером администрирования установлена 32-разрядная операционная система:

```
REGEDIT4
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
```

```
"KLSRV_CheckClones"=dword:00000003
```

- Если на устройстве с Сервером администрирования установлена 64-разрядная операционная система:

```
REGEDIT4
```

```
[HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]
```

```
"KLSRV_CheckClones"=dword:00000003
```

Проблемы с Сервером мобильных устройств Exchange ActiveSync

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием Сервера мобильных устройств Exchange ActiveSync.

Ошибка во время установки Сервера мобильных устройств Exchange ActiveSync

Если во время локальной или удаленной установки возникла ошибка, то причину ошибки можно узнать, открыв файл error.log, который расположен на устройстве, где производилась установка программы, по пути C:\Windows\Temp\klmdm4exch-2014-11-28-15-56-37\ (где цифры – это дата и время установки программы). Как правило, информации из файла error.log достаточно для решения возникшей проблемы.

В таблице ниже приведены примеры типичных ошибок, регистрируемых в файле error.log.

Таблица 10. Типичные ошибки

Ошибка	Описание	Причина
Error occurred on installation step: 'Test connection to PowerShell'	Error: Processing data from remote server failed with the following error message: The user "oreh-security.ru/Users/TestInstall" isn't assigned to any management roles.	Аккаунт, под которым производилась установка программы, не обладает ролью Organization Management.
Error occurred on installation step: 'Test connection to PowerShell'	Connecting to remote server failed with the following error message: The WinRM client cannot process the request. The authentication mechanism requested by the client is not supported by the server or unencrypted traffic is disabled in the service configuration. Verify the unencrypted traffic setting in the service configuration or specify one of the authentication mechanisms supported by the server. To use Kerberos, specify the computer name as the remote destination. Also verify that the client computer and the destination computer are joined to a domain. To use Basic, specify the computer name as the remote destination, specify Basic authentication and provide user name and password. Possible authentication mechanisms reported by server: Digest For more information, see the about_Remote_Troubleshooting Help topic.	Механизм аутентификации Windows в настройках веб-сервера IIS для виртуальной директории PowerShell не включен.

Список устройств и почтовых аккаунтов пуст

Причину, из-за которой не удастся получить список устройств и почтовых аккаунтов, можно узнать из событий, сохраненных в Консоли администрирования в узле Сервер администрирования на закладке **События** в выборке событий **Отказы функционирования**. Если в событиях нет информации, необходимо проверить подключение между Агентом администрирования устройства, на котором развернут Сервер мобильных устройств Exchange ActiveSync и Сервером администрирования.

Проблемы с Сервером iOS MDM

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием Сервера iOS MDM, а также о способах их решения.

В этом разделе

Портал support.kaspersky.ru.....	473
Проверка доступности сервиса APN.....	473
Рекомендуемая последовательность действий для решения проблем с веб-сервисом iOS MDM.....	474

Портал support.kaspersky.ru

Информация о некоторых проблемах, возникающих при использовании Сервера iOS MDM, приведена в Базе знаний на веб-сайте Службы технической поддержки <http://support.kaspersky.ru/ks10mob>.

Проверка доступности сервиса APN

Для проверки доступности сервиса APN вы можете использовать следующие команды утилиты Telnet:

- Со стороны веб-сервиса iOS MDM:

```
$ telnet gateway.push.apple.com 2195
```

- Со стороны iOS MDM-устройства (проверку необходимо провести из сети, в которой находится устройство):

```
$ telnet 1-courier.push.apple.com 5223
```

Рекомендуемая последовательность действий для решения проблем с веб-сервисом iOS MDM

► Если при использовании веб-сервиса iOS MDM возникают проблемы, выполните следующие действия:

1. Проверьте, что сертификаты корректны.
2. Проверьте события Консоли администрирования на наличие ошибок и невыполненных команд со стороны Сервера iOS MDM.
3. Проверьте мобильное устройство с помощью консоли приложения iPhone Configuration Utility.
4. Проверьте файлы трассировки веб-сервиса iOS MDM: внутренние сервисы, такие как RPC-сервис и веб-сервис (100 потоков), должны быть успешно запущены.

Проверка корректности сертификата веб-сервиса iOS MDM с помощью мультиплатформенной утилиты OpenSSL

Пример команды:

```
$ openssl s_client -connect mymdm.mycompany.com:443
```

Результат выполнения:

```
CONNECTED(00000003)
```

```
...
```

```
---
```

```
Certificate chain
```

```
0 s:/C=RU/ST=Msk/L=Msk/O=My Company/OU=AdminKit/CN=mymdm.mycompany.com
```

```
i:/CN=Kaspersky iOS MDM Server CA
```

```
...
```

```
.
```

Проверка трассировок веб-сервиса iOS MDM

О том, как получить трассировки веб-сервиса iOS MDM, см. статью в Базе знаний на веб-сайте Службы технической поддержки <http://support.kaspersky.ru/9792>.

Пример успешных трассировок:

```
I1117 20:58:39.050226 7984] [MAIN]: Starting service...  
I1117 20:58:39.050226 7984] [RPC]: Starting rpc service...  
...  
I1117 20:58:39.081428 7984] [RPC]: Rpc service started  
I1117 20:58:39.081428 3724] [WEB]: Starting web service...  
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T000]  
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T001]  
...  
I1117 20:58:39.455832 3724] [WEB]: Starting thread [T099]
```

Пример трассировок с занятым портом:

```
[WEB]: Starting web service...  
  
Error 28 fault: SOAP-ENV:Server [no subcode] "Only one usage of each socket address  
(protocol/network address/port) is normally permitted."  
  
Detail: [no detail]  
  
[WEB]: Web service terminated
```

Проверка трассировок с помощью консоли приложения iPhone Configuration Utility

Пример успешных трассировок:

Службы, отвечающие за MDM – profiled, mdmd

mdmd[174] <Notice>: (Note) MDM: mdmd starting...

mdmd[174] <Notice>: (Note) MDM: Looking for managed app states to clean up

profiled[175] <Notice>: (Note) profiled: Service starting...

mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note) MDM: Polling MDM server <https://10.255.136.71> for commands

mdmd[174] <Notice>: (Note) MDM: Transaction completed. Status: 200

mdmd[174] <Notice>: (Note) MDM: Attempting to perform MDM request: DeviceLock

mdmd[174] <Notice>: (Note) MDM: Handling request type: DeviceLock

mdmd[174] <Notice>: (Note) MDM: Command Status: Acknowledged

profiled[175] <Notice>: (Note) profiled: Recomputing passcode requirement message

profiled[175] <Notice>: (Note) profiled: Locking device

mdmd[174] <Notice>: (Note) MDM: Transaction completed. Status: 200

mdmd[174] <Notice>: (Note) MDM: Server has no commands for this device.

mdmd[174] <Notice>: (Note) MDM: mdmd stopping...

