



# Kaspersky Security Center 10

*Руководство администратора*

*Версия программы: 10 Service Pack 2, Maintenance Release 1*

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.

Дата редакции документа: 13.12.2016

© АО «Лаборатория Касперского», 2017.

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

# Содержание

Об этом документе.....	15
В этом документе .....	15
Условные обозначения .....	19
Источники информации о программе .....	21
Источники для самостоятельного поиска информации .....	21
Обсуждение программ «Лаборатории Касперского» на форуме.....	23
Kaspersky Security Center .....	24
Что нового .....	25
Комплект поставки .....	29
Аппаратные и программные требования .....	30
Интерфейс программы .....	46
Главное окно программы .....	47
Дерево консоли .....	48
Рабочая область .....	53
Элементы рабочей области .....	55
Набор информационных блоков.....	57
Блок фильтрации данных .....	57
Контекстное меню .....	59
Настройка интерфейса.....	59
Лицензирование программы .....	62
О Лицензионном соглашении .....	62
О лицензии.....	63
О лицензионном сертификате.....	64
О ключе .....	64
Варианты лицензирования Kaspersky Security Center .....	65
Об ограничениях базовой функциональности .....	68
О коде активации .....	69
О файле ключа .....	70
О подписке .....	70

Мастер первоначальной настройки Сервера администрирования .....	72
Основные понятия.....	74
Сервер администрирования .....	74
Иерархия Серверов администрирования .....	75
Виртуальный Сервер администрирования .....	77
Сервер мобильных устройств .....	78
Веб-сервер .....	79
Агент администрирования. Группа администрирования .....	80
Рабочее место администратора .....	81
Плагин управления программой .....	82
Политики, параметры программы и задачи .....	82
Взаимосвязь политики и локальных параметров программы .....	85
Агент обновлений .....	87
Управление Серверами администрирования .....	91
Подключение к Серверу администрирования и переключение между Серверами администрирования .....	91
Права доступа к Серверу администрирования и его объектам .....	94
Условия подключения к Серверу администрирования через интернет .....	96
Защищенное подключение к Серверу администрирования .....	97
Аутентификация Сервера при подключении устройства .....	97
Аутентификация Сервера при подключении Консоли администрирования ...	98
Сертификат Сервера администрирования .....	98
Отключение от Сервера администрирования .....	99
Добавление Сервера администрирования в дерево консоли .....	99
Удаление Сервера администрирования из дерева консоли .....	99
Смена учетной записи службы Сервера администрирования. Утилита klsrvswch.....	100
Просмотр и изменение параметров Сервера администрирования .....	101
Настройка общих параметров Сервера администрирования.....	102
Обработка и хранение событий на Сервере администрирования.....	103
Контроль возникновения вирусных эпидемий .....	103
Ограничение трафика .....	104
Настройка параметров Веб-сервера.....	104
Работа с внутренними пользователями .....	105

Управление группами администрирования .....	106
Создание групп администрирования .....	107
Перемещение групп администрирования .....	109
Удаление групп администрирования .....	110
Автоматическое создание структуры групп администрирования .....	111
Автоматическая установка программ на устройства группы администрирования .....	113
Удаленное управление программами .....	114
Управление политиками .....	114
Создание политики .....	116
Отображение унаследованной политики во вложенной группе .....	117
Активация политики .....	118
Автоматическая активация политики по событию «Вирусная атака» .....	119
Применение политики для автономных пользователей .....	119
Изменение политики. Откат изменений .....	119
Удаление политики .....	120
Копирование политики .....	121
Экспорт политики .....	121
Импорт политики .....	122
Конвертация политик .....	122
Управление профилями политик .....	123
О профиле политики .....	123
Создание профиля политики .....	126
Изменение профиля политики .....	127
Удаление профиля политики .....	128
Управление задачами .....	129
Создание групповой задачи .....	130
Создание задачи Сервера администрирования .....	131
Создание задачи для набора устройств .....	132
Создание локальной задачи .....	133
Отображение унаследованной групповой задачи в рабочей области вложенной группы .....	134
Автоматическое включение устройств перед запуском задачи .....	135
Автоматическое выключение устройства после выполнения задачи .....	135
Ограничение времени выполнения задачи .....	136

Экспорт задачи .....	136
Импорт задачи .....	137
Конвертация задач .....	137
Запуск и остановка задачи вручную .....	138
Приостановка и возобновление задачи вручную .....	139
Наблюдение за ходом выполнения задачи.....	139
Просмотр результатов выполнения задачи, хранящихся на Сервере администрирования .....	140
Настройка фильтра информации о результатах выполнения задачи.....	140
Изменение задачи. Откат изменений .....	141
Просмотр и изменение локальных параметров программы .....	141
Управление клиентскими устройствами.....	143
Подключение клиентских устройств к Серверу администрирования.....	144
Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover .....	145
Туннелирование соединения клиентского устройства с Сервером администрирования .....	147
Удаленное подключение к рабочему столу клиентского устройства .....	148
Настройка перезагрузки клиентского устройства .....	150
Аудит действий на удаленном клиентском устройстве .....	151
Проверка соединения клиентского устройства с Сервером администрирования .....	152
Автоматическая проверка соединения клиентского устройства с Сервером администрирования .....	153
Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk .....	153
Идентификация клиентских устройств на Сервере администрирования .....	155
Добавление устройств в состав группы администрирования .....	155
Смена Сервера администрирования для клиентских устройств .....	156
Удаленное включение, выключение и перезагрузка клиентских устройств.....	158
Отправка сообщения пользователям устройств.....	159
Контроль изменения состояния виртуальных машин .....	159
Автоматическое назначение тегов устройствам.....	160
Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center .....	162
Подключение утилиты удаленной диагностики к клиентскому устройству...	163

Включение и выключение трассировки, загрузка файла трассировки .....	166
Загрузка параметров программ .....	166
Загрузка журналов событий .....	167
Запуск диагностики и загрузка ее результатов.....	167
Запуск, остановка и перезапуск программ .....	168
Управление учетными записями пользователей .....	169
Работа с учетными записями пользователей .....	170
Добавление учетной записи пользователя .....	171
Настройка проверки уникальности имени внутреннего пользователя .....	172
Добавление группы пользователей.....	173
Добавление пользователя в группу.....	174
Настройка прав. Роли пользователей.....	175
Добавление роли пользователя .....	176
Назначение роли пользователю или группе пользователей .....	177
Назначение пользователя владельцем устройства.....	178
Рассылка сообщений пользователям .....	179
Просмотр списка мобильных устройств пользователя.....	180
Установка сертификата пользователю .....	180
Просмотр списка сертификатов, выписанных пользователю .....	181
Работа с отчетами, статистикой и уведомлениями .....	182
Работа с отчетами .....	182
Создание шаблона отчета .....	183
Создание и просмотр отчета.....	184
Сохранение отчета.....	184
Создание задачи рассылки отчета.....	185
Работа со статистической информацией.....	186
Настройка параметров уведомлений о событиях.....	187
Создание сертификата для SMTP-сервера.....	188
Выборки событий .....	189
Просмотр выборки событий .....	190
Настройка параметров выборки событий .....	191
Создание выборки событий .....	191
Экспорт выборки событий в текстовый файл .....	192
Удаление событий из выборки .....	192

Экспорт событий в SIEM-систему .....	193
Выборки устройств.....	194
Просмотр выборки устройств.....	195
Настройка параметров выборки устройств.....	195
Создание выборки устройств.....	196
Экспорт параметров выборки устройств в файл.....	196
Создание выборки устройств по импортированным параметрам.....	197
Удаление устройств из групп администрирования в выборке.....	197
Политики .....	198
Задачи .....	198
Нераспределенные устройства.....	199
Опрос сети .....	199
Просмотр и изменение параметров опроса сети Windows .....	201
Просмотр и изменение параметров опроса групп Active Directory.....	201
Просмотр и изменение параметров опроса IP-диапазонов.....	202
Работа с доменами Windows. Просмотр и изменение параметров домена .....	202
Работа с IP-диапазонами .....	203
Создание IP-диапазона.....	203
Просмотр и изменение параметров IP-диапазона .....	203
Работа с группами Active Directory. Просмотр и изменение параметров группы .....	204
Создание правил автоматического перемещения устройств в группы администрирования .....	204
Использование динамического режима VDI на клиентских устройствах .....	205
Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования .....	206
Поиск устройств, являющихся частью VDI.....	206
Перемещение в группу администрирования устройств, являющихся частью VDI .....	207
Управление программами на клиентских устройствах.....	208
Группы программ .....	208
Создание категорий программ.....	211
Настройка управления запуском программ на клиентских устройствах .....	212
Просмотр результатов статического анализа правил запуска исполняемых файлов.....	213



Просмотр реестра программ .....	214
Создание групп лицензионных программ .....	216
Управление ключами для групп лицензионных программ .....	216
Инвентаризация программного обеспечения Kaspersky Security Center .....	218
Инвентаризация исполняемых файлов .....	219
Просмотр информации об исполняемых файлах .....	220
Уязвимости в программах .....	220
Просмотр информации об уязвимостях в программах .....	221
Поиск уязвимостей в программах .....	222
Закрытие уязвимостей в программах .....	223
Обновления программного обеспечения .....	224
Просмотр информации о доступных обновлениях .....	225
Синхронизация обновлений Windows Update с Сервером администрирования .....	226
Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства .....	227
Офлайн-модель получения обновлений .....	229
Включение и выключение офлайн-модели получения обновлений .....	232
Установка обновлений на устройства вручную .....	233
Настройка обновлений Windows в политике Агента администрирования ....	236
Дистанционная установка операционных систем и программ .....	238
Создание образов операционных систем .....	241
Добавление драйверов для среды предустановки Windows (WinPE) .....	241
Добавление драйверов в инсталляционный пакет с образом операционной системы .....	242
Настройка параметров утилиты sysprep.exe .....	243
Развертывание операционных систем на новых устройствах в сети .....	244
Развертывание операционных систем на клиентских устройствах .....	245
Создание инсталляционных пакетов программ .....	246
Выписка сертификата для инсталляционных пакетов программ .....	247
Установка программ на клиентские устройства .....	248
Управление мобильными устройствами .....	249
Управление мобильными устройствами с помощью MDM-политики .....	249
Работа с командами для мобильных устройств .....	252
Команды для управления мобильным устройством .....	252

Использование Google Firebase Cloud Messaging.....	256
Отправка команд .....	257
Просмотр статусов команд в журнале команд.....	258
Работа с сертификатами.....	259
Установка сертификата .....	259
Настройка правил выдачи сертификатов .....	260
Интеграция с инфраструктурой открытых ключей .....	262
Включение поддержки Kerberos Constrained Delegation.....	263
Добавление мобильного устройства в список управляемых устройств .....	264
Управление мобильными устройствами Exchange ActiveSync .....	269
Добавление профиля управления .....	271
Удаление профиля управления.....	273
Просмотр информации о EAS-устройстве .....	274
Отключение EAS-устройства от управления .....	274
Управление iOS MDM-устройствами .....	275
Выписка сертификата iOS MDM-профиля.....	275
Добавление конфигурационного профиля .....	276
Установка конфигурационного профиля на устройство .....	278
Удаление конфигурационного профиля с устройства .....	280
Добавление provisioning-профиля .....	281
Установка provisioning-профиля на устройство .....	282
Удаление provisioning-профиля с устройства .....	283
Добавление управляемого приложения .....	285
Установка приложения на мобильное устройство .....	286
Удаление приложения с устройства .....	287
Установка приложения Kaspersky Safe Browser на мобильное устройство .....	289
Просмотр информации о iOS MDM-устройстве.....	290
Отключение iOS MDM-устройства от управления .....	290
Управление KES-устройствами .....	291
Создание пакета мобильных приложений для KES-устройств .....	292
Включение двухфакторной аутентификации KES-устройств .....	293
Просмотр информации о KES-устройстве .....	294
Отключение KES-устройства от управления .....	294

Self Service Portal.....	296
О Self Service Portal .....	296
Добавление устройства .....	299
Подключение пользователя к Self Service Portal .....	300
Шифрование и защита данных.....	303
Просмотр списка зашифрованных устройств.....	304
Просмотр списка событий шифрования .....	305
Экспорт списка событий шифрования в текстовый файл .....	306
Формирование и просмотр отчетов о шифровании .....	307
Инвентаризация оборудования, обнаруженного в сети .....	310
Добавление информации о новых устройствах.....	311
Настройка критериев определения корпоративных устройств.....	312
Обновление баз и программных модулей .....	313
Создание задачи загрузки обновлений в хранилище .....	314
Создание задачи загрузки обновлений в хранилища агентов обновлений .....	316
Настройка параметров задачи загрузки обновлений в хранилище .....	317
Проверка полученных обновлений .....	317
Настройка проверочных политик и вспомогательных задач.....	319
Просмотр полученных обновлений .....	321
Автоматическое распространение обновлений .....	321
Автоматическое распространение обновлений на клиентские устройства..	322
Автоматическое распространение обновлений на подчиненные Серверы администрирования .....	323
Автоматическая установка обновлений программных модулей Агентов администрирования .....	324
Назначение устройств агентами обновлений.....	325
Удаление устройства из списка агентов обновлений .....	327
Получение обновлений агентами обновлений .....	327
Отмена установленных обновлений .....	328
Работа с ключами программ .....	329
Просмотр информации об используемых ключах .....	329
Добавление ключа в хранилище Сервера администрирования .....	330
Удаление ключа Сервера администрирования .....	331
Распространение ключа на клиентские устройства .....	331

Автоматическое распространение ключа .....	332
Создание и просмотр отчета об использовании ключей .....	333
Хранилища данных .....	334
Экспорт списка объектов, находящихся в хранилище, в текстовый файл .....	335
Инсталляционные пакеты .....	335
Карантин и резервное хранилище .....	336
Включение удаленного управления файлами в хранилищах .....	337
Просмотр свойств файла, помещенного в хранилище .....	337
Удаление файлов из хранилища .....	338
Восстановление файлов из хранилища .....	338
Сохранение файла из хранилища на диск .....	339
Проверка файлов на карантине .....	339
Файлы с отложенной обработкой .....	340
Лечение файла с отложенной обработкой .....	340
Сохранение файла с отложенной обработкой на диск .....	341
Удаление файлов из папки «Файлы с отложенной обработкой» .....	342
Kaspersky Security Network (KSN) .....	343
О KSN .....	343
О предоставлении данных .....	344
Настройка доступа к KSN .....	345
Включение и отключение KSN .....	347
Просмотр статистики прокси-сервера KSN .....	348
Обращение в Службу технической поддержки .....	350
Способы получения технической поддержки .....	350
Техническая поддержка по телефону .....	351
Техническая поддержка через Kaspersky CompanyAccount .....	351
Приложения .....	353
Дополнительные возможности .....	353
Автоматизация работы Kaspersky Security Center. Утилита klakaut .....	354
Автономные пользователи .....	354
Создание профиля подключения к Серверу администрирования для автономных пользователей .....	356
Создание правила переключения Агента администрирования .....	357
События в работе программ .....	358

Определение уровня важности события о превышении лицензионного ограничения .....	359
Уведомление о событиях с помощью исполняемого файла .....	360
Работа с программой Kaspersky Security для виртуальных сред.....	361
Отслеживание состояния антивирусной защиты с помощью информации в системном реестре.....	361
Кластеры и массивы серверов .....	363
Алгоритм установки патча для программы «Лаборатории Касперского» в кластерной модели.....	363
Поиск устройств .....	364
Подключение к устройствам с помощью Windows Desktop Sharing.....	366
Об используемых учетных записях.....	367
Работа с внешними инструментами.....	367
Экспорт списков из диалоговых окон .....	368
Режим клонирования диска Агента администрирования .....	368
Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования .....	370
Резервное копирование и восстановление данных Сервера администрирования .....	372
Создание задачи резервного копирования данных.....	373
Утилита резервного копирования и восстановления данных (klbackup) ..	374
Резервное копирование и восстановление данных в интерактивном режиме.....	375
Резервное копирование и восстановление данных в неинтерактивном режиме.....	376
Перенос Сервера администрирования на другое устройство .....	378
Резервное копирование и восстановление данных в интерактивном режиме .....	380
Установка программы с помощью групповых политик Active Directory .....	381
Особенности работы с интерфейсом управления.....	383
Как вернуть исчезнувшее окно свойств .....	383
Как перемещаться по дереву консоли .....	384
Как открыть окно свойств объекта в рабочей области .....	384
Как выбрать группу объектов в рабочей области .....	384
Как изменить набор граф в рабочей области .....	385
Справочная информация.....	385
Использование агента обновлений в качестве шлюза.....	386

Использование масок в строковых переменных .....	387
Команды контекстного меню .....	387
О менеджере соединений .....	392
Права пользователя для управления мобильными устройствами Exchange ActiveSync.....	392
Об администраторе виртуального Сервера.....	394
Список управляемых устройств. Значение граф.....	395
Статусы устройств, задач и политик .....	399
Значки статусов файлов в Консоли администрирования.....	401
Использование регулярных выражений в строке поиска .....	403
Глоссарий .....	405
АО «Лаборатория Касперского» .....	417
Информация о стороннем коде .....	419
Дополнительная защита с использованием Kaspersky Security Network.....	420
Уведомления о товарных знаках.....	421
Предметный указатель .....	423

---

# Об этом документе

Руководство администратора Kaspersky Security Center 10 (далее «Kaspersky Security Center») адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security Center, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security Center.

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

Также из этого руководства вы можете узнать об источниках информации о программе и способах получения технической поддержки.

## В этом разделе

В этом документе .....	<a href="#">15</a>
Условные обозначения .....	<a href="#">19</a>

## В этом документе

Руководство администратора Kaspersky Security Center содержит введение, разделы с описанием интерфейса программы, ее настройки и обслуживания, разделы с описанием решения основных задач, а также глоссарий.

### Источники информации о программе (см. стр. [21](#))

Этот раздел содержит описание источников информации о программе.

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

### Kaspersky Security Center (см. стр. [24](#))

В этом разделе представлена информация о назначении, ключевых возможностях и составе программы Kaspersky Security Center.

## **Интерфейс программы (см. стр. [46](#))**

В этом разделе описаны основные элементы интерфейса Kaspersky Security Center, а также настройка интерфейса.

## **Лицензирование программы (см. стр. [62](#))**

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

## **Мастер первоначальной настройки (см. стр. [72](#))**

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

## **Основные понятия (см. стр. [74](#))**

Этот раздел содержит развернутые определения основных понятий, относящихся к программе Kaspersky Security Center.

## **Управление Серверами администрирования (см. стр. [91](#))**

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

## **Управление группами администрирования (см. стр. [106](#))**

Этот раздел содержит информацию о работе с группами администрирования.

## **Удаленное управление программами (см. стр. [114](#))**

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.

## **Управление клиентскими устройствами (см. стр. [143](#))**

Этот раздел содержит информацию о работе с клиентскими устройствами.



## **Работа с отчетами, статистикой и уведомлениями (см. стр. [182](#))**

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.

## **Нераспределенные устройства (см. стр. [199](#))**

В этом разделе представлена информация о работе с устройствами сети организации, не входящими в группы администрирования.

## **Управление программами на клиентских компьютерах (см. стр. [208](#))**

В этом разделе описана работа с группами программ, а также процесс обновления программного обеспечения и закрытия уязвимостей, которые Kaspersky Security Center обнаруживает на клиентских устройствах.

## **Удаленная установка операционных систем и программ (см. стр. [238](#))**

Этот раздел содержит информацию о создании образов операционных систем и разворачивании их на клиентских компьютерах по сети, а также об удаленной установке программ «Лаборатории Касперского» и других производителей программного обеспечения.

## **Управление мобильными устройствами (см. стр. [249](#))**

В этом разделе описано управление мобильными устройствами, подключенными к Серверу администрирования.

## **Self Service Portal (см. стр. [296](#))**

Этот раздел содержит информацию о Self Service Portal. В разделе приведены инструкции по авторизации пользователей на Self Service Portal, созданию учетных записей Self Service Portal, а также по добавлению мобильных устройств на Self Service Portal.

## **Шифрование и защита данных (см. стр. [303](#))**

В этом разделе представлена информация об управлении шифрованием данных, хранящихся на жестких дисках устройств и съемных дисках.

## **Инвентаризация оборудования, обнаруженного в сети (см. стр. [310](#))**

В этом разделе представлена информация об инвентаризации оборудования, подключенного к сети организации.

## **Обновление баз и программных модулей (см. стр. [313](#))**

В этом разделе описаны загрузка и распространение обновлений баз и программных модулей с помощью Kaspersky Security Center.

## **Работа с ключами программ (см. стр. [329](#))**

В этом разделе описаны возможности Kaspersky Security Center по работе с ключами управляемых программ «Лаборатории Касперского».

## **Хранилища данных (см. стр. [334](#))**

Этот раздел содержит информацию о данных, которые хранятся на Сервере администрирования и используются для отслеживания состояния клиентских устройств и для их обслуживания.

## **Обращение в Службу технической поддержки (см. стр. [350](#))**

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

## **Глоссарий**

В разделе перечислены термины, используемые в этом документе.

## **АО «Лаборатория Касперского» (см. стр. [417](#))**

В этом разделе приведена информация об АО «Лаборатория Касперского».

## **Информация о стороннем коде (см. стр. [419](#))**

Информация о стороннем коде содержится в файле legal\_notices.txt, расположенном в папке установки программы.

## **Уведомления о товарных знаках (см. стр. [421](#))**

В этом разделе приведены уведомления о зарегистрированных товарных знаках.

## Предметный указатель

С помощью этого раздела вы можете быстро найти необходимые сведения в документе.

# Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
<b>Пример:</b> ...	Примеры приведены в блоках на голубом фоне под заголовком «Пример».
<i>Обновление</i> – это... Возникает событие <i>Базы</i> <i>устарели</i> .	Курсивом выделены следующие элементы текста: <ul style="list-style-type: none"><li>• новые термины;</li><li>• названия статусов и событий программы.</li></ul>
Нажмите на клавишу <b>ENTER</b> . Нажмите комбинацию клавиш <b>ALT+F4</b> .	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами.  Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку <b>Включить</b> .	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.

Пример текста	Описание условного обозначения
<p>► <i>Чтобы настроить расписание задачи, выполните следующие действия:</i></p>	<p>Вводные фразы инструкций выделены курсивом и значком «стрелка».</p>
<p>В командной строке введите текст <code>help</code></p> <p>Появится следующее сообщение:</p> <p>Укажите дату в формате ДД:ММ:ГГ.</p>	<p>Специальным стилем выделены следующие типы текста:</p> <ul style="list-style-type: none"> <li>• текст командной строки;</li> <li>• текст сообщений, выводимых программой на экран;</li> <li>• данные, которые требуется ввести с клавиатуры.</li> </ul>
<p>&lt;Имя пользователя&gt;</p>	<p>Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.</p>

---

# Источники информации о программе

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 .....	<a href="#">21</a>
Обсуждение программ «Лаборатории Касперского» на форуме .....	<a href="#">23</a>

## 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» (см. раздел «Обращение в Службу технической поддержки» на стр. [350](#)).

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 (<http://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 руководств.

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

В руководстве по внедрению 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.

В руководстве «Начало работы» вы можете найти информацию для быстрого начала работы с программой (описание интерфейса и основных задач, которые можно выполнять с помощью Kaspersky Security Center).

## Обсуждение программ «Лаборатории Касперского» на форуме

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

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

---

# Kaspersky Security Center

В этом разделе представлена информация о назначении, ключевых возможностях и составе программы Kaspersky Security Center.

Программа Kaspersky Security Center предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ «Лаборатории Касперского».

Программа Kaspersky Security Center адресована администраторам сетей организаций и сотрудникам, отвечающим за защиту устройств в организациях.

При помощи Kaspersky Security Center вы можете:

- Формировать иерархию Серверов администрирования для управления сетью собственной организации, а также сетями удаленных офисов или организаций-клиентов.

Под *организациями-клиентами* здесь подразумеваются организации, антивирусную защиту которых обеспечивает сервис-провайдер.

- Формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым.
- Управлять системой антивирусной безопасности, построенной на основе программ «Лаборатории Касперского».
- Централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку программ «Лаборатории Касперского» и других производителей программного обеспечения.
- Удаленно управлять программами «Лаборатории Касперского» и других производителей, установленными на клиентских устройствах: устанавливать обновления, искать и закрывать уязвимости.



- Централизованно распространять ключи программ «Лаборатории Касперского» на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.
- Получать статистику и отчеты о работе программ и устройств.
- Получать уведомления о критических событиях в работе программ «Лаборатории Касперского».
- Управлять мобильными устройствами, поддерживающими протоколы Kaspersky Security для Android™, Exchange ActiveSync® или iOS Mobile Device Management (iOS MDM).
- Управлять шифрованием информации, хранящейся на жестких дисках устройств и съемных дисках, и доступом пользователей к зашифрованным данным.
- Проводить инвентаризацию оборудования, подключенного к сети организации.
- Централизованно работать с файлами, помещенными программами защиты на карантин или в резервное хранилище, а также с файлами, обработка которых отложена программами защиты.

## В этом разделе

Что нового .....	<a href="#">25</a>
Комплект поставки .....	<a href="#">29</a>
Аппаратные и программные требования .....	<a href="#">30</a>

## Что нового

Изменения, внесенные в программу Kaspersky Security Center по сравнению с предыдущей версией:

- Реализовано сохранение изменений параметров политик, задач и Сервера администрирования Kaspersky Security Center.

- Реализована возможность отката параметров объекта к выбранной версии объекта (см. раздел «Изменение политики. Откат изменений» на стр. [119](#)).
- Реализована возможность фильтровать историю ревизий по пользователям и времени изменений.
- Реализован регулируемый период хранения ревизии (по умолчанию 3 месяца).
- Реализован механизм сравнения ревизий политики и задач.
- Реализован экспорт ревизий политик и задач в текстовый файл.
- Улучшенная диагностика процесса автоматической установки патча. Добавлены дополнительные предупреждения при создании резервной копии данных Сервера администрирования в мастере установки Kaspersky Security Center:
  - Подчеркнута важность наличия новой резервной копии файлов и дистрибутивов предыдущей версии Kaspersky Security Center и всех установленных патчей.
  - Объяснено, как действовать в случае сбоя обновления.
  - Реализовано дополнительное подтверждение пользователя, в случае если пользователь не создает резервную копию данных.
- Реализована поддержка Агента администрирования Kaspersky Security Center (Windows 8 / 8.1, MS Surface) планшетами, работающими на основе операционной системы Windows.
- Оптимизирован Агент администрирования для уменьшения времени загрузки Windows для устройств с установленным Kaspersky Endpoint Security для Windows и Агентом администрирования.
- Оптимизирована работа Агента администрирования во время состояния ожидания (спящий режим, режим гибернации) системы Windows.
- В мастер установки Kaspersky Security Center добавлена возможность проверки последних версий плагинов и инсталляционных пакетов «Лаборатории Касперского», а также возможность применения доступных обновлений. В главном окне программы Kaspersky Security Center также отображается наличие обновлений для плагинов/программ и приложений/компонентов Kaspersky Security Center.

- Терминология программы Kaspersky Security Center приведена к более общему и независимому от других программ виду. Например, термин «компьютер» был заменен на термин «устройство».
- Реализован новый мастер установки обновлений программного обеспечения (см. раздел «Установка обновлений на устройства вручную» на стр. [233](#)).
- Добавлена информация о ходе выполнения задачи. В список граф окна **Результаты выполнения задачи** были добавлены графы:
  - Счетчики для устройств, на которых задача запущена, завершена или завершена с ошибкой.
  - Состояние (с описанием состояния задачи).
- Добавлена возможность вручную присвоить имя для инсталляционного пакета.
- Реализован запрос подтверждения у пользователя, в случае если пользователь создает политику для программ «Лаборатории Касперского» в группе администрирования, в которой политика для данной программы уже существует.
- В рабочую область папки **Нераспределенные устройства** добавлена кнопка **Настроить правила** для автоматического перемещения нераспределенных устройств (см. раздел «Создание правил автоматического перемещения устройств в группы администрирования» на стр. [204](#)).
- Добавлен флажок **Запустить мастер развертывания защиты на рабочих станциях** в мастер первоначальной настройки.
- Страницы рабочей области на закладке **Статистика** узла Сервера администрирования визуально разделены.
- Улучшена навигация при использовании правил автоматического назначения тегов.
- Доработано управление доступом на основе ролей в свойствах Сервера администрирования.
- Добавлен фильтр для текстового описания поля **События**.
- Добавлена возможность создавать теги в правилах активации профиля политики.