Проблемы с KES-устройствами

Этот раздел содержит информацию об ошибках и проблемах, связанных с использованием KES-устройств, а также о способах их решения.

В этом разделе

Портал support.kaspersky.ru.....	478
Проверка настроек сервиса Google Firebase Cloud Messaging.....	478
Проверка доступности сервиса Google Firebase Cloud Messaging	478

Портал support.kaspersky.ru

Информация о проблемах, возникающих при работе с KES-устройствами, приведена в Базе знаний на веб-сайте Службы технической поддержки <http://support.kaspersky.ru/ks10mob>.

Проверка настроек сервиса Google Firebase Cloud Messaging

Проверка настроек сервиса Google Firebase Cloud Messaging может быть выполнена на портале Google [https://code.google.com/apis/console/#project:\[YOUR\]](https://code.google.com/apis/console/#project:[YOUR]).

Проверка доступности сервиса Google Firebase Cloud Messaging

Для проверки доступности сервиса Google Firebase Cloud Messaging со стороны Kaspersky Security Center вы можете использовать команду утилиты Telnet:

```
telnet android.googleapis.com 443
```

Обновление антивирусных баз в ручном режиме

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

1. В программе Kaspersky Security Center, находящейся 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 программами, 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, программы 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 программы на дисках.

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программного обеспечения, 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 программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: <http://support.kaspersky.ru/subscribe>). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (<http://www.bdu.fstec.ru>, <https://support.kaspersky.ru/vulnerability>).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы 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.
- На форуме "Лаборатории Касперского" (<https://forum.kaspersky.com>).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. [534](#)).

Приложения

В этом разделе рассматриваются сведения справочного характера, описывающие дополнительные возможности программы, особенности интерфейса программы и работы с ним.

В этом разделе

Дополнительные возможности	483
Особенности работы с интерфейсом управления	495
Справочная информация	497
Поиск и экспорт данных	515

Дополнительные возможности

В этом разделе рассматривается ряд дополнительных функций программы Kaspersky Security Center, предназначенных для расширения возможностей централизованного управления программами на устройствах.

В этом разделе

Автоматизация работы Kaspersky Security Center. Утилита klakaut	484
Работа с внешними инструментами	484
Режим клонирования диска Агента администрирования	485
Настройка получения сообщений от компонента Контроль целостности системы	487
Обслуживание базы данных Сервера администрирования	490
Окно Способ уведомления пользователей	491
Раздел Учетная запись	492
Раздел Общие	493
Окно Выборка устройств	493
Окно Определение названия создаваемого объекта	493
Раздел Настройка событий	493
Раздел Категории программ	494

Автоматизация работы Kaspersky Security Center. Утилита klakaut

Вы можете автоматизировать работу Kaspersky Security Center с помощью утилиты klakaut. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center.

Работа с внешними инструментами

Kaspersky Security Center позволяет сформировать список *внешних инструментов* (далее также *инструментов*) – программ, которые вызываются для клиентского устройства из

Консоли администрирования при помощи группы контекстного меню **Внешние инструменты**. Для каждого инструмента из списка создается отдельная команда меню, с помощью которой Консоль администрирования запускает соответствующую инструменту программу.

Программа запускается на рабочем месте администратора. В качестве аргументов командной строки программа может принимать атрибуты удаленного клиентского устройства (NetBIOS-имя, DNS-имя, IP-адрес). Подключение к удаленному устройству может выполняться при помощи туннелированного соединения.

По умолчанию для каждого клиентского устройства список внешних инструментов содержит следующие сервисные программы:

- **Удаленная диагностика** – утилита удаленной диагностики Kaspersky Security Center.
- **Удаленный рабочий стол** – стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу".
- **Управление компьютером** – стандартный компонент Microsoft Windows.

► *Чтобы добавить или удалить внешние инструменты, а также изменить их параметры,*

в контекстном меню клиентского устройства выберите пункт **Внешние инструменты** → **Настроить внешние инструменты**.

В результате откроется окно **Внешние инструменты**. В этом окне вы можете добавлять и удалять внешние инструменты, а также настраивать их параметры с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

Режим клонирования диска Агента администрирования

Клонирование жесткого диска "эталонного" устройства является распространенным способом установки программного обеспечения на новые устройства. Если Агент администрирования на жестком диске "эталонного" устройства во время клонирования работает в обычном режиме, возникает следующая проблема:

После развертывания на новых устройствах эталонного образа диска с Агентом администрирования эти устройства отображаются в Консоли администрирования одним значком. Проблема возникает потому, что при клонировании на новых устройствах сохраняются одинаковые внутренние данные, позволяющие Серверу администрирования связать устройство со значком в Консоли администрирования.

Избежать проблемы с неверным отображением новых устройств в Консоли администрирования после клонирования помогает специальный *режим клонирования диска Агента администрирования*. Используйте этот режим, если вы разворачиваете программное обеспечение (с Агентом администрирования) на новых устройствах путем клонирования диска.

В режиме клонирования диска Агент администрирования работает, но не подключается к Серверу администрирования. При выходе из режима клонирования Агент администрирования удаляет внутренние данные, из-за наличия которых Сервер администрирования связывает несколько устройств с одним значком в Консоли администрирования. По завершении клонирования образа "эталонного" устройства, новые устройства отображаются в Консоли администрирования нормально (отдельными значками).

Сценарий использования режима клонирования диска Агента администрирования

1. Администратор устанавливает Агент администрирования на "эталонном" устройстве.
2. Администратор проверяет подключение Агента администрирования к Серверу администрирования с помощью утилиты `klagchk` (см. раздел "Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита `klagchk`" на стр. [120](#)).
3. Администратор включает режим клонирования диска Агента администрирования.
4. Администратор устанавливает на устройство программное обеспечение, патчи и выполняет любое количество перезагрузок устройства.
5. Администратор выполняет клонирование диска "эталонного" устройства на любое число устройств.
6. Для каждой клонированной копии должны быть выполнены следующие условия:

- a. имя устройства изменено;
- b. устройство перезагружено;
- c. режим клонирования диска выключен.

Включение и выключение режима клонирования диска с помощью утилиты klmover

► Чтобы включить / выключить режим клонирования диска Агента администрирования, выполните следующие действия:

1. Запустите утилиту klmover на устройстве с установленным Агентом администрирования, который нужно клонировать.

Утилита klmover находится в папке установки Агента администрирования.

2. Чтобы включить режим клонирования диска, в командной строке Windows введите команду `klmover -cloningmode 1`.

Агент администрирования переключается в режим клонирования диска.

3. Чтобы запросить текущее состояние режима клонирования диска, в командной строке введите команду `klmover -cloningmode`.

В результате в окне утилиты отобразится информация о том, включен или выключен режим клонирования диска.

4. Чтобы выключить режим клонирования диска, в командной строке утилиты введите команду `klmover -cloningmode 0`.