- Реализован быстрый переход к профилям политик из рабочей области папки **Политики** и с закладки **Политики** в узле Сервера администрирования.
- Добавлена возможность выбора положения столбцов в списках.
- Добавлен индикатор процесса обновления инсталляционных пакетов.
- Изменен значок установки Сервера администрирования в главном окне установки программы Kaspersky Security Center.
- Доработаны формулировки в мастере конвертации политик и задач.
- Добавлено описание ключа Server flags LP\_ConsoleMustUsePort13291 и LP\_InterUserUniqVsScope.
- Упрощена установка Сервера iOS MDM. Реализован мастер установки Сервера iOS MDM.
- Упрощена установка Self Service Portal.
- Доработан мастер подключения нового мобильного устройства.
- Мобильное устройство не блокируется в результате успешного выполнения команд **Определить местоположение** и **Воспроизвести звуковой сигнал** (см. раздел «Команды для управления мобильным устройством» на стр. [252](#)).
- Реализована возможность установки статуса Android-устройства **Критический** или **Предупреждение** вручную администратором, если на таких устройствах для приложения Kaspersky Endpoint Security для Android не включен доступ к службам специальных возможностей, так как в этом случае не работает Веб-Фильтр.
- Упрощена настройка Google Firebase Cloud Messaging. Добавлены подсказки и объяснения в интерфейс программы.
- Реализована утилита резервного копирования файлов из командной строки для Сервера iOS MDM.
- Реализована возможность для администратора Kaspersky Security Center вручную указать даты истечения срока действия сертификата Kaspersky Security для мобильных устройств в процессе выдачи (или повторной выдачи) сертификата.

- Реализовано отображение номера версии Self Service Portal в интерфейсе Self Service Portal.
- Если во время установки Kaspersky Security Center был установлен флажок **Поддержка мобильных устройств**, все необходимые настройки функциональности управления мобильными устройствами и Kaspersky Security для мобильных устройств выполняются в мастере первоначальной настройки Kaspersky Security Center.
- Доработан дизайн функциональности управления патчами и обновлениями.
- Доработан компонент Управление уязвимостями и патчами.
- Расширен мониторинг и поиск уязвимостей.
- Расширен контроль выполняемых задач.
- Реализована передача событий в формате Syslog (RFC 5424) в SIEM-системы (см. раздел «Экспорт событий в SIEM-систему» на стр. [193](#)).
- Унифицированы типы оборудования в интерфейсе Kaspersky Security Center.
- Дополнена информация о результатах выполнения задач **Установка требуемых обновлений и закрытие уязвимостей** и **Поиск уязвимостей и требуемых обновлений**.
- Реализована дополнительная проверка перед запуском задачи **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. Проверка выполняется на наличие прав у учетной записи, указанной администратором, на запись в заданную папку общего доступа для временного сохранения образа.
- Реализовано автоматическое создание инцидента, в случае если на устройстве, выполняющем роль агента обновлений, заканчивается свободное пространство (см. раздел «Агент обновлений» на стр. [87](#)).

## Комплект поставки

Вы можете приобрести программу через интернет-магазины «Лаборатории Касперского» (например, <http://www.kaspersky.ru>, раздел **Интернет-магазин**) или компаний-партнеров.

Приобретая Kaspersky Security Center через интернет-магазин, вы копируете программу с сайта интернет-магазина. Информация, необходимая для активации программы, высылается вам по электронной почте после оплаты.

За подробной информацией о способах приобретения и комплекте поставки вы можете обратиться в Департамент продаж.

## Аппаратные и программные требования

### Сервер администрирования

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 4 ГБ.
- Объем свободного места на диске: 10 ГБ. При использовании функциональности Системное администрирование объем свободного места на диске должен быть не менее 100 ГБ.

Программные требования:

- Microsoft® Data Access Components (MDAC) 2.8;
- Windows DAC 6.0;
- Microsoft Windows Installer 4.5.

Операционная система:

- Microsoft Windows 10 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education 32-разрядная / 64-разрядная;

- Microsoft Windows 10 Pro RS1 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS1 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS1 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro RS2 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise RS2 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education RS2 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Professional SP1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Enterprise SP1 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Ultimate SP1 32-разрядная / 64-разрядная;
- Microsoft Small Business Server 2008 Standard 64-разрядная;
- Microsoft Small Business Server 2008 Premium 64-разрядная;
- Microsoft Small Business Server 2011 Essentials 64-разрядная;
- Microsoft Small Business Server 2011 Premium Add-on 64-разрядная;
- Microsoft Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Server® 2008 Datacenter SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная;

- Microsoft Windows Server 2008;
- Windows Server 2008 SP1;
- Microsoft Windows Server 2008 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard SP1 64-разрядная;
- Microsoft Windows Server 2012 Server Core 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 Essentials 64-разрядная;
- Microsoft Windows Server 2012 Foundation 64-разрядная;
- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная;
- Windows Storage Server 2008 R2 64-разрядная;



- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Server 2016 Datacenter Edition 64-разрядная;
- Windows Server 2016 Standard Edition 64-разрядная.

Сервер баз данных (может быть установлен на другом компьютере):

- Microsoft SQL Server® 2008 Express 32-разрядная;
- Microsoft SQL 2008 R2 Express 64-разрядная;
- Microsoft SQL 2012 Express 64-разрядная;
- Microsoft SQL 2014 Express 64-разрядная;
- Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная;
- Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
- Microsoft SQL Server 2012 (все редакции) 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft Azure SQL Database;
- MySQL 5.5 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.5 32-разрядная / 64-разрядная;
- MySQL 5.6 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.6 32-разрядная / 64-разрядная;
- MySQL 5.7 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.7 32-разрядная / 64-разрядная.

Поддерживаются следующие виртуальные платформы:

- VMware vSphere™ 5.5;
- VMware vSphere 6;
- VMware™ Workstation 9.x;
- VMware Workstation 10.x;
- Microsoft Hyper-V® Server 2008;
- Microsoft Hyper-V Server 2008 R2;
- Microsoft Hyper-V Server 2012;
- Microsoft Hyper-V Server 2012 R2;
- Microsoft Virtual PC 2007 (6.0.156.0);
- Citrix® XenServer 6.1;
- Citrix XenServer 6.2;
- Parallels Desktop 7;
- Oracle® VM VirtualBox 4.0.4-70112 (поддерживаются гостевые операционные системы Windows).

Для установки Сервера администрирования на устройства с операционной системой Microsoft Windows Server 2008 необходимо использовать пакет установки «lite». Перед установкой Сервера администрирования необходимо самостоятельно установить базу данных, например, Microsoft SQL Server 2014.

### **Kaspersky Security Center Web Console**

Аппаратные требования:

- Процессор: с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Программные требования:

- Для работы под управлением операционных систем Microsoft Windows с установленным Сервером администрирования Kaspersky Security Center версии Service Pack 2:
  - Microsoft Windows 10 Pro 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Enterprise 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Education 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Pro RS1 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Enterprise RS1 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Education RS1 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Pro RS2 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Enterprise RS2 32-разрядная / 64-разрядная;
  - Microsoft Windows 10 Education RS2 32-разрядная / 64-разрядная;
  - Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
  - Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
  - Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;
  - Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
  - Microsoft Windows 7 Professional SP1 32-разрядная / 64-разрядная;
  - Microsoft Windows 7 Enterprise SP1 32-разрядная / 64-разрядная;
  - Microsoft Windows 7 Ultimate SP1 32-разрядная / 64-разрядная;
  - Microsoft Small Business Server 2008 Standard 64-разрядная;
  - Microsoft Small Business Server 2008 Premium 64-разрядная;
  - Microsoft Small Business Server 2011 Essentials 64-разрядная;

- Microsoft Small Business Server 2011 Premium Add-on 64-разрядная;
- Microsoft Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Server® 2008 Datacenter SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная;
- Microsoft Windows Server 2008;
- Windows Server 2008 SP1;
- Microsoft Windows Server 2008 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2008 R2 Foundation SP1 64-разрядная;
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard 64-разрядная;
- Microsoft Windows Server 2008 R2 Standard SP1 64-разрядная;
- Microsoft Windows Server 2012 Server Core 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 Essentials 64-разрядная;

- Microsoft Windows Server 2012 Foundation 64-разрядная;
- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная;
- Windows Storage Server 2008 R2 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Server 2016 Datacenter Edition 64-разрядная;
- Windows Server 2016 Standard Edition 64-разрядная;
- Debian GNU/Linux® 7.x 32-разрядная;
- Debian GNU/Linux 7.x 64-разрядная;
- Ubuntu Server 14.04 LTS 32-разрядная;
- Ubuntu Server 14.04 LTS 64-разрядная;
- CentOS 6.x (до 6.6) 64-разрядная.

Kaspersky Security Center 10 Web Console не поддерживает версии операционных систем, работающих с systemd, например, Fedora® 17.

Веб-сервер:

- Apache 2.4.25 (для Windows) 32-разрядный;
- Apache 2.4.25 (для Linux) 32-разрядный / 64-разрядный.

Для работы с Kaspersky Security Center 10 Web Console можно использовать следующие браузеры:

- Microsoft Internet Explorer® 9 и выше;
- Microsoft® Edge;
- Chrome™ 53 и выше;
- Firefox™ 47 и выше;
- Safari® 8 под управлением Mac OS X 10.10 (Yosemite);
- Safari 9 под управлением Mac OS X 10.11 (El Capitan).

### **Сервер мобильных устройств iOS Mobile Device Management (iOS MDM)**

Аппаратные требования:

- Процессор: с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 2 ГБ.
- Объем свободного места на диске: 2 ГБ.

Программные требования: операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования).

### **Сервер мобильных устройств Exchange ActiveSync**

Программные и аппаратные требования для Сервера мобильных устройств Exchange ActiveSync полностью включены в требования для сервера Microsoft Exchange Server.

Поддерживается работа с Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 и Microsoft Exchange Server 2013.

## **Консоль администрирования**

### Аппаратные требования:

- Процессор: с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

### Программные требования:

- Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования);
- Microsoft Management Console 2.0;
- Microsoft Windows Installer 4.5;
- Microsoft Internet Explorer 7.0 и выше при работе с Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 или Microsoft Windows Vista®;
- Microsoft Internet Explorer 8.0 и выше при работе с Microsoft Windows 7;
- Microsoft Internet Explorer 10.0 и выше при работе с Microsoft Windows 8 и 10;
- Microsoft Edge при работе с Microsoft Windows 10.

## **Агент администрирования**

### Аппаратные требования:

- Процессор: с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Если устройство, на котором установлен Агент администрирования, будет дополнительно выполнять роль агента обновлений, это устройство должно удовлетворять следующим аппаратным требованиям:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 1 ГБ.
- Объем свободного места на диске: 4 ГБ.

Программные требования:

- Windows Embedded POSReady 7 32-разрядная / 64-разрядная;
- Windows Embedded Standard 7 SP1 32-разрядная / 64-разрядная;
- Windows Embedded 8 Standard 32-разрядная / 64-разрядная;
- Windows Embedded 8 Industry Pro 32-разрядная / 64-разрядная;
- Windows Embedded 8 Industry Enterprise 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Pro 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Enterprise 32-разрядная / 64-разрядная;
- Windows Embedded 8.1 Industry Update 32-разрядная / 64-разрядная;
- Windows 10 Home 32-разрядная / 64-разрядная;
- Windows 10 Pro 32-разрядная / 64-разрядная;
- Windows 10 Enterprise 32-разрядная / 64-разрядная;
- Windows 10 Education 32-разрядная / 64-разрядная;
- Windows 10 Home RS1 32-разрядная / 64-разрядная;
- Windows 10 Pro RS1 32-разрядная / 64-разрядная;
- Windows 10 Enterprise RS1 32-разрядная / 64-разрядная;
- Windows 10 Education RS1 32-разрядная / 64-разрядная;



- Windows 10 Home RS2 32-разрядная / 64-разрядная;
- Windows 10 Pro RS2 32-разрядная / 64-разрядная;
- Windows 10 Enterprise RS2 32-разрядная / 64-разрядная;
- Windows 10 Education RS2 32-разрядная / 64-разрядная;
- Microsoft Windows 2000 Server;
- Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
- Windows 8 Pro 32-разрядная / 64-разрядная;
- Windows 8 Enterprise 32-разрядная / 64-разрядная;
- Windows 7 Professional SP1 32-разрядная / 64-разрядная;
- Windows 7 Enterprise SP1 32-разрядная / 64-разрядная;
- Windows 7 Ultimate SP1 32-разрядная / 64-разрядная;
- Windows 7 Professional 32-разрядная / 64-разрядная;
- Windows 7 Enterprise 32-разрядная / 64-разрядная;
- Windows 7 Ultimate 32-разрядная / 64-разрядная;
- Windows 7 Home Basic 32-разрядная / 64-разрядная;
- Windows 7 Premium 32-разрядная / 64-разрядная;
- Windows Vista Business SP1 32-разрядная / 64-разрядная;
- Windows Vista Enterprise SP1 32-разрядная / 64-разрядная;
- Windows Vista Ultimate SP1 32-разрядная / 64-разрядная;
- Windows Vista Business SP2 32-разрядная / 64-разрядная;
- Windows Vista Enterprise SP2 32-разрядная / 64-разрядная;
- Windows Vista Ultimate SP2 32-разрядная / 64-разрядная;

- Windows XP Professional SP3 32-разрядная;
- Windows XP Professional SP2 32-разрядная / 64-разрядная;
- Windows XP Home SP3 32-разрядная;
- Essential Business Server 2008 64-разрядная;
- Small Business Server 2003 Standard SP1 32-разрядная;
- Small Business Server 2003 Premium SP1 32-разрядная;
- Small Business Server 2008 Standard 64-разрядная;
- Small Business Server 2008 Premium 64-разрядная;
- Small Business Server 2011 Essentials 64-разрядная;
- Small Business Server 2011 Premium Add-on 64-разрядная;
- Small Business Server 2011 Standard 64-разрядная;
- Windows Home Server 2011 64-разрядная;
- Windows MultiPoint™ Server 2011 64-разрядная;
- Windows Server 2003 Enterprise SP2 32-разрядная / 64-разрядная;
- Windows Server 2003 Standard SP2 32-разрядная / 64-разрядная;
- Windows Server 2003 R2 Enterprise SP2 32-разрядная / 64-разрядная;
- Windows Server 2003 R2 Standard SP2 32-разрядная / 64-разрядная;
- Windows Server 2008 Datacenter SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная;
- Windows Server 2008 SP1 Server Core 32-разрядная / 64-разрядная;
- Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная;
- Windows Server 2008 32-разрядная / 64-разрядная;

- Windows Server 2008 R2 Server Core 64-разрядная;
- Windows Server 2008 R2 Datacenter 64-разрядная;
- Windows Server 2008 R2 Datacenter SP1 64-разрядная;
- Windows Server 2008 R2 Enterprise 64-разрядная;
- Windows Server 2008 R2 Enterprise SP1 64-разрядная;
- Windows Server 2008 R2 Foundation 64-разрядная;
- Windows Server 2008 R2 Foundation SP1 64-разрядная;
- Windows Server 2008 R2 SP1 Core Mode 64-разрядная;
- Windows Server 2008 R2 Standard 64-разрядная;
- Windows Server 2008 R2 Standard SP1 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;
- Windows Server 2016 Datacenter Edition;
- Windows Server 2016 Standard Edition;
- Windows Nano Server 2016;

- Windows Storage Server 2008 R2 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Debian GNU / Linux 8.x 32-разрядная;
- Debian GNU / Linux 8.x 64-разрядная;
- Debian GNU / Linux 7.x (до 7.8) 32-разрядная;
- Debian GNU / Linux 7.x (до 7.8) 64-разрядная;
- Ubuntu Server 16.04 LTS x32 32-разрядная;
- Ubuntu Server 16.04 LTS x64 64-разрядная;
- Ubuntu Server 14.04 LTS x32 32-разрядная;
- Ubuntu Server 14.04 LTS x64 64-разрядная;
- Ubuntu Desktop 16.04 LTS x32 32-разрядная;
- Ubuntu Desktop 16.04 LTS x64 64-разрядная;
- Ubuntu Desktop 14.04 LTS x32 32-разрядная;
- Ubuntu Desktop 14.04 LTS x64 64-разрядная;
- CentOS 6.x (до 6.6) 64-разрядная;
- CentOS 7.0 64-разрядная;
- Red Hat Enterprise Linux Server 7.0 64-разрядная;
- SUSE Linux Enterprise Server 12 64-разрядная;
- SUSE Linux Enterprise Desktop 12 64-разрядная;
- Mac OS X® 10.4 (Tiger®);
- Mac OS X 10.5 (Leopard®);
- Mac OS X 10.6 (Snow leopard®);

- OS X 10.7 (Lion);
- OS X 10.8 (Mountain Lion);
- OS X 10.9 (Mavericks);
- OS X 10.10 (Yosemite);
- OS X 10.11 (El Capitan);
- macOS® Sierra (10.12);
- VMware vSphere™ 5.5;
- VMware vSphere 6;
- VMware Workstation 9.x;
- VMware Workstation 10.x;
- VMware Workstation 11.x;
- VMware Workstation 12.x Pro;
- Microsoft Hyper-V Server 2008;
- Microsoft Hyper-V Server 2008 R2;
- Microsoft Hyper-V Server 2008 R2 SP1;
- Microsoft Hyper-V Server 2012;
- Microsoft Hyper-V Server 2012 R2;
- Citrix XenServer 6.2;
- Citrix XenServer 6.5;
- Citrix XenServer 7.

Вы можете получить сведения о последней версии аппаратных и программных требований на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center, в разделе Системные требования (<http://support.kaspersky.ru/ksc10#requirements>).

---

# Интерфейс программы

В этом разделе описаны основные элементы интерфейса Kaspersky Security Center, а также настройка интерфейса.

Просмотр, создание, изменение и настройка групп администрирования, централизованное управление работой установленных на клиентских устройствах программ «Лаборатории Касперского» осуществляется с рабочего места администратора. Интерфейс управления обеспечивает компонент Консоль администрирования. Он представляет собой специализированную автономную оснастку, интегрированную в Microsoft Management Console (MMC), поэтому интерфейс Kaspersky Security Center является стандартным для MMC.

Консоль администрирования позволяет подключаться к удаленному Серверу администрирования через интернет.

Для локальной работы с клиентскими устройствами программа предусматривает возможность установки удаленного соединения с устройством через Консоль администрирования с помощью стандартной программы Microsoft Windows «Подключение к удаленному рабочему столу».

Чтобы использовать эту возможность, на клиентском устройстве необходимо разрешить удаленное подключение к рабочему столу.

## В этом разделе

Главное окно программы .....	<a href="#">47</a>
Дерево консоли .....	<a href="#">48</a>
Рабочая область .....	<a href="#">53</a>
Блок фильтрации данных.....	<a href="#">57</a>
Контекстное меню .....	<a href="#">59</a>
Настройка интерфейса .....	<a href="#">59</a>

# Главное окно программы

Главное окно программы (см. рис. ниже) состоит из меню, панели инструментов, дерева консоли и рабочей области. Меню обеспечивает управление окнами и предоставляет доступ к справочной системе. Пункт меню **Действие** дублирует команды контекстного меню для текущего объекта дерева консоли.

Набор кнопок в панели инструментов обеспечивает прямой доступ к некоторым пунктам меню. Набор кнопок изменяется в зависимости от текущего узла или папки дерева консоли.

Вид рабочей области главного окна зависит от того, к какому узлу (папке) дерева консоли относится рабочая область и какие функции выполняет.

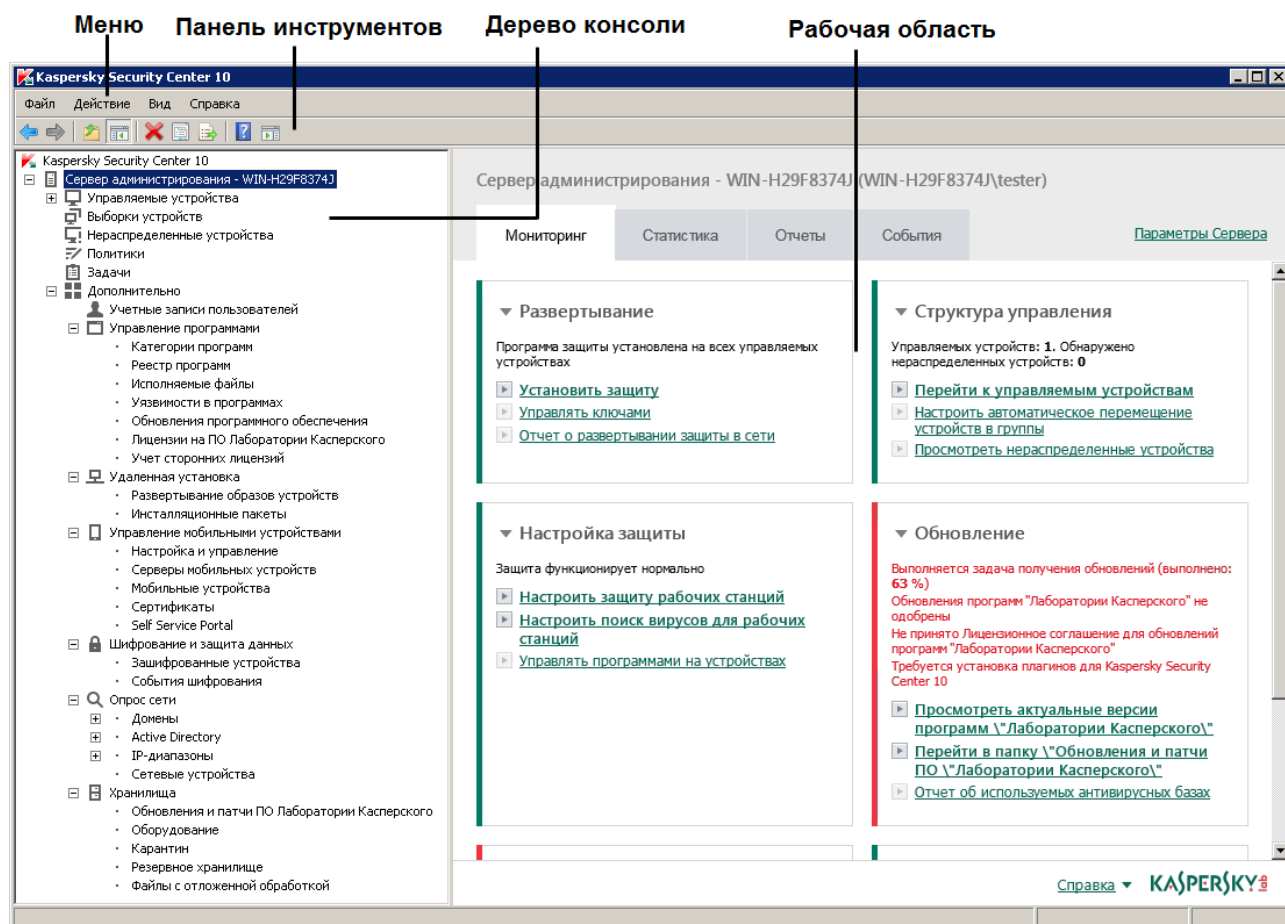


Рисунок 1. Главное окно программы Kaspersky Security Center

# Дерево консоли

Дерево консоли (см. рис. ниже) предназначено для отображения сформированной в сети иерархии Серверов администрирования, структуры их групп администрирования, а также других объектов программы (например, папок **Хранилища** и **Управление программами**). Пространство имен Kaspersky Security Center может содержать несколько узлов с именами серверов, соответствующих установленным и включенным в структуру сети Серверам администрирования.

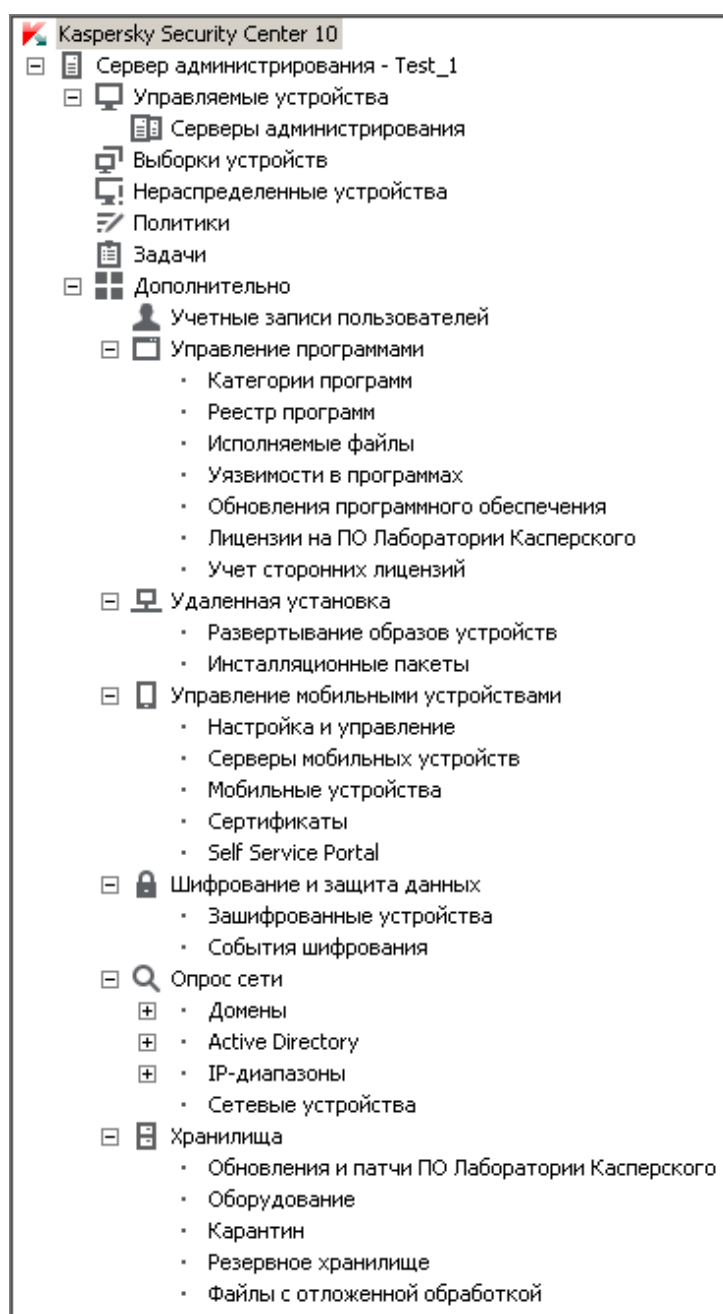


Рисунок 2. Дерево консоли



## Узел Сервер администрирования

Узел **Сервер администрирования** – **<Имя устройства>** является контейнером и отображает структурную организацию указанного Сервера администрирования.

В рабочей области узла **Сервер администрирования** содержится сводная информация о текущем состоянии программы и устройств, находящихся под управлением Сервера администрирования. Информация в рабочей области распределена по закладкам:

- **Мониторинг.** На закладке **Мониторинг** в реальном времени отображается информация о работе программы и текущем состоянии клиентских устройств. Важные сообщения для администратора (например, сообщения об уязвимостях, ошибках, обнаружении вирусов) выделяются цветом. По ссылкам на закладке **Мониторинг** можно выполнять типовые задачи администратора (например, установить и настроить программу защиты на клиентских устройствах), а также переходить к другим папкам дерева консоли.
- **Статистика.** Содержит набор диаграмм, сгруппированных по темам (состояние защиты, антивирусная статистика, обновления и прочее). В диаграммах в визуальной форме представлена текущая информация о работе программы и состоянии клиентских устройств.
- **Отчеты.** Содержит шаблоны отчетов, формируемых программой. На закладке вы можете формировать отчеты из предустановленных шаблонов, а также создавать собственные шаблоны отчетов.
- **События.** Содержит записи о событиях, зарегистрированных во время работы программы. Для удобства чтения и сортировки записи распределены по тематическим выборкам. На закладке вы можете просмотреть выборки событий, сформированные автоматически, а также создать собственные выборки.

## Папки в составе узла Сервер администрирования

В состав узла **Сервер администрирования** – **<Имя устройства>** входят следующие папки:

- **Управляемые устройства.** Папка предназначена для хранения, отображения, настройки и изменения структуры групп администрирования, групповых политик и групповых задач.
- **Выборки устройств.** Папка предназначена для быстрого выбора устройств, соответствующих определенным критериям (выборки устройств), среди всех управляемых устройств. Например, вы можете быстро выбрать устройства, на которых не установлена программа защиты, и перейти к этим устройствам (просмотреть их список). С выбранными устройствами можно выполнять действия, например, назначать для них задачи. Вы можете использовать предустановленные выборки, а также создавать собственные (пользовательские) выборки.
- **Нераспределенные устройства.** В папке содержится список устройств, не входящих в какую-либо группу администрирования. Вы можете выполнять действия с нераспределенными устройствами: перемещать их группы администрирования, устанавливать на них программы.
- **Политики.** Папка предназначена для просмотра и создания политик.
- **Задачи.** Папка предназначена для просмотра и создания задач.
- **Дополнительно.** Папка содержит набор вложенных папок, соответствующих различным группам функциональностей программы.

## Папка Дополнительно. Перемещение папок в дереве консоли

В состав папки **Дополнительно** входят следующие папки:

- **Учетные записи пользователей.** Папка содержит список учетных записей пользователей сети.
- **Управление программами.** Папка предназначена для управления программами, установленными на устройствах в сети. Папка **Управление программами** содержит следующие вложенные папки:
  - **Категории программ.** Предназначена для работы с пользовательскими категориями программ.

- **Реестр программ.** Содержит список программ на устройствах с установленным Агентом администрирования.
- **Исполняемые файлы.** Содержит список исполняемых файлов, хранящихся на клиентских устройствах с установленным Агентом администрирования.
- **Уязвимости в программах.** Содержит список уязвимостей в программах на устройствах с установленным Агентом администрирования.
- **Обновления программного обеспечения.** Содержит список обновлений программ, полученных Сервером администрирования, которые могут быть распространены на устройства.
- **Лицензии на ПО «Лаборатории Касперского».** Содержит список доступных ключей для программ «Лаборатории Касперского». В рабочей области папки вы можете добавлять новые ключи в хранилище ключей, распространять ключи на управляемые устройства, просматривать отчет об использовании ключей.
- **Учет сторонних лицензий.** Содержит список групп лицензионных программ. С помощью групп лицензионных программ можно отслеживать использование лицензий на сторонние программы (не программы «Лаборатории Касперского») и нарушение лицензионных ограничений.
- **Удаленная установка.** Папка предназначена для управления удаленной установкой операционных систем и программ. Папка **Удаленная установка** содержит следующие вложенные папки:
  - **Развертывание образов устройств.** Предназначена для развертывания образов операционных систем на устройствах.
  - **Инсталляционные пакеты.** Содержит список инсталляционных пакетов, которые могут использоваться для удаленной установки программ на устройства.
- **Управление мобильными устройствами.** Папка предназначена для управления мобильными устройствами. Папка **Управление мобильными устройствами** содержит следующие вложенные папки:
  - **Мобильные устройства.** Предназначена для управления мобильными устройствами KES, Exchange ActiveSync и iOS MDM.

- **Сертификаты.** Предназначена для управления сертификатами мобильных устройств.
- **Шифрование и защита данных.** Папка предназначена для управления процессом шифрования данных на жестких и съемных дисках.
- **Опрос сети.** Папка предназначена для отображения сети, в которой установлен Сервер администрирования. 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 сети организации. Результаты опросов отображаются в рабочих областях соответствующих папок: **Домены, IP-диапазоны и Active Directory.**
- **Хранилища.** Папка предназначена для работы с объектами, которые используются для мониторинга состояния устройств и их обслуживания. Папка **Хранилища** содержит следующие вложенные папки:
  - **Обновления и патчи ПО «Лаборатории Касперского».** Содержит список обновлений, полученных Сервером администрирования, которые могут быть распространены на устройства.
  - **Оборудование.** Содержит список оборудования, подключенного к сети организации.
  - **Карантин.** Содержит список объектов, помещенных антивирусными программами в карантинные папки на устройствах.
  - **Резервное хранилище.** Папка содержит список резервных копий файлов, удаленных или измененных в процессе лечения на устройствах.
  - **Файлы с отложенной обработкой.** Содержит список файлов, для которых антивирусные программы определили необходимость отложенного лечения.

Вы можете изменять набор папок, вложенных в папку **Дополнительно**. Вложенные папки, которые активно используются, можно перемещать из папки **Дополнительно** на уровень выше. Папки, которые используются в работе редко, можно помещать в папку **Дополнительно**.

- Чтобы вынести из папки **Дополнительно** вложенную папку, выполните следующие действия:

1. В дереве консоли выберите вложенную папку, которую вы хотите переместить из папки **Дополнительно**.
2. В контекстном меню вложенной папки выберите пункт **Вид** → **Переместить из папки Дополнительно**.

Вы также можете вынести вложенную папку из папки **Дополнительно** в рабочей области папки **Дополнительно**, по ссылке **Переместить из папки Дополнительно** в блоке с названием вложенной папки.

- Чтобы переместить папку в папку **Дополнительно**, выполните следующие действия:

3. В дереве консоли выберите папку, которую нужно переместить в папку **Дополнительно**.
4. В контекстном меню папки выберите пункт **Вид** → **Переместить в папку Дополнительно**.

## Рабочая область

Рабочая область (см. рис. ниже) содержит следующие элементы:

- списки объектов, которыми администратор управляет с помощью программы (устройства, группы администрирования, учетные записи пользователей, политики, задачи, записи о событиях, другие программы и прочее) (см. раздел «Элементы рабочей области» на стр. [55](#));
- элементы управления (кнопки, раскрывающиеся списки команд, ссылки для выполнения команд и перехода к другим папкам дерева консоли);
- информацию в текстовой и графической форме (сообщения программы, диаграммы в информационных панелях, статистическую и справочную информацию) (см. раздел «Набор информационных блоков» на стр. [57](#)).

Содержание рабочей области соответствует узлу или папке, выбранной в дереве консоли.

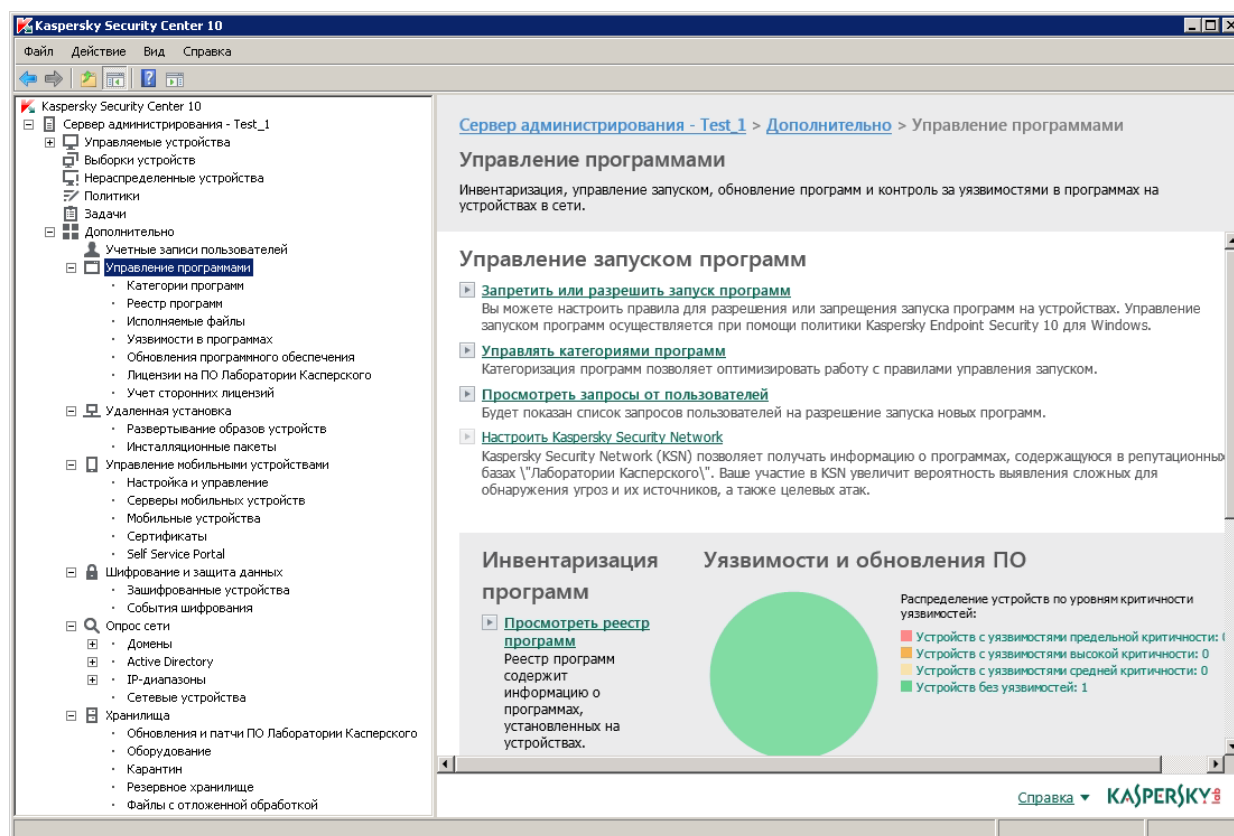


Рисунок 3. Рабочая область

Рабочая область узла или папки может содержать несколько закладок (см. рис. ниже). Каждая закладка соответствует определенной группе (типу) объектов или функций программы.

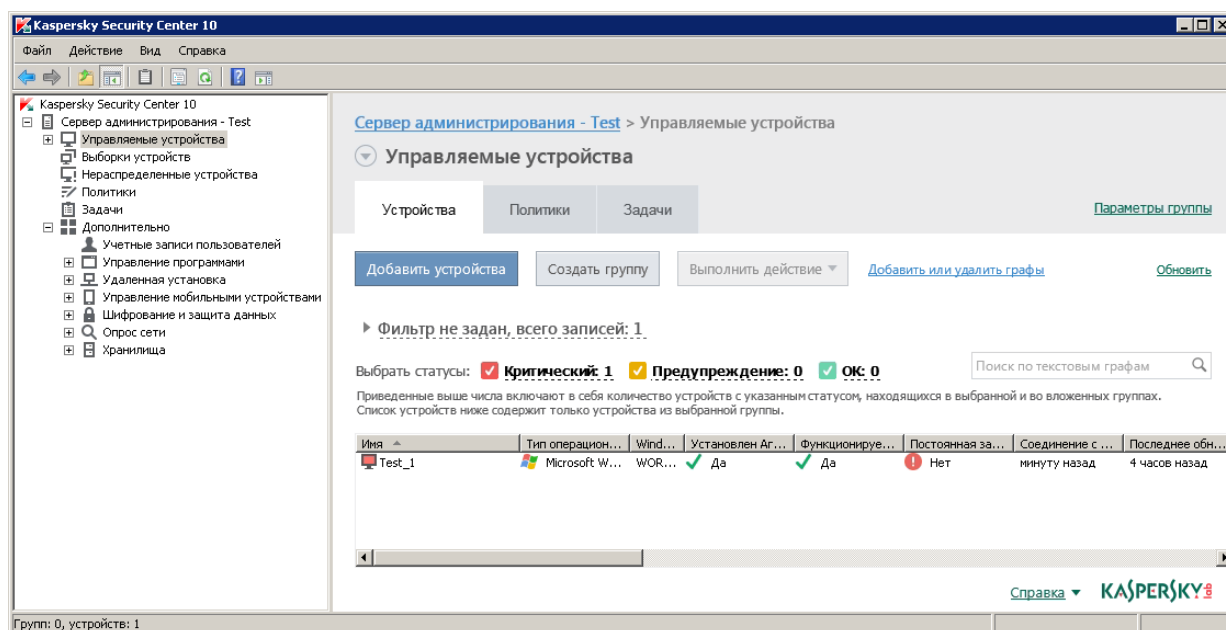


Рисунок 4. Рабочая область, разделенная на закладки

## В этом разделе

Элементы рабочей области .....	<a href="#">55</a>
Набор информационных блоков .....	<a href="#">57</a>

## Элементы рабочей области

Рабочая область папки или узла может содержать следующие элементы (см. рис. ниже):

- Блок управления списком. Содержит кнопки, раскрывающиеся списки команд и ссылки. Предназначен для действий с объектами, выбранными в списке.
- Список объектов. Содержит объекты управления (например, устройства, учетные записи пользователей, политики, задачи). Вы можете сортировать и фильтровать объекты в списке, выполнять с ними действия с помощью блока управления и команд из контекстного меню объекта. Вы также можете настраивать набор граф, отображаемых в списке.
- Блок работы с выбранным объектом. Содержит сводную информацию о выбранном объекте. Блок также может содержать ссылки для быстрых действий с выбранным объектом. Например, блок работы с выбранной политикой содержит ссылку на окно настройки политики.

- Блок фильтрации данных. С помощью блока фильтрации вы можете настраивать отображение объектов в списке. Например, с помощью блока фильтрации данных можно настроить список устройств так, чтобы в нем отображались только устройства со статусом «Критический».

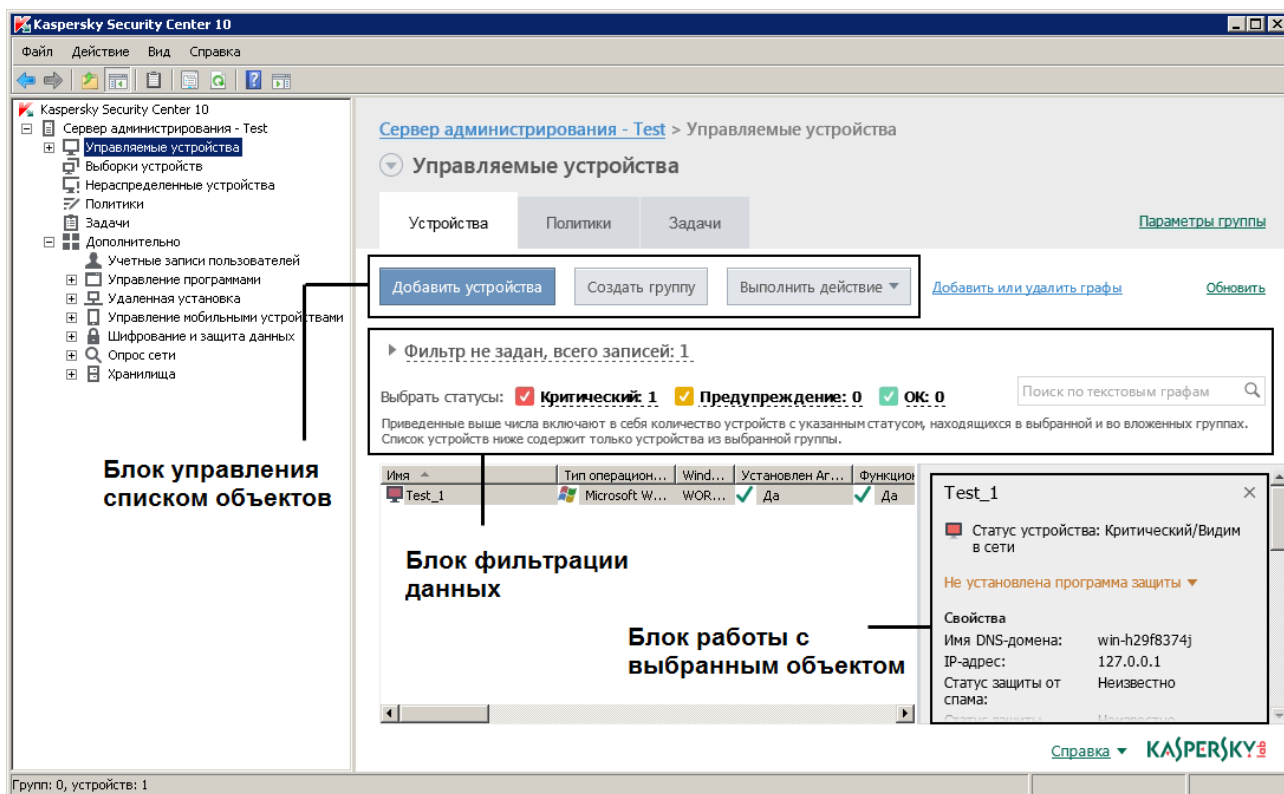


Рисунок 5. Информационная область, представленная списком объектов управления



# Набор информационных блоков

В рабочей области узла **Сервер администрирования** на закладке **Статистика** отображаются статистические данные на информационных панелях. Информационные панели распределены по нескольким тематическим страницам (см. рис. ниже). Вы можете настраивать представление данных на информационных панелях: изменять типы диаграмм и набор данных для них, изменять и добавлять информационные панели, а также целые страницы на закладке **Статистика** (см. раздел «Работа со статистической информацией» на стр. 186).

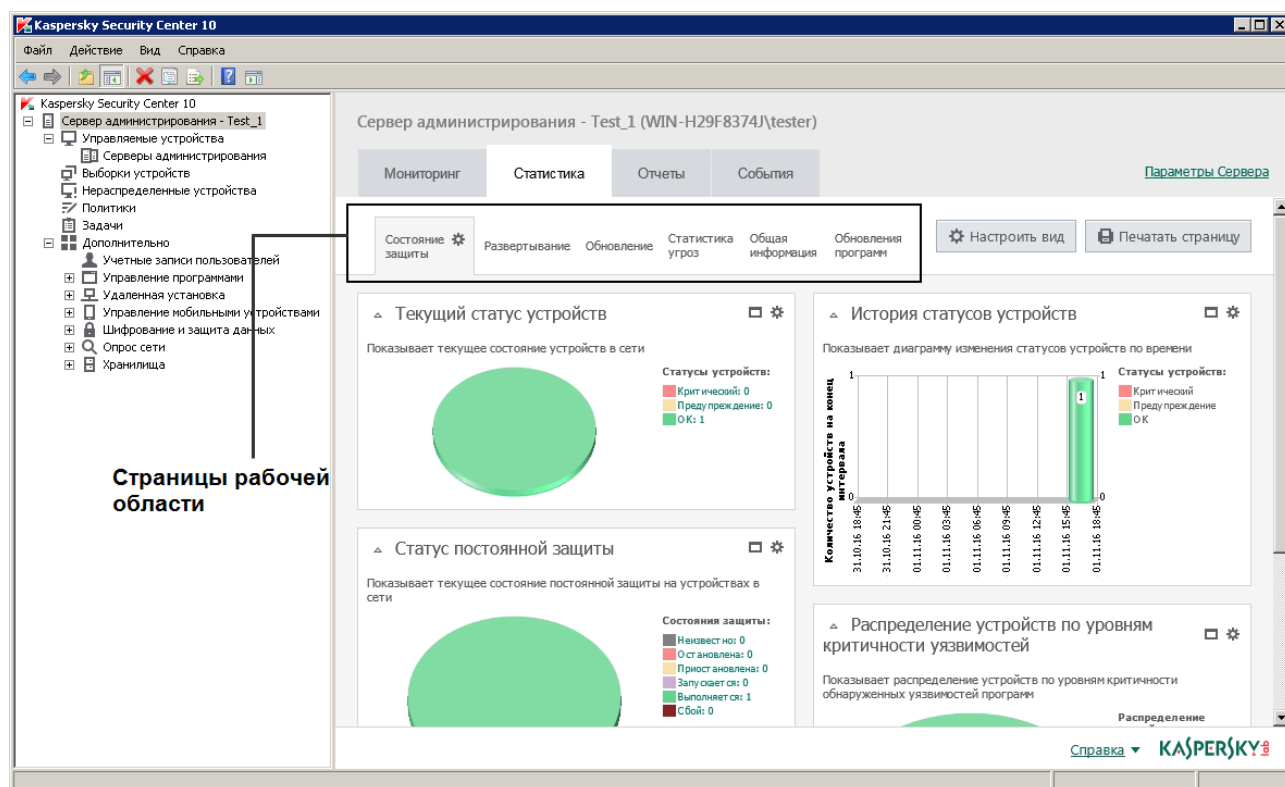
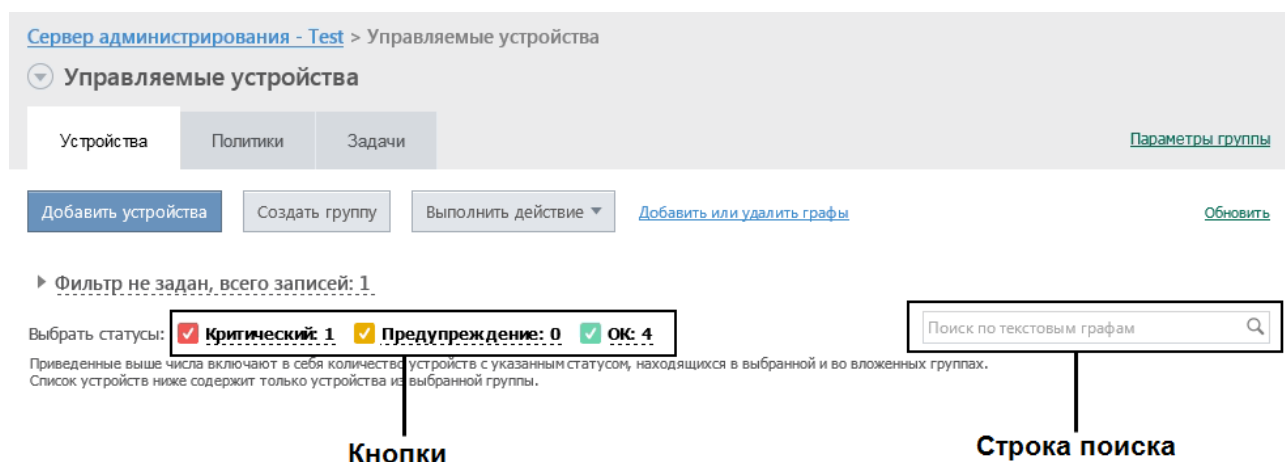


Рисунок 6. Рабочая область, разделенная на страницы

## Блок фильтрации данных

*Блок фильтрации данных* (далее также *блок фильтрации*) используется в рабочих областях и разделах диалоговых окон, которые содержат списки объектов (например, устройств, программ, уязвимостей, пользователей).

Блок фильтрации может включать строку поиска, фильтр и кнопки (см. рис. ниже).



### Блок фильтрации **расширенного вида**. Настройка фильтрации

Для фильтрации данных вы можете использовать блок фильтрации стандартного и расширенного вида (см. рис. ниже). В блоке фильтрации стандартного вида вы можете фильтровать данные с помощью строки поиска и кнопок в блоке **Выбрать статусы**. В блоке фильтрации расширенного вида вы можете использовать дополнительные критерии фильтрации. Дополнительные критерии фильтрации доступны по ссылке **Настроить фильтр**.

► Чтобы настроить фильтрацию, выполните следующие действия:

1. Нажмите на область **Фильтр не задан**.

В правой части окна отобразится ссылка **Настроить фильтр**.

2. По ссылке **Настроить фильтр** выберите критерии фильтрации.

Выбранные критерии отобразятся на сером фоне в поле **Фильтр**.

3. Укажите значение для каждого критерия (например, «Установлен Агент»).

4. В блоке **Выбрать статусы** настройте дополнительную фильтрацию устройств по статусам (*Критический*, *Предупреждение*, *ОК*).

Устройства, соответствующие фильтру, отобразятся в списке. Вы также можете искать устройства по ключевым словам и регулярным выражениям (см. раздел «Что нового» на стр. [25](#)) в поле **Поиск**.

[Настроить правила выпуска сертификатов](#)

[Интегрировать с инфраструктурой открытых ключей](#)

[Обновить](#)

▼ Фильтр не задан, всего записей: 3

Настроить фильтр

[Добавить или удалить графы](#)

Поиск по текстовым графам

**Блок фильтрации  
стандартного вида**

[Настроить правила выпуска сертификатов](#)

[Интегрировать с инфраструктурой открытых ключей](#)

[Обновить](#)

▼ Фильтр не задан, всего записей: 3

Настроить фильтр

Тип:  
= ▼

Протокол:  
= ▼

Пользователь:  
= ▼

Состояние:  
= ▼

[Добавить или удалить графы](#)

Поиск по текстовым графам

**Блок фильтрации  
расширенного вида**

## Контекстное меню

В дереве консоли Kaspersky Security Center каждый объект имеет контекстное меню. В нем к стандартным командам контекстного меню Microsoft Management Console добавлены дополнительные команды, при помощи которых осуществляется работа с этим объектом. Перечень дополнительных команд контекстного меню, соответствующих различным объектам дерева консоли, приведен в Приложениях (см. раздел «Команды контекстного меню» на стр. [387](#)).

Некоторые объекты в рабочей области (например, устройства в списке управляемых устройств, другие объекты в списках) также имеют контекстное меню с дополнительными командами.

## Настройка интерфейса

Вы можете настраивать интерфейс Kaspersky Security Center:

- отображать и скрывать объекты в дереве консоли, рабочей области, окнах свойств объектов (папки, разделы) в зависимости от используемой функциональности;
- отображать и скрывать части главного окна (например, дерево консоли, стандартные меню **Действия** и **Вид**).

- Чтобы настроить интерфейс Kaspersky Security Center в соответствии с используемой функциональностью, выполните следующие действия:

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В меню окна программы выберите пункт **Вид → Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** настройте отображение элементов интерфейса с помощью следующих флажков:

- **Отображать Системное администрирование.**

Если флажок установлен, в папке **Удаленная установка** отображается вложенная папка **Развертывание образов устройств**, а в папке **Хранилища** отображается вложенная папка **Оборудование**.

По умолчанию флажок снят.

- **Отображать шифрование и защиту данных.**

Если флажок установлен, доступно управление шифрованием данных на устройствах, подключаемых к сети. После перезапуска программы в дереве консоли отобразится папка **Шифрование и защита данных**.

По умолчанию флажок снят.

- **Отображать параметры контроля рабочего места.**

Если флажок установлен, в разделе **Контроль рабочего места** окна свойств политики Kaspersky Endpoint Security 10 для Windows отображаются следующие подразделы:

- **Контроль запуска программ.**
- **Мониторинг уязвимостей.**
- **Контроль устройств.**
- **Веб-Контроль.**

Если флажок снят, указанные выше подразделы не отображаются в разделе **Контроль рабочего места**.

По умолчанию флажок снят.

- **Отображать Управление мобильными устройствами.**

Если флажок установлен, доступна функциональность **Управление мобильными устройствами**. После перезапуска программы в дереве консоли отобразится папка **Мобильные устройства**.

По умолчанию флажок снят.

- **Отображать подчиненные Серверы администрирования.**

Если флажок установлен, в дереве консоли отображаются узлы подчиненных и виртуальных Серверов администрирования в составе групп администрирования. При этом доступна функциональность, связанная с подчиненными и виртуальными Серверами администрирования (например, создание задач удаленной установки программ на подчиненные Серверы администрирования).

По умолчанию флажок установлен.

- **Отображать разделы с параметрами безопасности.**

Если флажок установлен, в окнах свойств Сервера администрирования, групп администрирования и других объектов будет отображаться раздел **Безопасность**. Это позволит предоставлять пользователям и группам пользователей права на работу с объектами, отличные от заданных по умолчанию.

По умолчанию флажок установлен.

#### 4. Нажмите на кнопку **ОК**.

Для применения некоторых изменений нужно закрыть и снова открыть главное окно программы.

► *Чтобы настроить отображение элементов главного окна программы, выполните следующие действия:*

1. В меню окна программы выберите пункт **Вид** → **Настроить**.
2. В открывшемся окне **Настройка вида** настройте отображение элементов главного окна с помощью флажков.
3. Нажмите на кнопку **ОК**.

---

# Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

## В этом разделе

О Лицензионном соглашении .....	<a href="#">62</a>
О лицензии .....	<a href="#">63</a>
О лицензионном сертификате .....	<a href="#">64</a>
О ключе .....	<a href="#">64</a>
Варианты лицензирования Kaspersky Security Center .....	<a href="#">65</a>
Об ограничениях базовой функциональности .....	<a href="#">68</a>
О коде активации .....	<a href="#">69</a>
О файле ключа .....	<a href="#">70</a>
О подписке .....	<a href="#">70</a>

## О Лицензионном соглашении

*Лицензионное соглашение* – это юридическое соглашение между вами и АО «Лаборатория Касперского», в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Security Center.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

## О лицензии

*Лицензия* – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.

Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security Center прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

Вы можете активировать программу по пробной лицензии только один раз.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Security Center). Чтобы продолжить использование Kaspersky Security Center в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

# О лицензионном сертификате

*Лицензионный сертификат* – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

## О ключе

*Ключ* – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами «Лаборатории Касперского».