Настройка получения сообщений от компонента Контроль целостности системы

Получение сообщений от компонента Контроля целостности системы осуществляется с помощью программ Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент. Kaspersky Security Center позволяет также следить за неизменностью критически важных областей систем (например, веб-серверы, банкоматы) и оперативно реагировать на нарушения целостности таких систем. Для этого реализована

поддержка получения сообщений от компонента Контроль целостности системы. Компонент Контроль целостности системы позволяет следить не только за файловой системой устройства, но и за ветками реестра, состоянием сетевого экрана и состоянием подключенного оборудования.

Требуется выполнить настройку Kaspersky Security Center, чтобы получать сообщения от компонента Контроль целостности системы без использования программ Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент.

► *Чтобы настроить параметры получения сообщений от компонента Контроль целостности системы, выполните следующие действия:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.

2. Перейдите в раздел:

- для 64-разрядной системы:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34  
\1093\1.0.0.0\ServerFlags
```

- для 32-разрядной системы:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Components\34\1093\1.0.0.0\ServerFlags
```

3. Создайте ключи:

- Создайте ключ KLSRV_EVP_FIM_PERIOD_SEC, чтобы указать период времени подсчета числа обработанных событий. Задайте следующие параметры:

a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_SEC.

b. Укажите тип ключа DWORD.

c. Задайте диапазон значений промежутка времени от 43200 до 172800 секунд. По умолчанию промежуток времени равен 86400 сек.

- Создайте ключ `KLSRV_EVP_FIM_LIMIT` для ограничения количества принимаемых событий за указанный промежуток времени. Задайте следующие параметры:
 - i. Укажите название ключа `KLSRV_EVP_FIM_LIMIT`.
 - ii. Укажите тип ключа `DWORD`.
 - iii. Задайте диапазон значений принимаемых событий от 2000 до 50 000. По умолчанию количество событий равно 2000.
- Создайте ключ `KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC` для подсчета событий с точностью до определенного промежутка времени. Задайте следующие параметры:
 - a. Укажите название ключа `KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC`.
 - b. Укажите тип ключа `DWORD`.
 - c. Задайте диапазон значений от 120 до 600 секунд. По умолчанию промежуток времени равен 300 секунд.
- Создайте ключ `KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC`, чтобы после указанного значения времени программа выполняла проверку того, что число событий, обработанных за промежуток времени, становится меньше заданного ограничения. Проверка выполняется при достижении ограничения приема событий. Если условие выполняется, возобновляется сохранение событий в базу данных. Задайте следующие параметры:
 - i. Укажите название ключа `KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC`.
 - ii. Укажите тип ключа `DWORD`.
 - iii. Задайте диапазон значений от 600 до 3600 секунд. По умолчанию промежуток проверки равен 1800 секунд.

Если ключи не созданы, используются значения по умолчанию.

4. Перезапустите службу Сервера администрирования.

Ограничения получения событий от компонента Контроля целостности системы будут настроены. Результаты работы компоненты Контроля целостности системы вы можете посмотреть в отчетах **10 правил Контроля целостности системы, которые чаще всего срабатывали на устройствах и 10 устройств, на которых произошло максимальное количество срабатываний правил Контроля целостности системы.**

Обслуживание базы данных Сервера администрирования

Обслуживание базы данных Сервера администрирования позволяет сократить объем базы данных, повысить производительность и надежность работы программы. Рекомендуется обслуживать базу данных Сервера администрирования не реже раза в неделю.

Обслуживание базы данных Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания базы данных программа выполняет следующие действия:

- проверяет базу данных на наличие ошибок;
- перестраивает индексы базы данных;
- обновляет статистику базы данных;
- сжимает базу данных (если необходимо).

Задача обслуживания базы данных Сервера администрирования не поддерживает MySQL. Если в качестве СУБД используется MySQL, администратору следует обслуживать базу данных самостоятельно.

► *Чтобы создать задачу обслуживания базы данных Сервера администрирования, выполните следующие действия:*

1. В дереве консоли выберите узел Сервера администрирования, для которого нужно создать задачу обслуживания базы данных.
2. Выберите папку **Задачи**.
3. В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

В результате запускается мастер создания задачи.

4. В окне мастера **Выбор типа задачи** выберите тип задачи **Обслуживание базы данных** и нажмите на кнопку **Далее**.
5. Если во время обслуживания нужно сжимать базу данных Сервера администрирования, в окне мастера **Параметры** установите флажок **Сжать базу данных**.
6. Следуйте дальнейшим шагам мастера.

Созданная задача отображается в списке задач в рабочей области папки **Задачи**. Для одного Сервера администрирования может выполняться только одна задача обслуживания баз. Если задача обслуживания баз для Сервера администрирования уже создана, создание еще одной задачи обслуживания баз невозможно.

Окно Способ уведомления пользователей

В окне **Способ уведомления пользователя** можно настроить параметры уведомления пользователя об установке сертификата на мобильное устройство:

- **Показать ссылку на инсталляционный пакет.** При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.
- **Сообщить пользователю о подключении устройства.** При выборе этого варианта вы можете настроить параметры оповещения пользователя о подключении устройства.

В блоке параметров **По электронной почте** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ оповещения доступен только если настроен SMTP-сервер.

В блоке параметров **С помощью SMS** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен только если настроено SMS-оповещение.

По ссылке **Редактировать сообщение** в блоках параметров **По электронной почте** и **С помощью SMS** просмотрите и при необходимости отредактируйте текст уведомления.

См. также

| Установка сертификата пользователю [182](#)

Раздел Учетная запись

В разделе **Учетная запись** можно указать, под какой учетной записью запускать выбранную задачу.

Автоматически созданная учетная запись

Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

По умолчанию выбран этот вариант.

Задать учетную запись

Доступны для изменения поля ввода **Учетная запись**, **Пароль**, в которых можно указать учетную запись, обладающую достаточными правами для выполнения задачи.

Учетная запись

Учетная запись, от имени которой будет запускаться задача.

Пароль

Пароль учетной записи, от имени которой будет запускаться задача.

См. также

Учетные записи для запуска задач [103](#)

Раздел Общие

В этом разделе можно настраивать общие параметры профиля для мобильных устройств Exchange ActiveSync.

Название

Разрешить неинициализируемые устройства

Интервал обновления

Окно Выборка устройств

В этом окне можно указать выборку устройств, сведения о которых будут отображаться в рабочей области на закладке **Статистика** узла **Отчеты и уведомления**.

Выберите выборку из списка **Выборка устройств**. В списке перечислены выборки, заданные по умолчанию, и выборки, созданные пользователем.

Окно Определение названия создаваемого объекта

В окне укажите название создаваемого объекта. Имя не может превышать 100 символов и не может содержать специальные символы ("*<>?\":|).

Для перехода к следующему шагу нажмите на кнопку **Далее**.