Вы можете добавить ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. Ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Ключ может быть заблокирован «Лабораторией Касперского», если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для работы программы требуется добавить другой ключ.



Ключ может быть активным и дополнительным.

*Активный ключ* – ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного ключа.

*Дополнительный ключ* – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Дополнительный ключ может быть добавлен только при наличии активного ключа.

Ключ для пробной лицензии может быть добавлен только в качестве активного ключа. Ключ для пробной лицензии не может быть добавлен в качестве дополнительного ключа.

## Варианты лицензирования Kaspersky Security Center

В Kaspersky Security Center лицензия может распространяться на разные группы функциональности.

### **Базовая функциональность Консоли администрирования**

Доступны следующие функции:

- создание виртуальных Серверов администрирования для управления сетью удаленных офисов или организаций-клиентов;
- формирование иерархии групп администрирования для управления набором устройств как единым целым;
- контроль состояния антивирусной безопасности организации;
- удаленная установка программ;
- просмотр списка образов операционных систем, доступных для удаленной установки;
- централизованная настройка параметров программ, установленных на клиентских устройствах;
- просмотр и изменение существующих групп лицензионных программ;

- получение статистики и отчетов о работе программ, а также уведомлений о критических событиях;
- управление процессом шифрования и защиты данных;
- просмотр и редактирование вручную списка оборудования, обнаруженного в результате опроса сети;
- централизованная работа с файлами, помещенными на карантин или в резервное хранилище, а также с файлами, обработка которых отложена.

Программа Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования поставляется в составе продуктов «Лаборатории Касперского», предназначенных для защиты сети организации. Кроме того, она доступна для загрузки с веб-сайта «Лаборатории Касперского» (<http://www.kaspersky.ru>).

До активации программы или по истечении срока действия коммерческой лицензии Kaspersky Security Center работает в режиме базовой функциональности Консоли администрирования (см. раздел «Об ограничениях базовой функциональности» на стр. [68](#)).

### **Функциональность Системное администрирование**

Доступны следующие функции:

- удаленная установка операционных систем;
- удаленная установка обновлений программного обеспечения, поиск и закрытие уязвимостей;
- инвентаризация оборудования;
- управление группами лицензионных программ;
- удаленное разрешение подключения к клиентским устройствам с помощью компонента Microsoft® Windows® «Подключение к удаленному рабочему столу»;
- удаленное подключение к клиентским устройствам с помощью Windows Desktop Sharing;
- управление ролями пользователей.

Единицей управления для функциональности Системного администрирования является клиентское устройство в группе «Управляемые устройства».

В рамках функциональности Системное администрирование при инвентаризации доступны подробные сведения об оборудовании устройств.

Для правильной работы функциональности Системного администрирования объем свободного места на жестком диске должен составлять не менее 100 ГБ.

### **Функциональность Управление мобильными устройствами**

Функциональность Управление мобильными устройствами предназначена для управления мобильными устройствами Exchange ActiveSync и iOS MDM.

Для мобильных устройств Exchange ActiveSync доступны следующие функции:

- создание и редактирование профилей управления мобильными устройствами, назначение профилей почтовым ящикам пользователей;
- настройка параметров работы мобильного устройства (синхронизация почты, использование приложений, пароль пользователя, шифрование данных, подключение съемных дисков);
- установка сертификатов на мобильные устройства.

Для iOS MDM-устройств доступны следующие функции:

- создание и редактирование конфигурационных профилей, установка конфигурационных профилей на мобильные устройства;
- установка приложений на мобильное устройство через App Store® или с помощью манифест-файлов (.plist);
- возможность блокировать мобильное устройство, сбрасывать пароль мобильного устройства и удалять все данные с мобильного устройства.

Также в рамках функциональности Управление мобильными устройствами доступно выполнение команд, предусмотренных соответствующими протоколами.

Единицей управления функциональности Управления мобильными устройствами является мобильное устройство. Мобильное устройство считается управляемым, как только оно подключается к Серверу мобильных устройств.

## Об ограничениях базовой функциональности

До активации программы или по истечении срока действия коммерческой лицензии Kaspersky Security Center работает в режиме базовой функциональности Консоли администрирования. Далее приведено описание ограничений, которые накладываются на работу программы в этом режиме.

### Управление мобильными устройствами

Невозможно создать новый профиль и назначить его мобильному устройству (iOS MDM) или почтовому ящику (Exchange ActiveSync). Изменение существующих профилей и их назначение почтовым ящикам доступно всегда.

### Управление программами

Невозможно запустить задачи установки и удаления обновлений. Все задачи, запущенные до истечения срока действия лицензии, выполняются до конца, но последние обновления не устанавливаются. Например, если до истечения срока действия лицензии была запущена задача установки критических обновлений, то будут установлены только критические обновления, найденные до истечения срока действия лицензии.

Запуск и редактирование задач синхронизации, поиска уязвимостей и обновления базы уязвимостей доступны всегда. Ограничения также не накладываются на просмотр, поиск и сортировку записей в списке уязвимостей и обновлений.

### Удаленная установка операционных систем и программ

Невозможно запустить задачи снятия и установки образа операционной системы. Задачи, запущенные до истечения срока действия лицензии, выполняются до конца.

## **Инвентаризация оборудования**

Недоступно получение информации о новых устройствах с помощью Сервера мобильных устройств. При этом информация о компьютерах и подключаемых устройствах обновляется.

Не работают оповещения об изменении конфигурации устройств.

Список оборудования доступен для просмотра и редактирования вручную.

## **Управление группами лицензионных программ**

Невозможно добавить новый ключ.

Не рассылаются оповещения о том, что превышены ограничения на использование ключей.

## **Удаленное подключение к клиентским устройствам**

Удаленное подключение к клиентским устройствам недоступно.

## **Антивирусная безопасность**

Антивирус использует базы, установленные до истечения срока действия лицензии.

# **О коде активации**

*Код активации* – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации «Лаборатории Касперского».

Если программа была активирована с помощью кода активации, в некоторых случаях после активации программа регулярно отправляет запросы на серверы активации «Лаборатории Касперского» для проверки текущего статуса ключа. Для отправки запросов необходимо предоставить программе доступ в интернет.

Если код активации был потерян после активации программы, вы можете восстановить его. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Способы получения технической поддержки» на стр. [350](#)).

## О файле ключа

*Файл ключа* – это файл с расширением key, который вам предоставляет «Лаборатория Касперского». Файл ключа предназначен для добавления ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации «Лаборатории Касперского».

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться в Службу технической поддержки (<http://support.kaspersky.ru>).
- Получить файл ключа на веб-сайте «Лаборатории Касперского» (<https://activation.kaspersky.com/ru/>) на основе имеющегося кода активации.

## О подписке

*Подписка на Kaspersky Security Center* – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Security Center можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме, или отказаться от нее.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security Center после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Security Center по подписке, требуется применить код активации, предоставленный поставщиком услуг.

Вы можете применить другой код активации для использования Kaspersky Security Center только после окончания подписки или отказа от нее.

В зависимости от поставщика услуг, наборы возможных действий для управления подпиской могут различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность программы сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security Center.

При использовании программы по подписке Kaspersky Security Center автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Вы можете продлить подписку на веб-сайте поставщика услуг.

---

# Мастер первоначальной настройки Сервера администрирования

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Программа Kaspersky Security Center позволяет настроить минимальный набор параметров, необходимых для построения системы централизованного управления защитой с помощью мастера первоначальной настройки. В процессе работы мастера в программе происходят следующие изменения:

- Добавляются ключи или коды, которые можно автоматически распространять на устройства в группах администрирования.
- Настраивается взаимодействие с Kaspersky Security Network (KSN). KSN позволяет получать информацию об установленных на управляемых устройствах программах из репутационных баз «Лаборатории Касперского». Если вы разрешили использование KSN, мастер включает службу прокси-сервера KSN, которая обеспечивает взаимодействие между KSN и устройствами.
- Настраивается рассылка по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых программ (чтобы уведомление прошло успешно, на Сервере администрирования и всех устройствах-получателях должна быть запущена служба сообщений Messenger).
- Настраиваются параметры обновлений и закрытия уязвимостей программ, установленных на устройствах.
- Для верхнего уровня иерархии управляемых устройств формируется политика защиты рабочих станций и серверов, а также задачи поиска вирусов, получения обновлений и резервного копирования данных.



Мастер первоначальной настройки создает политики защиты только для тех программ, для которых они еще не присутствуют в папке **Управляемые устройства**. Мастер первоначальной настройки не создает задачи, если задачи с такими именами уже созданы для верхнего уровня иерархии управляемых устройств.

Программа предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Мастер первоначальной настройки можно также запустить вручную с помощью контекстного меню узла **Сервер администрирования <Имя устройства>**.

---

# Основные понятия

Этот раздел содержит развернутые определения основных понятий, относящихся к программе Kaspersky Security Center.

## В этом разделе

Сервер администрирования.....	<a href="#">74</a>
Иерархия Серверов администрирования.....	<a href="#">75</a>
Виртуальный Сервер администрирования.....	<a href="#">77</a>
Сервер мобильных устройств .....	<a href="#">78</a>
Веб-сервер .....	<a href="#">79</a>
Агент администрирования. Группа администрирования .....	<a href="#">80</a>
Рабочее место администратора .....	<a href="#">81</a>
Плагин управления программой .....	<a href="#">82</a>
Политики, параметры программы и задачи .....	<a href="#">82</a>
Взаимосвязь политики и локальных параметров программы .....	<a href="#">85</a>
Агент обновлений.....	<a href="#">87</a>

## Сервер администрирования

Компоненты Kaspersky Security Center позволяют осуществлять удаленное управление программами «Лаборатории Касперского», установленными на клиентских устройствах.

Устройства, на которых установлен компонент Сервер администрирования, называются *Серверами администрирования* (далее также *Серверами*).

Сервер администрирования устанавливается на устройство в качестве службы со следующим набором атрибутов:

- под именем «Сервер администрирования Kaspersky Security Center»;
- с автоматическим типом запуска при старте операционной системы;
- с учетной записью **Локальная система** либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов программ;
- удаленная установка программ на клиентские устройства и удаление программ;
- обновление баз и модулей программ «Лаборатории Касперского»;
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе программ «Лаборатории Касперского»;
- распространение ключей на клиентские устройства, хранение информации о ключах;
- отправка уведомлений о ходе выполнения задач (например, об обнаружении вирусов на клиентском устройстве).

## Иерархия Серверов администрирования

Серверы администрирования могут образовывать иерархию вида «главный сервер – подчиненный сервер». Каждый Сервер администрирования может иметь несколько *подчиненных Серверов администрирования* (далее также *подчиненных Серверов*) на разных уровнях иерархии. Уровень вложенности подчиненных Серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования* (см. раздел «Виртуальный Сервер администрирования» на стр. [77](#)).

Иерархию Серверов администрирования можно использовать для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).
- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми устройствами сети, которые могут находиться, например, в других регионах. Достаточно установить в каждом участке сети подчиненный Сервер администрирования, распределить устройства в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.
- Использование Kaspersky Security Center сервис-провайдерами. Сервис-провайдеру достаточно установить Kaspersky Security Center и Kaspersky Security Center 10 Web Console. Для управления большим числом клиентских устройств различных организаций сервис-провайдер может включать в иерархию Серверов администрирования виртуальные Серверы администрирования.

Каждое устройство, включенное в иерархию групп администрирования, может быть подключено только к одному Серверу администрирования. Вам нужно самостоятельно проверять подключение устройств к Серверам администрирования. Для этого можно использовать функцию поиска устройств по сетевым атрибутам в группах администрирования различных Серверов.

# Виртуальный Сервер администрирования

*Виртуальный Сервер администрирования* (далее также *виртуальный Сервер*) – компонент программы Kaspersky Security Center, предназначенный для управления сетью организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования использует для работы базу данных главного Сервера администрирования: задачи резервного копирования и восстановления данных, проверки и получения обновлений не поддерживаются на виртуальном Сервере. Эти задачи решаются в рамках главного Сервера администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.
- Для удаленной установки программ «Лаборатории Касперского» на клиентские устройства, работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу это устройство автоматически назначается агентом обновлений и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером.
- Виртуальный Сервер может опрашивать сеть только через агенты обновлений.
- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Kaspersky Security Center перезапускает главный Сервер администрирования и все виртуальные Серверы.

Администратор виртуального Сервера обладает всеми правами в рамках этого виртуального Сервера.

## Сервер мобильных устройств

*Сервер мобильных устройств* – это компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

Существуют два вида Серверов мобильных устройств:

- Сервер мобильных устройств Exchange ActiveSync. Устанавливается на устройство, на котором установлен сервер Microsoft Exchange, и позволяет получать данные с сервера Microsoft Exchange и передавать их на Сервер администрирования. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими протокол Exchange ActiveSync.
- Сервер iOS MDM. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими сервис Apple Push Notifications (APNs).

Серверы мобильных устройств Kaspersky Security Center позволяют управлять следующими объектами:

- Отдельным мобильным устройством.
- Несколькими мобильными устройствами.
- Несколькими мобильными устройствами, подключенными к кластеру серверов, одновременно. При подключении к кластеру серверов Сервер мобильных устройств, установленный на этом кластере, отображается в Консоли администрирования как один сервер.

# Веб-сервер

*Веб-сервер Kaspersky Security Center* (далее также *Веб-сервер*) – это компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

При создании автономный пакет установки автоматически публикуется на Веб-сервере. Ссылка для скачивания автономного пакета отображается в списке созданных автономных пакетов установки. При необходимости вы можете отменить публикацию автономного пакета или повторно опубликовать его на Веб-сервере.

При создании iOS MDM-профиль для мобильного устройства пользователя также автоматически публикуется на Веб-сервере. Опубликованный профиль автоматически удаляется с Веб-сервера после успешной установки на мобильное устройство пользователя (подробнее о создании и установке iOS MDM-профиля см. *Руководство по внедрению Kaspersky Security Center*).

Папка общего доступа используется для размещения информации, доступной всем пользователям, устройства которых находятся под управлением Сервера администрирования. Если у пользователя нет прямого доступа к папке общего доступа, ему можно передать информацию из этой папки с помощью Веб-сервера.

Для передачи пользователям информации из папки общего доступа с помощью Веб-сервера администратору требуется создать в папке общего доступа вложенную папку public и поместить в нее информацию.

Синтаксис ссылки для передачи информации пользователю выглядит следующим образом:

```
https://<имя Веб-сервера>:<порт HTTPS>/public/<объект>
```

где

- <имя Веб-сервера> – имя Веб-сервера Kaspersky Security Center.
- <порт HTTPS> – HTTPS-порт Веб-сервера, заданный администратором. HTTPS-порт можно задать в разделе **Веб-сервер** окна свойств Сервера администрирования. По умолчанию используется порт 8061.
- <объект> – вложенная папка или файл, доступ к которым требуется открыть для пользователя.

Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

По полученной ссылке пользователь может загрузить на локальное устройство предназначенную для него информацию.

## Агент администрирования. Группа администрирования

Взаимодействие между Сервером администрирования и устройствами осуществляет компонент программы Kaspersky Security Center *Агент администрирования*. Агент администрирования требуется установить на все устройства, где управление работой программ «Лаборатории Касперского» выполняется с помощью Kaspersky Security Center.

Агент администрирования устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- под именем «Агент администрирования Kaspersky Security Center»;
- с автоматическим типом запуска, при старте операционной системы;
- с учетной записью **Локальная система**.

Устройство, сервер или рабочая станция, на которых установлен Агент администрирования и управляемые программы «Лаборатории Касперского», называется *клиентом Сервера администрирования* (далее также *клиентским устройством* или *устройством*).

Множество устройств сети организации может быть разбито на группы, организующие иерархическую структуру. Такие группы называются *группами администрирования*. Иерархия групп администрирования отображается в дереве консоли в узле Сервера администрирования.



*Группа администрирования* (далее также *группа*) – это набор клиентских устройств, объединенных по какому-либо признаку, с целью управления устройствами группы как единым целым. Для всех клиентских устройств в группе устанавливаются:

- единые параметры работы программ – с помощью *групповых политик*;
- единый режим работы программ – путем создания *групповых задач* с заданным набором параметров (например, создание и установка единого *инсталляционного пакета*, обновление баз и модулей программ, проверка устройства по требованию и постоянная защита).

Клиентское устройство может входить в состав только одной группы администрирования.

Вы можете создавать иерархию Серверов и групп любой глубины вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и клиентские устройства.

## Рабочее место администратора

Устройства, на которых установлен компонент *Консоль администрирования*, называются *рабочими местами администраторов*. С этих устройств администраторы могут осуществлять удаленное централизованное управление программами «Лаборатории Касперского», установленными на клиентских устройствах.

После установки Консоли администрирования на устройстве в меню **Пуск → Программы → Kaspersky Security Center** появляется значок для ее запуска.

Количество рабочих мест администратора не ограничивается. С каждого рабочего места администратора можно управлять группами администрирования сразу нескольких Серверов администрирования в сети. Рабочее место администратора можно подключить к Серверу администрирования (как к физическому, так и к виртуальному) любого уровня иерархии.

Рабочее место администратора можно включить в состав группы администрирования в качестве клиентского устройства.

В пределах групп администрирования любого Сервера одно и то же устройство может быть одновременно и клиентом Сервера администрирования, и Сервером администрирования, и рабочим местом администратора.

## Плагин управления программой

Управление программами «Лаборатории Касперского» через Консоль администрирования выполняется при помощи специального компонента – *плагины управления программой*. Он входит в состав всех программ «Лаборатории Касперского», управление которыми может осуществляться при помощи Kaspersky Security Center.

Плагин управления программой устанавливается на рабочее место администратора. С помощью плагина управления программой в Консоли администрирования можно выполнять следующие действия:

- создавать и редактировать политики и параметры программы, а также параметры задач этой программы;
- получать информацию о задачах программы, событиях в ее работе, а также о статистике работы программы, получаемой с клиентских устройств.

## Политики, параметры программы и задачи

Именованное действие, выполняемое программой «Лаборатории Касперского», называется *задачей*. В соответствии с выполняемыми функциями задачи разделяют по *типам*.

Каждой задаче соответствует набор параметров работы программы при ее выполнении. Набор параметров работы программы, общий для всех типов ее задач, составляет параметры программы. Параметры работы программы, специфичные для каждого типа задач, образуют параметры задачи.

Подробное описание типов задач для каждой программы «Лаборатории Касперского» приводится в Руководствах к ним.

Параметры программы, которые определяются для отдельного клиентского устройства через локальный интерфейс или удаленно через Консоль администрирования, называются *локальными параметрами программы*.

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


*Политика* – это набор параметров работы программы, определенный для группы администрирования. Политика определяет не все параметры программы.

Для одной программы может быть определено несколько политик с различными значениями параметров, но активная политика для программы может быть только одна.

Для разных групп параметры работы программы могут быть различными. В каждой группе может быть создана собственная политика для программы.

Параметры программы определяются параметрами политик и задач.

Вложенные группы и подчиненные Серверы администрирования наследуют задачи групп более высоких уровней иерархии. Задача, определенная для группы, выполняется не только на клиентских устройствах, включенных в состав этой группы, но и на клиентских устройствах, включенных в состав вложенных в нее групп и подчиненных Серверов, на всех последующих уровнях иерархии.

Каждый параметр, представленный в политике, имеет атрибут «замок»: . «Замок» показывает, наложен ли запрет на изменение параметра в политиках вложенного уровня иерархии (для вложенных групп и подчиненных Серверов администрирования), в параметрах задач и локальных параметрах программы. Если в политике для параметра установлен «замок», переопределить значение будет невозможно (см. раздел «Взаимосвязь политики и локальных параметров программы» на стр. [85](#)).

Если в окне свойств унаследованной политики снять флажок **Наследовать параметры из политики верхнего уровня**, расположенный в блоке **Наследование параметров** раздела **Общие**, действие «замка» для этой политики отменяется.

Предусмотрена возможность активировать политику, не являющуюся активной, при наступлении события, что позволяет, например, устанавливать более жесткие параметры антивирусной защиты в периоды вирусных эпидемий.

Также можно сформировать политику для автономных пользователей.

Создание и настройка задач для объектов, находящихся под управлением одного Сервера администрирования, осуществляется централизованно. Могут быть определены задачи следующих типов:

- *групповая задача* – задача, определяющая параметры работы программ, установленных на устройствах, включенных в группу администрирования;
- *локальная задача* – задача для отдельного устройства;
- *задача для набора устройств* – задача для произвольного набора устройств, как входящих, так и не входящих в группы администрирования;
- *задача Сервера администрирования* – задача, определяемая непосредственно для Сервера администрирования.

Для группы может быть определена групповая задача, даже если программа «Лаборатории Касперского» установлена не на все клиентские устройства группы. В этом случае групповая задача выполняется только для тех устройств, на которых указанная программа установлена.

Задачи, созданные для клиентского устройства локально, выполняются только для этого устройства. При синхронизации клиентского устройства с Сервером администрирования локальные задачи добавляются в перечень сформированных задач для клиентского устройства.

Поскольку параметры работы программы определяются политикой, в параметрах задачи могут быть переопределены те из них, на которые в политике не наложен запрет на изменение, а также параметры, которые могут быть установлены только для конкретного экземпляра задачи. Например, для задачи проверки диска это имя диска и маски проверяемых файлов.

Задача может запускаться автоматически (по расписанию) или вручную. Результаты выполнения задач сохраняются на Сервере администрирования и локально. Администратор

может получать уведомления о том, как выполнена та или иная задача, а также просматривать подробные отчеты.

Информация о политиках, параметрах программы, параметрах задач для наборов устройств и о групповых задачах сохраняется на Сервере и распространяется на клиентские устройства в ходе синхронизации. При этом на Сервере администрирования сохраняются сведения о локальных изменениях, разрешенных политикой и проведенных на клиентских устройствах. Кроме того, обновляется список программ, функционирующих на клиентском устройстве, их статус и перечень сформированных задач.

## Взаимосвязь политики и локальных параметров программы

При помощи политик могут быть установлены одинаковые значения параметров работы программы для всех устройств, входящих в состав группы.

Переопределить значения параметров, заданные политикой, для отдельных устройств в группе можно при помощи локальных параметров программы. При этом можно установить значения только тех параметров, изменение которых не запрещено политикой (параметр не закрыт «замком»).

Значение параметра, которое использует программа на клиентском устройстве (см. рис. ниже), определяется наличием «замка» у параметра в политике:

- Если на изменение параметра наложен запрет, на всех клиентских устройствах используется одно и то же значение – заданное политикой.
- Если запрет не наложен, то на каждом клиентском устройстве программа использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры программы.



Рисунок 7. Политика и локальные параметры программы

Таким образом, при выполнении задачи на клиентском устройстве программа использует параметры, заданные двумя разными способами:

- параметрами задачи и локальными параметрами программы, если в политике не был установлен запрет на изменение параметра;
- политикой группы, если в политике был установлен запрет на изменение параметра.

Локальные параметры программы изменяются после первого применения политики в соответствии с параметрами политики.

## Агент обновлений

Агент обновлений – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в сети. Агент обновлений может выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства группы (в том числе и с помощью широковещательной рассылки по протоколу UDP). Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений «Лаборатории Касперского». В последнем случае для устройства, являющегося агентом обновлений, должна быть создана задача обновления (см. раздел «Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства» на стр. [227](#)).

Агенты обновлений ускоряют распространение обновлений и позволяют высвободить ресурсы Сервера администрирования.

- Распространять политики и групповые задачи с помощью широковещательной рассылки по протоколу UDP.
- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования (см. раздел «Использование агента обновлений в качестве шлюза» на стр. [386](#)).

Если нет возможности создать прямое соединение между управляемыми устройствами группы и Сервером администрирования, агент обновлений можно назначить шлюзом соединений этой группы с Сервером администрирования. В этом

случае управляемые устройства подключаются к шлюзу соединений, который, в свою очередь, подключается к Серверу администрирования.

Наличие агента обновлений, работающего в режиме шлюза соединений, не исключает прямого соединения управляемых устройств с Сервером администрирования. Если шлюз соединений недоступен, а прямое соединение с Сервером администрирования технически возможно, управляемые устройства напрямую подключаются к Серверу.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об обнаруженных устройствах. Агент обновлений может выполнять те же виды опроса сети, что и Сервер администрирования.
- Выполнять удаленную установку как сторонних программ, так и программ «Лаборатории Касперского» средствами Microsoft Windows, в том числе на клиентские устройства без установленного Агента администрирования.

Эта функция позволяет удаленно передавать инсталляционные пакеты Агента администрирования на клиентские устройства, расположенные в сетях, к которым у Сервера администрирования нет прямого доступа.

Передача файлов агенту обновлений Сервером администрирования осуществляется по протоколу HTTP или, если настроено использование SSL-соединения, по протоколу HTTPS. Использование протокола HTTP или HTTPS обеспечивает более высокую производительность по сравнению с использованием протокола SOAP за счет сокращения трафика.

Устройства с установленным Агентом администрирования могут быть назначены агентами обновлений вручную администратором или автоматически Сервером администрирования (см. раздел «Назначение устройств агентами обновлений» на стр. [325](#)). Полный список агентов обновлений для указанных групп администрирования можно увидеть, создав отчет по списку агентов обновлений.



Областью действия агента обновлений является группа администрирования, для которой он назначен администратором, а также ее подгруппы всех уровней вложенности. Если в иерархии групп администрирования назначено несколько агентов обновлений, Агент администрирования управляемого устройства подключается к наиболее близкому по иерархии агенту обновлений.

Областью действия агентов обновлений также может являться NLA-подсеть. NLA-подсеть используется для формирования вручную набора устройств, на которые агент обновлений будет распространять обновления.

Если агенты обновлений назначаются автоматически Сервером администрирования, то Сервер назначает агенты обновлений по широковежательным доменам, а не по группам администрирования. Это происходит после того, как становятся известны широковежательные домены. Агент администрирования обменивается с другими Агентами администрирования своей подсети сообщениями и отправляет Серверу администрирования информацию о себе и краткую информацию о других Агентах администрирования. На основании этой информации Сервер администрирования может сгруппировать Агенты администрирования по широковежательным доменам. Широковежательные домены становятся известны Серверу администрирования после того, как опрошено более 70% Агентов администрирования в группах администрирования. Сервер администрирования опрашивает широковежательные домены каждые два часа.

После того как агенты обновлений назначены по широковежательным доменам, их нельзя назначить снова по группам администрирования.

Агенты администрирования с активным профилем соединения не участвуют в определении широковежательного домена.

Когда на одном участке сети или в группе администрирования назначаются два и более агентов обновлений, один из них становится активным агентом обновлений, остальные назначаются резервными. Активный агент обновлений скачивает обновления и инсталляционные пакеты непосредственно с Сервера администрирования, резервные агенты обновлений обращаются за обновлениями только к активному агенту обновлений. В этом случае файлы загружаются только один раз с Сервера администрирования и далее распределяются между агентами обновлений. Если активный агент обновлений по каким-либо причинам становится недоступным, один из резервных агентов обновлений назначается активным. Сервер администрирования назначает агента обновлений резервным автоматически.

Статус агента обновлений (*Активный / Резервный*) отображается флажком в отчете утилиты `klmagchk` (см. раздел «Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита `klmagchk`» на стр. [153](#)).

Для работы агента обновлений необходимо не менее 4 ГБ свободного места на жестком диске. Если объем свободного места на диске агента обновлений меньше 2 ГБ, Kaspersky Security Center создает инцидент с уровнем важности *Предупреждение*. Инцидент будет опубликован в свойствах устройства в разделе **Инциденты**.

При наличии на Сервере администрирования задач удаленной установки, на устройстве с агентом обновлений дополнительно потребуется количество места на диске, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей, на устройстве с агентом обновлений дополнительно потребуется количество места на диске, равное удвоенному суммарному размеру всех устанавливаемых патчей.

---

# Управление Серверами администрирования

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

## В этом разделе

Подключение к Серверу администрирования и переключение между Серверами администрирования .....	<a href="#">91</a>
Права доступа к Серверу администрирования и его объектам .....	<a href="#">94</a>
Условия подключения к Серверу администрирования через интернет .....	<a href="#">96</a>
Защищенное подключение к Серверу администрирования .....	<a href="#">97</a>
Отключение от Сервера администрирования .....	<a href="#">99</a>
Добавление Сервера администрирования в дерево консоли .....	<a href="#">99</a>
Удаление Сервера администрирования из дерева консоли .....	<a href="#">99</a>
Смена учетной записи службы Сервера администрирования. Утилита klsrvswch.....	<a href="#">100</a>
Просмотр и изменение параметров Сервера администрирования .....	<a href="#">101</a>

## 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.

► *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 8. 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.