Раздел Настройка событий

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Критическое событие.** Закладка **Критическое событие** не отображается в свойствах политики Агента администрирования.
- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

В списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке.

Для выбора нескольких типов событий используйте клавиши Shift или Ctrl, для выбора всех типов используйте кнопку **Выбрать все**.

Используйте эти параметры в следующих задачах

| Контроль возникновения вирусных эпидемий [42](#)

Раздел Категории программ

В этом разделе можно настроить распространение информации о категориях программ на клиентские устройства.

Передавать все данные (для Агентов администрирования версии Service Pack 2 и ниже)

Передавать только измененные данные (для Агентов администрирования версии Service Pack 2 и выше)

Используйте эти параметры в следующих задачах

| Создание категорий программ [246](#)

Особенности работы с интерфейсом управления

В этом разделе

Как вернуть исчезнувшее окно свойств	495
Как перемещаться по дереву консоли	495
Как открыть окно свойств объекта в рабочей области.....	496
Как выбрать группу объектов в рабочей области.....	496
Как изменить набор граф в рабочей области	497

Как вернуть исчезнувшее окно свойств

Иногда открытое окно свойств объекта исчезает с экрана. Это происходит из-за того, что оно перекрывается главным окном программы (эта ситуация является особенностью работы Microsoft Management Console).

- ▶ *Чтобы перейти к исчезнувшему окну свойств объекта,*
нажмите комбинацию клавиш **ALT+TAB**.

Как перемещаться по дереву консоли

Для перемещения по дереву консоли вы можете использовать следующие кнопки, расположенные в панели инструментов:

-  – переход на один шаг назад;
-  – переход на один шаг вперед;
-  – переход на один уровень вверх.

Можно также воспользоваться навигационной цепочкой, расположенной в правом верхнем углу рабочей области. Навигационная цепочка содержит полный путь к той папке дерева консоли, в которой вы находитесь в текущий момент. Все элементы цепочки, кроме последнего, являются ссылками на объекты дерева консоли.

Как открыть окно свойств объекта в рабочей области

Свойства большинства объектов Консоли администрирования можно изменять в окне свойств объекта.

- ▶ *Чтобы открыть окно свойств объекта, расположенного в рабочей области, выполните одно из следующих действий:*
 - в контекстном меню объекта выберите пункт **Свойства**;
 - выберите объект и нажмите комбинацию клавиш **ALT+ENTER**.

Как выбрать группу объектов в рабочей области

Вы можете выбрать группу объектов в рабочей области. Выбор группы объектов можно использовать, например, для создания набора устройств и последующего формирования задач для него.

- ▶ *Чтобы выбрать диапазон объектов, выполните следующие действия:*
 1. Выберите первый объект диапазона и нажмите на клавишу **SHIFT**.
 2. Удерживая нажатой клавишу **SHIFT**, выберите последний объект диапазона.

Диапазон будет выбран.
- ▶ *Чтобы объединить отдельные объекты в группу, выполните следующие действия:*
 1. Выберите первый объект в составе группы и нажмите на клавишу **CTRL**.
 2. Удерживая нажатой клавишу **CTRL**, выберите остальные объекты группы.

Объекты будут объединены в группу.

Как изменить набор граф в рабочей области

Консоль администрирования позволяет изменять набор граф, отображаемых в рабочей области.

► *Чтобы изменить набор граф в рабочей области, выполните следующие действия:*

1. Выберите объект дерева консоли, для которого вы хотите изменить набор граф.
2. В рабочей области папки откройте окно настройки набора граф по ссылке **Добавить или удалить графы**.
3. В окне **Добавление или удаление граф** сформируйте набор граф для отображения.

Справочная информация

В этом разделе в таблицах представлена сводная информация о контекстном меню объектов Консоли администрирования, а также о статусах объектов дерева консоли и рабочей области.

В этом разделе

Команды контекстного меню.....	498
Список управляемых устройств. Значение граф.....	504
Статусы устройств, задач и политик	509
Значки статусов файлов в Консоли администрирования	513

Команды контекстного меню

В этом разделе содержится перечень объектов Консоли администрирования и соответствующий им набор пунктов контекстного меню (см. таблицу ниже).

Таблица 11. Элементы контекстного меню объектов Консоли администрирования

Объект	Пункт меню	Назначение пункта меню
Общие пункты контекстного меню	Поиск	Открыть окно поиска устройств.
	Обновить	Обновить отображение выбранного объекта.
	Экспортировать список	Экспортировать текущий список в файл.
	Свойства	Открыть окно свойств выбранного объекта.
	Вид → Добавить или удалить графы	Добавить или удалить графы в таблице объектов в рабочей области.
	Вид → Крупные значки	Отображать объекты в рабочей области в виде крупных значков.
	Вид → Мелкие значки	Отображать объекты в рабочей области в виде мелких значков.
	Вид → Список	Отображать объекты в рабочей области в виде списка.

Объект	Пункт меню	Назначение пункта меню
	Вид → Таблица	Отображать объекты в рабочей области в виде таблицы.
	Вид → Настроить	Настроить отображение элементов Консоли управления.
Kaspersky Security Center	Создать → Сервер администрирования	Добавить в дерево консоли Сервер администрирования.
<Имя Сервера администрирования>	Подключиться к Серверу администрирования	Подключиться к Серверу администрирования.
	Отключиться от Сервера администрирования	Отключиться от Сервера администрирования.
Управляемые устройства	Установить программу	Запустить мастер удаленной установки программы.
	Вид → Настройка интерфейса	Настроить отображение элементов интерфейса.
	Удалить	Удалить Сервер администрирования из дерева консоли.
	Установить программу	Запустить мастер удаленной установки для группы администрирования.

Объект	Пункт меню	Назначение пункта меню
	Обнулить счетчик вирусов	Обнулить счетчики вирусов для устройств, входящих в состав группы администрирования.
	Просмотреть отчет об угрозах	Создать отчет об угрозах и вирусной активности устройств, входящих в состав группы администрирования.
	Создать → Группу	Создать группу администрирования.
	Все задачи → Создать структуру групп	Создать структуру групп администрирования на основе структуры доменов или Active Directory.
	Все задачи → Показать сообщение	Запустить мастер создания сообщения для пользователей устройств, входящих в группу администрирования.
Управляемые устройства → Серверы администрирования	Создать → Подчиненный Сервер администрирования	Запустить мастер добавления подчиненного Сервера администрирования.
	Создать → Виртуальный Сервер администрирования	Запустить мастер добавления виртуального Сервера администрирования.

Объект	Пункт меню	Назначение пункта меню
Управление мобильными устройствами → Мобильные устройства	Создать → Мобильное устройство	Подключить новое мобильное устройство пользователя.
Управление мобильными устройствами → Сертификаты	Создать → Сертификат	Создать сертификат.
	Создать → Мобильное устройство	Подключить новое мобильное устройство пользователя.
Выборки устройств	Создать → Новая выборка	Создать выборку устройств.
	Все задачи → Импортировать	Импортировать выборку из файла.
Лицензии Лаборатории Касперского	Добавить код активации или ключ	Добавить ключ в хранилище Сервера администрирования.
	Активировать программу	Запустить мастер создания задачи активации программы.
	Отчет о ключах	Создать и просмотреть отчет о ключах на клиентских устройствах.

Объект	Пункт меню	Назначение пункта меню
Управление программами → Категории программ	Создать → Категория	Создать категорию программ.
Управление программами → Реестр программ	Фильтр	Настроить фильтр для списка программ.
	Наблюдаемые программы	Настроить публикацию событий об установке программ.
	Удалить неустановленные программы	Удалить из списка информацию о программах, которые уже не установлены на устройствах сети.
Управление программами → Обновления программного обеспечения	Принять Лицензионные соглашения обновлений	Принять Лицензионные соглашения обновлений программного обеспечения.
Управление программами → Учет сторонних лицензий	Создать → Группу лицензионных программ	Создать группу лицензионных программ.
Удаленная установка → Инсталляционные пакеты	Показать актуальные версии программ	Просмотреть список актуальных версий программ "Лаборатории Касперского", выложенных на интернет-серверах.
	Создать → Инсталляционный пакет	Создать инсталляционный пакет.

Объект	Пункт меню	Назначение пункта меню
	Все задачи → Обновить базы	Обновить базы программ в инсталляционных пакетах.
	Все задачи → Показать общий список автономных пакетов	Просмотреть список автономных пакетов установки, созданных для инсталляционных пакетов.
Опрос сети → Домены	Все задачи → Активность устройств	Настроить параметры реакции Сервера администрирования на отсутствие активности устройств в сети.
Опрос сети → IP-диапазоны	Создать → IP-диапазон	Создать IP-диапазон.
Хранилища → Обновления и патчи ПО Лаборатории Касперского	Загрузить обновления	Запустить задачу загрузки обновлений в хранилище Сервера администрирования.
	Параметры загрузки обновлений	Настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования.
	Отчет об используемых базах	Создать и просмотреть отчет о версиях баз.
	Все задачи → Очистить хранилище обновлений	Очистить хранилище обновлений на Сервере администрирования.

Объект	Пункт меню	Назначение пункта меню
Хранилища → Оборудование	Создать → Устройство	Создать сетевое устройство.

Список управляемых устройств. Значение граф

В таблице ниже представлены названия и описания граф списка управляемых устройств.

Таблица 12. Значение граф списка управляемых устройств

Название графы	Значение
Имя	NetBios-имя клиентского устройства. Описание значков имени устройств приведено в приложении (см. раздел "Статусы устройств, задач и политик" на стр. 509).
Тип операционной системы	Тип операционной системы клиентского устройства.
Windows-домен	Наименование Windows-домена, в котором находится клиентское устройство.
Установлен Агент	Результат установки на клиентское устройство Агента администрирования.
Функционирует Агент	Результат функционирования Агента администрирования.
Постоянная защита	Установлена программа защиты (<i>Да, Нет</i>).
Соединение с Сервером	Время, прошедшее с момента соединения клиентского устройства с Сервером администрирования.
Последнее обновление	Время, прошедшее с момента последнего обновления Сервера администрирования Kaspersky Security Center.
Статус	Текущий статус клиентского устройства (<i>ОК, Критический, Предупреждение</i>).

Название графы	Значение
<p>Описание статуса</p>	<p>Причины изменения статуса клиентского устройства на <i>Критический</i> или <i>Предупреждение</i>.</p> <p>Статус устройства изменяется на <i>Предупреждение</i> или <i>Критический</i> по следующим причинам:</p> <ul style="list-style-type: none"> • Не установлена программа защиты. • Найдено много вирусов. • Уровень постоянной защиты отличается от уровня, установленного администратором. • Давно не выполнялся поиск вирусов. • Базы устарели. • Давно не подключался. • Есть необработанные объекты. • Требуется перезагрузка. • Установлены несовместимые программы. • Обнаружены уязвимости в программах. • Давно не выполнялся поиск обновлений Windows. • Определенное состояние шифрования данных. • Параметры мобильного устройства не соответствуют политике. • Есть необработанные инциденты. • Срок действия лицензии скоро истечет. <p>Статус устройства изменяется только на <i>Критический</i> по следующим причинам:</p> <ul style="list-style-type: none"> • Срок действия лицензии истек. • Контроль над устройством потерян. • Выключена защита. • Не запущена программа защиты. <p>Управляемые программы "Лаборатории Касперского" на клиентских устройствах могут пополнять список описаний статусов. Kaspersky Security Center может получать описание статуса клиентского устройства от управляемых программ "Лаборатории Касперского" на этом устройстве.</p>

Название графы	Значение
Обновление информации	Время, прошедшее с момента последней успешной синхронизации клиентского устройства с Сервером администрирования.
Имя DNS-домена	Имя DNS-домена клиентского устройства.
DNS домен	Основной DNS-суффикс.
IP-адрес	IP-адрес клиентского устройства. Рекомендовано использовать IPv4 адрес.
Видим в сети	Продолжительность видимости клиентского устройства в сети.
Проверка по требованию	Дата и время последней проверки клиентского устройства, выполненной программой защиты по требованию пользователя.
Обнаружено вирусов	Количество обнаруженных вирусов.
Статус постоянной защиты	Статус постоянной защиты (<i>Запускается, Выполняется, Выполняется (максимальная защита), Выполняется (максимальная скорость), Выполняется (рекомендуемый), Выполняется (с пользовательскими параметрами), Остановлена, Приостановлена, Сбой</i>).
IP-адрес соединения	IP-адрес подключения к Серверу администрирования Kaspersky Security Center.
Версия Агента администрирования	Версия Агента администрирования.
Версия защиты	Версия программы защиты, установленной на клиентском устройстве.
Версия баз	Версия антивирусных баз.

Название графы	Значение
Время включения	Дата и время последнего включения клиентского устройства.
Перезагрузка	Требуется перезагрузка клиентского устройства.
Агент обновлений	Имя устройства, выполняющего роль агента обновлений для этого клиентского устройства.
Описание	Описание клиентского устройства, полученное при сканировании сети.
Состояние WUA	Состояние Windows Update Agent клиентского устройства. Значение <i>Да</i> соответствует клиентским устройствам, которые получают обновления через Windows Update от Сервера администрирования. Значение <i>Нет</i> соответствует клиентским устройствам, которые получают обновления через Windows Update из других источников.
Разрядность операционной системы	Разрядность операционной системы клиентского устройства.
Статус защиты от спама	Статус компонента защиты от спама (<i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно</i>).
Статус защиты данных от утечек	Статус компонента защиты от утечки данных (<i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно</i>).
Статус защиты для серверов совместной работы	Статус компонента контентной фильтрации (<i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно</i>).