# 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**.

# 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 должны быть открыты входящие порты 13000 и 14000.
- 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 SSL (Secure Socket Layer). Протокол SSL позволяет идентифицировать стороны, взаимодействующие при подключении, осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. В основе протокола SSL лежит аутентификация взаимодействующих сторон и шифрование данных по методу открытых ключей.

## В этом разделе

Аутентификация Сервера при подключении устройства .....	<a href="#">97</a>
Аутентификация Сервера при подключении Консоли администрирования.....	<a href="#">98</a>
Сертификат Сервера администрирования .....	<a href="#">98</a>

## 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. [372](#)).

# 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**.

# 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.

► *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 иницирует 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 пользователя в открывшемся окне **Выбор: «Пользователь»**.

Закройте окно **Выбор: «Пользователь»** и нажмите на кнопку **Далее**.

2. В окне **Пароль учетной записи** задайте пароль для учетной записи выбранного пользователя, если требуется.

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 Антивируса Касперского. 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 .....	<a href="#">102</a>
Обработка и хранение событий на Сервере администрирования .....	<a href="#">103</a>
Контроль возникновения вирусных эпидемий.....	<a href="#">103</a>
Ограничение трафика .....	<a href="#">104</a>
Настройка параметров Веб-сервера.....	<a href="#">104</a>
Работа с внутренними пользователями.....	<a href="#">105</a>

# 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 **Оповещение о событиях** окна свойств Сервера администрирования. В разделе **Оповещение о событиях** 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 **Оповещение о событиях** окна свойств Сервера администрирования (см. раздел «Обработка и хранение событий на Сервере администрирования» на стр. [103](#)), 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.

## 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. Под именем учетной записи внутреннего пользователя администратор виртуального Сервера может запускать Kaspersky Security Center 10 Web Console для просмотра сведений о состоянии антивирусной безопасности сети. 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. [170](#)).

---

# 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.....	<a href="#">107</a>
Перемещение групп администрирования .....	<a href="#">109</a>
Удаление групп администрирования .....	<a href="#">110</a>
Автоматическое создание структуры групп администрирования.....	<a href="#">111</a>
Автоматическая установка программ на устройства группы администрирования.....	<a href="#">113</a>

# 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 Серверы администрирования.

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

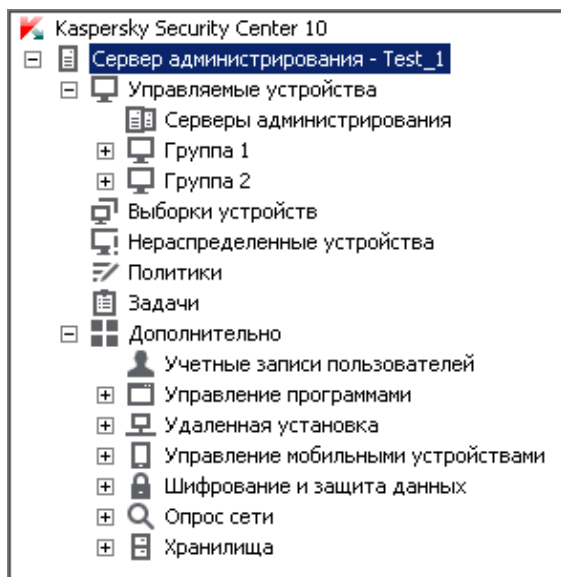


Рисунок 9. Просмотр иерархии групп администрирования

► 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.

---

# 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.....	<a href="#">114</a>
Управление профилями политик .....	<a href="#">123</a>
Управление задачами .....	<a href="#">129</a>
Просмотр и изменение локальных параметров программы .....	<a href="#">141</a>

## 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. [399](#)).

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, распространятся 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.

## В этом разделе

Создание политики.....	<a href="#">116</a>
Отображение унаследованной политики во вложенной группе .....	<a href="#">117</a>
Активация политики .....	<a href="#">118</a>
Автоматическая активация политики по событию «Вирусная атака» .....	<a href="#">119</a>
Применение политики для автономных пользователей .....	<a href="#">119</a>
Изменение политики. Откат изменений .....	<a href="#">119</a>
Удаление политики .....	<a href="#">120</a>
Копирование политики .....	<a href="#">121</a>
Экспорт политики .....	<a href="#">121</a>
Импорт политики .....	<a href="#">122</a>
Конвертация политик .....	<a href="#">122</a>

## 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.

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**.

## 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.

## О профиле политики

Профиль политики – это именованный набор переменных параметров политики, который активируется на клиентском устройстве (компьютере, мобильном устройстве) при выполнении определенных условий. При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

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 10 Service Pack 1 и выше.

## Преимущества профилей политик

Профили политик облегчают управление клиентскими устройствами с помощью политик:

- Профили содержат только те параметры, которые отличаются от «базовой» политики.
- Не требуется поддерживать и применять вручную несколько копий одной политики, которые различаются только небольшим количеством параметров.
- Не требуется отдельная политика для автономных пользователей.
- Новые профили политики удобно создавать, так как поддерживаются экспорт и импорт профилей, а также создание новых профилей на основе существующих с помощью копирования.
- На одном клиентском устройстве могут быть активны несколько профилей политики одновременно.
- Поддерживается иерархия политик.

## Правила активации профиля. Приоритеты профилей

Профиль политики активируется на клиентском устройстве при выполнении правила активации. 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 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.

Профили, созданные для политики, упорядочены в порядке убывания приоритета. Например, если профиль X находится перед профилем Y в списке профилей, то профиль X имеет более

высокий приоритет, чем  $Y$ . Приоритеты профилей необходимы, так как на клиентском устройстве одновременно может быть активно несколько профилей.

### Политики в иерархии групп администрирования

В то время как политики влияют друг на друга в соответствии с иерархией групп администрирования, профили с одинаковыми именами объединяются. Профили более «высокой» политики 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  $P(A)$ .

Активная политика является суммой главной политики и всех активных профилей этой политики, то есть тех профилей, для которых выполняются правила активации. Активная политика повторно вычисляется при запуске Агента администрирования, при включении и выключении автономного режима, а также при изменении списка тегов, назначенных клиентскому устройству.

### 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.
- Политика не может содержать параметры уведомлений.
- Если используется UDP-порт 15000 для подключения устройства к Серверу администрирования, то при назначении тега устройству соответствующий профиль политики должен активироваться в течение одной минуты.
- Правила подключения Агента администрирования к Серверу администрирования можно использовать при создании правил активации профиля.

# Создание профиля политики

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

► Чтобы создать профиль политики для группы администрирования, выполните следующие действия:

1. В дереве консоли выберите группу администрирования, для которой нужно создать профиль 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 **Профиль политики** в окне свойств политики и нажмите на кнопку **Добавить**.
5. В окне **Свойства: Новый профиль** настройте параметры профиля политики:
  - В разделе **Общие** укажите имя профиля.  
Имя профиля не может превышать 100 символов.
  - Включите или выключите профиль с помощью флажка **Включить профиль**.  
Если флажок снят, профиль не используется для управления устройством.
6. В разделе **Правила активации** создайте правила активации профиля:
  - Нажмите на кнопку **Добавить**.
  - Настройте правила активации профиля политики в окне **Свойство: Новое правило**.
  - Нажмите на кнопку **ОК**.
7. Измените параметры политики в соответствующих разделах.
8. После того, как настроен профиль и созданы правила активации, сохраните изменения по кнопке **ОК**.

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

Профили, созданные для политики, отображаются в свойствах политики в разделе **Профили политик**. Вы можете изменить профиль политики и приоритет профиля (см. раздел «Изменение профиля политики» на стр. [127](#)), а также удалить профиль (см. раздел «Удаление профиля политики» на стр. [128](#)).

Несколько профилей политики могут быть активированы одновременно при выполнении правил активации.

## 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.



# 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.

## Создание групповой 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.

## 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 (подробнее см. *Руководство по внедрению Kaspersky Security Center*);
- сообщение для пользователя (см. раздел «Отправка сообщения пользователям устройств» на стр. [159](#));
- смену Сервера администрирования (см. раздел «Смена Сервера администрирования для клиентских устройств» на стр. [156](#));

- управление устройством (см. раздел «Удаленное включение, выключение и перезагрузка клиентских устройств» на стр. [158](#));
- проверку обновлений (см. раздел «Проверка полученных обновлений» на стр. [317](#));
- распространение инсталляционного пакета (подробнее см. *Руководство по внедрению Kaspersky Security Center*);
- удаленную установку программы на подчиненные Серверы администрирования (подробнее см. *Руководство по внедрению Kaspersky Security Center*);
- удаленную деинсталляцию программы (подробнее см. *Руководство по внедрению Kaspersky Security Center*).

► 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:
  - a. В контекстном меню устройства выберите пункт **Свойства**.
  - b. 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 для наборов устройств**.
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. [94](#)).

► *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 задачи, 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**.

## 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 .....	<a href="#">144</a>
Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover.....	<a href="#">145</a>
Туннелирование соединения клиентского устройства с Сервером администрирования ..	<a href="#">147</a>
Удаленное подключение к рабочему столу клиентского устройства .....	<a href="#">148</a>
Настройка перезагрузки клиентского устройства.....	<a href="#">150</a>
Аудит действий на удаленном клиентском устройстве .....	<a href="#">151</a>
Проверка соединения клиентского устройства с Сервером администрирования.....	<a href="#">152</a>
Идентификация клиентских устройств на Сервере администрирования .....	<a href="#">155</a>
Добавление устройств в состав группы администрирования .....	<a href="#">155</a>
Смена Сервера администрирования для клиентских устройств.....	<a href="#">156</a>
Удаленное включение, выключение и перезагрузка клиентских устройств .....	<a href="#">158</a>
Отправка сообщения пользователям устройств .....	<a href="#">159</a>
Контроль изменения состояния виртуальных машин .....	<a href="#">159</a>
Автоматическое назначение тегов устройствам .....	<a href="#">160</a>
Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center .....	<a href="#">162</a>

# 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.

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

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. [151](#)).

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**.

См. также

Варианты лицензирования Kaspersky Security Center ..... [65](#)

## 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 потребуются 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 Systems Management;
- 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 соединения 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 .....	<a href="#">153</a>
Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита <code>klagchk</code> .....	<a href="#">153</a>

# 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 `klmagchk` 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 `klmagchk`,*

на устройстве запустите утилиту `klmagchk` из командной строки.

Синтаксис утилиты:

```
klmagchk [-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.

## 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.

## Добавление 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 **Добавить устройства** в блоке управления списком устройств.
- В контекстном меню списка устройств выберите пункт **Создать → Устройство**.

В результате запустится мастер добавления устройств. Следуя его указаниям, определите способ добавления 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 добавлены 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 добавить 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 групповой задачи» на стр. [130](#)).
  - 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. [132](#)).

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 Руководстве Администратора Kaspersky Endpoint Security 10 для Windows.

# 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 групповой задачи» на стр. [130](#)).
  - 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. [132](#)).

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.

# 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 групповой задачи» на стр. [130](#)).
  - 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. [132](#)).

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.

# 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 стороне устройства, так и на стороне Сервера 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.

## Автоматическое назначение тегов устройствам

Программа может автоматически назначать теги устройствам. Автоматическое назначение тегов устройствам выполняется с помощью правил. Вы можете создавать и изменять правила назначения тегов в окне свойств Сервера администрирования и / или в окне свойств устройства.

► *Чтобы создать и настроить правила автоматического назначения тегов устройствам, 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 **Правила назначения тегов**.



4. В разделе **Правила назначения тегов** нажмите на кнопку **Добавить**.

В результате откроется окно **Свойство: Новое правило**.

5. В разделе **Общие** окна **Свойства: Новое правило** настройте общие свойства правила:

- Укажите имя правила.

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

- В раскрывающемся списке **Назначаемый тег** выберите добавленный ранее тег или введите новый тег.
- Включите или выключите правило с помощью флажка **Включить правило**.

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

Откроется окно свойств нового условия или выбранного условия.

7. В открывшемся окне настройте условие назначения тега:

- В разделе **Общие** укажите название условия.
- В разделе **Сеть** настройте срабатывание правила по сетевым свойствам устройства (имя устройства в сети Windows, принадлежность устройства к домену, к IP-диапазону и прочее).
- В разделе **Active Directory** настройте срабатывание правила по нахождению устройства в подразделении Active Directory и по членству устройства в группе Active Directory.
- В разделе **Программы** настройте срабатывание правила по наличию на устройстве Агента администрирования, по типу, версии и архитектуре операционной системы.
- В разделе **Виртуальные машины** настройте срабатывание правила по принадлежности устройства к разным типам виртуальных машин.
- В разделе **Реестр программ** настройте срабатывание правила по наличию на устройстве программ различных производителей.

8. После настройки условия нажмите на кнопку **ОК** в окне **Свойство: Новое условие**.

9. Добавьте или настройте другие условия правила назначения тега.

Добавленные условия срабатывания правила отображаются в разделе **Условия** окна свойств правила.

10. Нажмите на кнопку **ОК** в окне свойств правила.

Правило активации тега будет сохранено. Правило выполняется на устройствах, соответствующих условиям правила. В результате выполнения правила устройствам назначается тег. Устройству автоматически назначается несколько тегов, если одновременно выполняются правила назначения этих тегов. Список всех добавленных тегов можно просмотреть в окне свойств любого устройства в разделе **Теги**. В разделе **Теги** вы также можете перейти к настройке правил автоматического назначения тегов по соответствующей ссылке.

## 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 .....	<a href="#">163</a>
Включение и выключение трассировки, загрузка файла трассировки .....	<a href="#">166</a>
Загрузка параметров программ .....	<a href="#">166</a>
Загрузка журналов событий .....	<a href="#">167</a>
Запуск диагностики и загрузка ее результатов .....	<a href="#">167</a>
Запуск, остановка и перезапуск программ .....	<a href="#">168</a>

# 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.

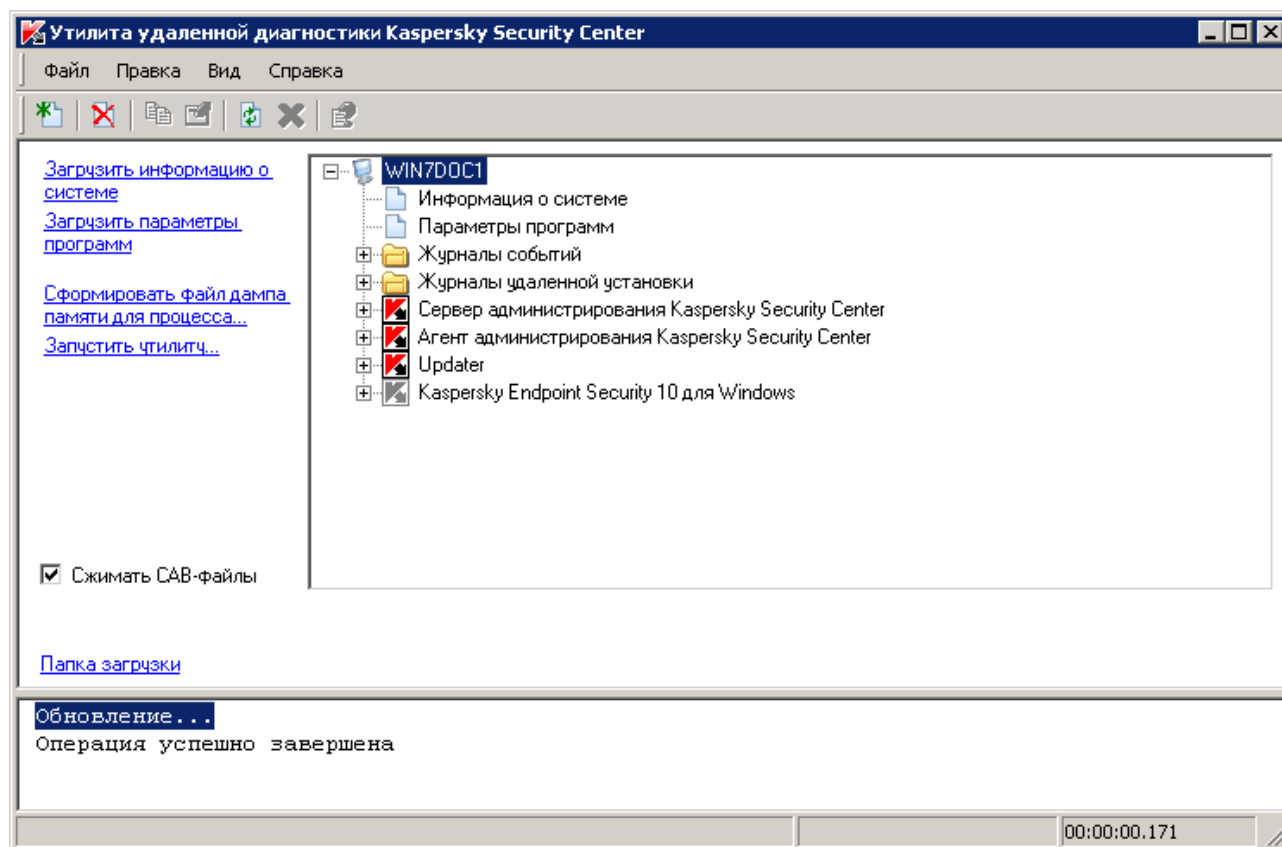


Рисунок 10. Утилита удаленной диагностики. Окно удаленной диагностики клиентского компьютера

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.



---

# Управление учетными записями пользователей

Этот раздел содержит информацию об учетных записях и ролях пользователей, которые поддерживает программа. 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 .....	<a href="#">170</a>
Добавление учетной записи пользователя .....	<a href="#">171</a>
Настройка проверки уникальности имени внутреннего пользователя.....	<a href="#">172</a>
Добавление группы пользователей .....	<a href="#">173</a>
Добавление пользователя в группу .....	<a href="#">174</a>
Настройка прав. Роли пользователей.....	<a href="#">175</a>
Назначение пользователя владельцем устройства.....	<a href="#">178</a>
Рассылка сообщений пользователям .....	<a href="#">179</a>
Просмотр списка мобильных устройств пользователя .....	<a href="#">180</a>
Установка сертификата пользователю .....	<a href="#">180</a>
Просмотр списка сертификатов выписанных пользователю .....	<a href="#">181</a>

# 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. [105](#)). Применяются для работы с виртуальными Серверами администрирования. Учетные записи внутренних пользователей создаются (см. раздел «Добавление учетной записи пользователя» на стр. [171](#)) 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. [175](#));
- рассылать сообщения пользователям с помощью электронной почты и SMS (см. раздел «Рассылка сообщений пользователям» на стр. [179](#));
- просматривать список мобильных устройств пользователя (см. раздел «Просмотр списка мобильных устройств пользователя» на стр. [180](#));
- выписывать и устанавливать сертификаты на мобильные устройства пользователя (см. раздел «Установка сертификата пользователю» на стр. [180](#));
- просматривать список сертификатов, выписанных пользователю (см. раздел «Просмотр списка сертификатов выписанных пользователю» на стр. [181](#)).

# 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 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.

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\.core\independent\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\.core\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**.

В окне **Свойства: Новая группа** настройте параметры добавляемой группы пользователей:

3. В разделе **Общие** укажите имя группы.

Имя группы не может превышать 100 символов. Имя группы должно быть уникальным.

4. В разделе **Пользователи** добавьте учетные записи пользователей в группу.

5. Нажмите на кнопку **ОК**.

Добавленная группа пользователей отобразится в папке **Учетные записи пользователей** в дереве консоли.

## 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.

## 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 с помощью Self Service Portal.

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

# 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. [177](#)) или отдельным пользователям.

Раздел **Роли пользователей** доступен, если в окне настройки интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. раздел «Настройка интерфейса» на стр. [59](#)).



# 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, которые используются для работы с виртуальными Серверами администрирования.

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** (см. раздел «Настройка интерфейса» на стр. [59](#)).

# 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. [201](#)). 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. [183](#)).

# 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. [181](#)).

## 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.

---

# 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.....	<a href="#">182</a>
Работа со статистической информацией .....	<a href="#">186</a>
Настройка параметров уведомлений о событиях .....	<a href="#">187</a>
Создание сертификата для SMTP-сервера .....	<a href="#">188</a>
Выборки событий .....	<a href="#">189</a>
Экспорт событий в SIEM-систему .....	<a href="#">193</a>
Выборки устройств.....	<a href="#">194</a>
Политики .....	<a href="#">198</a>
Задачи.....	<a href="#">198</a>

## 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 .....	<a href="#">183</a>
Создание и просмотр отчета.....	<a href="#">184</a>
Сохранение отчета.....	<a href="#">184</a>
Создание задачи рассылки отчета.....	<a href="#">185</a>

## 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. В окне мастера **Тип задачи** выберите тип задачи **Рассылка отчета**.

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 (см. раздел «Мастер первоначальной настройки Сервера администрирования» на стр. [72](#)).

# 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. 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 (см. раздел «Уведомление о событиях с помощью исполняемого файла» на стр. [360](#)).

► *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 ..... [103](#)

## Создание сертификата для SMTP-сервера

► 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**):
    - а. укажите файл закрытого ключа (файл с расширением prk или pem);
    - б. укажите пароль закрытого ключа;
    - с. 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 .....	<a href="#">190</a>
Настройка параметров выборки событий .....	<a href="#">191</a>
Создание выборки событий .....	<a href="#">191</a>
Экспорт выборки событий в текстовый файл.....	<a href="#">192</a>
Удаление событий из выборки.....	<a href="#">192</a>

## 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.



# Экспорт 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 онлайн справке на веб-ресурсе «Лаборатории Касперского» [https://click.kaspersky.com/?hl=ru-RU&link=online\\_help&pid=KSCEventExport&version=1.0&helpid=](https://click.kaspersky.com/?hl=ru-RU&link=online_help&pid=KSCEventExport&version=1.0&helpid=).

## 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 .....	<a href="#">195</a>
Настройка параметров выборки устройств .....	<a href="#">195</a>
Создание выборки устройств .....	<a href="#">196</a>
Экспорт параметров выборки устройств в файл.....	<a href="#">196</a>
Создание выборки устройств по импортированным параметрам .....	<a href="#">197</a>
Удаление устройств из групп администрирования в выборке .....	<a href="#">197</a>

## 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**.

## 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**.

## 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 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.

## 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.

---

# Нераспределенные устройства

В этом разделе представлена информация о работе с устройствами сети организации, не входящими в группы администрирования.

## В этом разделе

Опрос сети .....	<a href="#">199</a>
Работа с доменами Windows. Просмотр и изменение параметров домена.....	<a href="#">202</a>
Работа с IP-диапазонами .....	<a href="#">203</a>
Работа с группами Active Directory. Просмотр и изменение параметров группы .....	<a href="#">204</a>
Создание правил автоматического перемещения устройств в группы администрирования .....	<a href="#">204</a>
Использование динамического режима VDI на клиентских устройствах .....	<a href="#">205</a>

## 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 групп 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 .....	<a href="#">201</a>
Просмотр и изменение параметров опроса групп Active Directory .....	<a href="#">201</a>
Просмотр и изменение параметров опроса IP-диапазонов .....	<a href="#">202</a>



# 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: <Название 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 .....	<a href="#">203</a>
Просмотр и изменение параметров IP-диапазона .....	<a href="#">203</a>

## 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 предприятия 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. [206](#)) 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.....	<a href="#">206</a>
Поиск устройств, являющихся частью VDI.....	<a href="#">206</a>
Перемещение в группу администрирования устройств, являющихся частью VDI.....	<a href="#">207</a>

# 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.....	<a href="#">208</a>
Уязвимости в программах .....	<a href="#">220</a>
Обновления программного обеспечения .....	<a href="#">224</a>

## 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» (подробнее см. в *Руководстве администратора для программы Kaspersky Endpoint Security 10 для Windows*). 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 .....	<a href="#">211</a>
Настройка управления запуском программ на клиентских устройствах .....	<a href="#">212</a>
Просмотр результатов статического анализа правил запуска исполняемых файлов .....	<a href="#">213</a>
Просмотр реестра программ .....	<a href="#">214</a>
Создание групп лицензионных программ .....	<a href="#">216</a>
Управление ключами для групп лицензионных программ .....	<a href="#">216</a>
Инвентаризация программного обеспечения Kaspersky Security Center .....	<a href="#">218</a>
Инвентаризация исполняемых файлов .....	<a href="#">219</a>
Просмотр информации об исполняемых файлах .....	<a href="#">220</a>

## 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 ссылке **Создать категорию** запустите мастер создания пользовательской категории.
3. В окне мастера выберите тип пользовательской категории:
  - **Пополняемая вручную категория.** В этом случае вы можете вручную задать критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
  - **Автоматически пополняемая категория.** В этом случае вы можете указать 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.** В этом случае вы можете указать устройство. Исполняемые файлы, обнаруженные на устройстве, будут автоматически попадать в категорию.

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**.

## Настройка управления запуском программ на клиентских устройствах

► *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. [211](#)), запуском которых вы хотите управлять.
3. В папке **Управляемые устройства** на закладке **Политики** по ссылке **Создать политику Kaspersky Endpoint Security** 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 запуска программ** нажмите на кнопку **Добавить**.

Откроется окно **Правило контроля запуска программ**.

6. В окне **Правило контроля запуска программ** в раскрывающемся списке **Категория** выберите категорию программ, на которую будет распространяться правило запуска. Настройте параметры правила запуска для выбранной категории программ.

Подробнее о правилах контроля запуска программ см. *Руководство администратора Kaspersky Endpoint Security 10 для Windows*.

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 запуска 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 запуска 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** по ссылке **Управлять ключами лицензионных программ** откройте окно **Управление ключами лицензионных программ**.
3. В окне **Управление ключами лицензионных программ** нажмите на кнопку **Добавить**.

Откроется окно **Ключ**.



4. В окне **Ключ** укажите параметры 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\NagentFlags

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.

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/>).

## 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 программного обеспечения, применимые к устройствам сети, например, новые версии программ.

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 **Синхронизация обновлений Windows Update** 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 требуемые 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.....	<a href="#">225</a>
Синхронизация обновлений Windows Update с Сервером администрирования.....	<a href="#">226</a>
Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства..	<a href="#">227</a>
Офлайн-модель получения обновлений.....	<a href="#">229</a>
Включение и выключение офлайн-модели получения обновлений.....	<a href="#">232</a>
Установка обновлений на устройства вручную.....	<a href="#">233</a>
Настройка обновлений Windows в политике Агента администрирования .....	<a href="#">236</a>

## 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 (*целевые компьютеры*);
- список общесистемных компонентов (пререквизитов), 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**.

► 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 выпадающем списке выберите пункт **Настроить синхронизацию обновлений Windows Update**.

В результате запустится мастер создания задачи получения данных из центра обновлений Windows.

3. Следуйте указаниям мастера.

В результате работы мастера создается задача **Синхронизация обновлений Windows Update**, которая отображается в папке **Задачи**.

Задачу синхронизации обновлений Windows Update также можно создать в папке **Задачи** по кнопке **Создать задачу**.

Задача **Синхронизация обновлений Windows Update** загружает с серверов Microsoft только метаданные. Если в сети не используется WSUS-сервер, то есть каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

## 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 на стороне 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 продуктами 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 продуктах 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".

### **Преимущества и недостатки офлайн-модели получения обновлений**

Офлайн-модель получения обновлений имеет следующие преимущества:

- Kaspersky Security Center может самостоятельно определять, когда загружать обновления, избегая таким образом ошибок в обновлениях управляемых программ. Программы всегда будут иметь надежный доступ к последним обновлениям, которые могут быть загружены с Сервера администрирования.
- Сервер администрирования имеет возможность контролировать нагрузку при распределении обновлений.

Офлайн-модель получения обновлений имеет следующие недостатки:

- Сетевой трафик между Сервером администрирования и Агентом администрирования может быть увеличен, так как в офлайн-модели обновления распространяются на Агенты администрирования каждый раз после того как Сервер администрирования

получает новые обновления. В обычном режиме обновления распределяются по расписанию задачи обновления.

- Возможна дополнительная нагрузка на Сервер администрирования, так как Сервер определяет, какие обновления нужны для каждого управляемого устройства.

### Рекомендации по использованию офлайн-модели обновлений

- Всегда существует интервал времени между моментом, когда Сервер администрирования получил новые обновления программ, и моментом, когда Агент администрирования завершил загрузку обновлений с Сервера администрирования. Если задача обновления начинается в этот интервал времени, то управляемые устройства будут получать старые обновления баз от Агента администрирования.

Рекомендуется задать расписание задачи обновления так, чтобы обновление начиналось после того как Сервер администрирования получил обновления. В этом случае задачу обновления будет выполнять Kaspersky Security Center, и программы будут получать обновления как можно скорее.

- Если задача загрузки обновлений запускается слишком часто, Агенту администрирования может не хватить времени чтобы загрузить все обновления перед очередным запуском задачи.

Рекомендуется увеличить интервал между запусками задачи загрузки обновлений в хранилище.

## Включение и выключение офлайн-модели получения обновлений

► *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.

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 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 обновления программ**, 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 **Управляемые устройства** на закладке **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.

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** 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. Нажмите на кнопку **Применить**.

---

# Дистанционная установка операционных систем и программ

Kaspersky Security Center позволяет создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку программ «Лаборатории Касперского» и других производителей программного обеспечения.

## Захват образов операционных систем

Kaspersky Security Center может выполнять захват образов операционных систем устройств и доставлять эти образы на Сервер администрирования. Полученные в результате образы операционных систем хранятся на Сервере администрирования в общей папке. Снятие и создание образа операционной системы эталонного устройства выполняется с помощью задачи создания инсталляционного пакета (см. раздел «Создание инсталляционных пакетов программ» на стр. [246](#)).

Для создания образов операционной системы на Сервере администрирования должен быть установлен пакет инструментов Windows Automated Installation Kit (WAIK).

Функциональность захвата образа операционной системы имеет следующие особенности:

- Образ операционной системы нельзя снимать с устройства, на котором установлен Сервер администрирования.
- Во время снятия образа операционной системы происходит обнуление параметров эталонного устройства утилитой sysprep.exe. В случае необходимости восстановления параметров эталонного устройства, в мастере создания образа операционной системы необходимо установить флажок **Сохранять резервную копию состояния устройства**.
- В процессе снятия образа выполняется перезагрузка эталонного устройства.

## Развертывание образов операционных систем на новых устройствах

Администратор может использовать полученные образы для развертывания на новых устройствах в сети, на которых еще не была установлена операционная система. Для этой цели используется технология Preboot eXecution Environment (PXE). Администратор назначает устройство в сети, которое будет использоваться в качестве PXE-сервера. Это устройство должно отвечать следующим требованиям:

- На устройстве должен быть установлен Агент администрирования.
- На устройстве не должен работать DHCP-сервер, так как PXE-сервер использует те же порты, что и DHCP.
- В сегменте сети, в который входит устройство, не должно быть других PXE-серверов.

Для развертывания операционной системы необходимо, чтобы на устройстве была установлена сетевая карта, устройство было подключено к сети, а в процессе загрузки устройства в среде BIOS был выбран вариант установки Network boot.

Развертывание операционной системы выполняется в следующей последовательности:

1. PXE-сервер устанавливает соединение с новым клиентским устройством при загрузке клиентского устройства.
2. Клиентское устройство включается в среду Windows Preinstallation Environment (WinPE).

Для включения устройства в среду WinPE может потребоваться настройка состава драйверов для среды WinPE.

3. Клиентское устройство регистрируется на Сервере администрирования.
4. Администратор назначает клиентскому устройству инсталляционный пакет с образом операционной системы.

Администратор может добавлять необходимые драйверы в инсталляционный пакет с образом операционной системы и указывать конфигурационный файл с параметрами операционной системы (файл ответов), которые должны применяться во время установки.

5. Выполняется развертывание операционной системы на клиентском устройстве.

Администратор может вручную указать MAC-адреса еще не подключившихся клиентских устройств и назначить им инсталляционный пакет с образом операционной системы. Когда указанные клиентские устройства подключаются к PXE-серверу, автоматически выполняется установка операционной системы на этих устройствах.

### **Развертывание образов операционных систем на устройствах с уже установленной операционной системой**

Развертывание образов операционной системы на клиентских устройствах, на которых уже установлена рабочая операционная система, выполняется с помощью задачи удаленной установки для наборов устройств.

### **Установка программ «Лаборатории Касперского» и других производителей программного обеспечения**

Администратор может создавать инсталляционные пакеты любых программ, включая программы, указанные пользователем, и устанавливать эти программы на клиентские устройства с помощью задачи удаленной установки.

## **В этом разделе**

Создание образов операционных систем .....	<a href="#">241</a>
Добавление драйверов для среды предустановки Windows (WinPE).....	<a href="#">241</a>
Добавление драйверов в инсталляционный пакет с образом операционной системы ....	<a href="#">242</a>
Настройка параметров утилиты sysprep.exe.....	<a href="#">243</a>
Развертывание операционных систем на новых устройствах в сети .....	<a href="#">244</a>
Развертывание операционных систем на клиентских устройствах .....	<a href="#">245</a>
Создание инсталляционных пакетов программ .....	<a href="#">246</a>
Выписка сертификата для инсталляционных пакетов программ .....	<a href="#">247</a>
Установка программ на клиентские устройства .....	<a href="#">248</a>



# Создание образов операционных систем

Создание образов операционных систем выполняется при помощи задачи снятия образа операционной системы эталонного устройства.

► *Чтобы создать задачу снятия образа операционной системы, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать пакет с образом операционной системы**.
4. Следуйте указаниям мастера.

В результате работы мастера создается задача Сервера администрирования **Снятие образа ОС эталонного устройства**. Задачу можно просмотреть в папке **Задачи**.

В результате выполнения задачи **Снятие образа ОС эталонного устройства** создается инсталляционный пакет, который можно использовать для развертывания операционной системы на клиентских устройствах с помощью PXE-сервера или задачи удаленной установки. Просмотреть инсталляционный пакет можно в папке **Инсталляционные пакеты**.

## Добавление драйверов для среды предустановки Windows (WinPE)

► *Чтобы добавить драйверы для среды WinPE, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.
2. В рабочей области папки **Развертывание образов устройств** нажмите на кнопку **Дополнительные действия** и в выпадающем списке выберите пункт **Настроить синхронизацию обновлений Windows Update**.

В результате откроется окно **Драйверы для среды предустановки Windows**.

3. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **Добавить**.

Откроется окно **Добавление драйвера**.

4. В окне **Добавление драйвера** укажите имя драйвера и путь к пакету установки драйвера. Путь к пакету установки можно указать при нажатии на кнопку **Выбрать** в окне **Добавление драйвера**.

5. Нажмите на кнопку **ОК**.

Драйвер будет добавлен в хранилище Сервера администрирования. Добавленный в хранилище драйвер отображается в окне **Выбор драйвера**.

6. Нажмите на кнопку **ОК** в окне **Выбор драйвера**.

Драйвер будет добавлен в среду предустановки Windows (WinPE).

## Добавление драйверов в инсталляционный пакет с образом операционной системы

- *Чтобы добавить драйверы в инсталляционный пакет с образом операционной системы, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета.

3. В окне свойств инсталляционного пакета выберите раздел **Дополнительные драйверы**.
4. В разделе **Дополнительные драйверы** нажмите на кнопку **Добавить**.

Откроется окно **Выбор драйвера**.

5. В окне **Выбор драйвера** выберите драйверы, которые вы хотите добавить в инсталляционный пакет с образом операционной системы.

Новые драйверы можно добавить в хранилище Сервера администрирования при нажатии на кнопку **Добавить** в окне **Выбор драйвера**.

6. Нажмите на кнопку **ОК**.

Добавленные драйверы отображаются в разделе **Дополнительные драйверы** в окне свойств инсталляционного пакета с образом операционной системы.

## Настройка параметров утилиты sysprep.exe

Утилита sysprep.exe используется для подготовки устройства к созданию с него образа операционной системы.

► *Чтобы настроить параметры утилиты sysprep.exe, выполните следующие действия:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета.

3. В окне свойств инсталляционного пакета выберите раздел **Параметры sysprep.exe**.
4. В разделе **Параметры sysprep.exe** укажите конфигурационный файл, который будет использоваться при развертывании операционной системы на клиентском устройстве:
  - **Использовать конфигурационный файл по умолчанию.** Выберите этот вариант, чтобы использовать файл ответов, создаваемый по умолчанию во время снятия образа операционной системы.

- **Задать пользовательские значения основных параметров.** Выберите этот вариант, чтобы задать значения параметров с помощью пользовательского интерфейса.
- **Задать конфигурационный файл.** Выберите этот вариант, чтобы использовать собственный файл ответов.

5. Нажмите на кнопку **Применить**, чтобы внесенные изменения вступили в силу.

## Развертывание операционных систем на новых устройствах в сети

► Чтобы развернуть операционную систему на новых устройствах, на которых еще не установлена операционная система, выполните следующие действия:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.
2. Нажмите на кнопку **Дополнительные действия** и в выпадающем списке выберите пункт **Управлять списком PXE-серверов в сети**.

В результате откроется окно **Свойства: Развертывание образов устройств** на разделе **PXE-серверы**.

3. В разделе **PXE-серверы** нажмите на кнопку **Добавить** и в открывшемся окне **PXE-серверы** выберите устройство, которое будет использоваться как PXE-сервер.

Добавленное устройство отобразится в разделе PXE-серверы.

4. В разделе **PXE-серверы** выберите PXE-сервер и нажмите на кнопку **Свойства**.
5. В окне свойств выбранного PXE-сервера в разделе **Параметры подключения к PXE-серверу** выполните настройку параметров подключения Сервера администрирования к PXE-серверу.

6. Выполните загрузку клиентского устройства, на котором вы хотите развернуть операционную систему.

7. В среде BIOS клиентского устройства выберите вариант установки Network boot.

Клиентское устройство подключается к PXE-серверу и отображается в рабочей области папки **Развертывание образов устройств**.

8. В блоке **Действия** по ссылке **Назначить инсталляционный пакет** выберите инсталляционный пакет, который будет использоваться для установки операционной системы на выбранное устройство.

После добавления устройства и назначения для него инсталляционного пакета развертывание операционной системы на этом устройстве начинается автоматически.

9. Для отмены развертывания операционной системы на клиентском устройстве воспользуйтесь ссылкой **Отменить установку образов ОС** в блоке **Действия**.

► Чтобы добавить устройства по MAC-адресу,

- по ссылке **Добавить MAC-адрес устройства** в папке **Развертывание образов устройств** откройте окно **Новое устройство** и укажите MAC-адрес устройства, которое вы хотите добавить;
- по ссылке **Импортировать MAC-адреса устройств из файла** в папке **Развертывание образов устройств** выберите файл, содержащий список MAC-адресов всех устройств, на которых вы хотите развернуть операционную систему.

## Развертывание операционных систем на клиентских устройствах

► Чтобы выполнить развертывание операционной системы на клиентских устройствах с уже установленной операционной системой, выполните следующие действия:

1. В дереве консоли в папке **Удаленная установка** по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)** запустите мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет с образом операционной системы.
3. Следуйте указаниям мастера.

В результате работы мастера создается задача удаленной установки операционной системы на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

# Создание инсталляционных пакетов программ

► Чтобы создать инсталляционный пакет программы, выполните следующие действия:

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на одну из кнопок:
  - **Создать инсталляционный пакет для программы «Лаборатории Касперского»**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для программы «Лаборатории Касперского»
  - **Создать инсталляционный пакет для программы, указанной пользователем**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для программы, которую запросил пользователь.
  - **Создать инсталляционный пакет с образом ОС эталонного устройства**. Выберите этот вариант, если вы хотите создать инсталляционный пакет с образом операционной системы эталонного устройства.

В результате работы мастера создается задача Сервера администрирования **Снятие образа ОС эталонного устройства**. В результате выполнения этой задачи создается инсталляционный пакет, который можно использовать для развертывания образа операционной системы с помощью PXE-сервера или задачи удаленной установки.

4. Следуйте указаниям мастера.

В результате работы мастера создается инсталляционный пакет, который можно использовать для установки программы на клиентские устройства. Просмотреть инсталляционный пакет можно в папке **Инсталляционные пакеты**.

Подробную информацию о работе с инсталляционными пакетами см. в *Руководстве по внедрению Kaspersky Security Center*.

# Выписка сертификата для инсталляционных пакетов программ

► Чтобы выписать сертификат для инсталляционного пакета программы, 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. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Свойства**.

В результате откроется окно свойств папки **Инсталляционные пакеты**.

3. В окне свойств папки **Инсталляционные пакеты** выберите раздел **Подпись автономных пакетов**.

4. В разделе **Подпись автономных пакетов** нажмите на кнопку **Задать**.

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**:
  - а. укажите файл закрытого ключа (файл с расширением prk или pem);
  - б. укажите пароль закрытого ключа;
  - с. укажите файл открытого ключа (файл с расширением cer).

6. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат для инсталляционного пакета программы.

# Установка программ на клиентские устройства

► Чтобы установить программу на клиентские устройства, выполните следующие действия:

1. В дереве консоли в папке **Удаленная установка** по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)** запустите мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет программы, которую вы хотите установить.
3. Следуйте указаниям мастера.

В результате работы мастера создается задача удаленной установки программы на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

Вы можете устанавливать Агент администрирования на клиентские устройства с операционными системами Windows, Linux и MacOS с помощью мастера развертывания защиты.

Перед выполнением удаленной установки Агента администрирования на устройство с операционной системой Linux необходимо подготовить устройство (см. раздел «Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования» на стр. [370](#)).



---

# Управление мобильными устройствами

В этом разделе описано управление мобильными устройствами, подключенными к Серверу администрирования. Информацию о подключении мобильных устройств см. в *Руководстве по внедрению Kaspersky Security Center*.

## В этом разделе

Управление мобильными устройствами с помощью MDM-политики .....	<a href="#">249</a>
Работа с командами для мобильных устройств.....	<a href="#">252</a>
Работа с сертификатами.....	<a href="#">259</a>
Добавление мобильного устройства в список управляемых устройств.....	<a href="#">264</a>
Управление мобильными устройствами Exchange ActiveSync .....	<a href="#">269</a>
Управление iOS MDM-устройствами.....	<a href="#">275</a>
Управление KES-устройствами.....	<a href="#">291</a>

## Управление мобильными устройствами с помощью MDM-политики

Для управления iOS MDM и EAS-устройствами вы можете использовать плагин управления Kaspersky Mobile Device Management 10 Service Pack1, входящий в комплект поставки Kaspersky Security Center. Kaspersky Mobile Device Management позволяет создавать групповые политики для настройки конфигурационных параметров iOS MDM и EAS-устройств. Групповая политика, позволяющая настраивать конфигурационные параметры iOS MDM и EAS-устройств без использования iPhone Configuration Utility и профиля управления Exchange Active Sync, называется MDM-политикой.

MDM-политика 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 камер, 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.

Общие принципы работы MDM-политики не отличаются от принципов работы политик, созданных для управления другими программами. Особенностью MDM-политики является то, что она назначается на группу администрирования, в которую входят Сервер iOS MDM и Сервер мобильных устройств Exchange ActiveSync (далее серверы мобильных устройств). Все параметры, заданные в MDM-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 MDM-политики с главных серверов мобильных устройств и распространяют их на мобильные устройства.

Подробные сведения о работе с MDM-политикой в Консоли администрирования Kaspersky Security Center см. в *Руководстве администратора по комплексному решению Kaspersky Security для мобильных устройств*.

## 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.

### Команды для управления мобильным устройством

Программа 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.

Команды используются на трех типах мобильных устройств:

- iOS MDM-устройство;
- KES-устройство;
- EAS-устройство.

Каждый тип устройства поддерживает свой набор команд. В таблице ниже приведен список команд для каждого типа мобильного устройства.

Для всех типов устройств в случае успешного выполнения команды **Сбросить настройки до заводских** все данные будут удалены с мобильного устройства, настройки устройства будут сброшены до заводских.

Для iOS MDM-устройства в случае успешного выполнения команды **Удалить корпоративные данные** с мобильного 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 мобильного устройства будут удалены корпоративные данные, записи в Контактах, 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.

Таблица 2. 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 <b>Удалять вместе с iOS MDM-профилем</b> .
	Синхронизировать устройство	Данные мобильного устройства синхронизированы с Сервером администрирования.

Тип мобильного устройства	Команды	Результат выполнения команды
	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.
	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.

Тип мобильного устройства	Команды	Результат выполнения команды
	Удалить корпоративные данные	Удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок <b>Удалять вместе с iOS MDM-профилем</b> .
	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 мобильного 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 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 API** введите обычный ключ API, 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 выписки сертификатов. Раздел также содержит инструкции по интеграции программы с инфраструктурой открытых ключей и по настройке поддержки Kerberos.

## 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 с ссылкой для скачивания и установки сертификата на мобильное устройство. Список всех сертификатов можно просмотреть и экспортировать в файл (см. раздел «Просмотр списка сертификатов, выписанных пользователю» на стр. [181](#)). Можно удалять и перевыпускать сертификаты, а также просматривать их свойства.

## Настройка правил выписки сертификатов

- Чтобы настроить правила выписки сертификатов, выполните следующие действия:

1. В дереве консоли откройте папку **Управление мобильными устройствами** и выберите вложенную папку **Сертификаты**.

По умолчанию папка **Управление мобильными устройствами** вложена в папку **Дополнительно**.

2. В рабочей области папки **Сертификаты** по кнопке **Настроить правила выписки 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. [262](#)).

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 **Параметры шифрования** включите и настройте шифрование выпускаемых сертификатов.

Шифрование доступно только для сертификатов общего типа.

- a. Установите флажок **Включить шифрование сертификатов**.
- b. 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.

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**.

По умолчанию папка **Управление мобильными устройствами** вложена в папку **Дополнительно**.

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 выдачу 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 выпуска 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 мобильного устройства в список управляемых устройств

Чтобы добавить мобильное устройство пользователя в список управляемых устройств, на устройство нужно доставить и установить общий сертификат. 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, выполните следующие действия:*

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 мобильного устройства.

4. В окне **Операционная система** выберите тип операционной системы мобильного устройства (Android, iOS).

Ваши дальнейшие действия в мастере добавления мобильного устройства зависят от того, какой тип операционной системы мобильного устройства вы выбрали (см. инструкции ниже).



## 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:
  - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на мобильное устройство;
  - указать файл общего сертификата.
4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте.
5. 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 общий сертификат. После установки сертификата на мобильное устройство 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. [259](#)). 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:
  - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на мобильное устройство;
  - указать файл общего сертификата.
4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте.
5. 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. Если пользователь соглашается, iOS MDM-профиль загружается на мобильное устройство. 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:
    - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на мобильное устройство;
    - указать файл общего сертификата.

4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте.
5. 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 мобильных устройств и затем подключить устройство к Серверу администрирования, выполните следующие действия:*

Для установки используется приложение Kaspersky Endpoint Security для мобильных устройств, 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 собственный 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:
  - автоматически создать общий сертификат средствами Сервера администрирования и доставить сертификат на мобильное устройство;
  - указать файл общего сертификата.
4. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте.
5. В окне мастера **Результат** нажмите на кнопку **Готово для** завершения работы мастера установки сертификатов.

В результате пакет мобильного приложения Kaspersky Endpoint Security для мобильных Android-устройств 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. [271](#)). *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. [274](#)). 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. [274](#)).
- Настраивать параметры опроса Active Directory Сервером мобильных устройств Exchange ActiveSync, в результате которого обновляется информация о почтовых ящиках пользователей и их мобильных устройствах.

Информацию о подключении мобильных устройств Exchange ActiveSync к Серверу мобильных устройств Exchange ActiveSync см. в *Руководстве по внедрению Kaspersky Security Center*.

# 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 политик** 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 **Приложения для устройства**.

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 политик** 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.

## 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.

# 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 об установке Сервера iOS MDM см. в *Руководстве по внедрению Kaspersky Security Center*.

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. [290](#)).

## 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**.

Папка **Управление мобильными устройствами** по умолчанию вложена в папку **Дополнительно**.

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** рядом с полем **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**:
    - а. укажите файл закрытого ключа (файл с расширением pkc или pem);
    - б. укажите пароль закрытого ключа;
    - с. 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. [278](#)).

## 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. [280](#)).

# 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 мобильными устройствами** 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 мобильными устройствами**.

## 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. [282](#)).

# 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. [283](#)).

## 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 мобильными устройствами** 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 мобильными устройствами**.

# 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**.

Папка **Управление мобильными устройствами** по умолчанию вложена в папку **Дополнительно**. 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 мобильными устройствами** 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 приложение 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 мобильными устройствами**.

Информация об установленном приложении отображается в свойствах мобильного устройства iOS MDM (см. раздел «Просмотр информации о iOS MDM-устройстве» на стр. [290](#)). 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. [287](#)).

## 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 мобильными устройствами** 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 мобильными устройствами**.



# 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**.

Папка **Управление мобильными устройствами** по умолчанию вложена в папку **Дополнительно**. 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. [290](#)). 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. [287](#)).

## 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. [285](#)).

## 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 мобильным устройством» на стр. [252](#));
- просматривать информацию о параметрах управления KES-устройствами (см. раздел «Просмотр информации о KES-устройстве» на стр. [294](#));
- устанавливать приложения с помощью пакетов мобильных приложений (см. раздел «Создание пакета мобильных приложений для KES-устройств» на стр. [292](#));
- отключать KES-устройства от управления (см. раздел «Отключение KES-устройства от управления» на стр. [294](#)).

Подробное описание работы с KES-устройствами и информацию о подключении KES-устройств к Серверу администрирования см. в *Руководстве по внедрению Kaspersky Security Center 10*.

# Создание пакета мобильных приложений для KES-устройств

Для создания пакета мобильных приложений для KES-устройств необходима лицензия Kaspersky Endpoint Security 10 для мобильных устройств.

► 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 из выпадающего списка 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**.

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 10 для мобильных устройств в разделе **Контейнеры**. Подробная информация о контейнерах и работе с ними приведена в документации для программы Kaspersky Endpoint Security 10 для мобильных устройств.

Вы можете поместить в контейнер стороннюю программу. Нельзя помещать в контейнер дистрибутив Kaspersky Endpoint Security 10 для мобильных устройств.

## 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.

---

# Self Service Portal

Этот раздел содержит информацию о Self Service Portal. В разделе приведены инструкции по авторизации пользователей на Self Service Portal, созданию учетных записей Self Service Portal, а также по добавлению мобильных устройств на Self Service Portal.

## В этом разделе

О Self Service Portal .....	<a href="#">296</a>
Добавление устройства .....	<a href="#">299</a>
Подключение пользователя к Self Service Portal.....	<a href="#">300</a>

## О Self Service Portal

Self Service Portal – это веб-портал, который позволяет администратору передать пользователям часть операций по управлению их мобильными устройствами. Пользователь мобильного устройства, выполнивший авторизацию на Self Service Portal, может самостоятельно добавить на Self Service Portal свое мобильное устройство. При добавлении мобильного устройства на iOS MDM-устройство устанавливается iOS MDM-профиль, на KES-устройства устанавливается Kaspersky Endpoint Security для Android, и к устройству применяются корпоративные политики (см. раздел «Добавление устройства» на стр. [299](#)). После этого мобильное устройство становится управляемым.

Self Service Portal поддерживает автоматическую авторизацию пользователей с использованием Kerberos Constrained Delegation и доменную авторизацию.

Self Service Portal поддерживает мобильные устройства с операционными системами iOS и Android.



В Self Service Portal пользователь может выполнять следующие действия:

- Загружать приложения из корпоративного магазина приложений. Приложения должны быть предварительно добавлены в корпоративный магазин приложений в Kaspersky Security Center 10 Web Console. Подробная информация о добавлении приложений в магазин приложений приведена в *Руководстве пользователя Kaspersky Security Center 10 Web Console*. Для загрузки приложений в Self Service Portal пользователю необходимо выбрать закладку **Приложения** в окне Self Service Portal.
- Самостоятельно посылать на управляемое мобильное устройство команды, например, в случае кражи или утери мобильного устройства. Для отправки команд пользователю необходимо выбрать закладку **Устройства** в окне Self Service Portal. Для каждого типа мобильного устройства поддерживается собственный набор команд (см. таблицу ниже).
- Самостоятельно разблокировать мобильное устройство по ссылке **Показать код разблокировки**, в случае если мобильное устройство было заблокировано.

Таблица 3. Список поддерживаемых команд

Тип мобильного устройства	Команды	Результат выполнения команды
iOS MDM-устройство	Заблокировать	Мобильное устройство заблокировано.
	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки устройства сброшены до заводских, мобильное устройство перестает быть управляемым.
	Удалить корпоративные данные	Удалены корпоративные данные, удален iOS MDM-профиль, удален Агент администрирования, мобильное устройство перестает быть управляемым.
KES-устройство	Заблокировать	Мобильное устройство заблокировано.

Тип мобильного устройства	Команды	Результат выполнения команды
	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки устройства сброшены до заводских, мобильное устройство перестает быть управляемым.
	Удалить корпоративные данные	Удалены корпоративные данные, удален iOS MDM-профиль, удален Агент администрирования, мобильное устройство перестает быть управляемым.
	Определить местоположение	Местоположение мобильного устройства определено и показано на Google Картах. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
	Воспроизвести звуковой сигнал	Мобильное устройство воспроизводит звуковой сигнал.
	Сфотографировать	Мобильное устройство заблокировано. Фотография выполнена фронтальной камерой мобильного устройства и сохранена на Сервере администрирования. Фотографии доступны для просмотра в журнале команд на Self Service Portal. Оператор мобильной связи взимает оплату за передачу SMS и интернет.

Self Service Portal использует глобальный список пользователей Kaspersky Security Center. Пополнение списка производится автоматически при импорте из Active Directory (см. раздел «Просмотр и изменение параметров опроса групп Active Directory» на стр. [201](#)) или вручную (см. раздел «Добавление учетной записи пользователя» на стр. [171](#)).

В случае, если доменная авторизация на Self Service Portal запрещена администратором, пользователи могут использовать для авторизации псевдонимы. Создание псевдонимов для

авторизации на Self Service Portal доступно в свойствах учетных записей пользователей (см. раздел «Подключение пользователя к Self Service Portal» на стр. [300](#)).

Администратор может предоставить пользователям следующие права для использования Self Service Portal:

- Чтение.
- Изменение.
- Подключение новых устройств.
- Отправление только информационных команд на мобильные устройства (не изменяющих состояние мобильного устройства).

Команды **Сфотографировать**, **Определить** **местоположение** являются информационными.

- Отправление команд на мобильные устройства.

## Добавление устройства

Перед добавлением мобильного устройства на Self Service Portal пользователь должен принять Лицензионное соглашение для использования Self Service Portal и выполнить авторизацию на портале.

Алгоритм добавления мобильного устройства пользователя на Self Service Portal включает в себя следующие шаги:

1. Пользователь открывает главную страницу портала.
2. Self Service Portal создает установочный пакет, после чего отображает одноразовую ссылку для скачивания пакета и QR-код, в котором зашифрована ссылка. На экране отображается время, в течение которого будет доступна ссылка для скачивания установочного пакета. Сообщение с ссылкой для скачивания установочного пакета отправляется на электронную почту пользователя.

Установочный пакет необходим для установки на мобильное устройство агента управления и применения корпоративных политик.

Создать новый установочный пакет можно только после того, как созданный ранее пакет будет удален с Сервера администрирования.

3. По ссылке **Сформировать пакет для установки на новое устройство** пользователь переходит на страницу загрузки установочного пакета с мобильного устройства, которое нужно добавить на Self Service Portal.

4. Self Service Portal определяет операционную систему мобильного устройства пользователя.

Если операционную систему мобильного устройства удалось определить автоматически, открывается страница загрузки установочного пакета. Если определить операционную систему автоматически не удалось, открывается окно для выбора операционной системы вручную.

5. Пользователь скачивает установочный пакет и устанавливает агент управления на мобильное устройство.

6. После установки агента управления устройство подключается к Серверу администрирования.

В результате мобильное устройство будет добавлено в список управляемых устройств и к нему будут применены корпоративные политики. Ссылка на информацию о подключении к Серверу администрирования отправляется на электронную почту пользователя.

## Подключение пользователя к Self Service Portal

Если использование доменной авторизации пользователей в Self Service Portal запрещено, вы можете создавать в Консоли администрирования для пользователей псевдонимы (alias accounts). С помощью псевдонимов пользователи могут выполнять авторизацию на Self Service Portal.

► Чтобы подключить пользователя (под псевдонимом) к *Self Service Portal*, выполните следующие действия:

1. В папке **Управление мобильными устройствами** выберите вложенную папку **Self Service Portal**.
2. В рабочей области папки **Self Service Portal** нажмите на кнопку **Выслать приглашение для подключения к Self Service Portal**.

В результате запустится мастер подключения пользователя к *Self Service Portal*. Следуйте шагам мастера.

3. В окне мастера **Настройка прав** по ссылке **Настройка** вы можете настроить права доступа к *Self Service Portal* пользователей и групп пользователей.

Если флажок **Больше не показывать это сообщение** установлен, то при следующем запуске мастера окно **Настройка прав** не будет отображаться.

4. В окне **Выбор адреса Self Service Portal** вы можете указать адрес *Self Service Portal*, к которому будет подключаться пользователь.

Вы можете пропустить выбор адреса *Self Service Portal*. В этом случае в тексте приглашения адрес *Self Service Portal* нужно будет указать вручную.

5. В окне **Выбор пользователей для подключения к Self Service Portal** укажите пользователей, которых нужно подключить к *Self Service Portal*.

6. В окне мастера **Настройка псевдонимов учетных записей пользователей** настройте использование псевдонимов и доменных записей пользователей для подключения к **Self Service Portal**:

- Установите флажок **Применять псевдонимы учетных записей пользователей для доступа к Self Service Portal** чтобы настроить отправку приглашений для подключения к *Self Service Portal* выбранным пользователям.

Если флажок снят, приглашение для подключения к *Self Service Portal* будет отправлено только доменным пользователям, выбранным на предыдущем шаге мастера.

- Выберите вариант **Создать псевдонимы, если они отсутствуют у пользователей**, чтобы Kaspersky Security Center автоматически создал псевдонимы для всех учетных записей, у которых нет псевдонима. Приглашения для подключения к Self Service Portal будут высланы пользователям, для которых были созданы псевдонимы. Kaspersky Security Center не создает новые псевдонимы для пользователей, у которых псевдонимы уже есть.
- Выберите вариант **Пользователям без псевдонимов высылать приглашение на доменную учетную запись**, чтобы программа не создавала автоматически псевдонимы для доменных пользователей, у которых псевдонимов нет. В случае если у пользователя нет псевдонима, приглашение для подключения к Self Service Portal будет отправлено на доменную запись.
- Установите флажок **Создать новые пароли для псевдонимов**, чтобы Kaspersky Security Center создал новые пароли для всех псевдонимов (для новых и созданных ранее). Информация о новом и старом паролях будет выслана пользователям в тексте приглашения для подключения к Self Service Portal.

Если флажок снят, пароль будет сгенерирован только для вновь созданных псевдонимов.

- Задайте количество символов пароля подключения к Self Service Portal для псевдонимов пользователей. Длина пароля по умолчанию – 16 символов.

7. В окне **Рассылка приглашений на Self Service Portal** выберите способ доставки приглашения на Self Service Portal как для новых, так и для существующих пользователей.

8. По ссылке **Редактировать сообщение** просмотрите и при необходимости отредактируйте текст приглашения.

В результате работы мастера выбранные пользователи получают приглашение с информацией для подключения к Self Service Portal. Можно создавать неограниченное количество псевдонимов для Self Service Portal для одного пользователя. После создания псевдонима он отображается в окне свойств учетной записи пользователя в разделе **Псевдонимы пользователя для Self Service Portal**. После создания псевдонима пользователя для Self Service Portal псевдоним нельзя изменить. Вы можете удалить выбранный псевдоним по кнопке с красным крестом справа от списка псевдонимов для Self Service Portal.

---

# Шифрование и защита данных

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи / утери портативного устройства, съемного диска или жесткого диска, или при доступе к данным неавторизованных пользователей и программ.

Функциональность шифрования реализована в программе Kaspersky Endpoint Security 10 для Windows. Kaspersky Endpoint Security 10 для Windows позволяет шифровать файлы, хранящиеся на локальных дисках устройств и съемных дисках, съемные диски и жесткие диски целиком.

Настройка правил шифрования выполняется с помощью Kaspersky Security Center через определение политик. Шифрование и расшифровка по заданным правилам выполняются при применении политики.

Доступность функциональности управления шифрованием определяется параметрами пользовательского интерфейса (см. раздел «Настройка интерфейса» на стр. [59](#)).

Администратор может выполнять следующие действия:

- настраивать и выполнять шифрование и расшифровку файлов на локальных дисках устройства;
- настраивать и выполнять шифрование файлов на съемных дисках;
- формировать правила доступа программ к зашифрованным файлам;
- создавать и передавать пользователю файл ключа доступа к зашифрованным файлам, если на устройстве пользователя ограничена функциональность шифрования файлов;
- настраивать и выполнять шифрование жестких дисков;
- управлять доступом пользователей к зашифрованным жестким дискам и съемным дискам (управлять учетными записями агента аутентификации, формировать и передавать пользователям блоки ответа на запрос о восстановлении имени и пароля учетной записи и ключи доступа к зашифрованным устройствам);
- просматривать статусы шифрования и отчеты о шифровании файлов.

Эти операции выполняются средствами программы Kaspersky Endpoint Security 10 для Windows. Подробные инструкции по выполнению операций и описание особенностей функциональности шифрования приведены в *Руководстве администратора Kaspersky Endpoint Security 10 для Windows*.

## В этом разделе

Просмотр списка зашифрованных устройств.....	<a href="#">304</a>
Просмотр списка событий шифрования.....	<a href="#">305</a>
Экспорт списка событий шифрования в текстовый файл .....	<a href="#">306</a>
Формирование и просмотр отчетов о шифровании .....	<a href="#">307</a>

# Просмотр списка зашифрованных устройств

► Чтобы просмотреть список устройств, информация на которых была зашифрована, выполните следующие действия:

1. Выберите в дереве консоли Сервера администрирования папку **Шифрование и защита данных**.
2. Перейдите к списку зашифрованных устройств одним из следующих способов:
  - По ссылке **Перейти к списку зашифрованных устройств** в блоке **Управление зашифрованными устройствами**.
  - В дереве консоли выберите вложенную папку **Зашифрованные устройства**.

В результате в рабочей области будет представлена информация об имеющихся в сети устройствах, на которых есть зашифрованные файлы, и устройствах, зашифрованных на уровне дисков. После того, как информация на устройстве будет расшифрована, устройство будет автоматически удалено из списка.

Вы можете сортировать информацию в списке устройств по возрастанию или убыванию данных любой из граф.



Наличие или отсутствие папки **Шифрование и защита данных** в дереве консоли определяется параметрами пользовательского интерфейса (см. раздел «Настройка интерфейса» на стр. [59](#)).

## Просмотр списка событий шифрования

В процессе выполнения задач шифрования и расшифровки данных на устройствах Kaspersky Endpoint Security 10 для Windows отправляет в Kaspersky Security Center информацию о возникающих событиях следующих типов:

- невозможно зашифровать / расшифровать файл или создать зашифрованный архив из-за нехватки места на диске;
- невозможно зашифровать / расшифровать файл или создать зашифрованный архив из-за проблем с лицензией;
- невозможно зашифровать / расшифровать файл или создать зашифрованный архив из-за отсутствия прав доступа;
- программе запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

► *Чтобы просмотреть список событий, возникших при шифровании данных на устройствах, выполните следующие действия:*

1. Выберите в дереве консоли Сервера администрирования папку **Шифрование и защита данных**.
2. Перейдите к списку событий, возникших при шифровании, одним из следующих способов:
  - По ссылке **Перейти к списку ошибок** в блоке управления **Ошибки шифрования данных**.
  - В дереве консоли выберите вложенную папку **События шифрования**.

В результате в рабочей области будет представлена информация о проблемах, возникших при шифровании данных на устройствах.

Вы можете выполнять следующие действия со списком событий шифрования:

- сортировать записи по возрастанию или убыванию данных в любой из граф;
- выполнять быстрый поиск по записям (по текстовому совпадению с подстрокой в любом поле списка);
- экспортировать сформированный список событий в текстовый файл.

Наличие или отсутствие папки **Шифрование и защита данных** в дереве консоли определяется параметрами пользовательского интерфейса (см. раздел «Настройка интерфейса» на стр. [59](#)).

## Экспорт списка событий шифрования в текстовый файл

► Чтобы экспортировать список событий шифрования в текстовый файл, выполните следующие действия:

1. Сформируйте список событий шифрования (см. раздел «Просмотр списка событий шифрования» на стр. [305](#)).
2. В контекстном меню списка событий выберите пункт **Экспортировать список**.

Откроется окно **Экспорт списка**.

3. В окне **Экспорт списка** укажите имя текстового файла со списком событий, выберите папку, в которую он будет сохранен, и нажмите на кнопку **Сохранить**.

Список событий шифрования будет сохранен в указанный файл.

# Формирование и просмотр отчетов о шифровании

Администратор может формировать следующие отчеты:

- отчет о статусе шифрования запоминающих устройств, содержащий информацию о состоянии шифрования устройств для всех групп устройств;
- отчет о правах доступа к зашифрованным устройствам, содержащий информацию о состоянии учетных записей пользователей, которые имеют доступ к зашифрованным устройствам;
- отчет об ошибках шифрования файлов и папок, содержащий информацию об ошибках, которые возникли при выполнении задач шифрования и расшифровки данных на устройствах;
- отчет о статусе шифрования управляемых устройств, содержащий информацию о соответствии состояния шифрования устройств политике шифрования;
- отчет о блокировании доступа к файлам, содержащий информацию о блокировании доступа приложений к зашифрованным файлам.

► Чтобы просмотреть отчет о шифровании устройств, выполните следующие действия:

1. В дереве консоли выберите папку **Шифрование и защита данных**.
2. Выполните одно из следующих действий:
  - По ссылке **Отчет о шифровании устройств** запустите мастер создания шаблона отчета.
  - Выберите вложенную папку **Зашифрованные устройства**, а затем по кнопке **Отчет о шифровании устройств** запустите мастер создания шаблона отчета.
3. Следуйте шагам мастера создания шаблона отчета.

В узле **Сервер администрирования** на закладке **Отчеты** появится новый отчет. Запустится процесс формирования отчета. Отчет отобразится в рабочей области закладки **Отчеты**.

- Чтобы просмотреть отчет о правах доступа к зашифрованным устройствам, выполните следующие действия:

1. В дереве консоли выберите папку **Шифрование и защита данных**.
2. Выполните одно из следующих действий:
  - По ссылке **Отчет о правах доступа к зашифрованным устройствам** в блоке **Управление зашифрованными устройствами** запустите мастер создания шаблона отчета.
  - Выберите вложенную папку **Зашифрованные устройства**, а затем по ссылке **Отчет о правах доступа к зашифрованным устройствам** запустите мастер создания шаблона отчета.
3. Следуйте шагам мастера создания шаблона отчета.

В узле **Сервер администрирования** на закладке **Отчеты** появится новый отчет. Запустится процесс формирования отчета. Отчет отобразится в рабочей области закладки **Отчеты**.

- Чтобы просмотреть отчет об ошибках шифрования файлов и папок, выполните следующие действия:

1. В дереве консоли выберите папку **Шифрование и защита данных**.
2. Выполните одно из следующих действий:
  - По ссылке **Отчет об ошибках шифрования папок и файлов** в блоке управления **Ошибки шифрования данных** запустите мастер создания шаблона отчета.
  - Выберите вложенную папку **События шифрования**, а затем по ссылке **Отчет об ошибках шифрования файлов и папок** запустите мастер создания шаблона отчета.
3. Следуйте шагам мастера создания шаблона отчета.

В узле Сервера администрирования на закладке **Отчеты** появится новый отчет. Запустится процесс формирования отчета. Отчет отобразится в рабочей области закладки **Отчеты**.

► *Чтобы просмотреть отчет о статусе шифрования устройств, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. По кнопке **Создать шаблон отчета** запустите мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. В окне **Выбор типа шаблона отчета** в разделе **Прочее** выберите пункт **Отчет о статусе шифрования устройств**.

После завершения работы мастера создания шаблона отчета в узле Сервер администрирования на закладке **Отчеты** появится новый шаблон отчета.

5. В узле нужного вам Сервера администрирования на закладке **Отчеты** выберите шаблон отчета, созданный на предыдущих шагах инструкции.

Запустится процесс формирования отчета. Отчет отобразится в рабочей области закладки **Отчеты**.

Информацию о соответствии статусов шифрования устройств и съемных дисков политике шифрования также можно просматривать в информационных панелях на закладке **Статистика** узла Сервер администрирования (см. раздел «Работа со статистической информацией» на стр. [186](#)).

► *Чтобы просмотреть отчет о блокировании доступа к файлам, выполните следующие действия:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. По кнопке **Создать шаблон отчета** запустите мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. В окне **Выбор типа шаблона отчета** в разделе **Прочее** выберите пункт **Отчет о блокировании доступа к файлам**.

После завершения работы мастера создания шаблона отчета в узле **Сервер администрирования** на закладке **Отчеты** появится новый шаблон отчета.

5. В узле **Сервер администрирования** на закладке **Отчеты** выберите шаблон отчета, созданный на предыдущих шагах инструкции.

Запустится процесс формирования отчета. Отчет отобразится в рабочей области закладки **Отчеты**.

---

# 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.

## В этом разделе

Добавление информации о новых устройствах .....	<a href="#">311</a>
Настройка критериев определения корпоративных устройств .....	<a href="#">312</a>

# 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** по ссылке **Настроить критерии определения корпоративных устройств** откройте 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**.



---

# 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 .....	<a href="#">314</a>
Создание задачи загрузки обновлений в хранилища агентов обновлений.....	<a href="#">316</a>
Настройка параметров задачи загрузки обновлений в хранилище .....	<a href="#">317</a>
Проверка полученных обновлений .....	<a href="#">317</a>
Настройка проверочных политик и вспомогательных задач .....	<a href="#">319</a>
Просмотр полученных обновлений .....	<a href="#">321</a>
Автоматическое распространение обновлений .....	<a href="#">321</a>
Отмена установленных обновлений .....	<a href="#">328</a>

# 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».

# Создание задачи загрузки обновлений в хранилища агентов обновлений

► Чтобы создать задачу 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**, раскройте папку **Дополнительно** и выберите задачу **Принудительная загрузка обновлений в хранилища агентов обновлений**.
4. 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. Результаты выполнения задачи будут использовать только теми агентами обновлений, входящие в указанную группу администрирования, для которых нет явно указанной задачи Сервера администрирования **Загрузка обновлений в хранилище**.

# 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 **Изменить 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 **Изменить параметры политики (Изменить 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 .....	<a href="#">322</a>
Автоматическое распространение обновлений на подчиненные Серверы администрирования .....	<a href="#">323</a>
Автоматическая установка обновлений программных модулей Агентов администрирования .....	<a href="#">324</a>
Назначение устройств агентами обновлений .....	<a href="#">325</a>
Удаление устройства из списка агентов обновлений .....	<a href="#">327</a>
Получение обновлений агентами обновлений .....	<a href="#">327</a>

# 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 групповой задачи» на стр. [130](#)).
  - 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. [132](#)).

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 устройств агентами обновлений

Kaspersky Security Center позволяет назначать устройства агентами обновлений. Назначение можно выполнять автоматически (с помощью Сервера администрирования) и вручную.

Если структура групп администрирования отражает топологию сети, или выделенные части сети соответствуют какой-либо группе администрирования, можно использовать автоматическое назначение агентов обновлений.

Если построение структуры групп администрирования не отражает топологию сети, рекомендуется отключить автоматическое назначение агентов обновлений, и в каждой выделенной части сети вручную назначить один или несколько устройств агентами обновлений.

Рекомендуется назначать агенты обновлений вручную из расчета 100 – 200 обслуживаемых устройств на каждый агент обновлений.

► *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**.

В результате откроется окно **Добавление агента обновлений**.

4. В окне **Добавление агента обновлений** выполните следующие действия:
  - c. 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 (см. раздел «Агент обновлений» на стр. [87](#)).
  - d. Укажите набор устройств, на которые агент обновлений будет распространять обновления. Вы можете указать группу администрирования или подсеть Network Location Awareness (NLA-подсеть).

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 номер SSL-порта, адрес и номер порта IP-рассылки для многоадресной IP-рассылки, а также состав данных, распространяемых агентом обновлений (агент обновлений может распространять обновления и / или инсталляционные пакеты).
- В разделе **Область действия** укажите область, на которую агент обновлений распространяет обновления (группы администрирования и / или NLA-подсеть).
- 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.

В результате выбранные устройства будут выполнять роль агентов обновлений.

► *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** установите флажок **Назначать агенты обновлений автоматически**.

Если автоматическое назначение устройств агентами обновлений включено, нельзя 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 устройств агентами обновлений» на стр. [325](#)).

## 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 получения обновлений**:
  - Нажмите на кнопку **Выбрать**, чтобы выбрать уже сформированную задачу получения обновлений агентом обновлений.
  - Нажмите на кнопку **Новая задача**, чтобы создать задачу получения обновлений агентом обновлений.

Задача получения обновлений агентом обновлений – локальная задача. Для каждого устройства, выполняющего роль агента обновлений, задачу получения обновлений требуется создавать отдельно.

В результате агент обновлений будет получать обновления из указанного источника.

## Отмена установленных обновлений

► Чтобы отменить установленные обновления, 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 отменить.
3. В контекстном меню обновления выберите **Удалить файлы обновлений**.
4. Запустите задачу обновления (см. раздел «Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства» на стр. [227](#)).

В результате выполнения задачи установленное обновление на клиентском устройстве будет отменено и примет статус **Не установлено**.



---

# 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.....	<a href="#">329</a>
Добавление ключа в хранилище Сервера администрирования .....	<a href="#">330</a>
Удаление ключа Сервера администрирования.....	<a href="#">331</a>
Распространение ключа на клиентские устройства .....	<a href="#">331</a>
Автоматическое распространение ключа .....	<a href="#">332</a>
Создание и просмотр отчета об использовании ключей.....	<a href="#">333</a>

## Просмотр информации об используемых ключах

- Чтобы просмотреть информацию об используемых ключах, выберите в дереве консоли в папке **Управление программами** вложенную папку **Лицензии на ПО 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. [141](#)).

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 в папке **Управление программами** выберите вложенную папку **Лицензии на ПО Лаборатории Касперского**.
2. Запустите задачу добавления ключа одним из следующих способов:
  - в контекстном меню списка ключей выберите пункт **Добавить ключ**;
  - по ссылке **Добавить 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** (см. раздел «Варианты лицензирования Kaspersky Security Center» на стр. [65](#)) и **Управление мобильными устройствами** (см. раздел «Варианты лицензирования Kaspersky Security Center» на стр. [65](#)). Можно добавить (см. раздел «Добавление ключа в хранилище Сервера администрирования» на стр. [330](#)) 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 в папке **Управление программами** вложенную папку **Лицензии на ПО 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 в папке **Управление программами** вложенную папку **Лицензии на ПО 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 параметрах ключей.

---

# Хранилища данных

Этот раздел содержит информацию о данных, которые хранятся на Сервере администрирования и используются для отслеживания состояния клиентских устройств и 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. [321](#));
- список оборудования, обнаруженного в сети;
- ключи, обнаруженные на клиентских устройствах (см. раздел «Работа с ключами программ» на стр. [329](#));
- 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.....	<a href="#">335</a>
Инсталляционные пакеты .....	<a href="#">335</a>
Карантин и резервное хранилище .....	<a href="#">336</a>
Файлы с отложенной обработкой.....	<a href="#">340</a>

# 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 **Хранилище** 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 (см. раздел «Создание инсталляционных пакетов программ» на стр. [246](#)) или использовать уже созданный инсталляционный пакет. Список созданных инсталляционных пакетов содержится в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

Подробную информацию о работе с инсталляционными пакетами см. в *Руководстве по внедрению Kaspersky Security Center*.

# 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.

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.

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 .....	<a href="#">337</a>
Просмотр свойств файла, помещенного в хранилище .....	<a href="#">337</a>
Удаление файлов из хранилища .....	<a href="#">338</a>
Восстановление файлов из хранилища .....	<a href="#">338</a>
Сохранение файла из хранилища на диск.....	<a href="#">339</a>
Проверка файлов на карантине .....	<a href="#">339</a>



# 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. Откройте окно свойств файла одним из следующих способов:

- В контекстном меню файла выберите пункт **Свойства**.
- По ссылке **Открыть свойства объекта** в блоке работы с выбранным файлом.

## 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.

## Файлы с отложенной обработкой

Информация о файлах с отложенной обработкой, обнаруженных на клиентских устройствах, содержится в папке **Хранилища**, во вложенной папке **Файлы с отложенной обработкой**.

Отложенная обработка и лечение файлов программой защиты осуществляются по требованию или после наступления определенного события. Вы можете настраивать параметры отложенного лечения файлов.

## Лечение файла с отложенной обработкой

► Чтобы запустить лечение файла с отложенной обработкой, выполните следующие действия:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Файлы с отложенной обработкой**.
2. В рабочей области папки **Файлы с отложенной обработкой** 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 **Файлы с отложенной обработкой**. Если лечение файла невозможно, программа защиты, установленная на устройстве, удаляет файл с устройства. Запись о файле удаляется из списка папки **Файлы с отложенной обработкой**.

## Сохранение файла с отложенной обработкой на диск

Kaspersky Security Center позволяет сохранять на диск копии файлов с отложенной обработкой, обнаруженные на клиентских устройствах. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

► *Чтобы сохранить копию файла с отложенной обработкой на диск, выполните следующие действия:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Файлы с отложенной обработкой**.
2. В рабочей области папки **Файлы с отложенной обработкой** 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 файл с отложенной обработкой, сохранит копию файла в указанную папку.

## Удаление файлов из папки «Файлы с отложенной обработкой»

► Чтобы удалить файл из папки **Файлы с отложенной обработкой**, выполните следующие действия:

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Файлы с отложенной обработкой**.
2. В рабочей области папки **Файлы с отложенной обработкой** 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 **Файлы с отложенной обработкой**.

---

# Kaspersky Security Network (KSN)

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN). Приведена информация о KSN, а также инструкции по включению KSN, настройке доступа к KSN, по просмотру статистики использования прокси-сервера KSN.

## О KSN

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 KSN» на стр. [345](#)).

Программа предлагает присоединиться к KSN во время установки программы и во время работы Мастера первоначальной настройки (см. раздел «Мастер первоначальной настройки Сервера администрирования» на стр. [72](#)). Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с программой (см. раздел «Включение и отключение KSN» на стр. [347](#)).

Клиентские устройства, находящиеся под управлением Сервера администрирования, взаимодействуют с KSN при помощи 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.
- 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 KSN» на стр. [345](#)).

## 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.

Участвуя в программе Kaspersky Security Network, вы соглашаетесь в автоматическом режиме предоставлять в «Лабораторию Касперского» следующие данные, полученные в результате работы Kaspersky Security Center на устройстве:

- название, версия, используемый язык программного продукта, для которого устанавливается обновление;
- версия базы данных обновлений, используемой программным обеспечением при установке;
- результат установки обновления;
- идентификатор устройства и версия используемого на нем Агента администрирования;
- параметры программного обеспечения, используемые при установке обновлений, такие как идентификаторы выполненных операций, коды результатов выполнения операций.



В случае отказа от участия в программе Kaspersky Security Network перечисленные выше данные не передаются в «Лабораторию Касперского».

Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями и действующими правилами «Лаборатории Касперского». «Лаборатория Касперского» использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных данных и иных конфиденциальных данных. Исходная полученная информация хранится в зашифрованном виде и уничтожается по мере накопления (два раза в год). Данные общей статистики хранятся бессрочно.

Предоставление данных является добровольным. Функцию предоставления данных можно в любой момент включить или выключить в окне настройки программы.

## Настройка доступа к KSN

► Чтобы настроить доступ Сервера администрирования к KSN, выполните следующие действия:

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить доступ к KSN.
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 KSN.

5. Установите флажок **Я согласен участвовать в Kaspersky Security Network**.

Если флажок установлен, клиентские устройства будут передавать результаты установки патчей в «Лабораторию Касперского». Установив флажок, вы должны прочитать и принять условия Положения о KSN.

Если вы используете Локальный KSN (инфраструктура KSN расположена не на серверах «Лаборатории Касперского», а, например, внутри сети интернет-провайдера), установите флажок **Настроить Локальный KSN** и по кнопке **Выбрать файл с параметрами KSN** загрузите параметры Локального KSN (файлы с расширениями rkcs7, rem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами Локального KSN.

Работу с Локальным KSN поддерживают следующие программы «Лаборатории Касперского»:

- Kaspersky Security Center 10 Service Pack 1 и выше;
- Kaspersky Endpoint Security 10 Service Pack 1 и выше;
- Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2;
- Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент.

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.

6. 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.
7. 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**.

8. Нажмите на кнопку **ОК**.

В результате параметры доступа к KSN будут сохранены.

## Включение и отключение KSN

► Чтобы включить KSN, выполните следующие действия:

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить 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. Установите флажок **Использовать Сервер администрирования как прокси-сервер**.

В результате будет включена служба прокси-сервера KSN.

5. Установите флажок **Я согласен участвовать в Kaspersky Security Network**.

В результате KSN будет включен.

Если флажок установлен, клиентские устройства будут передавать результаты установки патчей в «Лабораторию Касперского». Установив флажок, вы должны прочитать и принять условия Положения о KSN.

6. Нажмите на кнопку **ОК**.

► *Чтобы выключить KSN, выполните следующие действия:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить 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 **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN, или снимите флажок **Я согласен участвовать в Kaspersky Security Network**.

Если флажок снят, клиентские устройства не будут передавать результаты установки патчей в «Лабораторию Касперского».

Если вы используете Локальный KSN, снимите флажок **Настроить Локальный KSN**

В результате KSN 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.

---

# Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

## В этом разделе

Способы получения технической поддержки .....	<a href="#">350</a>
Техническая поддержка по телефону .....	<a href="#">351</a>
Техническая поддержка через Kaspersky CompanyAccount .....	<a href="#">351</a>

## Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе (см. раздел «Источники информации о программе» на стр. [21](#)), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (<http://support.kaspersky.ru/support/rules>).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (<http://support.kaspersky.ru/support/contacts>);
- 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» (<http://support.kaspersky.ru/support/contacts>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (<http://support.kaspersky.ru/support/rules>).

## 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 ([http://support.kaspersky.ru/faq/companyaccount\\_help](http://support.kaspersky.ru/faq/companyaccount_help)).



---

# Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

## В этом разделе

Дополнительные возможности.....	<a href="#">353</a>
Особенности работы с интерфейсом управления .....	<a href="#">383</a>
Справочная информация .....	<a href="#">385</a>

## 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 .....	<a href="#">354</a>
Автономные пользователи.....	<a href="#">354</a>
События в работе программ .....	<a href="#">358</a>
Определение уровня важности события о превышении лицензионного ограничения .....	<a href="#">359</a>
Уведомление о событиях с помощью исполняемого файла.....	<a href="#">360</a>
Работа с программой Kaspersky Security для виртуальных сред.....	<a href="#">361</a>
Отслеживание состояния антивирусной защиты с помощью информации в системном реестре.....	<a href="#">361</a>
Кластеры и массивы серверов.....	<a href="#">363</a>
Алгоритм установки патча для программы «Лаборатории Касперского» в кластерной модели .....	<a href="#">363</a>

Поиск устройств .....	<a href="#">364</a>
Подключение к устройствам с помощью Windows Desktop Sharing .....	<a href="#">366</a>
Об используемых учетных записях .....	<a href="#">367</a>
Работа с внешними инструментами.....	<a href="#">367</a>
Экспорт списков из диалоговых окон .....	<a href="#">368</a>
Режим клонирования диска Агента администрирования .....	<a href="#">368</a>
Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования .....	<a href="#">370</a>
Резервное копирование и восстановление данных Сервера администрирования .....	<a href="#">372</a>
Резервное копирование и восстановление данных в интерактивном режиме.....	<a href="#">380</a>
Установка программы с помощью групповых политик Active Directory .....	<a href="#">381</a>

## 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.

## 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 скачивания обновлений.

## В этом разделе

Создание профиля подключения к Серверу администрирования для автономных пользователей.....	<a href="#">356</a>
Создание правила переключения Агента администрирования .....	<a href="#">357</a>

# 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:
    - а. Откройте окно свойств выбранного устройства.
    - б. В разделе **Программы** окна свойств устройства выберите Агент администрирования.
    - в. 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 только профиль <Без подключения>. Профиль недоступен для изменения и удаления. В нем 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 <Без подключения> применяется в условиях отключения устройств от сети.

5. В открывшемся окне **Новый профиль** настройте параметры профиля подключения и установите флажок **Активировать автономные политики**.

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 автономных пользователей.

## Создание правила переключения Агента администрирования

- *Чтобы создать правило 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.
2. Выполните одно из следующих действий:
  - Если вы хотите создать правило переключения 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 переключения 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 **Переключение профилей** нажмите на кнопку **Добавить**.
- 5. В открывшемся окне **Новое правило** настройте параметры правила переключения и установите флажок **Правило включено**, чтобы включить использование правила.

В результате будет создано правило переключения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в правиле профиль подключения.

Правила переключения проверяются на соответствие характеристикам сети в том порядке, в котором они представлены в списке. Если характеристики сети соответствуют нескольким правилам, будет использоваться первое из них. Вы можете изменить порядок

следования правил в списке с помощью кнопок



и



.

## События в работе программ

Kaspersky Security Center позволяет получать информацию о событиях в работе Сервера администрирования и других программ «Лаборатории Касперского», установленных на клиентских устройствах.

Для программ «Лаборатории Касперского» предусмотрено четыре уровня важности событий:

- **Критическое событие.**
- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

Вы можете настроить правила обработки событий отдельно для каждого уровня важности.

См. также

Настройка общих параметров Сервера администрирования ..... [102](#)

## Определение уровня важности события о превышении лицензионного ограничения

Kaspersky Security Center позволяет получать информацию о событиях превышения лицензионного ограничения программ «Лаборатории Касперского», установленных на клиентских устройствах.

Уровень важности событий о превышении лицензионного ограничения определяется по следующим правилам:

- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 90% – 100% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Информационное сообщение**.
- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 100% – 110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Предупреждение**.
- Если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Критическое событие**.

См. также

Настройка общих параметров Сервера администрирования ..... [102](#)

## Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору.

Таблица 4. Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события
%COMPUTER%	Имя устройства, на котором произошло событие
%DOMAIN%	Домен
%EVENT%	Событие
%DESCR%	Описание события
%RISE_TIME%	Время возникновения
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Название задачи
%KL_PRODUCT%	Агент администрирования Kaspersky Security Center
%KL_VERSION%	Номер версии Агента администрирования
%HOST_IP%	IP-адрес
%HOST_CONN_IP%	IP-адрес соединения



## Пример

Для уведомления о событии используется исполняемый файл (например, *script1.bat*), внутри которого запускается другой исполняемый файл (например, *script2.bat*) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл *script1.bat*, который, в свою очередь, запустит файл *script2.bat* с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

## 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 3.0. Подробнее см. в *Руководстве администратора Kaspersky Security для виртуальных сред 3.0*.

## 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 5. 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).
	8	Включена, используются параметры, настроенные пользователем.
	9	Сбой в работе.

Ключ (тип данных)	Значение	Описание
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.

## 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.

## 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 ..... [102](#)

## 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. [403](#)).

Полнотекстовый поиск в окне **Поиск** доступен:

- на закладке **Сеть** в поле **Комментарий**;
- на закладке **Оборудование** в полях **Устройство**, **Производитель**, **Описание**.

## 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.

## Об используемых учетных записях

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)**.

## 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**.

## 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**.

## 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. [153](#)).
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`.

## **Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования**

► *Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования, выполните следующие действия:*

1. Выполните проверку конфигурации устройства:
  - a. Проверьте, что возможно подключение к устройству с помощью SSH клиентской программы (например, программа PuTTY).

Если вы не можете подключиться к устройству, откройте файл `/etc/ssh/sshd_config` и убедитесь, что следующие параметры имеют значения:

```
PasswordAuthentication no  
ChallengeResponseAuthentication yes
```

Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду `sudo service ssh restart`.

- b. Отключите пароль запроса Sudo для учетной записи пользователя, которая используется для подключения к устройству.

Используйте команду `sudo visudo`, чтобы открыть конфигурационный файл `sudoers`. В открытом файле укажите: `username ALL = (ALL) NOPASSWD: ALL`. В этом случае `username` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH.

- c. Сохраните и закройте файл `sudoers`.
- d. Повторно подключитесь к устройству через SSH и проверьте, что служба Sudo не требует пароль, с помощью команды `sudo whoami`.

## 2. Загрузите и создайте инсталляционный пакет:

- a. Перед установкой на устройство убедитесь, что на нем установлены зависимости (программы, библиотеки) для данного пакета.

Вы можете самостоятельно посмотреть зависимости для каждого пакета, используя утилиты, специфичные для того дистрибутива Linux, на который будет устанавливаться пакет. С информацией об утилитах вы можете ознакомиться в документации к вашей операционной системе.

- b. Загрузите инсталляционный пакет Агент администрирования.
- c. Для создания пакета удаленной установки используйте файлы:
  - `klagent.kpd`;
  - `akinstall.sh`;
  - deb- или rpm-пакет Агента администрирования.

3. Создайте задачу удаленной установки программы с параметрами:

- В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
- В окне **Выбор учетной записи** для запуска задачи укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

4. Запустите задачу удаленной установки программы.

Установка может завершиться ошибкой, если вы устанавливаете Агент администрирования с использованием протокола SSH на устройства с операционными системами Fedora версии ниже 20. В этом случае для успешной установки Агента администрирования в файле `/etc/sudoers` закомментируйте параметр `Defaults requiretty`. Подробное описание того, почему параметр `Defaults requiretty` может вызвать проблемы при подключении по SSH, вы можете найти на сайте системы отслеживания проблем Bugzilla ([https://bugzilla.redhat.com/show\\_bug.cgi?id=1020147](https://bugzilla.redhat.com/show_bug.cgi?id=1020147)).

## 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 `klbackup` 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 klbackup.

## В этом разделе

Создание задачи резервного копирования данных .....	<a href="#">373</a>
Утилита резервного копирования и восстановления данных (klbackup) .....	<a href="#">374</a>
Резервное копирование и восстановление данных в интерактивном режиме.....	<a href="#">375</a>
Резервное копирование и восстановление данных в неинтерактивном режиме .....	<a href="#">376</a>
Перенос Сервера администрирования на другое устройство .....	<a href="#">378</a>

## 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. [375](#));
- неинтерактивном (см. раздел «Резервное копирование и восстановление данных в неинтерактивном режиме» на стр. [376](#)).

## 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 klbackup, 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 klbackup 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 2006-06-19 # 11-30-18` сохранится информация о состоянии Сервера администрирования на дату 19 июня 2006 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 `klbackup`, 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.

## Резервное копирование и восстановление данных в интерактивном режиме

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 баз 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.

## 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 msi 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.

## Особенности работы с интерфейсом управления

### В этом разделе

Как вернуть исчезнувшее окно свойств.....	<a href="#">383</a>
Как перемещаться по дереву консоли .....	<a href="#">384</a>
Как открыть окно свойств объекта в рабочей области.....	<a href="#">384</a>
Как выбрать группу объектов в рабочей области .....	<a href="#">384</a>
Как изменить набор граф в рабочей области .....	<a href="#">385</a>




## 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 меню Консоли администрирования выберите пункт **Вид → Добавить или удалить графы**.
3. В открывшемся окне 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

Использование агента обновлений в качестве шлюза .....	<a href="#">386</a>
Использование масок в строковых переменных .....	<a href="#">387</a>
Команды контекстного меню .....	<a href="#">387</a>
О менеджере соединений .....	<a href="#">392</a>
Права пользователя для управления мобильными устройствами Exchange ActiveSync .	<a href="#">392</a>
Об администраторе виртуального Сервера .....	<a href="#">394</a>
Список управляемых устройств. Значение граф .....	<a href="#">395</a>
Статусы устройств, задач и политик .....	<a href="#">399</a>
Значки статусов файлов в Консоли администрирования.....	<a href="#">401</a>
Использование регулярных выражений в строке поиска .....	<a href="#">403</a>

## Использование агента обновлений в качестве шлюза

Если Сервер администрирования находится вне демилитаризованной зоны (DMZ), Агенты администрирования, находящиеся в демилитаризованной зоне, теряют возможность соединения с ним.

Для соединения Сервера администрирования с Агентами администрирования в качестве шлюза можно использовать агент обновлений. Агент обновлений предоставляет Серверу администрирования порт для создания соединения. В момент запуска Сервер администрирования подключается к агенту обновлений и не разрывает соединение с ним в течение всего времени работы.

Получив сигнал от Сервера администрирования, агент обновлений посылает Агентам администрирования UDP-сигнал на подключение к Серверу администрирования. При получении сигнала Агенты администрирования подключаются к агенту обновлений, который передает информацию между ними и Сервером администрирования.

# 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.

## Команды контекстного меню

В этом разделе содержится перечень объектов Консоли администрирования и соответствующий им набор пунктов контекстного меню (см. таблицу ниже).

Таблица 6. 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.

Объект	Пункт меню	Назначение пункта меню
	<b>Вид → Мелкие значки</b>	Отображать объекты в рабочей области в виде мелких значков.
	<b>Вид → Список</b>	Отображать объекты в рабочей области в виде списка.
	<b>Вид → Таблица</b>	Отображать объекты в рабочей области в виде таблицы.
	<b>Вид → Настроить</b>	Настроить отображение элементов Консоли управления.
<b>Kaspersky Security Center</b>	<b>Создать → Сервер администрирования</b>	Добавить в дерево консоли Сервер администрирования.
<b>&lt;Имя Сервера администрирования&gt;</b>	<b>Подключиться к Серверу администрирования</b>	Подключиться к Серверу администрирования.
	<b>Отключиться от Сервера администрирования</b>	Отключиться от Сервера администрирования.
<b>Управляемые устройства</b>	<b>Установить программу</b>	Запустить мастер удаленной установки программы.
	<b>Вид → Настройка интерфейса</b>	Настроить отображение элементов интерфейса.
	<b>Удалить</b>	Удалить Сервер администрирования из дерева консоли.
	<b>Установить программу</b>	Запустить мастер удаленной установки для группы администрирования.

Объект	Пункт меню	Назначение пункта меню
	<b>Обнулить счетчик вирусов</b>	Обнулить счетчики вирусов для устройств, входящих в состав группы администрирования.
	<b>Вирусная активность</b>	Создать отчет о вирусной активности устройств, входящих в состав группы администрирования.
	<b>Создать → Группу</b>	Создать группу администрирования.
	<b>Все задачи → Создать структуру групп</b>	Создать структуру групп администрирования на основе структуры доменов или Active Directory.
	<b>Все задачи → Показать сообщение</b>	Запустить мастер создания сообщения для пользователей устройств, входящих в группу администрирования.
<b>Управляемые устройства → Серверы администрирования</b>	<b>Создать → Подчиненный Сервер администрирования</b>	Запустить мастер добавления подчиненного Сервера администрирования.
	<b>Создать → Виртуальный Сервер администрирования</b>	Запустить мастер добавления виртуального Сервера администрирования.
<b>Выборки устройств</b>	<b>Создать → Новая выборка</b>	Создать выборку устройств.
	<b>Все задачи → Импортировать</b>	Импортировать выборку из файла.
<b>Управление программами → Категории программ</b>	<b>Создать → Категория</b>	Создать категорию программ.

Объект	Пункт меню	Назначение пункта меню
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 → Лицензии на ПО «Лаборатории Касперского»	Добавить 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.
Управление программами → Учет сторонних лицензий	Создать → Группу лицензионных программ	Создать группу лицензионных программ.
Управление мобильными устройствами → Мобильные устройства	Создать → Мобильное устройство	Подключить новое мобильное устройство пользователя.
Управление	Создать → Сертификат	Создать сертификат.

Объект	Пункт меню	Назначение пункта меню
мобильными устройствами → Сертификаты	Создать → Мобильное устройство	Подключить новое мобильное устройство пользователя.
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.
	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 о версиях баз	Создать и просмотреть отчет о версиях баз.

Объект	Пункт меню	Назначение пункта меню
	<b>Все задачи → Очистить хранилище обновлений</b>	Очистить хранилище обновлений на Сервере администрирования.
<b>Хранилища → Оборудование</b>	<b>Создать → Устройство</b>	Создать сетевое устройство.

## 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.

## 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 7. 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"	Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=Mobile Mailbox Policies,CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Название домена>" -InheritanceType All -AccessRight GenericAll

Доступ	Объект	Командлет
Чтение	Ветка "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC= yourdomain"	Add-ADPermission -User <Имя пользователя или группы> -Identity "CN=<Название организации>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Название домена>" -InheritanceType All -AccessRight GenericRead
Чтение и запись	Свойства msExchMobileMailboxPolicyLink и msExchOmaAdminWirelessEnable для объектов в Active Directory	Add-ADPermission -User <Имя пользователя или группы> -Identity "DC=<Название домена>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable
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).

## Об администраторе виртуального Сервера

Администратор сети организации, находящейся под управлением виртуального Сервера, будет запускать Kaspersky Security Center 10 Web Console для просмотра сведений о состоянии антивирусной безопасности сети под именем учетной записи, указанной в этом окне.

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.

## Список управляемых устройств. Значение граф

В таблице ниже представлены названия и описания граф списка управляемых устройств.

Таблица 8. 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. <a href="#">399</a> ).
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 програма 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.

Название графы	Значение
Статус	Текущий статус клиентского устройства ( <i>ОК</i> , <i>Критический</i> , <i>Предупреждение</i> ).
Описание статуса	<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"> <li>• Не установлена программа защиты;</li> <li>• Найдено много вирусов;</li> <li>• Уровень постоянной защиты отличается от уровня, установленного администратором;</li> <li>• Давно не выполнялся поиск вирусов;</li> <li>• Базы устарели;</li> <li>• Давно не подключался;</li> <li>• Есть необработанные объекты;</li> <li>• Требуется перезагрузка;</li> <li>• Установлены несовместимые программы;</li> <li>• Обнаружены уязвимости в программах;</li> <li>• Давно не выполнялся поиск обновлений Windows;</li> <li>• Определенное состояние шифрования данных;</li> <li>• Параметры мобильного устройства не соответствуют политике;</li> <li>• Есть необработанные инциденты;</li> <li>• Срок действия лицензии скоро истечет.</li> </ul> <p>Статус устройства изменяется только на <i>Критический</i> по следующим причинам:</p> <ul style="list-style-type: none"> <li>• Срок действия лицензии истек;</li> <li>• Потеряно соединение с клиентским устройством;</li> </ul>

Название графы	Значение
	<ul style="list-style-type: none"> <li>• Выключена защита;</li> <li>• Не запущена программа защиты.</li> </ul> <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. Если статус, присвоенный устройству управляемыми программами, не совпадает со статусом, присвоенным Kaspersky Security Center, в Консоли администрирования отображается статус, наиболее критичный для безопасности устройства. Например, если одна из управляемых программ присвоила устройству статус <i>Критический</i>, а Kaspersky Security Center – статус <i>Предупреждение</i>, то в Консоли администрирования для устройства отобразится статус <i>Критический</i> и описание это статуса от управляемой программы.</p>
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	Статус постоянной защиты ( <i>Запускается, Выполняется,</i>





Название графы	Значение
защиты	<i>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.
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.
Статус шифрования	Статус шифрования данных клиентского устройства.
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.














Название графы	Значение
Статус защиты от спама	Статус защиты от спама ( <i>Выполняется, Запускается, Остановлена, Приостановлена, Сбой, Неизвестно</i> ).
Статус защиты данных от утечек	Статус защиты от утечки данных ( <i>Выполняется, Запускается, Остановлена, Приостановлена, Сбой, Неизвестно</i> ).
Статус защиты для серверов совместной работы	Статус контентной фильтрации ( <i>Выполняется, Запускается, Остановлена, Приостановлена, Сбой, Неизвестно</i> ).
Статус антивирусной защиты почтовых серверов	Статус антивирусной защиты почтовых серверов ( <i>Выполняется, Запускается, Остановлена, Приостановлена, 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 9. 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> .

Значок	Статус
	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>ОК</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.
	Активная политика.
	Неактивная политика.












Значок	Статус
	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. Значки сигнализируют о статусах, присвоенных файлам управляемыми программами «Лаборатории Касперского» на клиентских устройствах. Значки отображаются в рабочей области папок **Карантин**, **Резервное хранилище** и **Файлы с отложенной обработкой**.

Таблица 10. Соответствие значков статусам файлов

Значок	Статус
	Файл со статусом <i>Заражен</i> .
	Файл со статусом <i>Предупреждение</i> или <i>Возможно зараженный</i> .

Значок	Статус
	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 <b>Карантин</b> со статусом <i>Не заражен, 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 <b>Резервное хранилище</b> со статусом <i>Не заражен, 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 <b>Файлы с отложенной обработкой</b> со статусом <i>Не заражен, 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.

# 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 флажок **Группировать программы по названию** снят.

---

# Глоссарий

## Е

### EAS-устройство

Мобильное устройство, которое подключается к Серверу администрирования по протоколу Exchange ActiveSync. По протоколу Exchange ActiveSync могут подключаться и управляться устройства с операционными системами iOS, Android, Windows Phone®.

## И

### iOS MDM-профиль

Набор параметров подключения мобильных устройств iOS к Серверу администрирования. iOS MDM-профиль устанавливается пользователем на мобильное устройство, после чего это мобильное устройство подключается к Серверу администрирования.

### iOS MDM-устройство

Мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM. По протоколу iOS MDM могут подключаться и управляться устройства с операционной системой iOS.

## К

### Kaspersky Security Network (KSN)

Инфраструктура облачных 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.

## KES-устройство

Мобильное устройство, которое подключается к Серверу администрирования и управляется с помощью мобильного приложения Kaspersky Endpoint Security для Android

## M

### MDM-политика

Набор параметров работы программы, который применяется для управления мобильными устройствами через Kaspersky Security Center. Для управления разными типами мобильных устройств используются разные параметры работы программы. Политика включает в себя параметры для полной настройки всей функциональности программы.

## P

### Provisioning-профиль

Набор параметров для работы приложений на мобильных устройствах iOS. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

## W

### Windows Server Update Services (WSUS)

Программа, которая используется для распространения обновлений программ Microsoft на компьютерах пользователей в сети организации.

## А

### Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами «Лаборатории Касперского», установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ компании для Windows. Для программ «Лаборатории Касперского» для Novell®, Unix™ и Mac существуют отдельные версии Агента администрирования.

### Агент аутентификации

Интерфейс, позволяющий пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы после шифрования системного жесткого диска.

### Агент обновлений

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в составе группы администрирования и / или широковебательного домена. Агенты обновлений предназначены для уменьшения нагрузки на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Агенты обновлений могут быть назначены автоматически Сервером администрирования или вручную администратором.

### Административные права

Уровень прав и полномочий пользователя для администрирования объектов Exchange внутри организации Exchange.

### Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

## Активный ключ

Ключ, используемый в текущий момент для работы программы.

## Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами «Лаборатории Касперского» и обновляются каждый час.

## В

### Веб-сервер Kaspersky Security Center

Компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

### Виртуальный Сервер администрирования

Компонент программы Kaspersky Security Center, предназначенный для управления системой защиты сети организации-клиента.



Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования использует для работы базу данных главного Сервера администрирования: задачи резервного копирования и восстановления данных, проверки и получения обновлений не поддерживаются на виртуальном Сервере. Эти задачи решаются в рамках главного Сервера администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

## Вирусная атака

Ряд целенаправленных попыток заразить устройство вирусом.

## Владелец устройства

Владелец устройства – это пользователь устройства, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с устройством.

## Внутренние пользователи

Учетные записи внутренних пользователей используются для работы с виртуальными Серверами администрирования. Под именем учетной записи внутреннего пользователя администратор виртуального Сервера может запускать Kaspersky Security Center 10 Web Console для просмотра сведений о состоянии антивирусной безопасности сети. 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.

## Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

## Восстановление данных Сервера администрирования

Восстановление данных Сервера администрирования при помощи утилиты резервного копирования на основании информации, сохраненной в резервном хранилище. Утилита позволяет восстанавливать:

- информационную базу Сервера администрирования (политики, задачи, параметры программы, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

## Г

### Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ «Лаборатории Касперского». Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

### Группа лицензионных программ

Группа программ, созданная на основании заданных администратором критериев (например, по производителю), для которых ведется учет установок на клиентских устройствах.

## Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

## Д

### Демилитаризованная зона (DMZ)

Демилитаризованная зона – это сегмент локальной сети, в которой находятся серверы, отвечающие на запросы из глобальной сети. В целях обеспечения безопасности локальной сети организации доступ в локальную сеть из демилитаризованной зоны ограничен и защищен сетевым экраном.

### Домашний Сервер администрирования

Домашний Сервер администрирования – это Сервер администрирования, который был задан при установке Агента администрирования. Домашний Сервер администрирования может использоваться в параметрах профилей подключения Агента администрирования.

### Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

### Доступное обновление

Пакет обновлений модулей программы «Лаборатории Касперского», в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

## З

### Задача

Функции, выполняемые программой «Лаборатории Касперского», реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

### Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

## И

### Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы «Лаборатории Касперского» при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы.

## К

### Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые программы «Лаборатории Касперского».

## Консоль администрирования

Компонент программы Kaspersky Security Center, предоставляющий пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

## Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

## Л

### Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском устройстве.

## М

### Магазин приложений

Компонент программы Kaspersky Security Center. Магазин приложений используется для установки приложений на Android-устройства пользователей. В магазине приложений можно публиковать арк-файлы приложений и ссылки на приложения в Google Play.

## О

### Общий сертификат

Сертификат, предназначенный для идентификации мобильного устройства пользователя.

## П

### Подсеть Network Location Awareness

Подсеть Network Location Awareness (NLA-подсеть) это подсеть из набора устройств, заданных вручную. В рамках функциональности Kaspersky Security Center NLA-подсеть может использоваться для формирования вручную набора устройств, на которые агент обновлений будет распространять обновления.

### Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на компьютерах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

### Профиль

Набор параметров поведения мобильных устройств Exchange ActiveSync при подключении к серверу Microsoft Exchange.

## Р

### Ролевая группа

Группа пользователей мобильных устройств Exchange ActiveSync, которые обладают одинаковыми административными правами (см. раздел «Административные права» на стр. [407](#)).

## С

### Сервер iOS MDM

Компонент Kaspersky Security Center, который устанавливается на клиентское устройство и позволяет подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью сервиса Apple Push Notifications (APNs).

### Сервер мобильных устройств

Компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования.

### Сервер мобильных устройств Exchange ActiveSync

Компонент Kaspersky Security Center, который позволяет подключать мобильные устройства Exchange ActiveSync к Серверу администрирования. Устанавливается на клиентском устройстве.

## У

### Уровень важности патча

Характеристика патча. Для патчей сторонних производителей или Microsoft существует пять уровней важности:

- Предельный.
- Высокий.
- Средний.
- Низкий.
- Неизвестно.

Уровень важности патча стороннего производителя или Microsoft определяется наиболее неблагоприятным уровнем критичности уязвимости, которую закрывает патч.

## Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

## Ш

### Широковещательный домен

Логический участок компьютерной сети, в котором все узлы могут передавать данные друг другу с помощью широковещательного канала на уровне сетевой модели OSI ( Open Systems Interconnection Basic Reference Model).



---

# 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 (спам), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих 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»: <http://www.kaspersky.ru>

Вирусная энциклопедия: <https://securelist.ru/>

Вирусная лаборатория: <http://newvirus.kaspersky.ru/> (для проверки подозрительных файлов и сайтов)

Веб-форум «Лаборатории Касперского»: <http://forum.kaspersky.com>

---

# Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки программы.

---

# Дополнительная защита с использованием Kaspersky Security Network

«Лаборатория Касперского» предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков «Лаборатории Касперского» обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте «Лаборатории Касперского».

---

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, ActiveSync, Excel, Internet Explorer, Hyper-V, Microsoft, MultiPoint, SQL Server, Tahoma, Windows, Windows Server, Windows Phone и Windows Vista – 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, FaceTime, FileVault, iBook, iBooks, iPad, iPhone, iTunes, Leopard, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger – 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, Google, Google Play, Google Карты, Youtube – товарные знаки Google, Inc.

Firefox – товарный знак Mozilla Foundation.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Oracle и Java – зарегистрированные товарные знаки Oracle Corporation и /или ее аффилированных компаний.

QRadar – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

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.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

SPL, Splunk– товарные знаки и зарегистрированные в США и других странах товарные знаки Splunk, Inc.

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.

---

# Предметный указатель

## A

Active Directory .....381

## E

exes .....381

## I

IP-диапазон

изменение..... 202, 203

создание .....203

## A

Агенты обновлений ..... 325, 407

Антивирусная защита .....361

## B

Виртуальный Сервер администрирования .....77

Выборки событий

настройка.....191

просмотр журнала .....190

создание .....191

## Г

Группа лицензионных программ .....	216
Групповые задачи	
наследование .....	134
фильтр .....	140
Группы	
структура .....	111
Группы администрирования .....	74, 410

## Д

Дерево консоли .....	48
Добавление	
клиентский компьютер .....	155
Сервер администрирования .....	99

## З

Задача .....	82
добавления ключа .....	330
Задачи	
выполнение .....	139
групповые .....	130, 411
импорт .....	137
локальные .....	133



просмотр результатов .....	140
рассылка отчетов.....	185
резервное копирование .....	373
смена Сервера администрирования.....	156
управление клиентскими компьютерами .....	158
экспорт.....	136

## И

### Импорт

задачи .....	137
политики .....	122

Инсталляционный пакет .....	412
-----------------------------	-----

## К

Кластеры .....	363
----------------	-----

Клиентские компьютеры .....	80
-----------------------------	----

подключение к Серверу .....	145
-----------------------------	-----

сообщение пользователю .....	159
------------------------------	-----

Ключ.....	329
-----------	-----

отчет .....	333
-------------	-----

распространение .....	332
-----------------------	-----

удаление.....	331
---------------	-----

установка .....	330
-----------------	-----

Контекстное меню .....	59, 387
------------------------	---------

## Л

Лицензирование программы .....	62, 64
Лицензия .....	63
Лицензионное соглашение .....	62
файл ключа.....	70

## М

Массивы .....	363
Мастер конвертации политик и задач .....	122, 137
Мобильное устройство Exchange ActiveSync .....	269
Мобильное устройство iOS MDM .....	275
Мобильные пользователи	
правила переключения .....	357
профиль.....	356

## О

Обновление	
получение .....	314
проверка .....	317
просмотр.....	321
распространение .....	321, 322, 323, 325
Обновление программы .....	224

Образ .....	241
Ограничение трафика .....	104
Опрос	
IP-диапазоны .....	202
Windows-сеть .....	201
группы Active Directory .....	201
Опрос сети .....	199
Отчеты	
ключи .....	333
просмотр .....	184
рассылка .....	185
создание .....	184

## П

Политика .....	82, 414
создание .....	116
Политики	
активация .....	118
импорт .....	122
копирование .....	121
мобильные пользователи .....	354
удаление .....	120
экспорт .....	121

Профиль политики .....	123
Профиль политики	
создание.....	126
удаление .....	128

## Р

Резервное копирование	
задача .....	373
утилита .....	374
Роли пользователей .....	175
Роль пользователя	
добавить.....	176
назначить .....	177
Роль пользователя	
добавить .....	263

## С

Сервер администрирования .....	74
Сервер мобильных устройств Exchange ActiveSync .....	269
Сертификат	
VPN.....	180, 259
общий .....	180, 259
почтовый.....	180, 259
установка сертификата пользователю .....	180, 259
Сертификат Сервера администрирования .....	98

Статистика .....	186
------------------	-----

## У

Уведомления.....	187
------------------	-----

### Удаление

политика .....	120
----------------	-----

Сервер администрирования .....	99
--------------------------------	----

### Управление

клиентским компьютером .....	158
------------------------------	-----

ключи .....	329
-------------	-----

первоначальная настройка.....	72
-------------------------------	----

политики .....	114
----------------	-----

Управление программой .....	114
-----------------------------	-----

### Установка

Active Directory .....	381
------------------------	-----

Уязвимость.....	220
-----------------	-----

## Х

### Хранилища

инсталляционные пакеты .....	335
------------------------------	-----

ключи .....	329
-------------	-----

реестр программ.....	214
----------------------	-----

## Ш

### Шаблон отчета

создание .....183

Шифрование .....303