Название графы	Значение
Статус антивирусной защиты почтовых серверов	Статус компонента антивирусной защиты почтовых серверов (<i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно</i>).
Статус Endpoint Sensor	Статус компонента Endpoint Sensor (<i>Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно</i>).

Статусы устройств, задач и политик

В таблице ниже представлен список значков, отображающихся в дереве консоли и в рабочей области Консоли администрирования рядом с именами устройств, задач и политик. Эти значки характеризуют статус объектов.

Таблица 13. Статусы устройств, задач и политик

Значок	Статус
	Устройство с операционной системой для рабочих станций, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом <i>ОК</i> .
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> .
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом <i>Критический</i> .
	Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Устройство с операционной системой для серверов, обнаруженное в сети и не входящий в состав какой-либо группы администрирования.
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом <i>ОК</i> .
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> .
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом <i>Критический</i> .
	Устройство с операционной системой для серверов, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Мобильное устройство, обнаруженное в сети и не входящее в состав какой-либо группы администрирования.

	Мобильное устройство, входящее в состав группы администрирования, со статусом <i>OK</i> .
	Мобильное устройство, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> .
	Мобильное устройство, входящее в состав группы администрирования, со статусом <i>Критический</i> .
	Мобильное устройство, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно.
	Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>OK</i> . Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>OK</i> . Устройство с защитой на уровне UEFI не в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> . Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>Предупреждение</i> . Устройство с защитой на уровне UEFI не в сети.

	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>Критический</i> . Устройство с защитой на уровне UEFI в сети. Устройство с защитой на уровне UEFI в сети.
	Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом <i>Критический</i> . Устройство с защитой на уровне UEFI не в сети.
	Активная политика.
	Неактивная политика.
	Активная политика, унаследованная от группы, созданной на главном Сервере администрирования.
	Активная политика, унаследованная от группы верхнего уровня иерархии.
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии <i>Ожидает выполнения</i> или <i>Завершена</i> .
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии <i>Выполняется</i> .
	Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии <i>Завершена с ошибкой</i> .
	Задача, унаследованная от группы, созданной на главном Сервере администрирования.
	Задача, унаследованная от группы верхнего уровня иерархии.

Значки статусов файлов в Консоли администрирования

Для упрощения работы с файлами в Консоли администрирования Kaspersky Security Center рядом с именами файлов отображаются значки (см. таблицу ниже). Значки сигнализируют о статусах, присвоенных файлам управляемыми программами "Лаборатории Касперского" на клиентских устройствах. Значки отображаются в рабочей области папок **Карантин**, **Резервное хранилище** и **Необработанные файлы**.

Статусы присваиваются объектам программой Kaspersky Endpoint Security, установленной на клиентском устройстве, на котором находится объект.

Таблица 14. Соответствие значков статусам файлов

Значок	Статус
	Файл со статусом <i>Заражен</i> .
	Файл со статусом <i>Предупреждение</i> или <i>Возможно зараженный</i> .
	Файл со статусом <i>Помещен в папку пользователем</i> .
	Файл со статусом <i>Ложное срабатывание</i> .
	Файл со статусом <i>Вылечен</i> .
	Файл со статусом <i>Удален</i> .
	Файл в папке Карантин со статусом <i>Не заражен</i> , <i>Защищен паролем</i> или <i>Требуется отправки в "Лабораторию Касперского"</i> . Если рядом со значком нет описания статуса, это означает что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус.
	Файл в папке Резервное хранилище со статусом <i>Не заражен</i> , <i>Защищен паролем</i> или <i>Требуется отправки в "Лабораторию Касперского"</i> . Если рядом со значком нет описания статуса, это означает что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус.
	Файл в папке Необработанные файлы со статусом <i>Не заражен</i> , <i>Защищен паролем</i> или <i>Требуется отправки в "Лабораторию Касперского"</i> . Если рядом со значком нет описания статуса, это означает что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус.

Поиск и экспорт данных

В этом разделе содержится информация о способах поиска данных и об экспорте данных.

В этом разделе

Поиск устройств.....	515
Параметры поиска устройств	517
Использование масок в строковых переменных	532
Использование регулярных выражений в строке поиска.....	532
Экспорт списков из диалоговых окон	534

Поиск устройств

Kaspersky Security Center позволяет искать устройства на основании заданных критериев. Результаты поиска можно сохранить в текстовом файле.

Функция поиска позволяет находить следующие устройства:

- клиентские устройства в группах администрирования Сервера администрирования и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования и его подчиненных Серверов.

► *Чтобы искать клиентские устройства, входящие в группу администрирования, выполните следующие действия:*

1. В дереве консоли выберите папку группы администрирования.
2. В контекстном меню папки группы администрирования выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

► *Чтобы искать нераспределенные устройства, выполните следующие действия:*

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

► *Чтобы искать устройства независимо от того, входят они в состав групп администрирования или нет, выполните следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

В окне **Поиск** вы можете также искать группы администрирования и подчиненные Серверы администрирования с помощью раскрывающегося списка в правом верхнем углу окна. Поиск групп администрирования и подчиненных Серверов администрирования недоступен при открытии окна **Поиск** из папки **Нераспределенные устройства**.

Для поиска устройств вы можете использовать в полях ввода окна **Поиск** регулярные выражения (см. раздел «Использование регулярных выражений в строке поиска» на стр. [532](#)).

Полнотекстовый поиск в окне **Поиск** доступен:

- на закладке **Сеть** в поле **Комментарий**;

- на закладке **Оборудование** в полях **Устройство**, **Производитель**, **Описание**.

Параметры поиска устройств

Ниже представлены описания параметров поиска управляемых устройств. Результаты поиска отображаются в таблице в нижней части окна.

Сеть

На закладке **Сеть** можно настроить критерии поиска устройств на основании их сетевых данных:

- **Имя устройства**

Имя устройства в сети Windows (NetBIOS-имя).

- **Windows-домен**

Будут отображаться все устройства, входящие в указанный домен Windows.

- **Группа администрирования**

Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие** или в разделе **Заметки**.

Для описания текста в поле **Комментарий** допустимо использовать следующие символы:

- Внутри одного слова:
 - *. Заменяет любую строку длиной 0 и более символов.

Пример:

Для описания слов **Сервер**, **Серверный** или **Серверная** можно использовать строку **Сервер***

- ?. Заменяет любой один символ.

Пример:

Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

Символ * или ? не может использоваться как первый символ в описании текста.

- Для связи нескольких слов:
 - Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами.

Пример:

Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

- +. При написании перед словом обозначает обязательное наличие слова в тексте.

Пример:

Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- -. При написании перед словом обозначает обязательное отсутствие слова в тексте.

Пример:

Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- "<фрагмент текста>". Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

Пример:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-интервал**

Если флажок установлен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

По умолчанию флажок снят.

Теги

На закладке **Теги** можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

- **Применять, если есть хотя бы один из выбранных тегов**

Если флажок установлен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если флажок снят, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию флажок снят.

- **Тег должен присутствовать**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска

устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Active Directory

На закладке **Active Directory** можно настроить критерии поиска устройств на основании их данных Active Directory:

- **Устройство находится в подразделении Active Directory**

Если флажок установлен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

По умолчанию флажок снят.

- **Включая дочерние подразделения**

Если флажок установлен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

По умолчанию флажок снят.

- **Устройство является членом группы Active Directory**

Если флажок установлен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

По умолчанию флажок снят.

Сетевая активность

На закладке **Сетевая активность** можно указать критерии поиска устройств на основании их сетевой активности:

- **Является агентом обновлений**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** В выборку будут включены устройства, являющиеся агентами обновлений.
- **Нет.** Устройства, являющиеся агентами обновлений, не будут включены в выборку.
- **Значение не выбрано.** Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Включен.** В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
- **Выключен.** В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
- **Значение не выбрано.** Критерий не применяется.

- **Переключение профиля подключения**

В раскрываемом списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Нет.** В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
- **Значение не выбрано.** Критерий не применяется.

- **Время последнего соединения с Сервером администрирования**

С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

Если флажок установлен, в полях ввода можно указать значения

интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

Если флажок установлен, то в выборку попадают только новые устройства, обнаруженные при опросе сети за количество дней, которое указано в поле **Период обнаружения (сут)**.

Если флажок снят, то в выборку попадают все устройства, обнаруженные при опросе сети.

По умолчанию флажок снят.

- **Устройство видимо в сети**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да.** Программа включает в выборку устройства, которые видимы в сети в настоящий момент.
- **Нет.** Программа включает в выборку устройства, которые не видимы в сети в настоящий момент.
- **Значение не выбрано.** Критерий не применяется.

Программа

На закладке **Программа** можно указать критерии поиска устройств на основании выбранной управляемой программы:

- **Название программы**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию программы "Лаборатории Касперского".

В списке представлены названия только тех программ, для которых на рабочем месте администратора установлены плагины управления.

Если программа не выбрана, то критерий не применяется.

- **Версия программы**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии программы "Лаборатории Касперского".

Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для программы наименованию или номеру пакета обновления.

Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей программы**

С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей программ, установленных на устройствах.

Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей программ, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Устройство под управлением Kaspersky Security Center 10**

В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security

Center:

- **Да.** Программа включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
- **Нет.** Программа включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
- **Значение не выбрано.** Критерий не применяется.

- **Установлена программа защиты**

В раскрываемом списке можно включить в состав выборки устройства, на которых установлена программа защиты:

- **Да.** Программа включает в выборку устройства, на которых установлена программа защиты.
- **Нет.** Программа включает в выборку устройства, на которых не установлена программа защиты.
- **Значение не выбрано.** Критерий не применяется.

Операционная система

На закладке **Операционная система** можно настроить критерии поиска устройств на основании установленной на них операционной системы:

- **Версия операционной системы**

Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Архитектура операционной системы**

В раскрываемом списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Неизвестно, x86, AMD64, IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы (X.Y.)**

В поле можно указать версию пакета установленной операционной системы (в формате X.Y), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

Статус устройства

На закладке **Статус устройства** можно указать критерии поиска устройств по статусу устройства от управляемой программы:

- **Статус устройства**

Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК*, *Критический*, *Предупреждение*.

- **Описание статуса устройства**

В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *ОК*, *Критический*, *Предупреждение*.

- **Статус постоянной защиты**

Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

Компоненты защиты

На закладке **Компоненты защиты** можно настроить параметры поиска клиентских устройств по состоянию защиты:

- **Дата выпуска баз**

Если флажок установлен, поиск клиентских устройств выполняется по дате выпуска баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

По умолчанию флажок снят.

- **Количество записей в базах**

Если флажок установлен, поиск клиентских устройств выполняется по количеству записей в базах. В полях ввода можно задать нижнее и верхнее значения количества записей.

По умолчанию флажок снят.

- **Время последнего поиска вирусов**

Если флажок установлен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого поиск вирусов выполнялся в последний раз.

По умолчанию флажок снят.

- **Количество найденных вирусов**

Если флажок установлен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию флажок снят.

Реестр программ

На закладке **Реестр программ** можно настроить параметры поиска устройств в зависимости от того, какие программы на них установлены:

- **Название программы**

Раскрывающийся список, в котором можно выбрать программу. Устройства, на которых установлена указанная программа, будут включены в выборку.

- **Версия программы**

Поле ввода, в котором указывается версия выбранной программы.

- **Производитель**

Раскрывающийся список, в котором можно выбрать производителя

установленной на устройстве программы.

- **Искать по обновлению**

Если флажок установлен, поиск будет выполняться по данным об обновлении программ, установленных на искомым устройствах. После установки флажка названия полей ввода **Название программы** и **Версия программы** меняются на **Имя обновления** и **Версия обновления**.

По умолчанию флажок снят.

- **Название несовместимой программы безопасности**

Раскрывающийся список, в котором можно выбрать программы защиты сторонних производителей. Во время поиска устройства, на которых установлена выбранная программа, будут включены в выборку.

Иерархия Серверов администрирования

На закладке **Иерархия Серверов администрирования** можно включить или отключить учет информации, хранящейся на подчиненных Серверах администрирования, во время поиска устройств:

- **Включая данные с подчиненных Серверов до уровня**

Если флажок установлен, при поиске устройств будет учитываться информация с подчиненных Серверов администрирования.

В поле ввода указывается уровень вложенности подчиненных Серверов администрирования, информация с которых будет учитываться при поиске устройств.

По умолчанию флажок снят.

Виртуальные машины

На закладке Виртуальные машины можно настроить параметры поиска устройств в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

В раскрываемом списке можно выбрать следующие элементы:

- **Да.** Искомые устройства должны являться виртуальными машинами.
- **Нет.** Искомые устройства не должны являться виртуальными машинами.

- **Тип виртуальной машины**

В раскрываемом списке можно выбрать производителя виртуальной машины.

Раскрываемый список доступен, если в раскрываемом списке **Является виртуальной машиной** указано значение **Да**.

- **Часть Virtual Desktop Infrastructure**

В раскрываемом списке можно выбрать следующие элементы:

- **Да.** Искомые устройства должны являться частью Virtual Desktop Infrastructure.
- **Нет.** Искомые устройства не должны являться частью Virtual Desktop Infrastructure.

Оборудование

На закладке **Оборудование** можно настроить поиск клиентских устройств по установленному на них оборудованию:

- **Устройство**

В раскрываемом списке можно выбрать тип оборудования, которое должно быть установлено на клиентском устройстве, чтобы оно отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Производитель**

В раскрываемом списке можно выбрать производителя

оборудования, которое должно быть установлено на устройстве, чтобы устройство отображалось в результатах поиска.

В поле поддерживается полнотекстовый поиск.

- **Инвентарный номер**

Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Описание**

Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Частота процессора (МГц)**

Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

Уязвимости и обновления

На закладке **Уязвимости и обновления** можно настроить параметры поиска устройств по источнику обновлений Windows Update:

- **WUA переключен на Сервер администрирования**

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да.** Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Windows Update с Сервера администрирования.
- **Нет.** Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Windows Update из другого источника.

Пользователи

На закладке **Пользователи** можно настроить параметры поиска устройств по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

Если флажок установлен, при нажатии на кнопку **Выбрать** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Описания статусов от управляемой программы

На закладке **Описания статусов от управляемой программы** можно настроить поиск по описаниям статусов устройств от управляемой

программы:

- **Описание статуса устройства**

Вы можете установить флажки для описаний статусов от управляемой программы, при получении которых устройства будут включаться в выборку.

Статусы компонентов управляемых программ

На закладке **Статусы компонентов управляемых программ** можно настроить поиск по статусам компонентов управляемых программ:

- **Статус защиты данных от утечек**

Поиск устройств по статусу компонента защиты от утечки данных (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу компонента защиты для серверов совместной работы (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу компонента антивирусной защиты почтовых серверов (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Выполняется, Запускается, Остановлен, Приостановлен, Сбой, Неизвестно*).

См. также

Использование регулярных выражений в строке поиска.....	532
Поиск устройств.....	515

Использование масок в строковых переменных

Для строковых переменных допустимо использование масок. Для создания масок вы можете использовать следующие регулярные выражения:

- * – любая строка длиной 0 или более символов;
- ? – один любой символ;
- [<интервал>] – один символ из заданного диапазона или множества.

Например: [0–9] – любая цифра; [abcdef] – один из символов a, b, c, d, e, f.

Использование регулярных выражений в строке поиска

Для поиска отдельных слов и символов вы можете использовать в строке поиска следующие регулярные выражения:

- *. Заменяет последовательность любого количества символов. Например, для поиска слов "Сервер", "Серверный" или "Серверная" в строке поиска нужно ввести выражение `Сервер*`.
- ?. Заменяет любой один символ. Например, для поиска слов "Окно" или "Окна" в строке поиска нужно ввести выражение `Окн?`.

Текст в строке поиска не может начинаться с ?.

- [<интервал>]. Заменяет один символ из заданного диапазона или множества. Например, для поиска любой цифры в строке поиска нужно ввести выражение `[0–9]`. Для поиска одного из символов a, b, c, d, e, f в строке поиска нужно ввести выражение `[abcdef]`.

Для полнотекстового поиска вы можете использовать в строке поиска следующие регулярные выражения:

- Пробел. Обозначает наличие в тексте хотя бы одного из слов, разделенных пробелами. Например, для поиска фразы, содержащей слово "Подчиненный" или "Виртуальный" (или оба этих слова), в строке поиска нужно ввести выражение Подчиненный Виртуальный.
- Знак "плюс" (+), AND или &&. При написании перед словом обозначает обязательное наличие слова в тексте. Например, для поиска фразы, содержащей и слово "Подчиненный", и слово "Виртуальный", в строке поиска можно ввести выражения: +Подчиненный+Виртуальный, Подчиненный AND Виртуальный, Подчиненный && Виртуальный.
- OR или ||. При написании между словами обозначает наличие одного или другого слова в тексте. Например, для поиска фразы, содержащей или слово "Подчиненный", или слово "Виртуальный", в строке поиска можно ввести выражения: Подчиненный OR Виртуальный, Подчиненный || Виртуальный.
- Знак "минус" (-). При написании перед словом обозначает обязательное отсутствие слова в тексте. Например, для поиска фразы, в которой должно присутствовать слово "Подчиненный", и должно отсутствовать слово "Виртуальный", нужно ввести в строке поиска выражение +Подчиненный-Виртуальный.
- "<фрагмент текста>". Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте. Например, для поиска фразы, содержащей словосочетание "Подчиненный Сервер", нужно ввести в строке поиска выражение "Подчиненный Сервер".

Полнотекстовый поиск доступен в следующих блоках фильтрации:

- в блоке фильтрации списка событий по графам **Событие** и **Описание**;
- в блоке фильтрации учетных записей пользователей по графе **Имя**;
- в блоке фильтрации реестра программ по графе **Название**, если в блоке **Показывать в списке** выбран критерий фильтрации **без группировки**.

Экспорт списков из диалоговых окон

В диалоговых окнах программы вы можете экспортировать в текстовые файлы списки объектов.

Экспорт списка объектов возможен для тех разделов диалогового окна, которые содержат кнопку **Экспортировать в файл**.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением 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:

- позвонить в Службу технической поддержки по телефону (<https://support.kaspersky.ru/b2c>);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<https://support.kaspersky.ru/b2c>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих программы "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).

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского": <https://www.kaspersky.ru>

Вирусная энциклопедия: <https://securelist.ru/>

Вирусная лаборатория: <https://virusdesk.kaspersky.ru/> (для проверки подозрительных файлов и сайтов)

Веб-форум "Лаборатории Касперского": <https://forum.kaspersky.com>

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft, MultiPoint, MS-DOS, PowerShell, PowerPoint, SQL Server, OneNote, Outlook, Tahoma, Win32, Windows, Windows PowerShell, Windows Server, Windows Phone, Windows Vista, Windows Azure – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Adobe – товарный знак или зарегистрированный в Соединенных Штатах Америки и/или в других странах товарный знак Adobe Systems Incorporated.

AirPlay, AirDrop, AirPrint, App Store, Apple, AppleScript, FaceTime, FileVault, iBook, iBooks, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, Touch ID – товарные знаки Apple Inc., зарегистрированные в США и других странах.

AMD, AMD64 – товарные знаки Advanced Micro Devices, Inc.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Cisco, Cisco Systems, IOS – зарегистрированные в Соединенных Штатах Америки и в других странах товарные знаки Cisco Systems, Inc. и / или ее аффилированных компаний.

Citrix, XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Android, Chrome, Dalvik, Google, Google Play, Google Карты, Google Analytics, Hangouts, YouTube – товарные знаки Google, Inc.

Firefox – товарный знак Mozilla Foundation.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

JavaScript, Python, TouchDown, Oracle и Java – зарегистрированные товарные знаки Oracle Corporation и / или ее аффилированных компаний.

QRadar, IBM – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Intel, Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Novell – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Parallels Desktop является зарегистрированным товарным знаком Parallels International GmbH в США и / или других странах.

SPL, Splunk – товарные знаки и зарегистрированные в США и других странах товарные знаки Splunk, Inc.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

VMware, VMware vSphere – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 15. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
виртуальная инфраструктура VMware	среда функционирования
файл виртуальной машины	объект воздействия
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь