KASPERSKY lab

Kaspersky Endpoint Security and Management

Часть I. Внедрение

Введение

Часть I. Внедрение

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

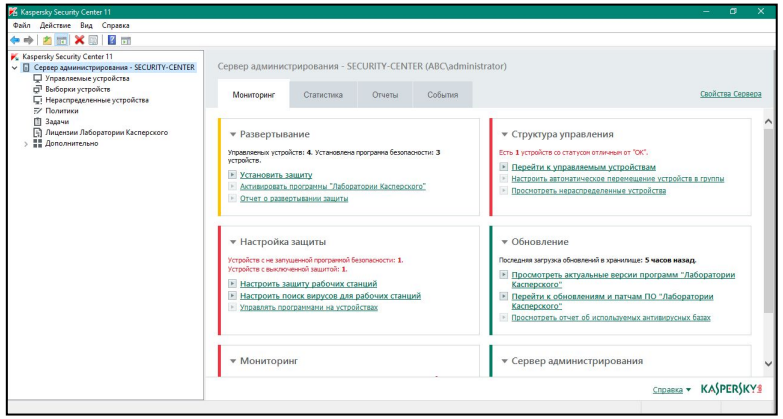
Основы Kaspersky Endpoint Security для бизнеса

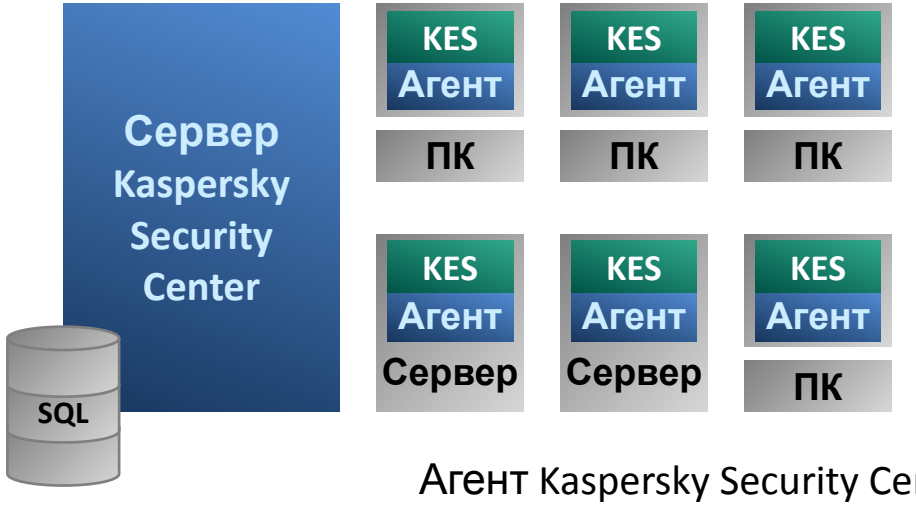
О чем этот курс

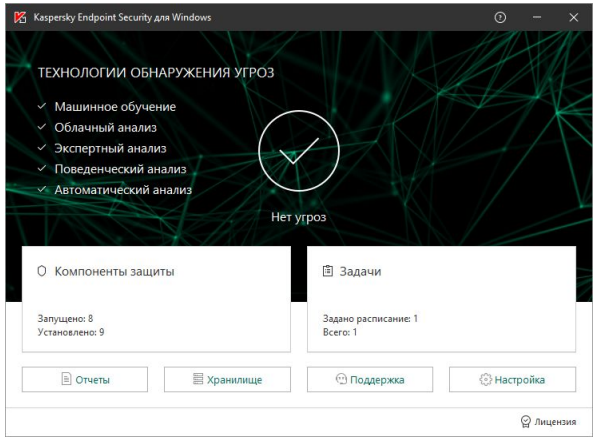
Вступление

- Какие продукты покрывает этот курс: Kaspersky Security Center и Kaspersky Endpoint Security для Windows, и немного Kaspersky Security для Windows Server
- Из чего состоит Kaspersky Endpoint Security для бизнеса
- Как взаимодействуют компоненты Kaspersky Endpoint Security для бизнеса
- Из чего состоит Kaspersky Endpoint Security для Windows
- Как администратор управляет защитой
- Как лицензируется Kaspersky Endpoint Security для бизнеса
- Что входит и что не входит в курс

Kaspersky Endpoint Security для бизнеса







Сервер Kaspersky Security Center:

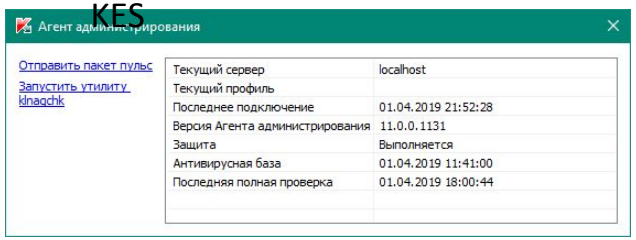
- Собирает события и строит отчеты
- Хранит и распространяет настройки
- Устанавливает и удаляет программы

Сервер SQL:

- хранит события и некоторые настройки

Агент Kaspersky Security Center:

- Передает события от KES к KSC
- Передает настройки от KSC к KES



Kaspersky Endpoint Security:

- Обнаруживает и блокирует угрозы
- Контролирует сетевые соединения
- Контролирует запуск программ
- Контролирует доступ к устройствам и веб-сайтам
- Шифрует файлы и диски

Консоль Kaspersky Security Center:

- Интерфейс сервера KSC, где администратор видит состояние защиты и настраивает параметры
- Существует два варианта консоли: традиционная MMC и новая Web Console

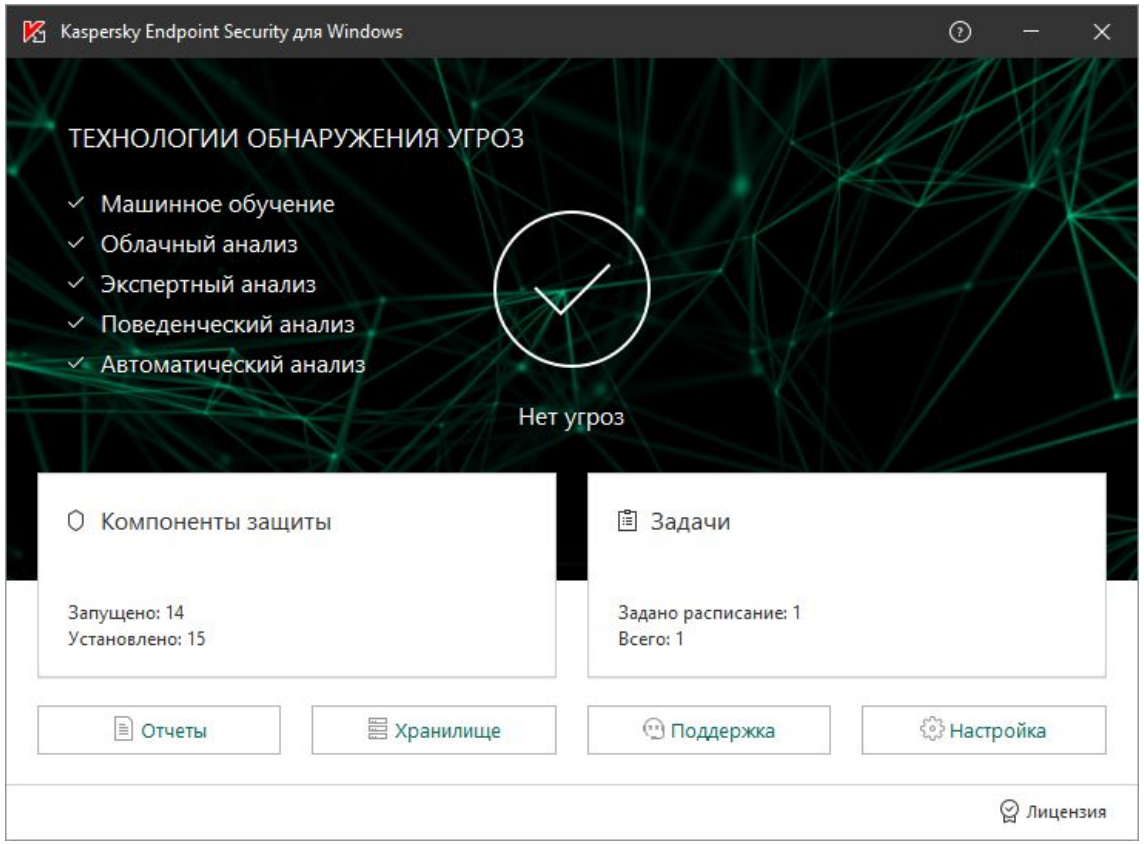
Из чего состоит Kaspersky Endpoint Security для Windows

Продвинутая защита

- Kaspersky Security Network
- Анализ поведения
- Защита от эксплойтов
- Откат вредоносных действий
- Предотвращение вторжений

Базовая защита

- Защита от файловых угроз
- Защита от почтовых угроз
- Защита от веб-угроз
- Защита от сетевых угроз
- Сетевой экран
- Защита от атак BadUSB
- AMSI Protection Provider



Контроль безопасности

- Веб-контроль
- Контроль программ
- Контроль устройств
- Adaptive Anomaly Control

Шифрование данных

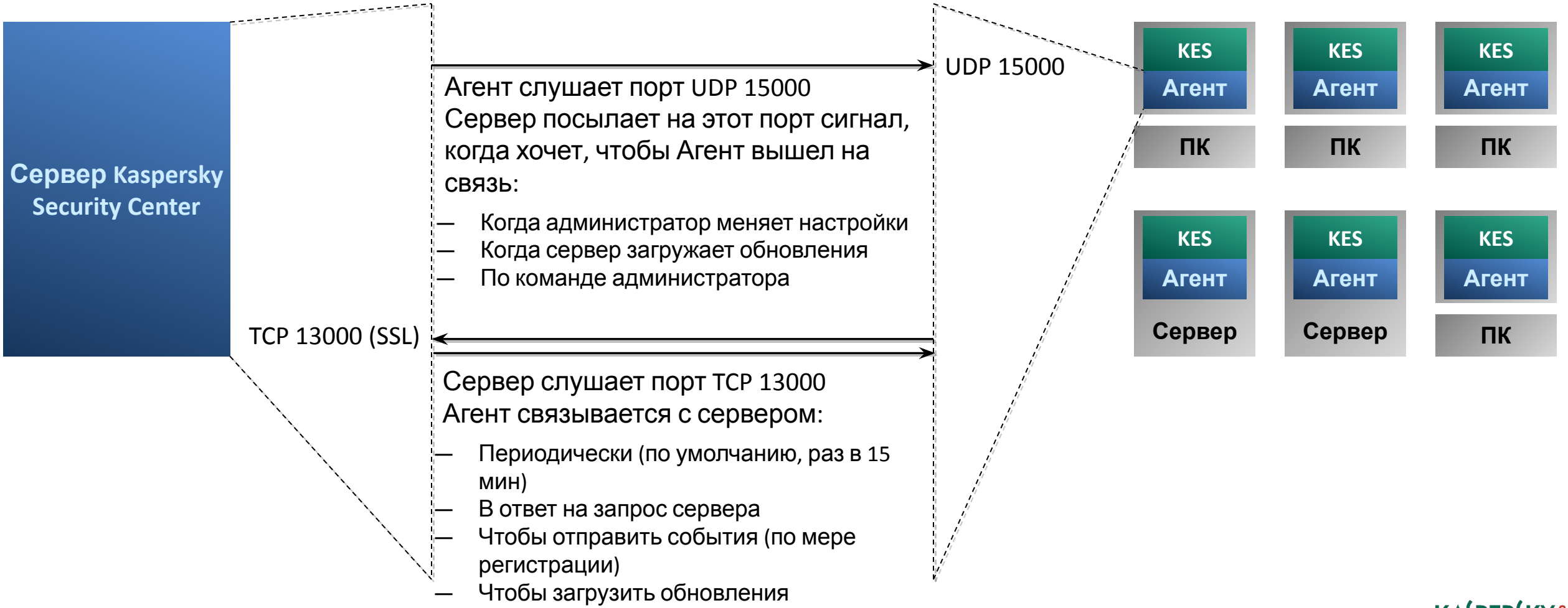
- Шифрование файлов
- Полнодисковое шифрование
- Управление Bitlocker

Endpoint Sensor (KATA/EDR)

Задачи

- Поиск вирусов
- Обновление
- Контроль целостности

Как Kaspersky Security Center управляет защитой

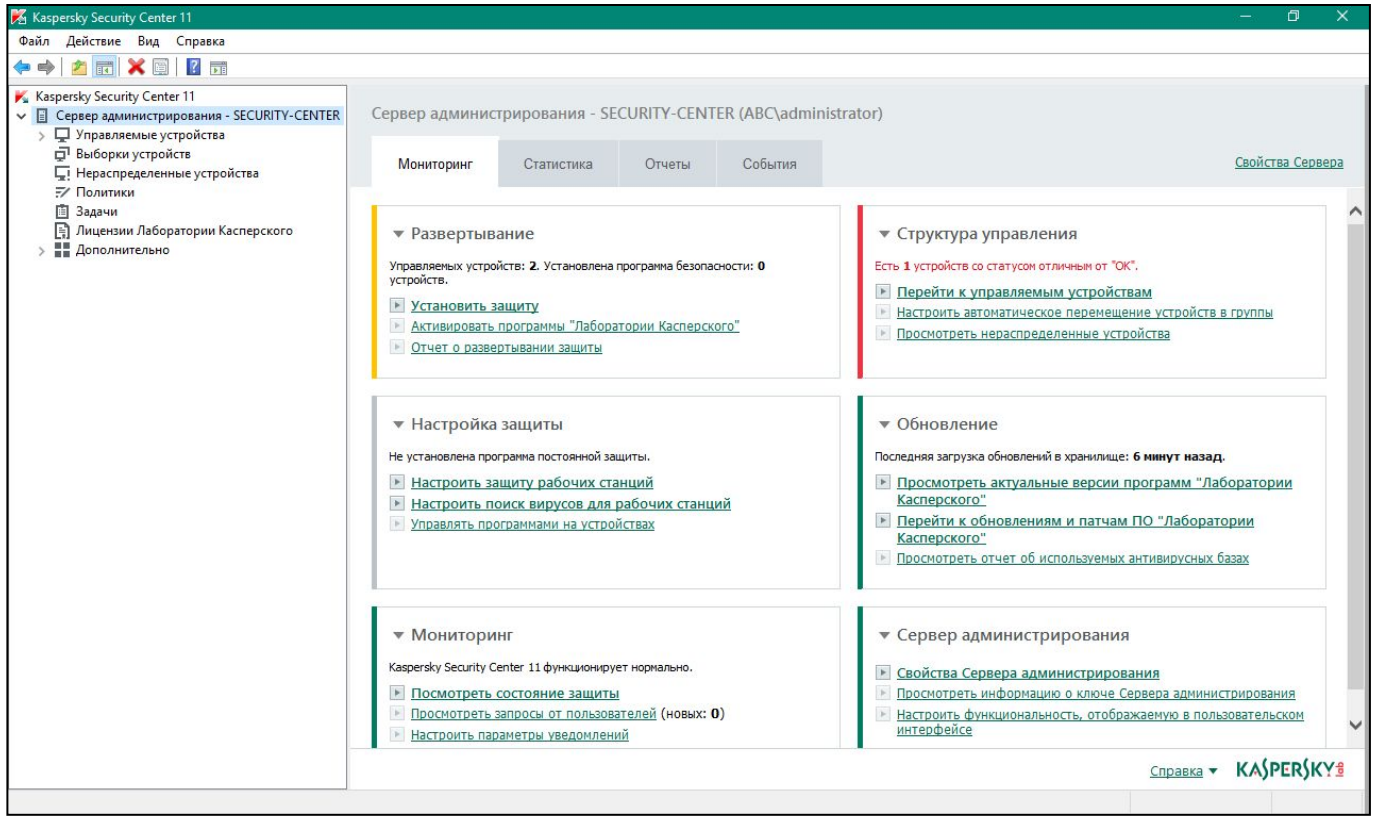


Как администратор управляет защитой

Чтобы дать компьютерам разные настройки, администратор делит компьютеры на группы и создает политики для групп

Администратор задает настройки в задачах и политиках:

- В задачах настройки поиска вирусов и обновления; у задач есть расписание
- В политике все остальные настойки

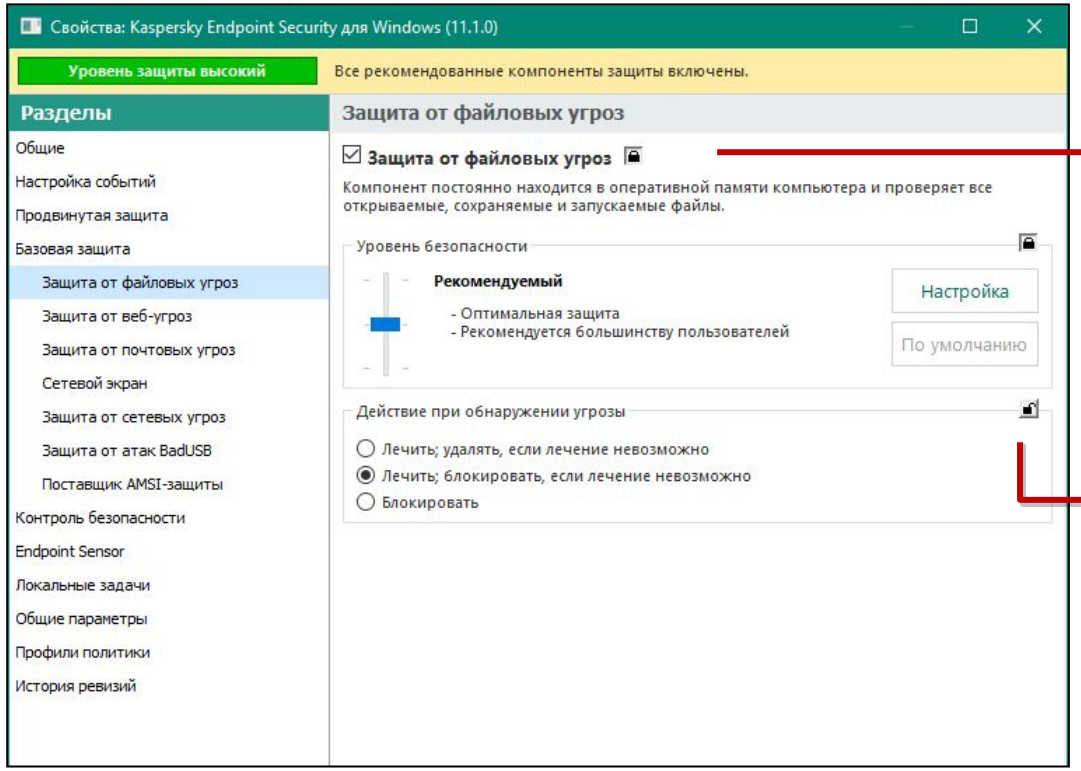


Администратор следит за защитой по:

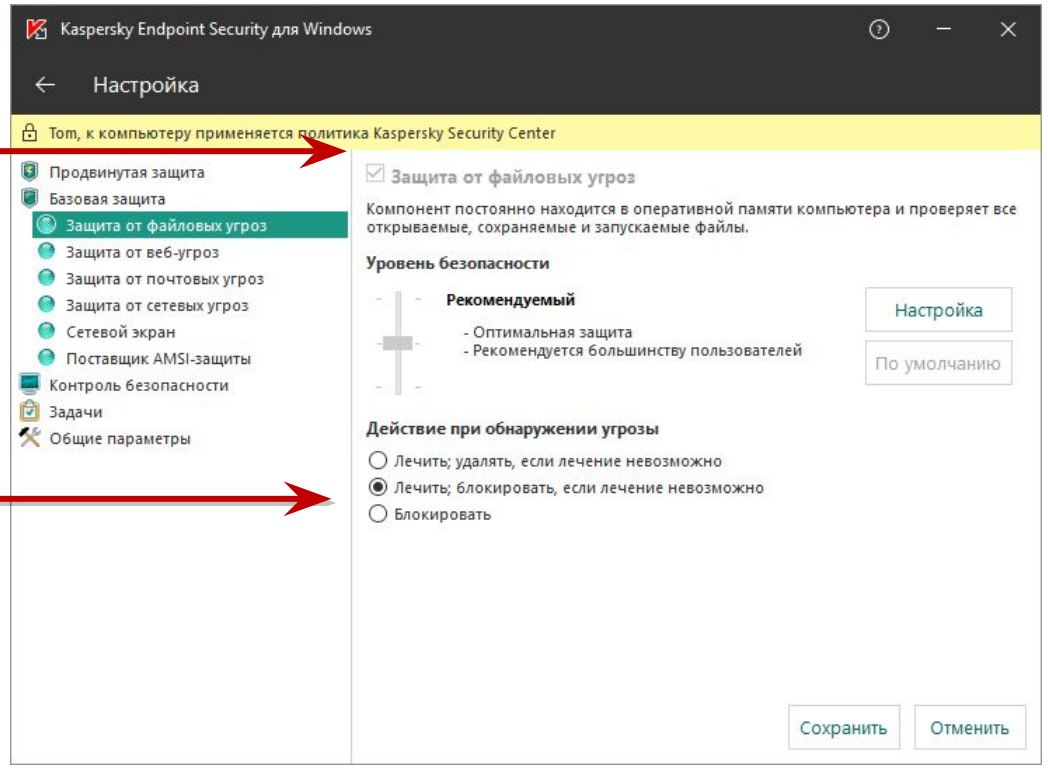
- Событиям
- Отчетам
- Дэшбордам
- Статусам

Как работает политика и зачем нужны замки

Политика Kaspersky Endpoint Security



Локальные настройки Kaspersky Endpoint Security



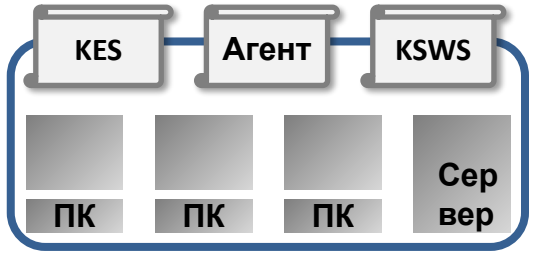
Параметры политики соответствуют локальным параметрам

Компьютеры в группах используют настройки политики, для которых закрыт замок

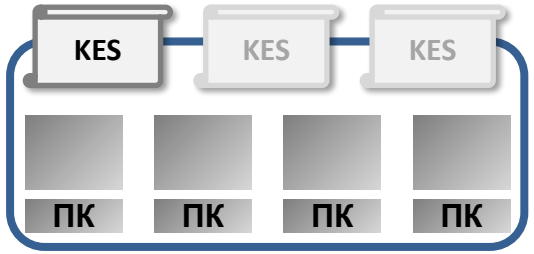
Если замок закрыт, локальный параметр принимает значение из политики и пользователь не может его изменить

Если замок открыт, пользователь может дать локальному параметру любое значение

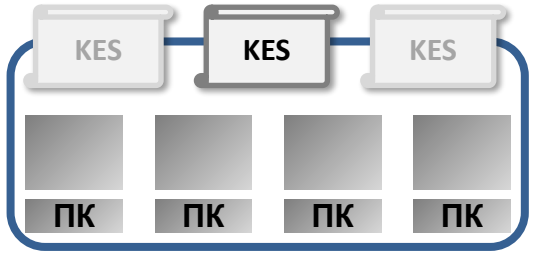
Как работают политики в группах



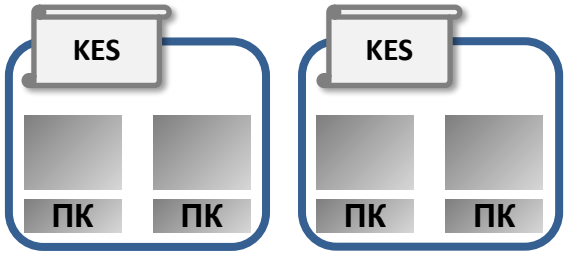
В группе могут быть политики для разных программ



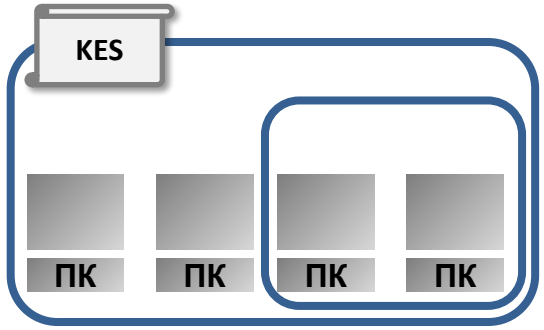
В группе может быть несколько политик одной программы, но только одна активная



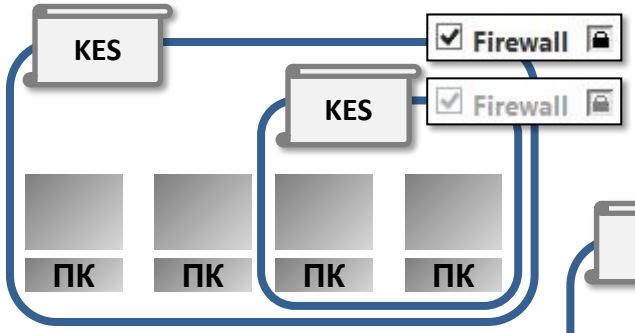
Администратор может вручную выбирать активную политику



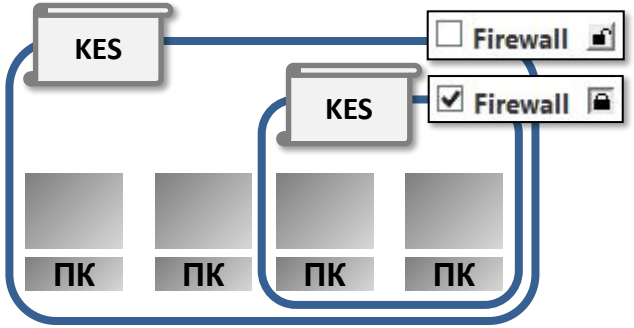
Чтобы дать компьютерам разные настройки, разделите их на подгруппы с разными политиками



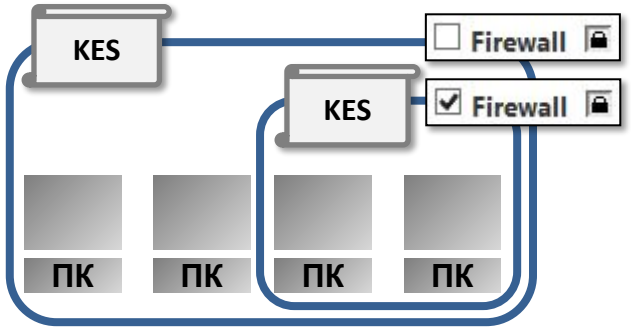
Если в подгруппе нет политики, ее компьютеры получают политику родительской группы



Если в подгруппе есть своя политика, она получает обязательные настройки из политики родительской группы



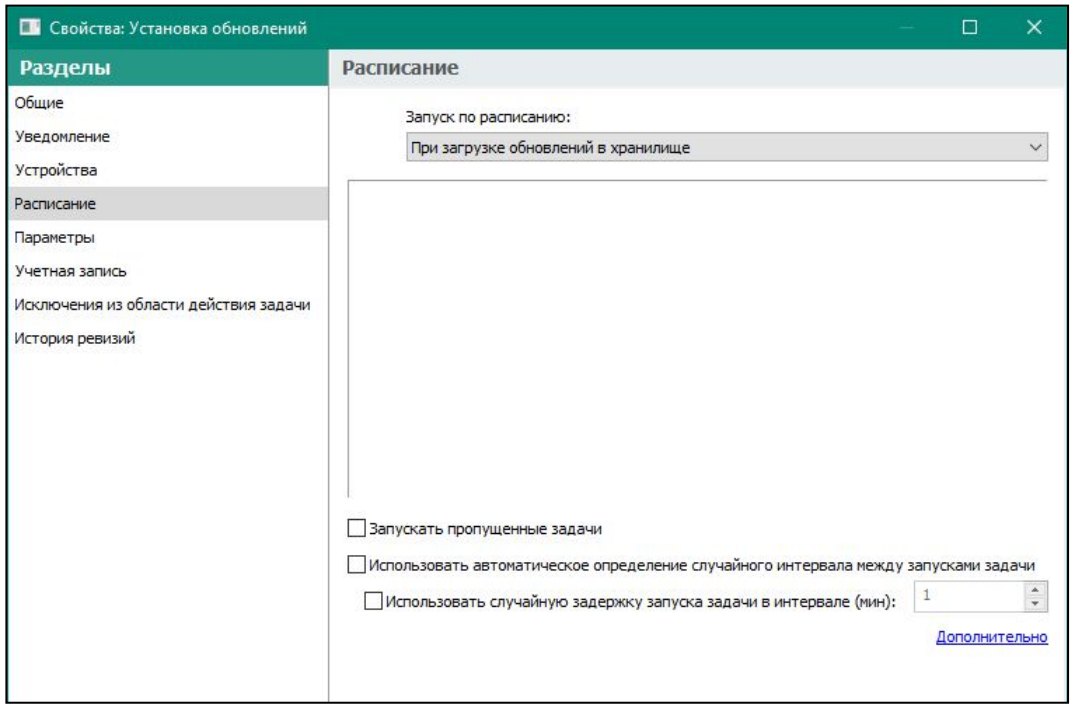
Если в политике родительской группы замок не закрыт, этот параметр можно менять в политике подгруппы



Администратор может отключить наследование в политике подгруппы и менять настройки, как будто политики в родительской группе нет

Как работают задачи

Групповая задача обновления

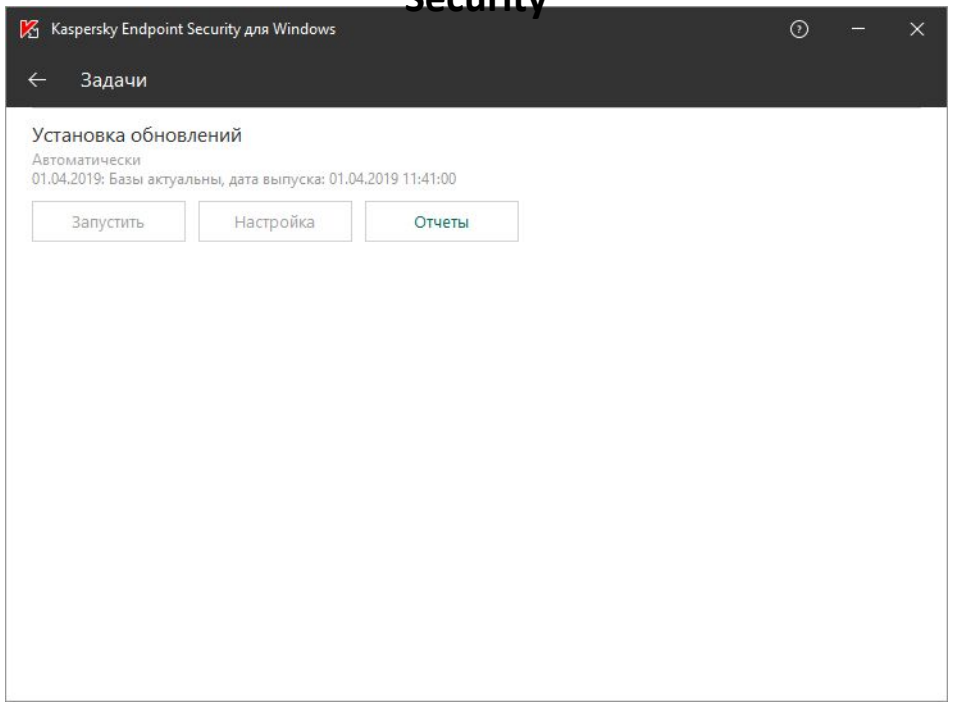


С помощью задач администратор управляет настройками обновления и поиска вирусов

У задач есть расписание запуска

В отличие от политик, замков в задачах нет

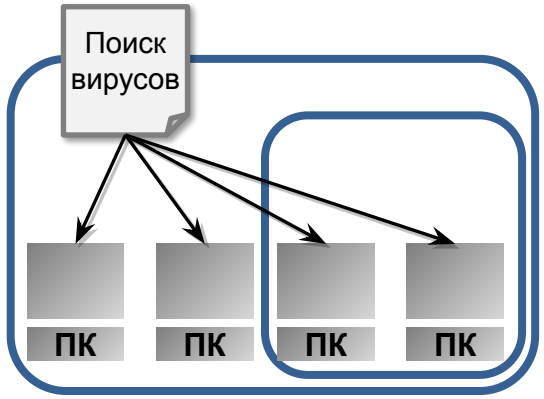
Задачи в интерфейсе Kaspersky Endpoint Security



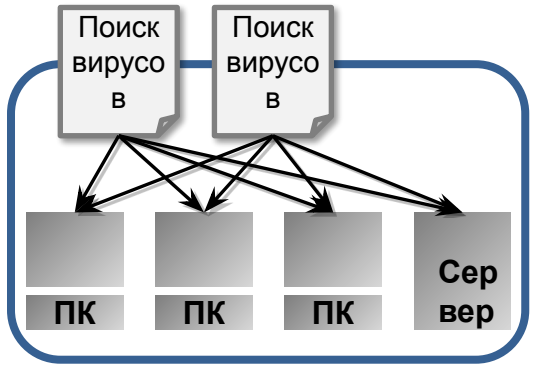
Компьютеры под политикой используют только групповые задачи. Локальные задачи есть, но они отключены

Локальный пользователь не может менять настройки групповых задач

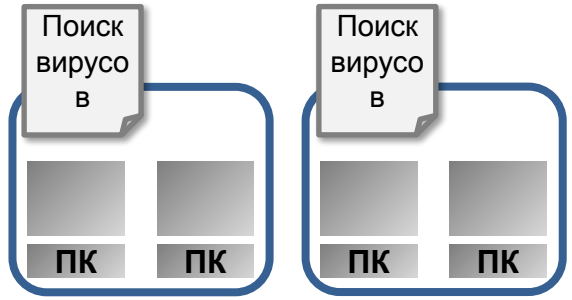
Как работают задачи в группах



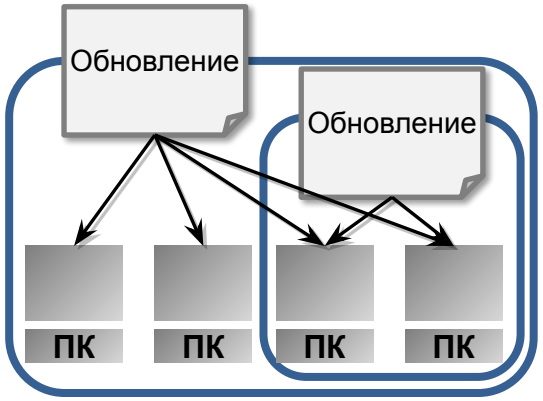
Задача группы применяется ко всем компьютерам группы, в том числе к компьютерам подгрупп



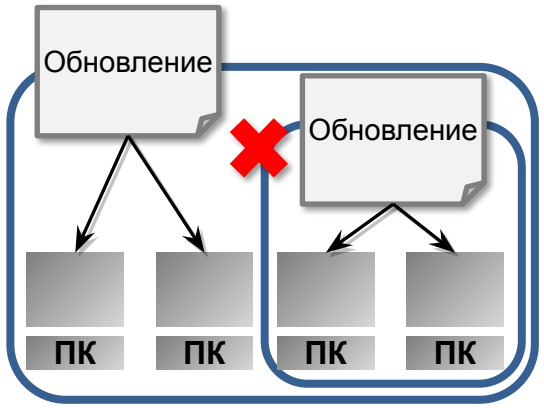
Если в группе две задачи одного типа, обе действуют на все компьютеры. Они могут отличаться настройками и расписанием



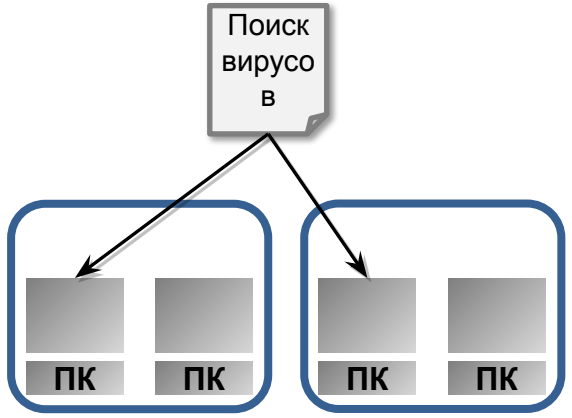
Чтобы запускать одну задачу с разными настройками на разных компьютерах, разделите компьютеры на группы



Если однотипные задачи есть и в группе и в подгруппе, в подгруппе будет действовать две задачи. Не делайте так, особенно с задачами обновления



Администратор может исключить подгруппу из области действия задачи родительской группы



Администратор может создать задачу для наборов компьютеров, которая действует на отдельные компьютеры разных групп

Как лицензируется защита для конечных узлов

Cloud	Стандартный	Расширенный
Защита рабочих станций		
Защита серверов		
Защита мобильных устройств		
Управление защитой		
Управление мобильными устройствами		
Веб-контроль		
Контроль устройств		
	Контроль программ	
Шифрование*		Адаптивный контроль аномалий
Поиск уязвимостей и установка обновлений*		Шифрование
		Поиск уязвимостей и установка обновлений

Targeted Security Solutions

- Шифрование
- Управление мобильными устройствами
- Поиск уязвимостей и установка обновлений

Введение

Часть I. Внедрение

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Основы Kaspersky Endpoint Security для бизнеса

О чем этот курс

Что есть и чего нет в этом курсе?

Есть	Нет
Защита рабочих станций и серверов Windows	Защита рабочих станций Linux и Mac, мобильных устройств и виртуальных сред
Kaspersky Endpoint Security для Windows Kaspersky Security для Windows Servers	Kaspersky Embedded Systems Security
Защита от угроз и контроль пользователей	Шифрование
Управление защитой компьютеров	Управление мобильными устройствами, поиск уязвимостей и установка обновлений
Управление защитой в небольших и несложных сетях (1 сервер администрирования, простая топология)	Управление защитой в больших и сложных сетях, подчиненные сервера администрирования, функции для сервис-провайдеров и пр.

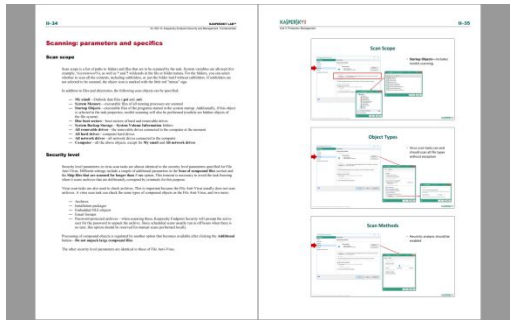
Где узнать больше?

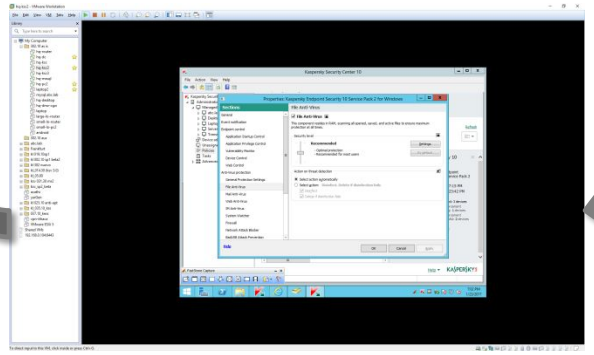
Тема	Курс	Длительность
Защита рабочих станций Linux	KL 013	1 день
Защита серверов Linux	KL 007	1 день
Защита рабочих станций Mac	KL 011	1 день
Защита серверов Windows	KL 005	1,5 дня
Защита встраиваемых систем	KL 037	1 день
Управление и защита мобильных устройств	KL 010	1 день
Шифрование	KL 008	1 день
Управление системами	KL 009	1 день
Управление защитой в сложных сетях	KL 302	1,5 дня
Защита виртуальных сред	KL 014 + KL 031	1 день + 1 день
Расширенная диагностика проблем	KL 016	1 день
Как реализовать политику Default Deny	KL 032	0,5 дня

Как устроен курс?

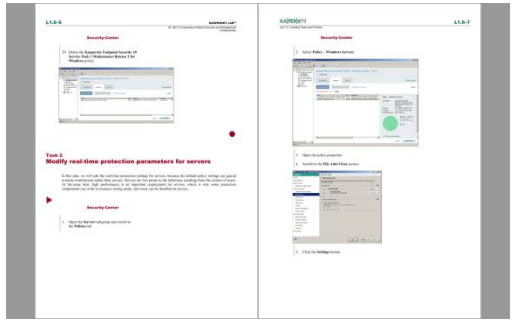
Слайды

Учебник





Лабораторная работа

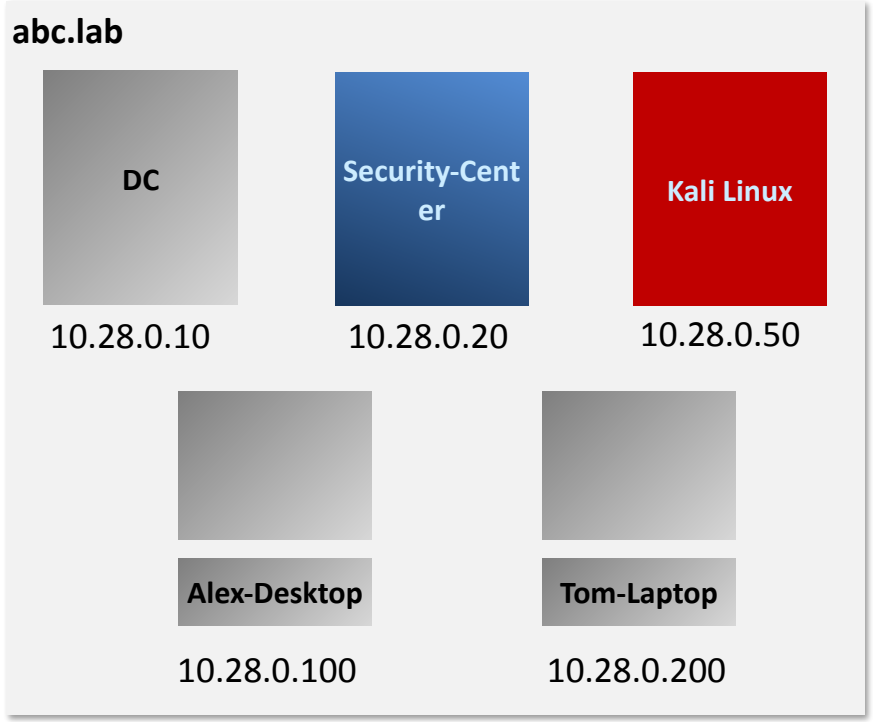


Руководство

Презентация чередуется с лабораторными работами

Все слайды есть в учебнике

22 лабораторных работы на 5 виртуальных машинах



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

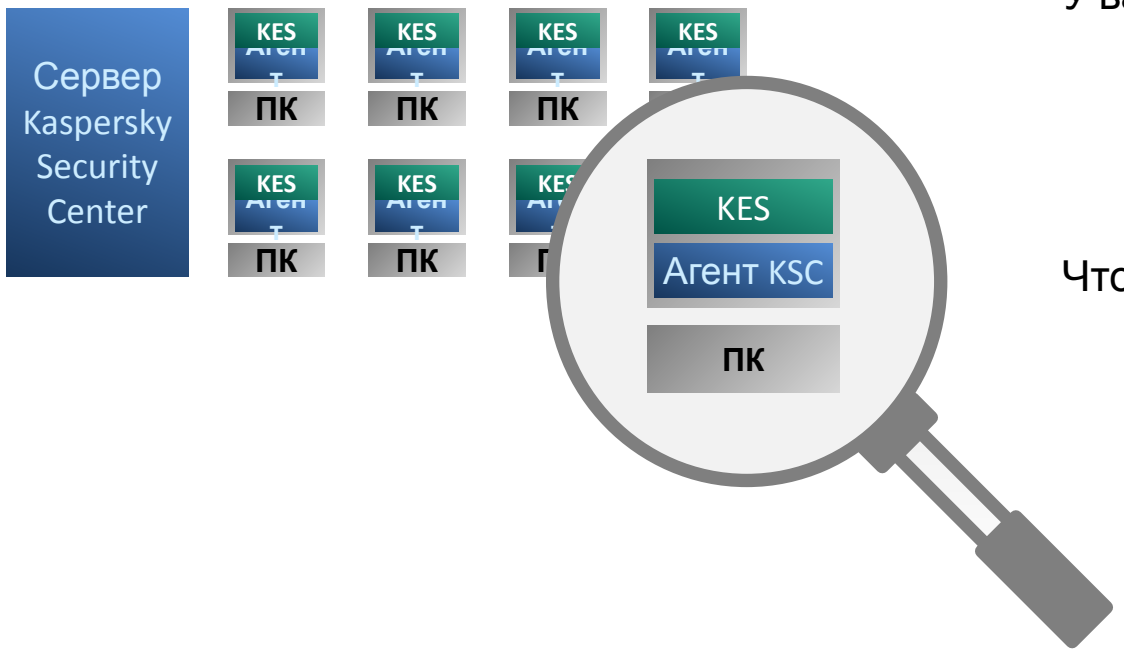
Что и в каком порядке устанавливать
Как все организовать

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Что и в каком порядке внедрять?



У вас есть компьютеры в сети. Вы хотите

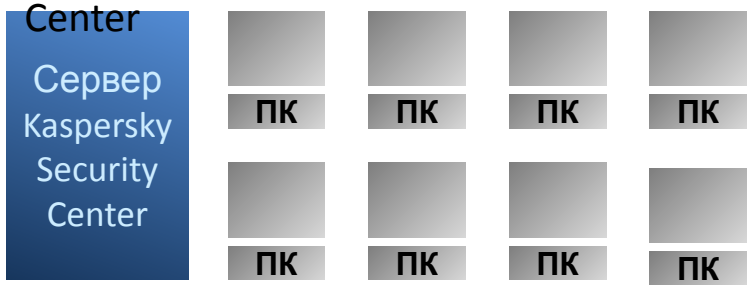
- защитить все ax
- получать отчеты и управлять защит nter

ax

Чтобы это получить

1. Установите сервер Kaspersky Security Center
2. Установите Kaspersky Endpoint Security и Агенты KSC
3. Организуйте компьютеры в группы

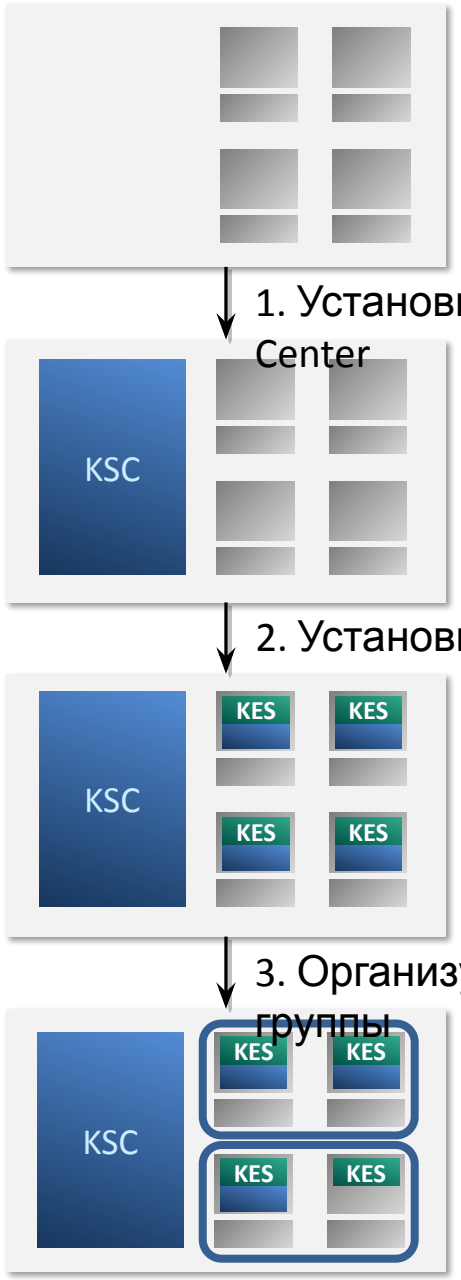
1. Установите Kaspersky Security Center

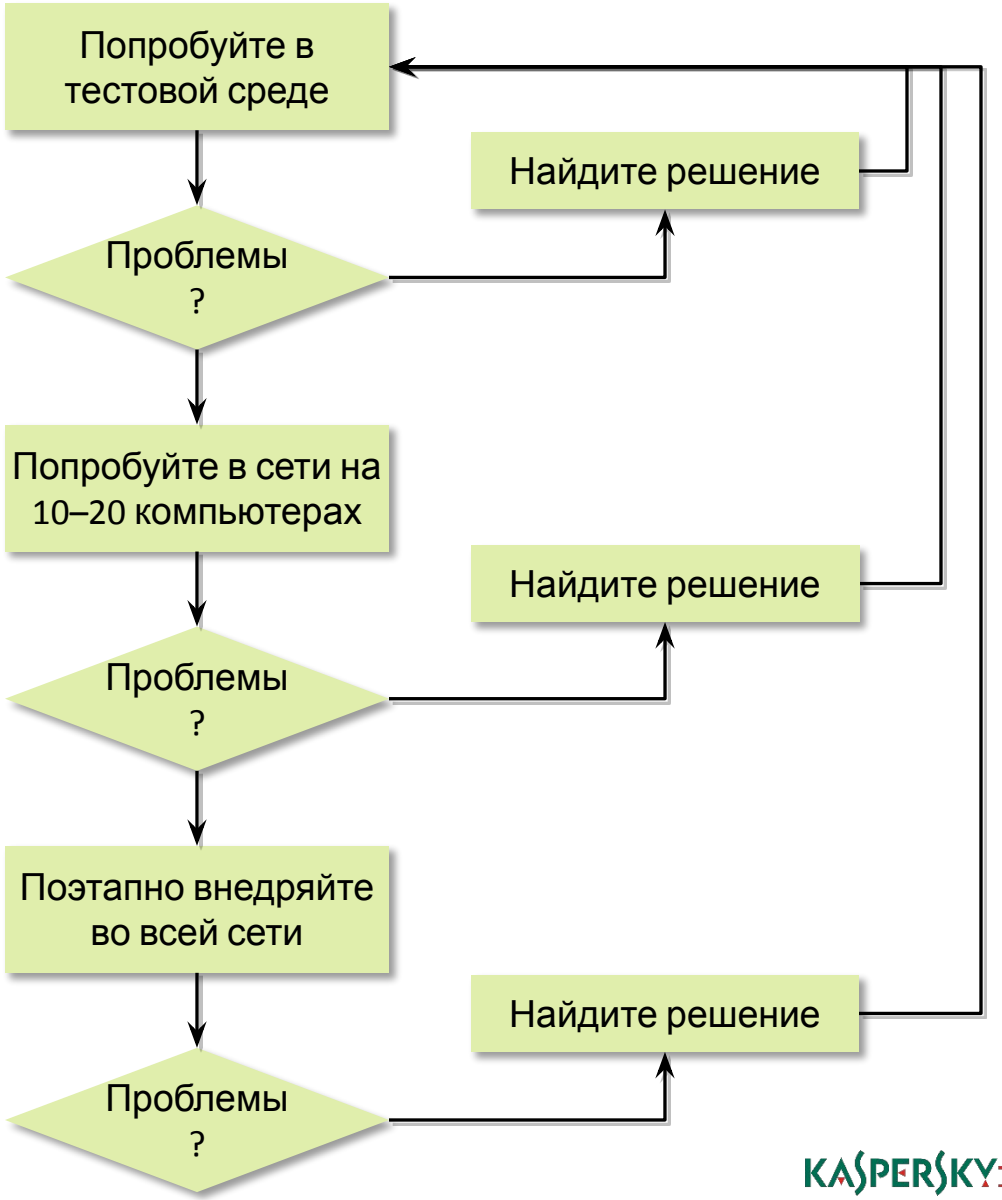


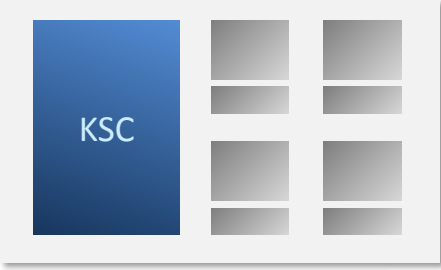
2. Установите KES и Агенты KSC

3. Организуйте компьютеры в группы

Как все организовать







Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Требования к Серверу администрирования

Установка Сервера администрирования

Установка Kaspersky Security Center Web Console

Мастер первоначальной настройки

Требования для установки Сервера администрирования

Операционные системы (Серверы)

- Microsoft Small Business Server 2008 64-bit
  - Standard / Premium
- Microsoft Small Business Server 2011 64-bit
  - Essentials / Standard / Premium Add-on
- Windows Storage Server 64-bit
  - 2008 R2 / 2012 / 2012 R2 / 2016
- Microsoft Windows Server 2008 SP2
  - Все редакции
- Microsoft Windows Server 2008 R2 SP1 64-bit
  - Standard
- Microsoft Windows Server 2012 Server 32-bit | 64-bit
  - Foundation / Essentials / Standard / Datacenter + Core
- Microsoft Windows Server 2012 R2
  - Foundation / Essentials / Standard / Datacenter + Core
- Microsoft Windows Server 2016
  - Standard / Datacenter + Core
- Microsoft Windows Server 2019
  - Standard / Datacenter

Требования для установки Сервера администрирования

Операционные системы (не серверы)

- Microsoft Windows 10 RS3-RS5 32-bit / 64-bit
  - Pro / Enterprise / Education
- Microsoft Windows 10 Pro for Workstation
  - RS3 / RS4 / RS5
- Microsoft Windows 8.1 32-bit / 64-bit
  - Pro / Enterprise
- Microsoft Windows 8 32-bit / 64-bit
  - Pro / Enterprise
- Microsoft Windows 7 SP1 32-bit / 64-bit
  - Professional / Enterprise / Ultimate

Виртуальные платформы

- VMware vSphere
  - 6 / 6.5
- VMware Workstation 14 Pro
- Microsoft Hyper-V Server 64-bit
  - 2008 / 2008 R2 / 2008 R2 SP1 / 2012 / 2012 R2 / 2016
- Citrix XenServer
  - 7 / 7.1 LTSR
- Parallels Desktop 11
- Oracle VM VirtualBox 5.x

Требования для установки Сервера администрирования

Серверы баз данных

- Microsoft SQL Server 2008 32-bit
  - Express
- Microsoft SQL Server 2008 64-bit
  - All editions
- Microsoft SQL 2008 R2 64-bit
  - All editions
- Microsoft SQL Server 2012 64-bit
  - All editions
- Microsoft SQL Server 2014 64-bit
  - All editions
- Microsoft SQL Server 2016 64-bit
  - All editions
- Microsoft SQL Server 2017 64-bit
  - All editions
- MySQL Standard Edition 32-bit / 64-bit
  - 5.6 / 5.7
- MySQL Enterprise Edition 32-bit / 64-bit
  - 5.6 / 5.7
- Microsoft Azure SQL Database
- Amazon RDS
  - MS SQL

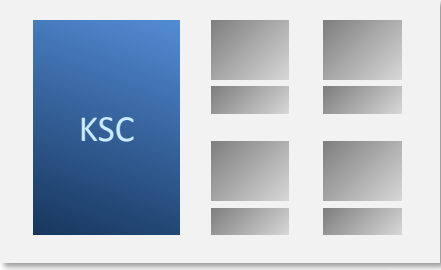
Другое ПО

- Microsoft .NET Framework 4 (for exporting reports to PDF)
- Microsoft Data Access Components 2.8
- Windows Data Access Components 6.0
- Windows Installer 4.5 (included)

Минимальные аппаратные требования

- Процессор: 1 ГГц для x86 / 1.4 ГГц для x64
- RAM: 4 ГБ
- Диск: 10 ГБ (100 GB для мониторинга уязвимостей и установки обновлений)

Рекомендуемые требования зависят от размера и конфигурации сети. Подробная информация доступна в руководстве администратора



Требования к Серверу администрирования

Установка Сервера администрирования

Установка Kaspersky Security Center Web Console

Мастер первоначальной настройки

Начало установки

Оболочка установки позволяет:

- Установить Сервер администрирования и другие компоненты Kaspersky Security Center
- Извлечь файлы для установки отдельных компонентов в выбранную папку
- Установить плагины для управления программами Лаборатории Касперского в консоли Kaspersky Security Center

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

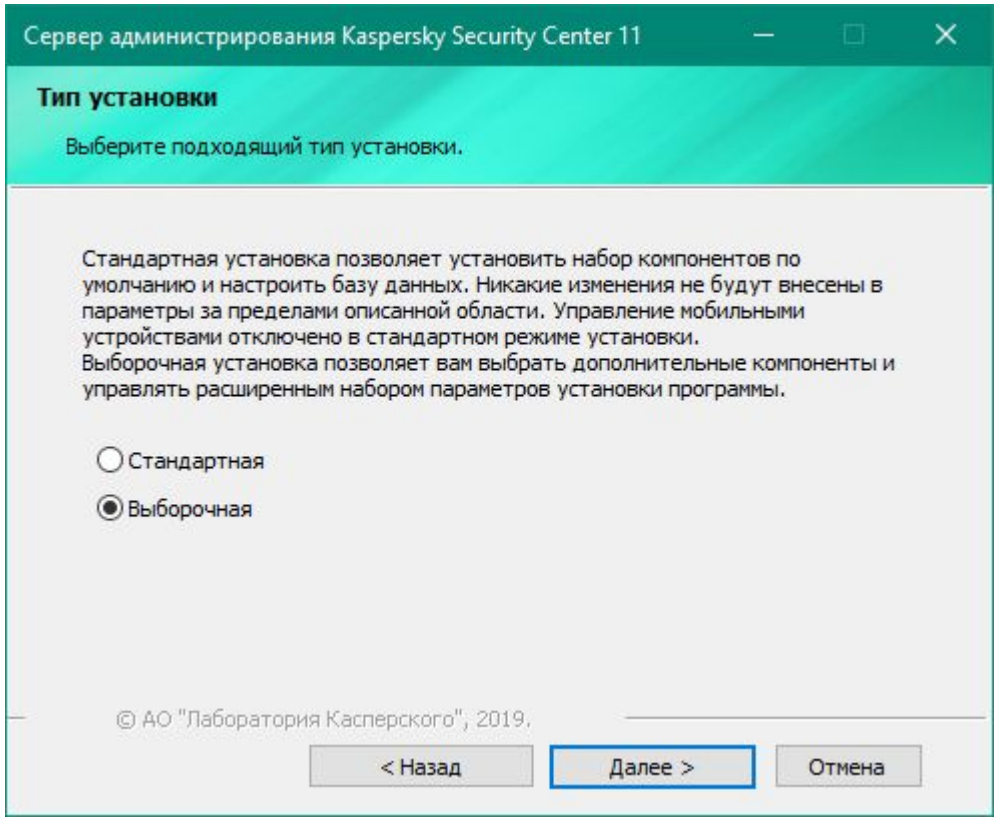
Что придется выбирать во время установки

- Компоненты и размещение программных файлов
- Размер сети
- Учетные записи (для запуска служб KSC)
- SQL Server
  - Microsoft SQL или MySQL
  - Адрес и порт
  - Параметры авторизации
  - Тип SQL-сервера после установки изменить уже нельзя
  - Чтобы изменить адрес и учетную запись SQL-сервера, придется переустановить Сервер KSC
- Общая папка
- Порты и адрес подключения
- Сертификат для аутентификации и защиты соединений
- Плагины управления программами (KES11, KES10SP2 и т.д.)

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

Тип установки



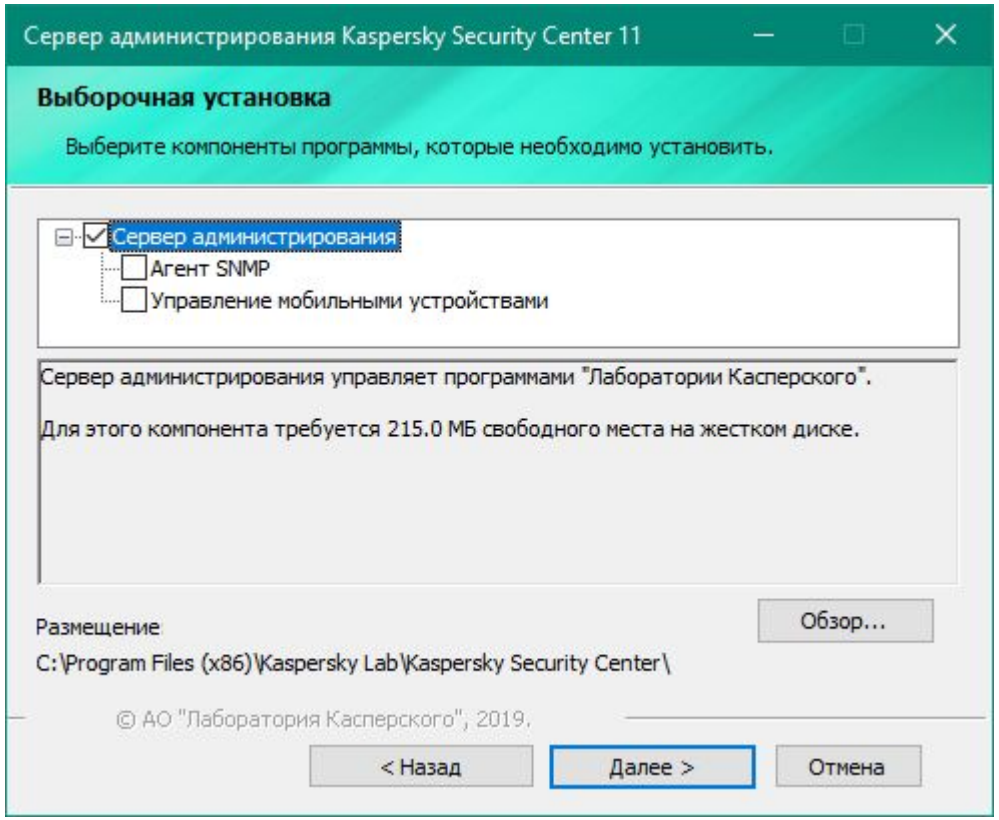
Стандартная установка — это если ничего не менять в выборочной установке

При установке на Windows Server в режиме ядра (Core) всегда выполняется выборочная установка

Компоненты и размещение программных файлов

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC



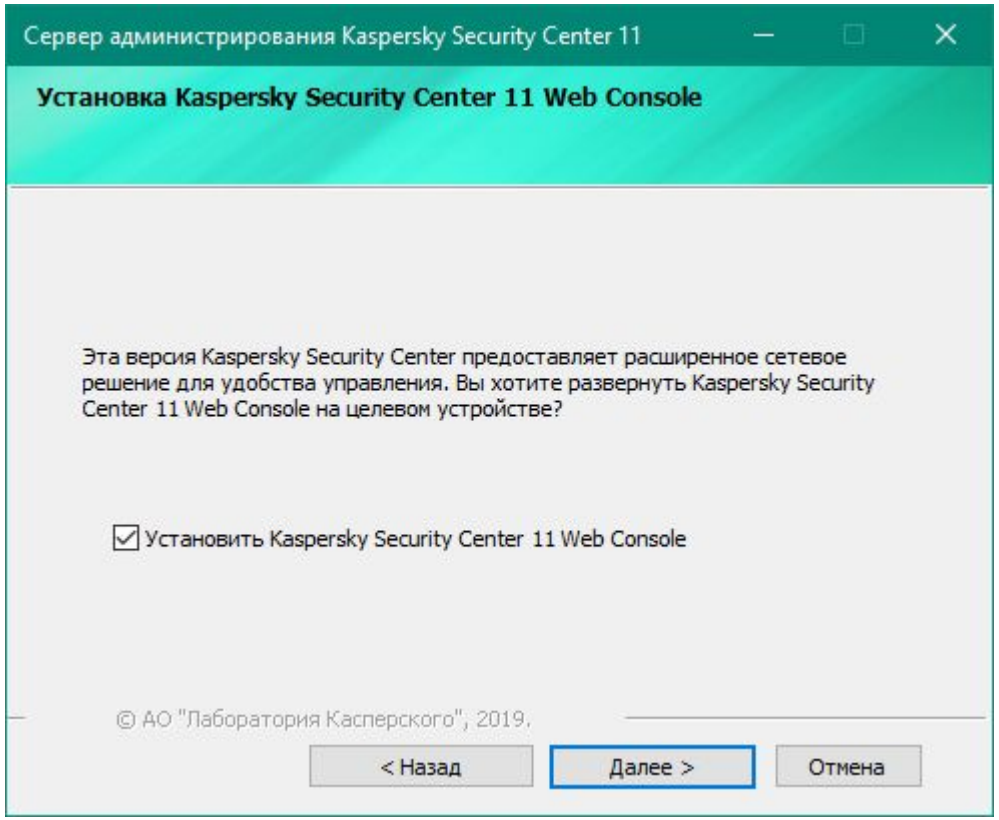
Агент SNMP — для отправки уведомлений по SNMP, требует наличия службы SNMP (компонент Windows)

Установка пакетов для поддержки мобильных устройств. Этот компонент всегда можно добавить прямо из консоли Kaspersky Security Center

Kaspersky Security Center 11 Web Console

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC



Web Console это отдельное приложение, его можно установить как на компьютер с Kaspersky Security Center, так и на отдельный компьютер

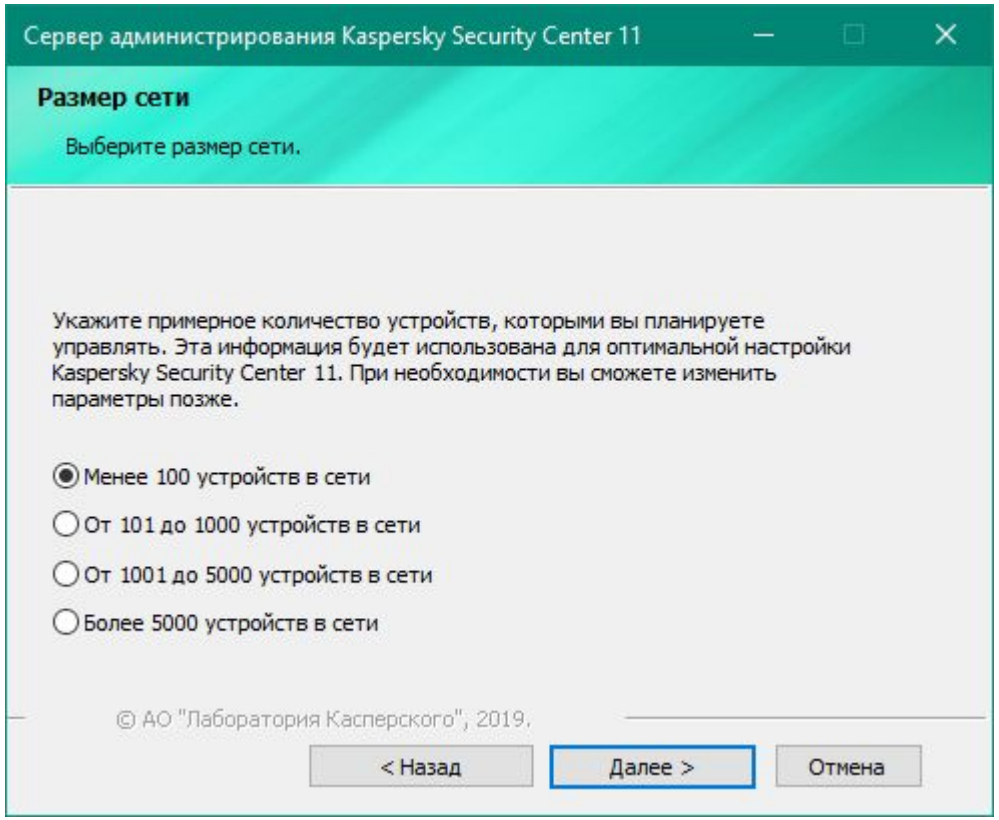
Web Console предоставляет альтернативный интерфейс управления Kaspersky Security Center

По умолчанию опция включена и Web Console устанавливается вместе с Сервером Администрирования

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

Размер сети



Количество компьютеров	0-100	100-1000	1000-5000	5000+
Автоматически определять период задержки запуска задач*	–	+	+	+
Отображать подчиненные Серверы администрирования	–	–	+	+
Отображать разделы с параметрами безопасности	–	–	+	+
Рекомендовать использовать полную версию MS SQL				+

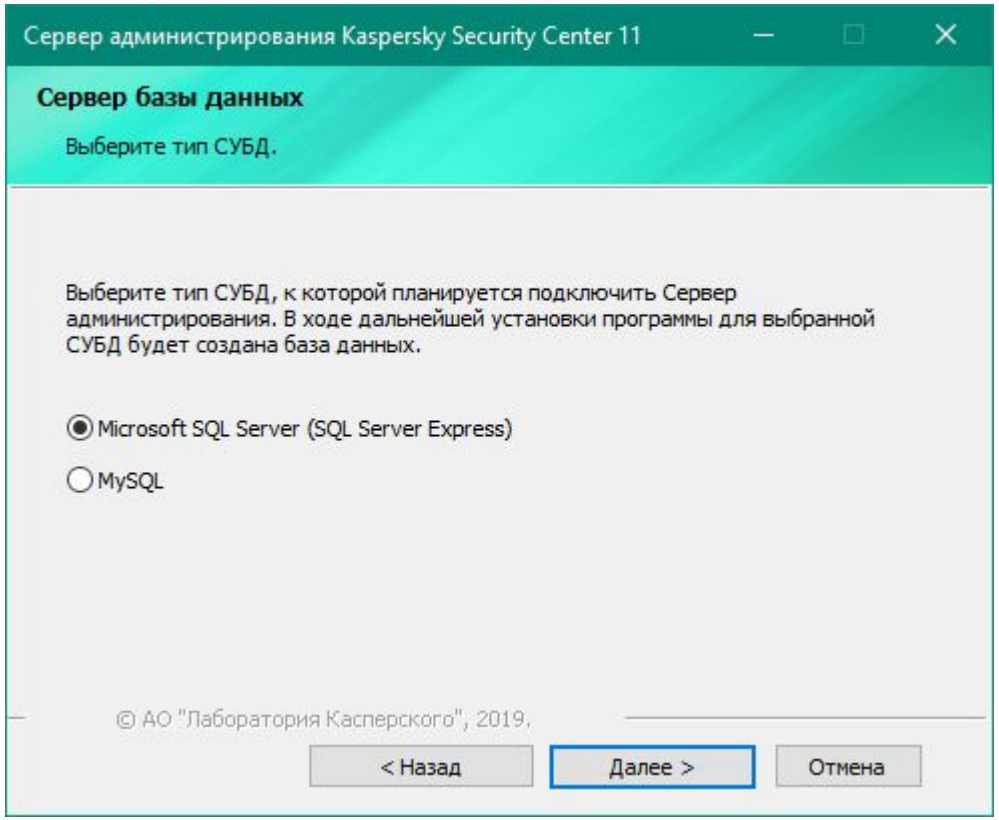
*Период задержки зависит от количества компьютеров, на которых выполняется задача

200-500	5 минут	5000-10000	30 минут
500-1000	10 минут	10000-20000	1 час
1000-2000	15 минут	20000-50000	2 часа
2000-5000	20 минут	50000+	3 часа

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

Тип SQL-сервера



Kaspersky Security Center поддерживает два типа баз данных:

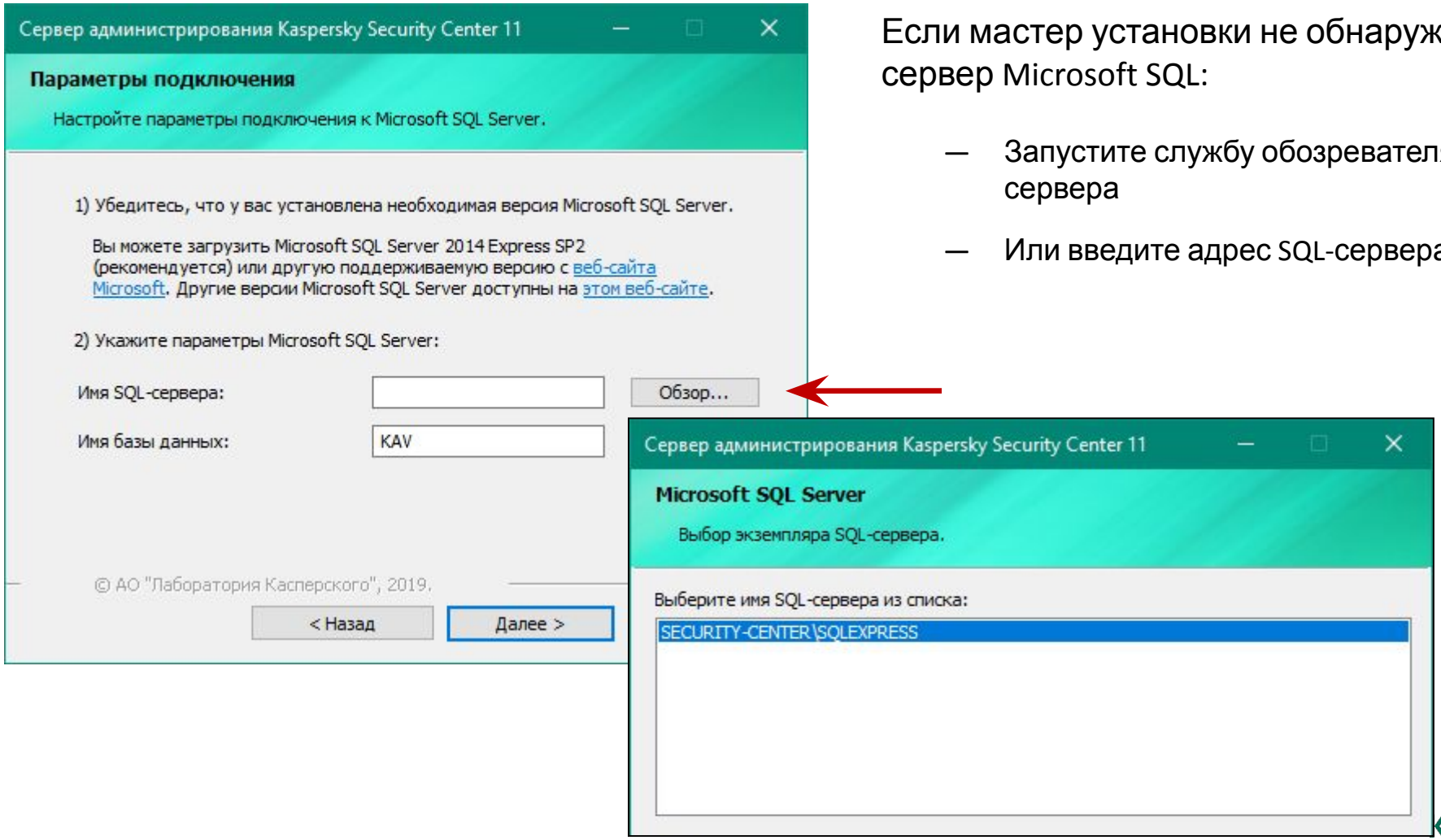
- Microsoft SQL Server
- MySQL

Рекомендуется использовать Microsoft SQL Server

Выбор существующего сервера Microsoft SQL

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC



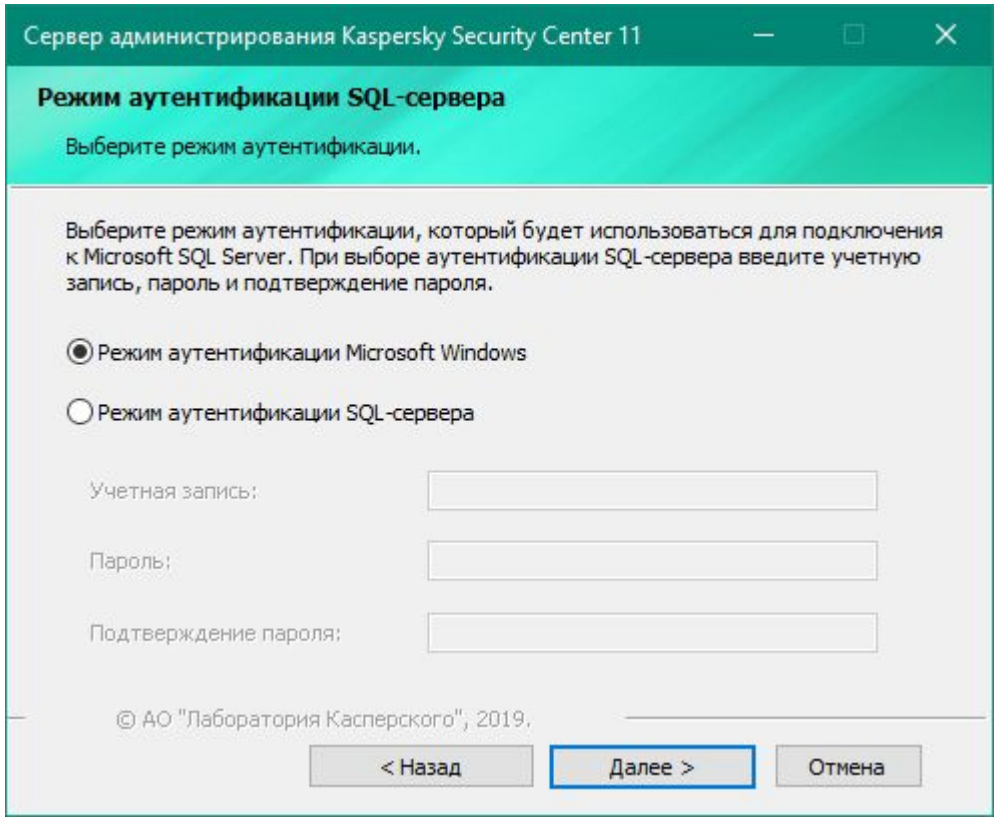
Если мастер установки не обнаруживает сервер Microsoft SQL:

- Запустите службу обозревателя SQL-сервера
- Или введите адрес SQL-сервера вручную

Режим аутентификации с Microsoft SQL Server

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC



На этом шаге вы можете задать учетную запись для доступа к серверу Microsoft SQL, и проверить, имеет ли ваша учетная запись права на подключение к нему

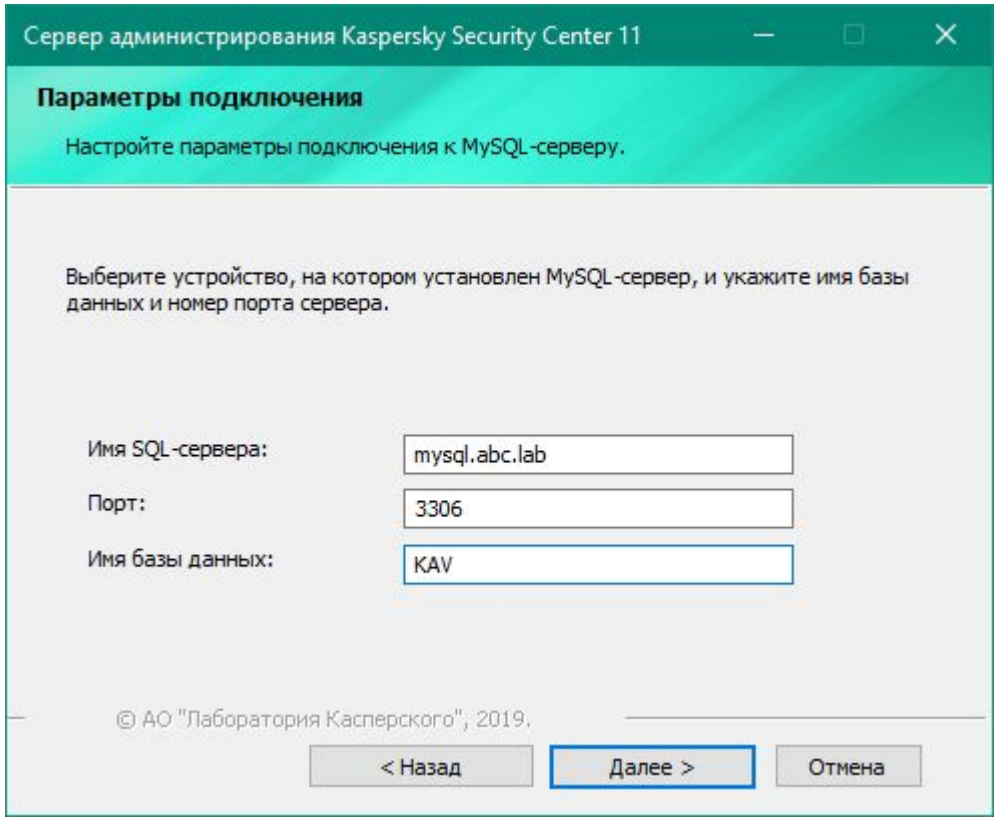
При режиме аутентификации Windows Сервер администрирования подключается к SQL-серверу от выбранной ранее учетной записи (KL-AK-* или выбранный пользователь)

Режим аутентификации SQL-сервера как правило не используется (выключен по умолчанию на стороне SQL-сервера)

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

Подключение к серверу MySQL



MySQL это система управления базами данных (СУБД) с открытым кодом, доступная в бесплатном и платном варианте

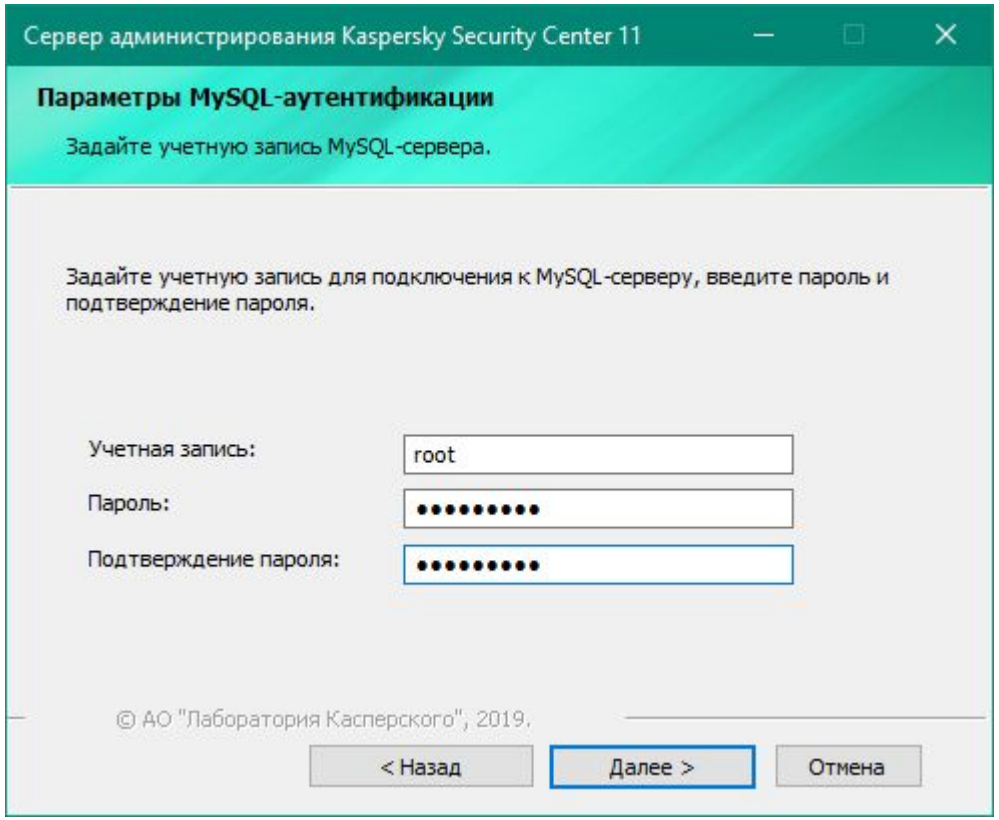
Инсталлятор KSC не обнаруживает серверы MySQL, администратор должен знать адрес сервера и порт, на котором MySQL принимает соединения (обычно, порт 3306)

Инсталлятор подключается к MySQL и создает базу данных с указанным именем, т.е. имя базы можно написать любое

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

Аутентификация на сервере MySQL



Укажите имя и пароль учетной записи, которая имеет права создавать базы данных на сервере MySQL

Как правило MySQL-сервер использует свои учетные записи, но в зависимости от настроек может принимать и учетные записи домена Windows

При нажатии на кнопку **Next** инсталлятор проверяет, может ли указанная учетная запись подключиться к выбранному серверу

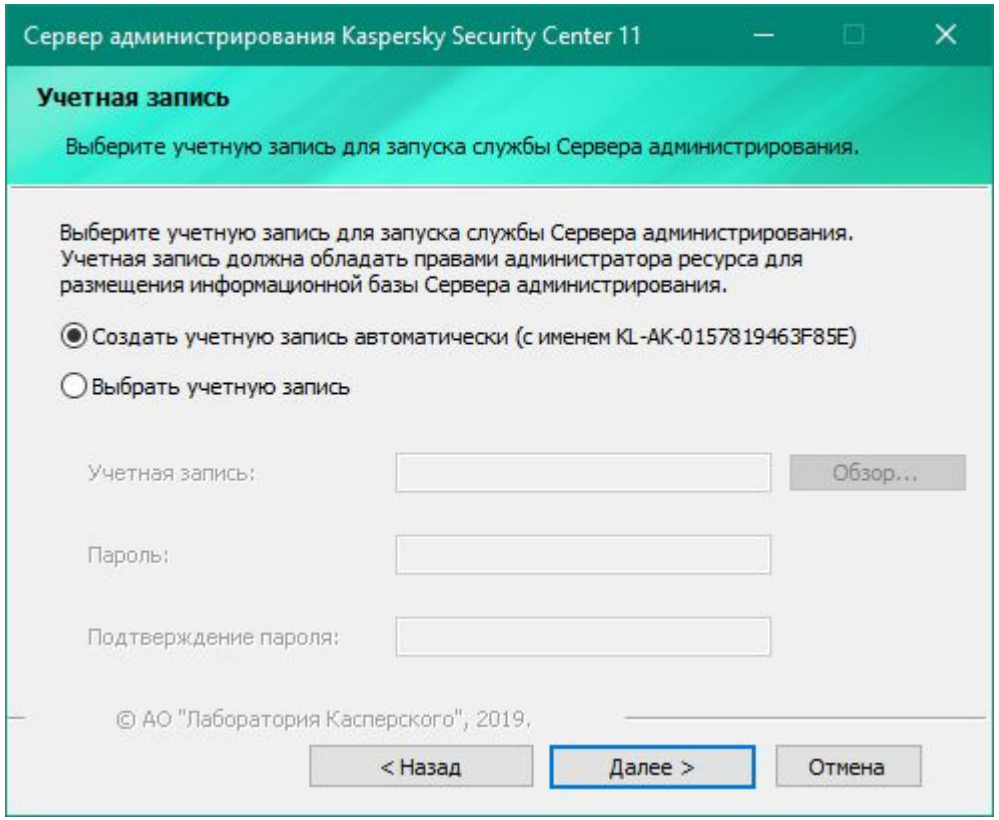
Если инсталлятор не может подключиться, то возвращает ошибку:

- У учетной записи недостаточно прав
- Невозможно найти сервер
- Версия сервера не поддерживается

Учетная запись для службы Сервера администрирования

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC



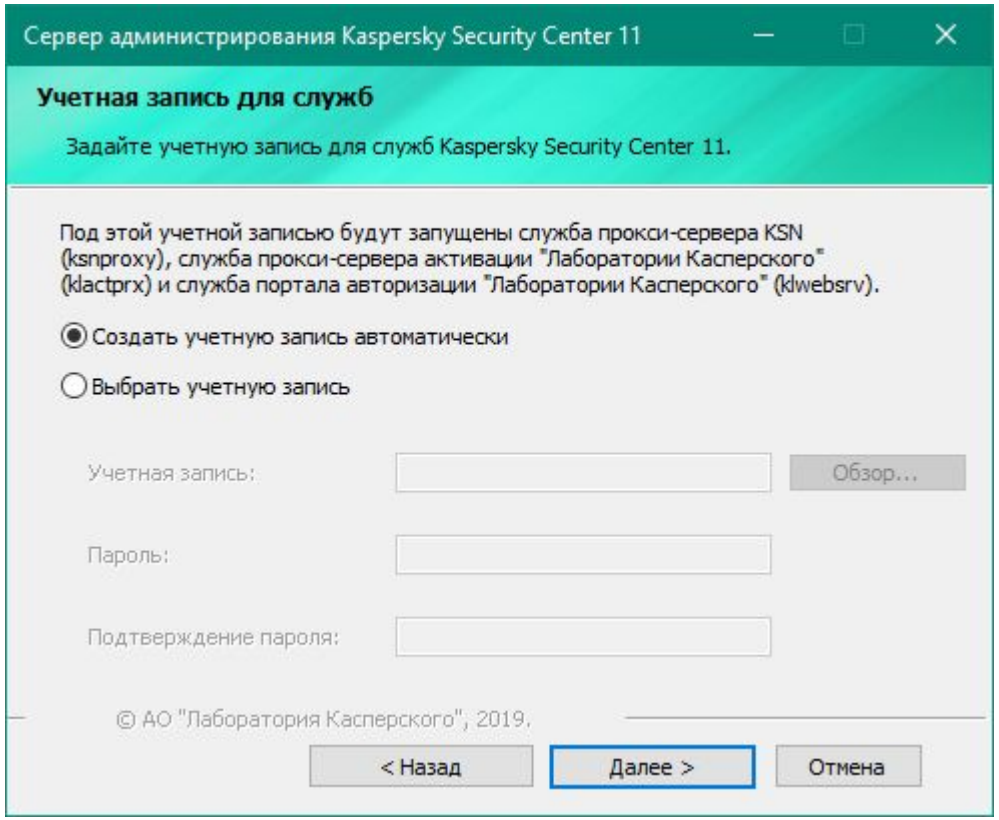
Учетная запись **KL-AK-*<набор символов>*** создается при установке и

- Имеет права эквивалентные правам локального администратора
- Не имеет права локального входа в операционную систему

Учетная запись для запуска других служб KSC

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC



Инсталлятор автоматически создает учетную запись **KlScSvc** и дает ей те же права что и учетной записи **KL-AK-***

Нужна для запуска служб:

- Прокси-сервер активации «Лаборатории Касперского»
- Веб-сервер «Лаборатории Касперского»
- Прокси-сервер Kaspersky Security Network

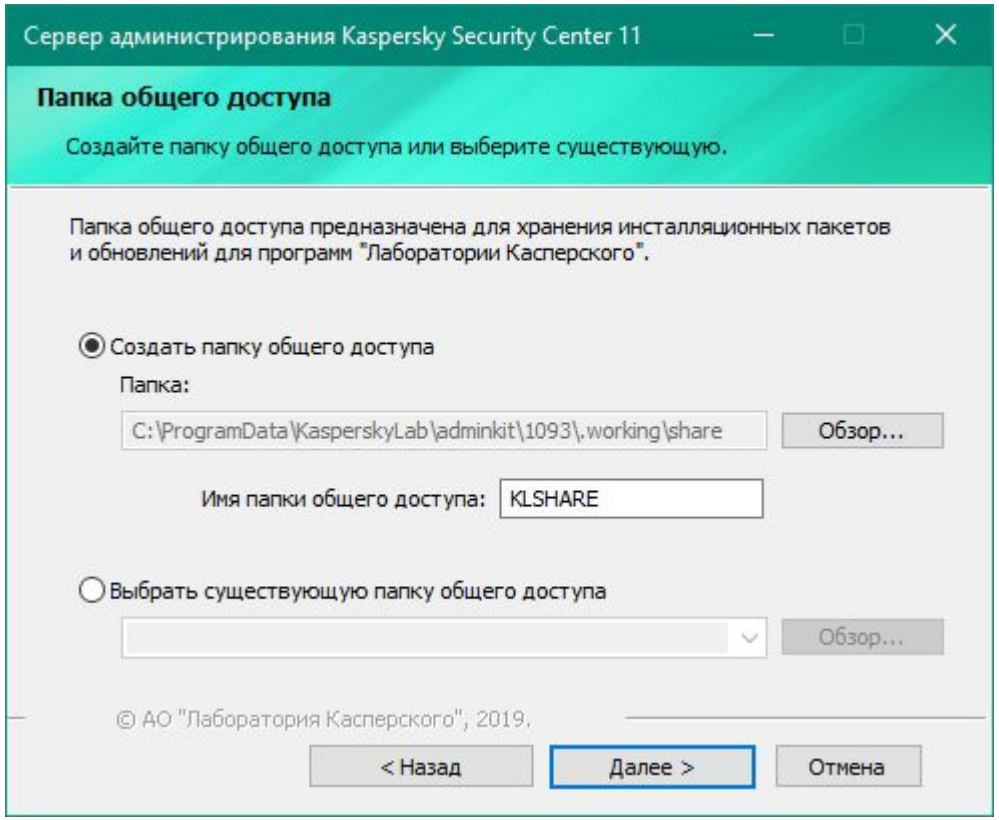
Еще две службы запускаются с правами локальной системы:

- Агент администрирования Kaspersky Security Center
- Объект автоматизации Kaspersky Security Center

Общая папка сервера администрирования

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC



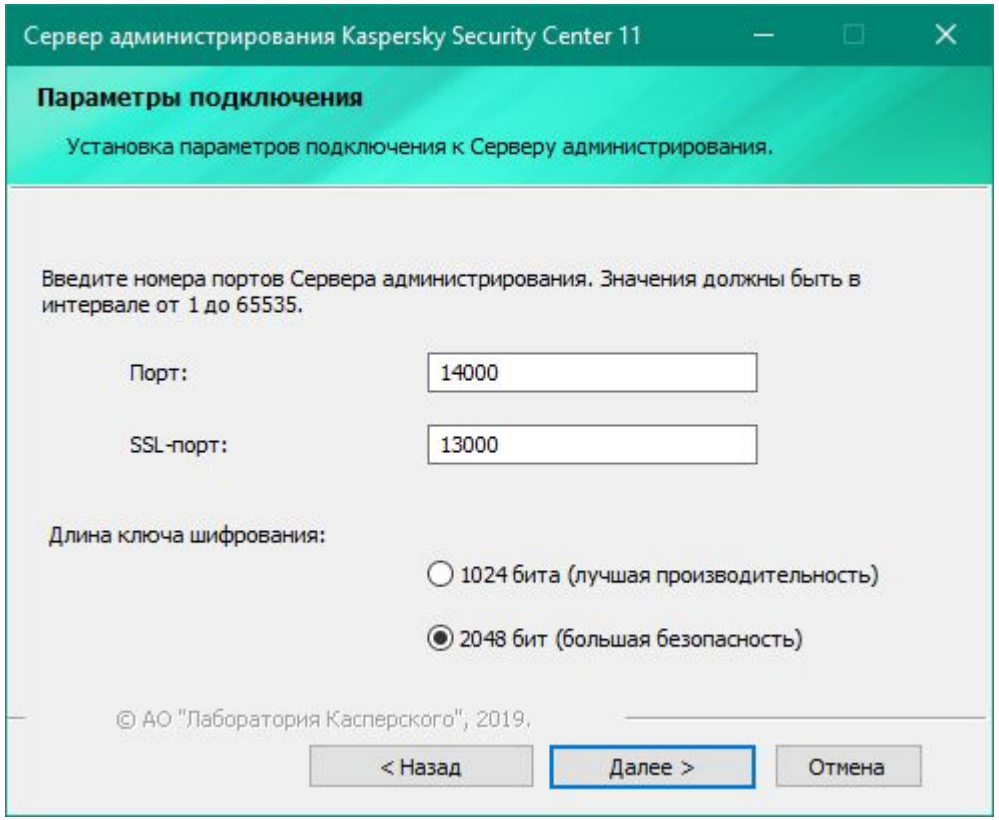
Общая папка используется для хранения:

- Обновлений
- Инсталляционных пакетов
- Автономных пакетов

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

Порты подключения



Порт 13000 (SSL) используется для подключения Агентов администрирования

Сертификат для SSL генерируется при установке Сервера администрирования и действителен в течении 10 лет

2048-битный сертификат устойчивее к атакам. На загрузку сервера администрирования длина сертификата практически не влияет

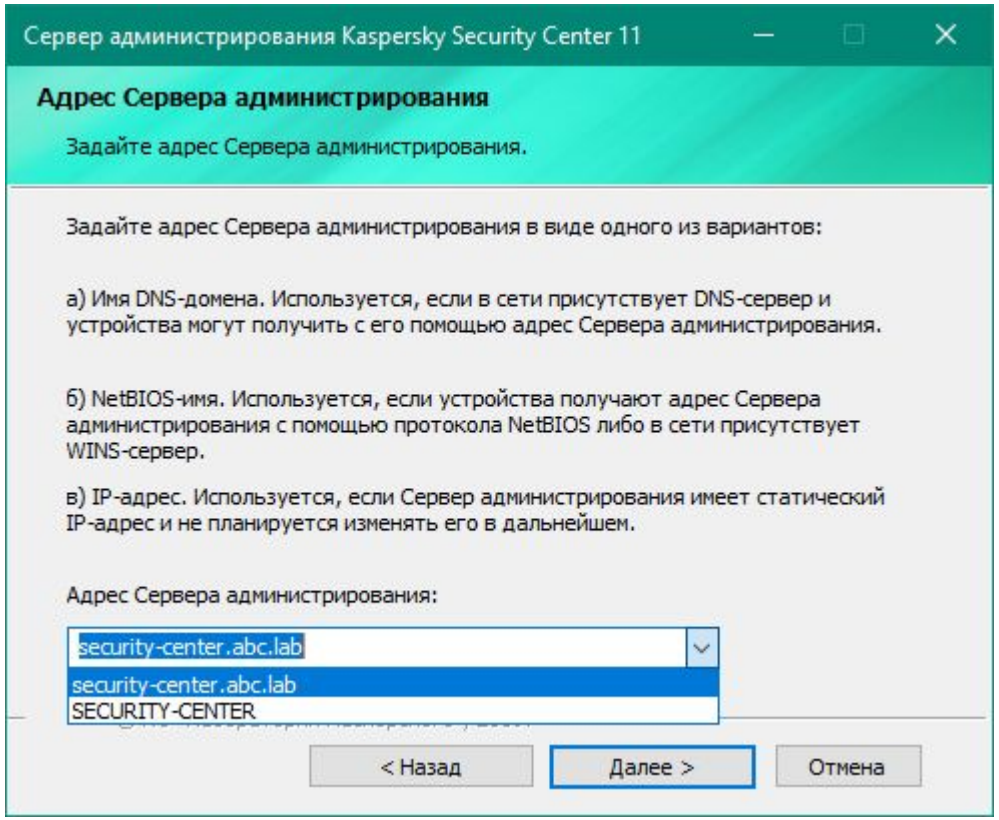
На TCP-порт 14000 подключаются агенты, на которых администратор отключил SSL. Используйте этот порт для поиска и устранения неполадок

Консоли KSC подключаются на TCP-порт 13291. Его можно изменить в свойствах сервера KSC после установки

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

Адрес подключения



Выбранный адрес Агенты администрирования будут использовать, чтобы соединиться с Сервером администрирования

Позже адрес можно изменить в свойствах инсталляционного пакета Агента администрирования

IP-адрес сервера в списке не отображается, но его можно ввести вручную.

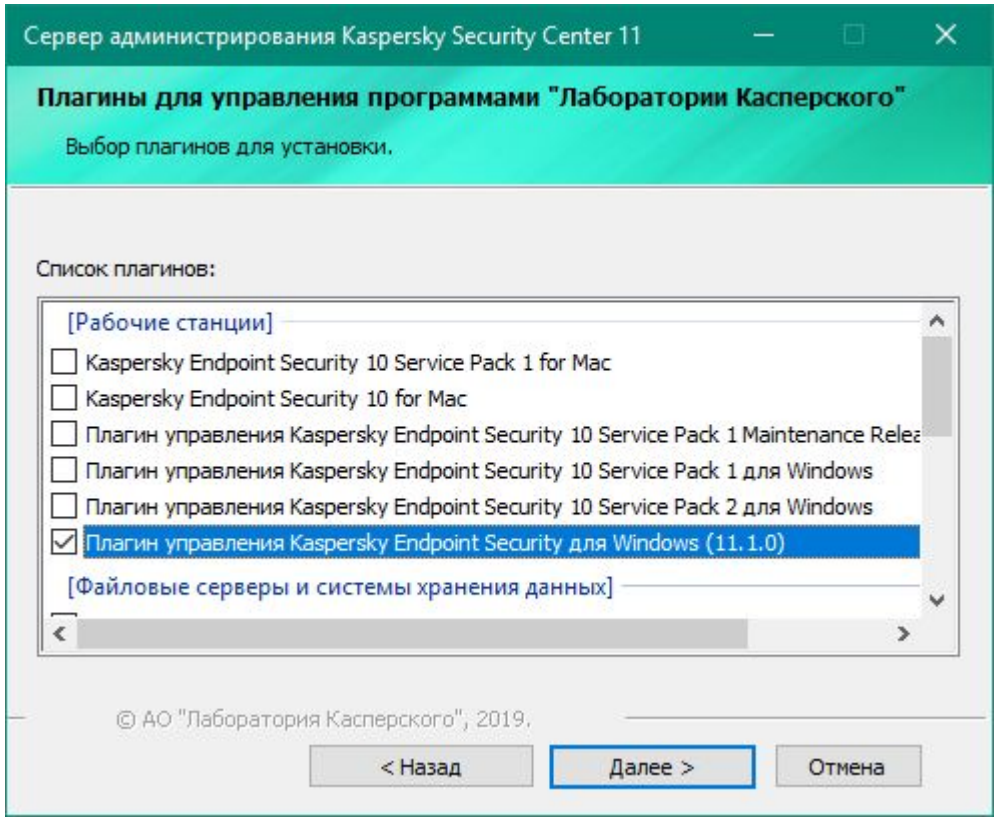
Не используйте для подключений динамический адрес Сервера администрирования

IPv6-адрес ввести нельзя. В IPv6-сетях используйте для подключений DNS-имя сервера

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

Плагины управления



По умолчанию выбран только плагин Kaspersky Endpoint Security for Windows (11.1.0)

Включите плагины программ, которые собираетесь устанавливать на компьютеры

Выключите плагины программ, которые использовать не собираетесь

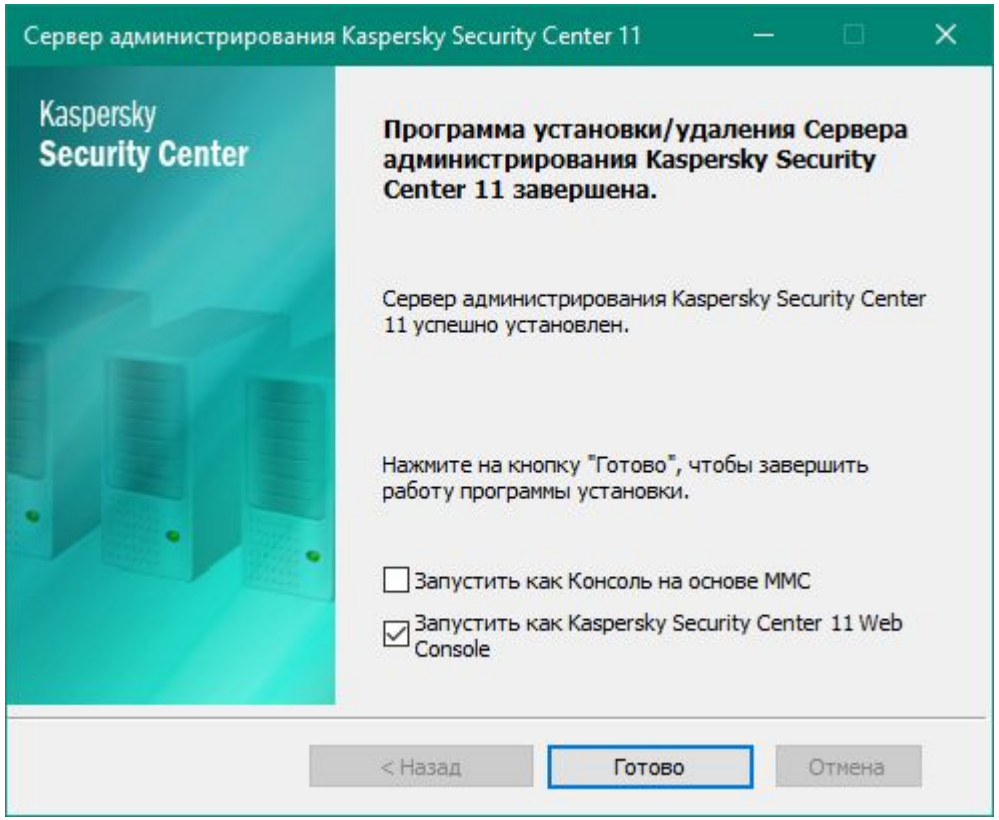
Можно установить позже из папки **Плагины** в дистрибутиве или из оболочки программы установки

Как удалить ненужные плагины, читайте в статье https://support.kaspersky.com/9303

Установка KSC:

1. Запустите мастер установки
2. Примите соглашение
3. Начните выборочную установку
4. Выберите компоненты
5. Установите Web Console
6. Укажите размер сети
7. Выберите тип SQL-сервера
8. Укажите адрес SQL-сервера
9. Укажите учетную запись SQL-сервера
10. Выберите учетную запись Сервера KSC
11. Выберите учетную запись вспомогательных служб
12. Выберите общую папку Сервера KSC
13. Выберите порты и сертификат сервера KSC
14. Выберите адрес сервера KSC
15. Выберите плагины
16. Начните установку
17. Подождите 5-15 минут
18. Завершите установку и запустите консоль KSC

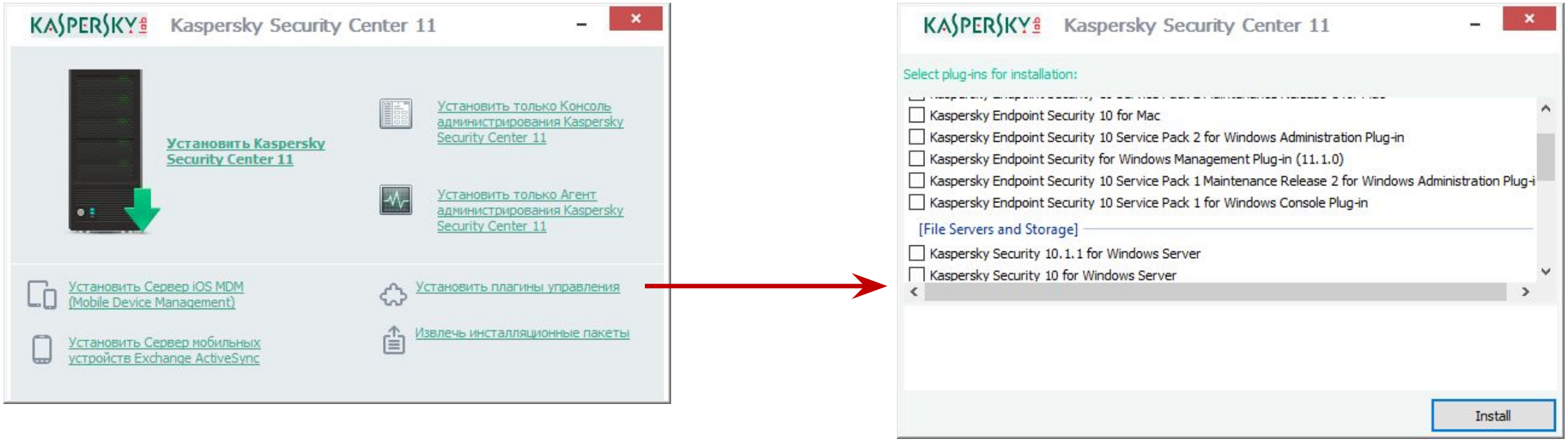
Завершение установки



Рекомендуется после установки запустить Консоль администрирования, чтобы задать первоначальные настройки Сервера администрирования

Запустить можно как MMC-консоль, так и Web Console (если вторая была установлена вместе с Kaspersky Security Center)

Установка дополнительных плагинов



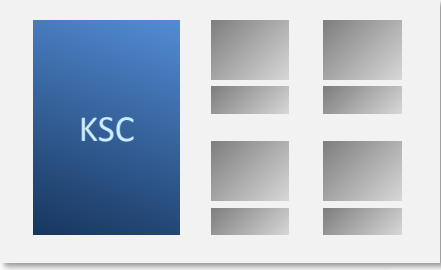
Необходимые плагины можно добавить из общей оболочки для установки компонентов Kaspersky Security Center

Результат стандартной установки

Параметр	Значение	
Компоненты	Kaspersky Security Center Administration Server Агент администрирования Kaspersky Security Center Консоль администрирования Kaspersky Security Center Kaspersky Security Center Web Console	
Пути установки	%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console 11 %ProgramData%\KasperskyLab\AdminKit %ProgramData%\KasperskySC\SC_Backup	
Службы	Сервер администрирования Kaspersky Security Center Агент администрирования Kaspersky Security Center Объект автоматизации Kaspersky Security Center Прокси-сервер Kaspersky Security Network Веб-сервер «Лаборатории Касперского» Прокси-сервер активации «Лаборатории Касперского» Kaspersky Security Center 11 Management Service Kaspersky Security Center 11 Web Console Kaspersky Security Center 11 Web Console Message Queue	(**KL-AK-***) (Локальная система) (Локальная система) (**KlScSvc**) (**KlScSvc**) (**KlScSvc**) (Локальная система) (Network Service) (Network Service)
Папка общего доступа	KLSHARE (%ProgramData%\KasperskyLab\adminkit\1093\.working\Share)	

Результат стандартной установки

Параметр	Значение
Группы	KLAdmins, KLOperators
Учетные записи	KL-AK-* KlScSvc
Порты	8060 — http-порт веб-сервера Лаборатории Касперского 8061 — https-порт веб-сервера Лаборатории Касперского 13000 — SSL-подключения Агентов 14000 — обычные подключения Агентов и Консолей администрирования 13291 — SSL-подключение для Консоли администрирования (MMC) 13111 — порт прокси-сервера KSN 17000 — порт SSL для прокси-сервера активации Лаборатории Касперского 13299 — SSL-подключение для Web Console
Плагины	Сервер администрирования Kaspersky Security Center 11 (11.0) Агент администрирования Kaspersky Security Center 11 (11.0) Kaspersky Endpoint Security 11.1 для Windows Kaspersky Mobile Device Management 11
Пакеты	Kaspersky Endpoint Security 11.1 для Windows Kaspersky Security Center 11 Network Agent Microsoft Exchange Mobile Devices Server iOS MDM Server



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Требования к Серверу администрирования

Установка Сервера администрирования

Установка Kaspersky Security Center Web Console

Мастер первоначальной настройки

Часть II. Управление защитой

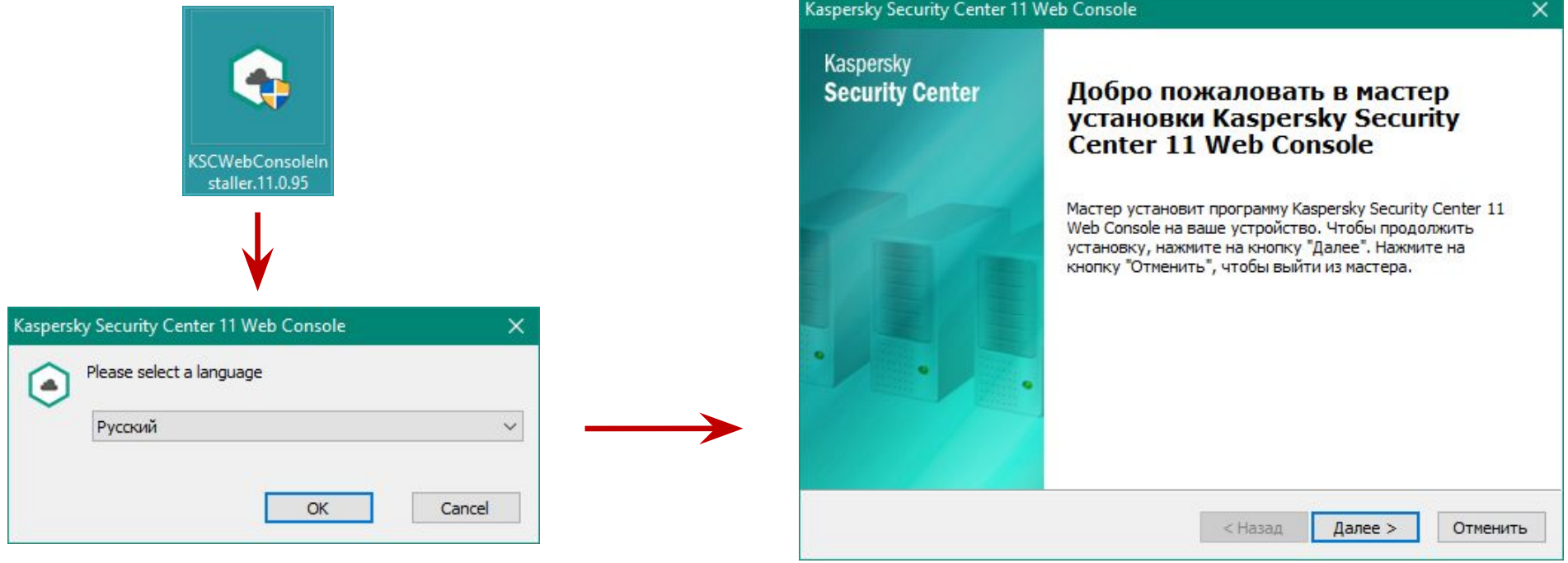
Часть III. Контроль

Часть IV. Сопровождение

Установка Web Console

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Укажите путь установки
4. Укажите параметры подключения к Web Console
5. Задайте учетные записи
6. Выберите сертификат
7. Укажите параметры подключения к Kaspersky Security Center
8. Запустите установку
9. Завершите установку – запустите KSC 11 Web Console



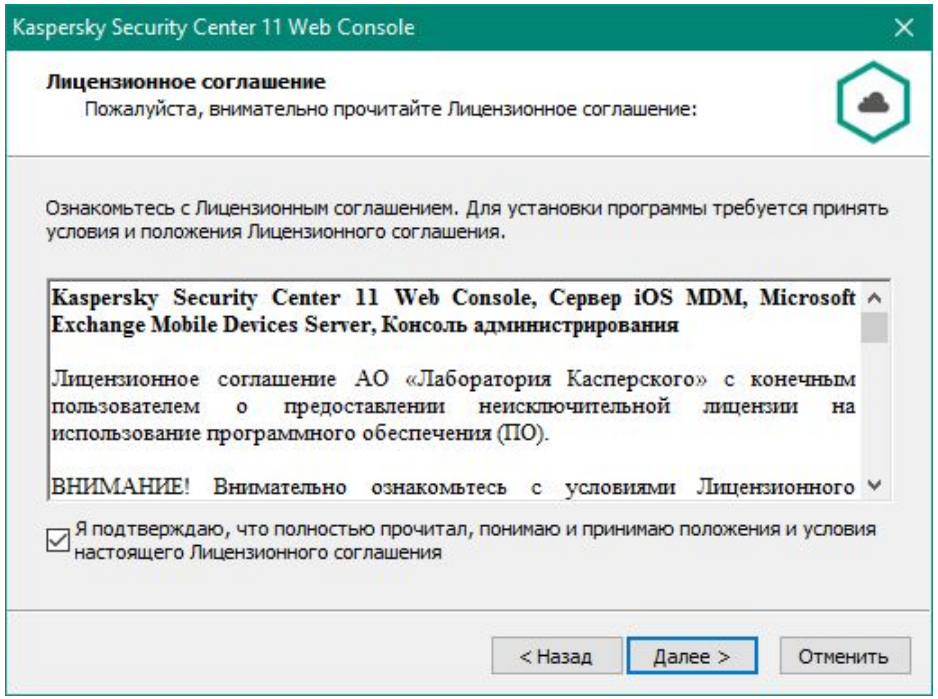
Web Console – это отдельный дистрибутив, который можно установить как вместе с Kaspersky Security Center, так и на отдельный компьютер

На первом шаге необходимо выбрать язык мастера установки

Установка Web Console

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Укажите путь установки
4. Укажите параметры подключения к Web Console
5. Задайте учетные записи
6. Выберите сертификат
7. Укажите параметры подключения к Kaspersky Security Center
8. Запустите установку
9. Завершите установку – запустите KSC 11 Web Console

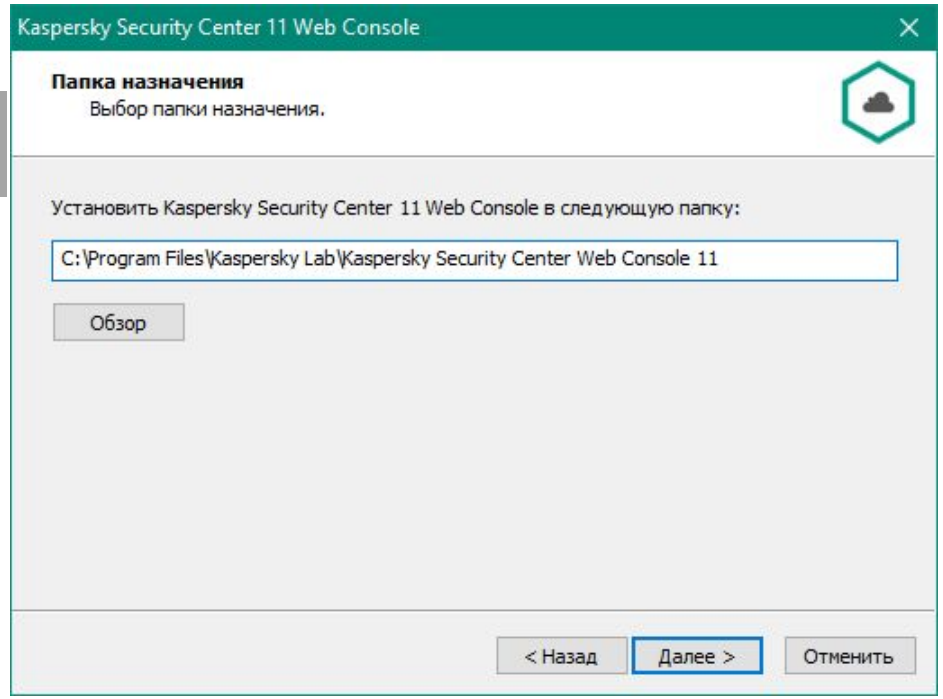


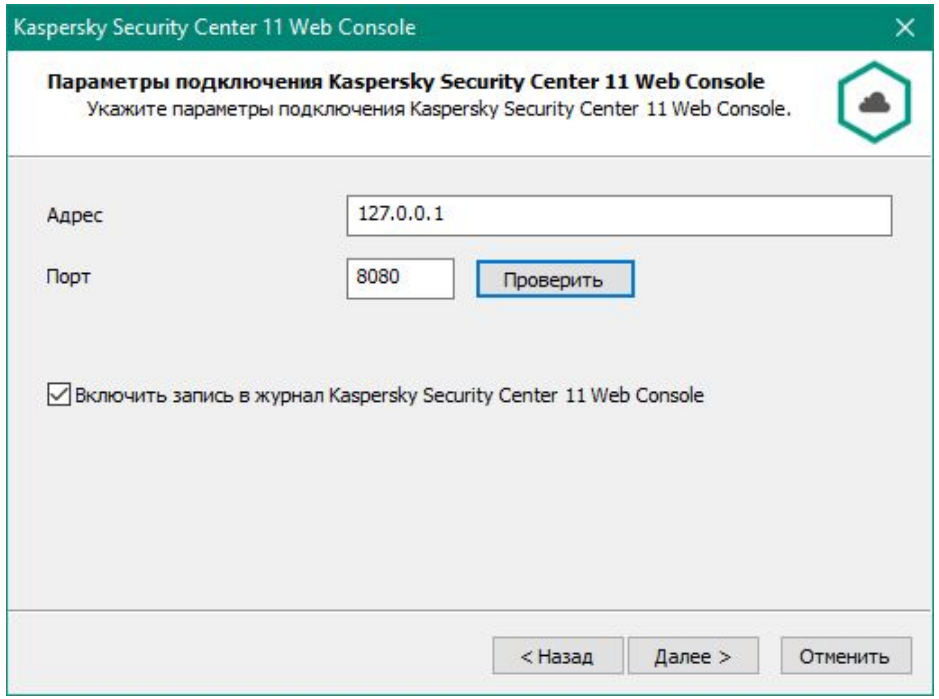
На следующем шаге необходимо принять лицензионное соглашение

Установка Web Console

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Укажите путь установки
4. Укажите параметры подключения к Web Console
5. Задайте учетные записи
6. Выберите сертификат
7. Укажите параметры подключения к Kaspersky Security Center
8. Запустите установку
9. Завершите установку – запустите KSC 11 Web Console





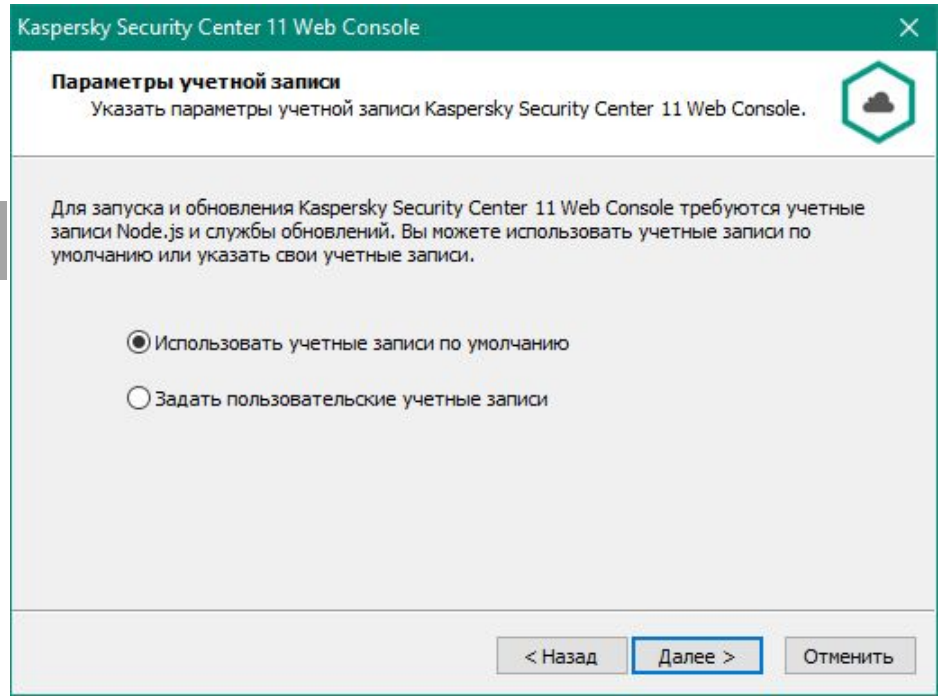
Далее необходимо указать путь установки, рекомендуется оставить по умолчанию

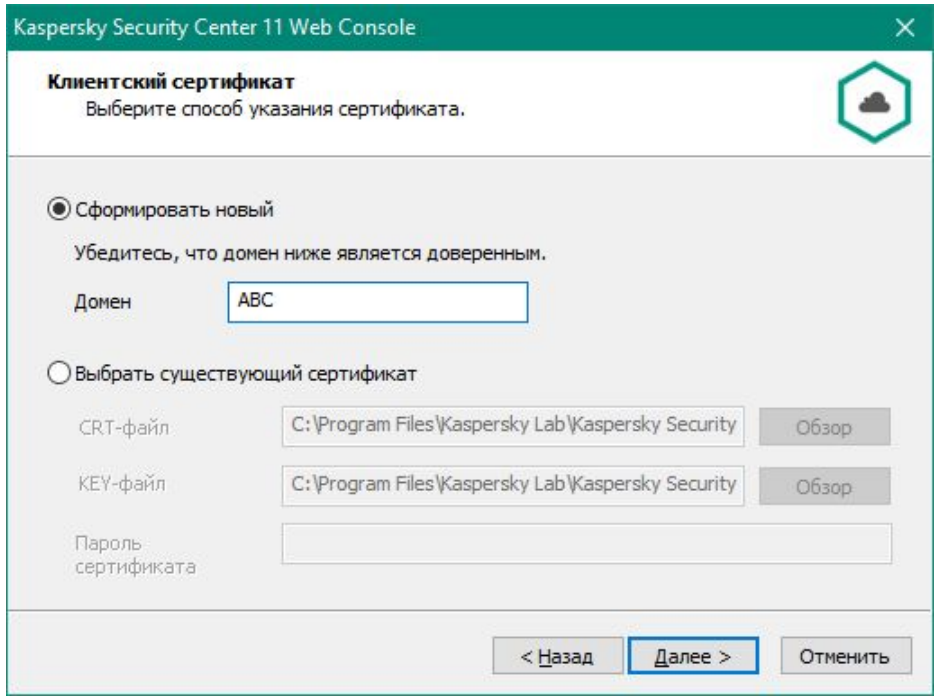
Затем надо указать адрес и порт, которые будут использоваться для подключения к Web Console

Установка Web Console

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Укажите путь установки
4. Укажите параметры подключения к Web Console
5. Задайте учетные записи
6. Выберите сертификат
7. Укажите параметры подключения к Kaspersky Security Center
8. Запустите установку
9. Завершите установку – запустите KSC 11 Web Console





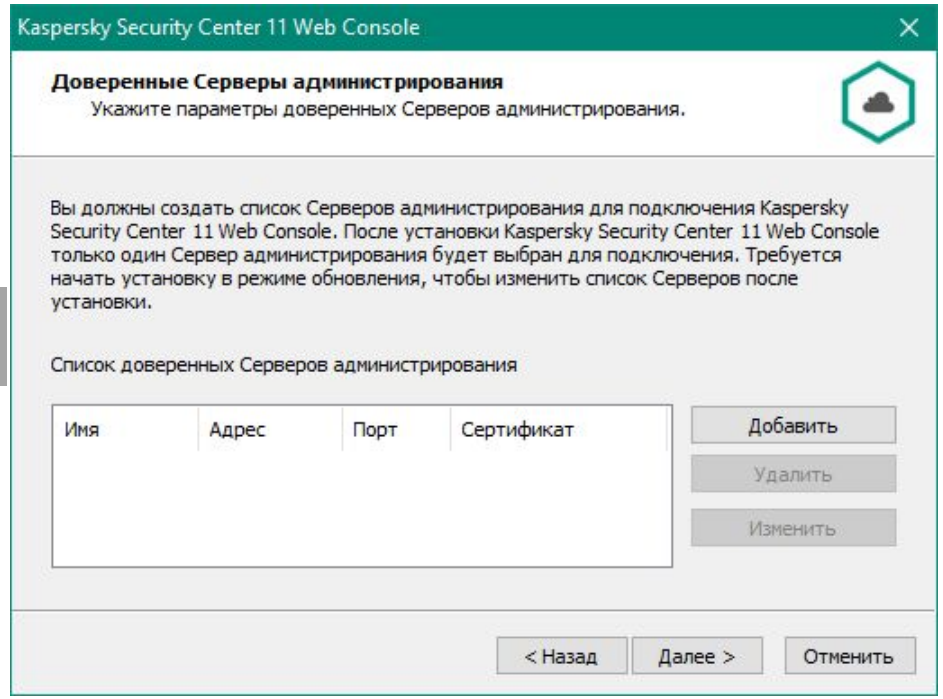
По умолчанию, службы Web Console будут запускаться под системными учетными записями, но можно задать свои

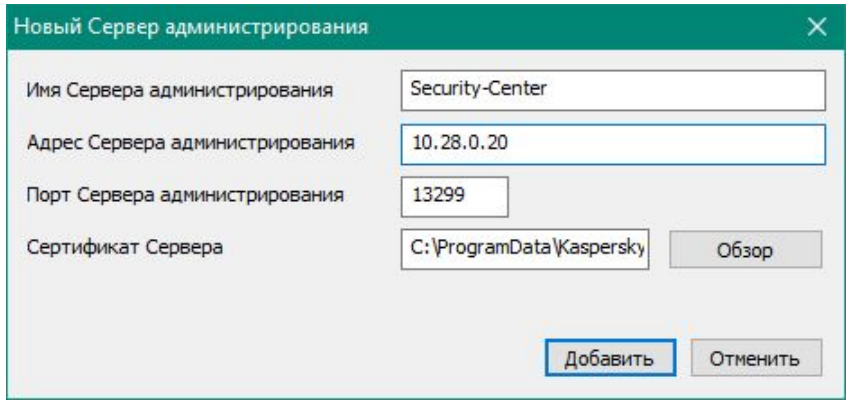
Следующий шаг это создание сертификата веб-сервера, на котором будет крутиться Web Console. Сертификат будет генерироваться автоматически или можно подложить свой.

Установка Web Console

Установка Web Console:

1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Укажите путь установки
4. Укажите параметры подключения к Web Console
5. Задайте учетные записи
6. Выберите сертификат
7. Укажите параметры подключения к Kaspersky Security Center
8. Запустите установку
9. Завершите установку – запустите KSC 11 Web Console





На этом шаге администратор указывает с какими Kaspersky Security Center сможет взаимодействовать Web Console

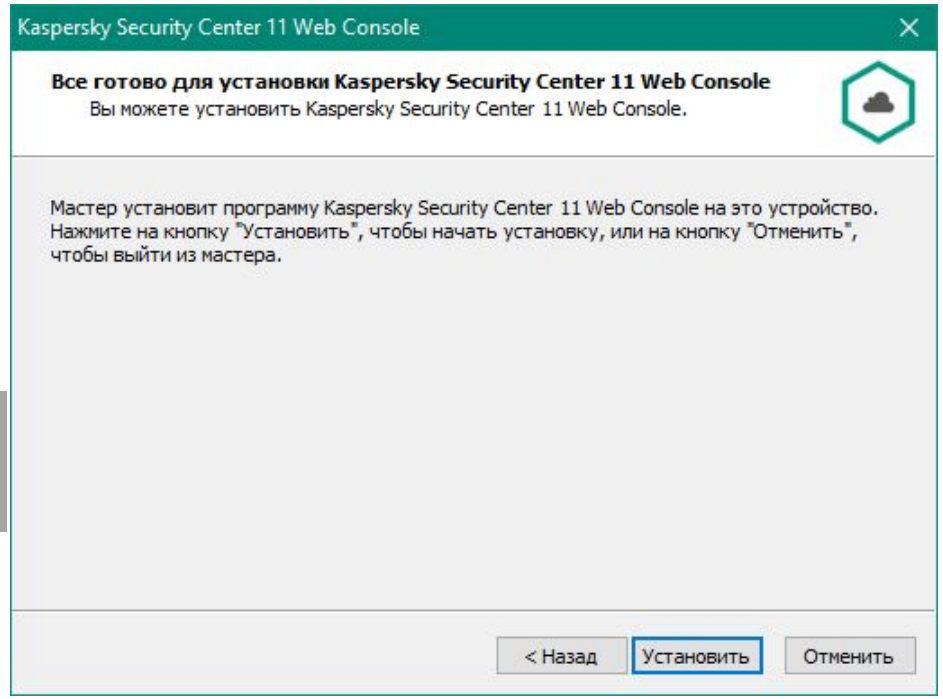
Порт Сервера администрирования, по умолчанию 13299, но его можно изменить в свойствах Сервера

Если Web Console ставится на компьютер, на котором уже установлен KSC, то этот KSC автоматически появится в списке

Установка Web Console

Установка Web Console:

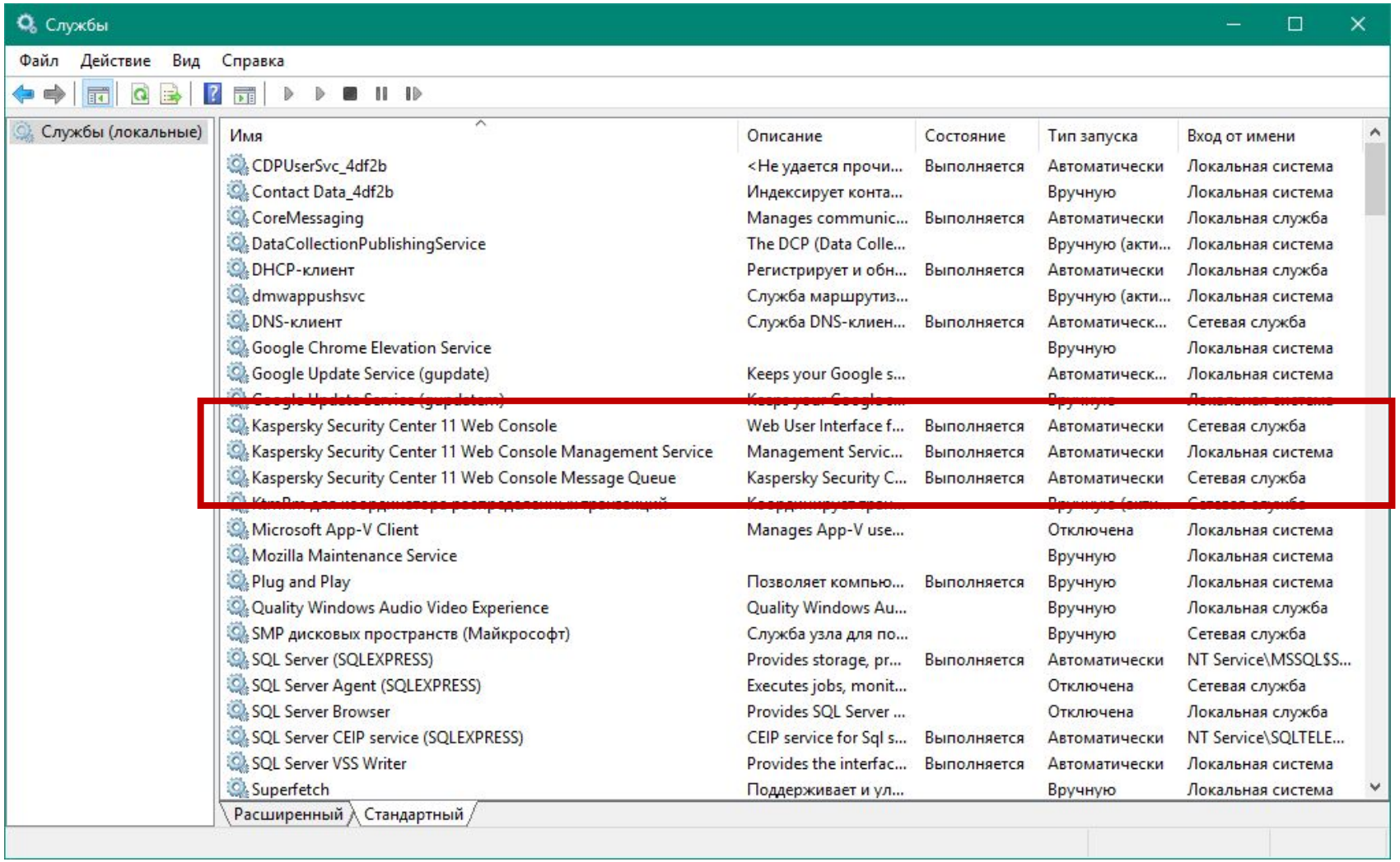
1. Запустите мастер установки
2. Примите лицензионное соглашение
3. Укажите путь установки
4. Укажите параметры подключения к Web Console
5. Задайте учетные записи
6. Выберите сертификат
7. Укажите параметры подключения к Kaspersky Security Center
8. Запустите установку
9. Завершите установку – запустите KSC 11 Web Console



Предпоследний шаг – это запустить процесс установки кнопкой **Установить**

Ну и последний шаг – запустить Web Console и завершить мастер или просто завершить мастер

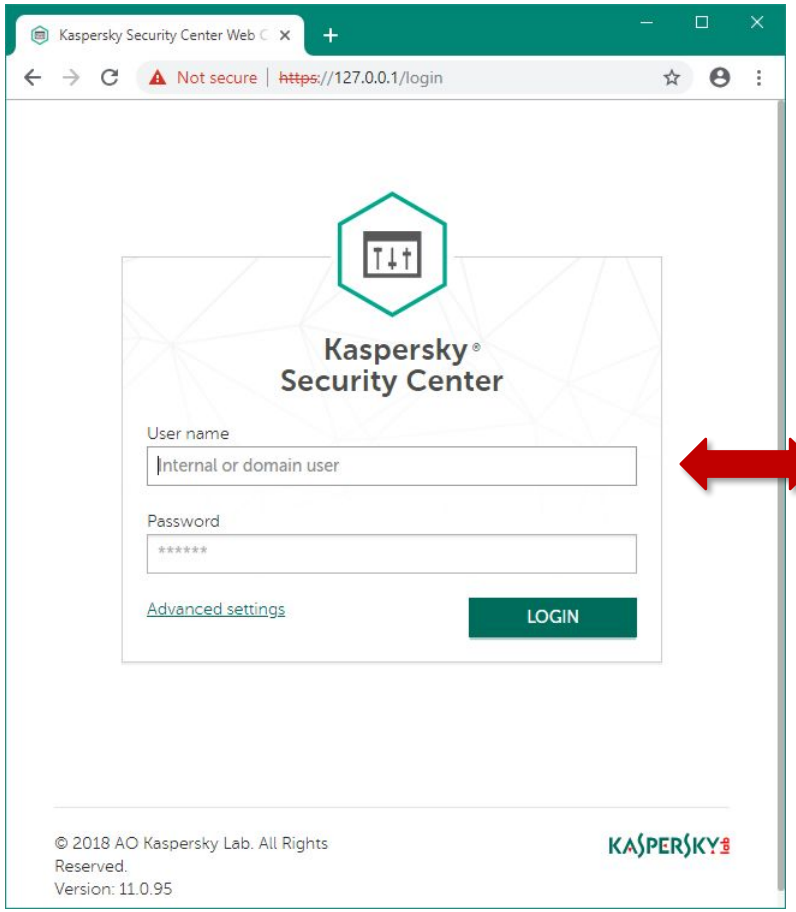
Службы Web Console

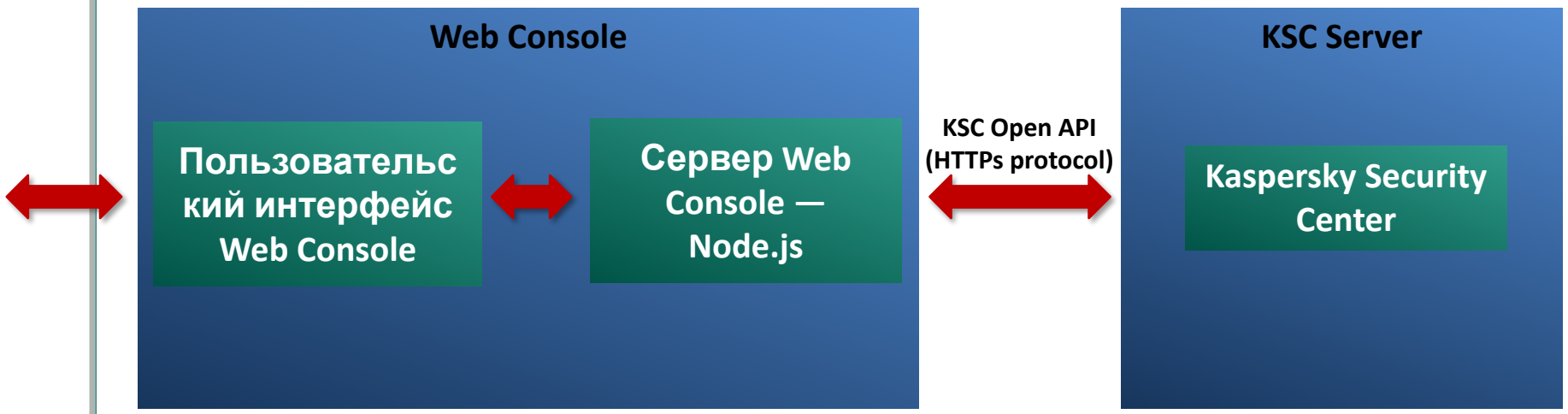


В процессе установки Web Console устанавливаются следующие службы:

- Kaspersky Security Center 11 Web Console Management Service
- Kaspersky Security Center 11 Web Console
- Kaspersky Security Center 11 Web Console Message Queue — платформа для обработки очереди сообщений на базе NSQ

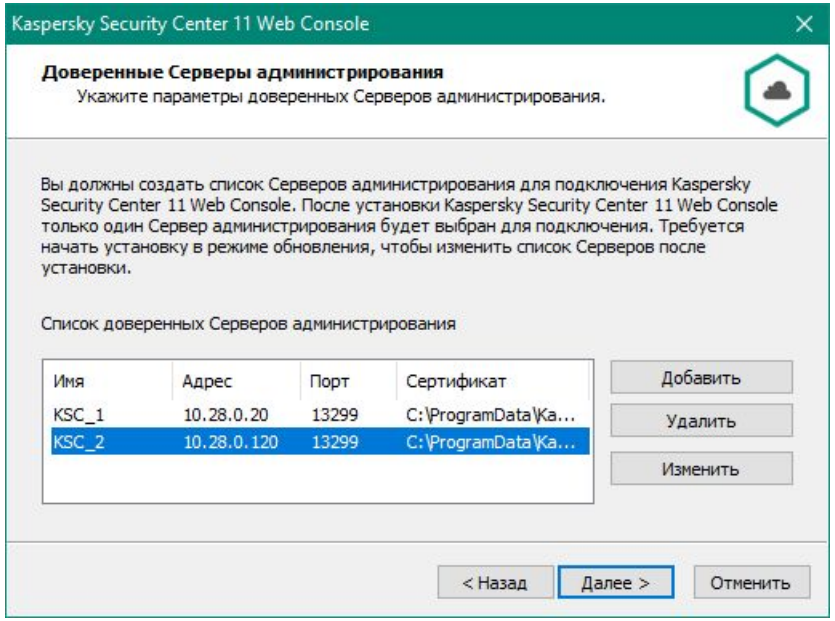
Web Console: взаимодействие

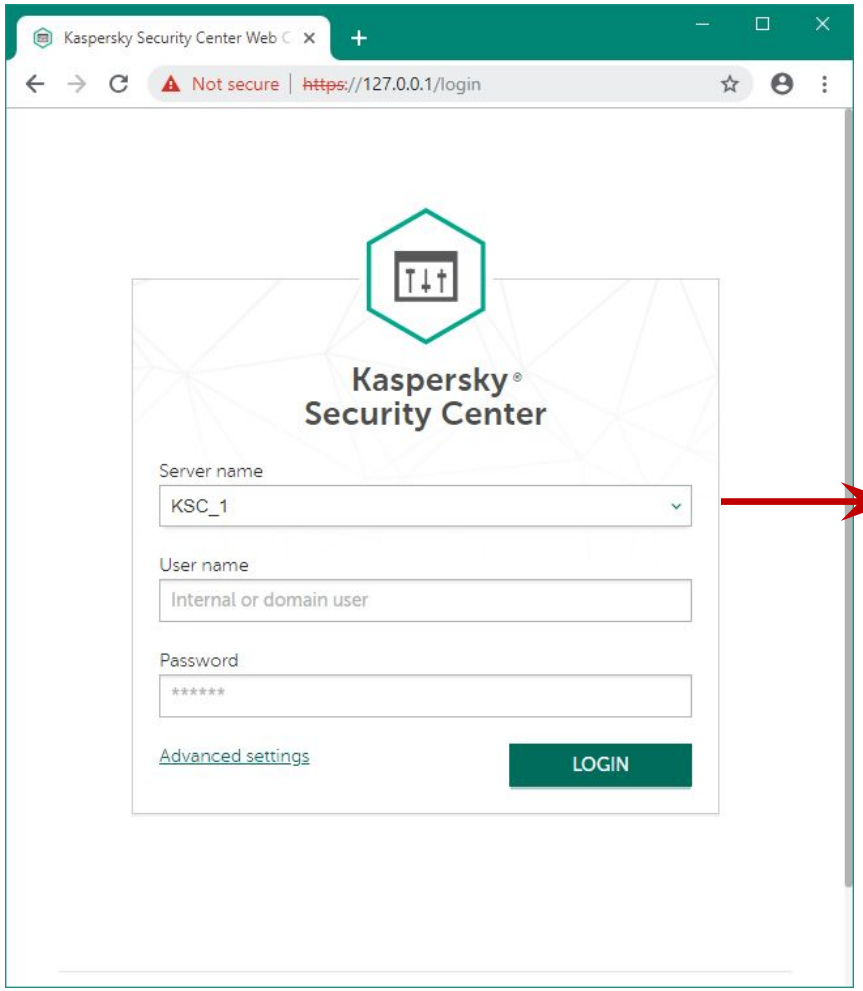




KASPERSKY

Подключение к нескольким KSC



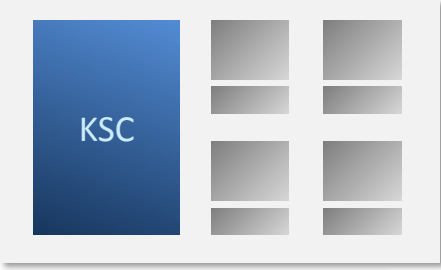


Запустить **Обновление** в мастере удаления программы

Если Web Console видит, что у нее больше одного доверенного сервера, то на странице входа появится дополнительное поле Server name

Требования к браузерам для работы с Web Console

- Поддерживаемые браузеры:
  - Google Chrome
  - Mozilla Firefox
  - Safari



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

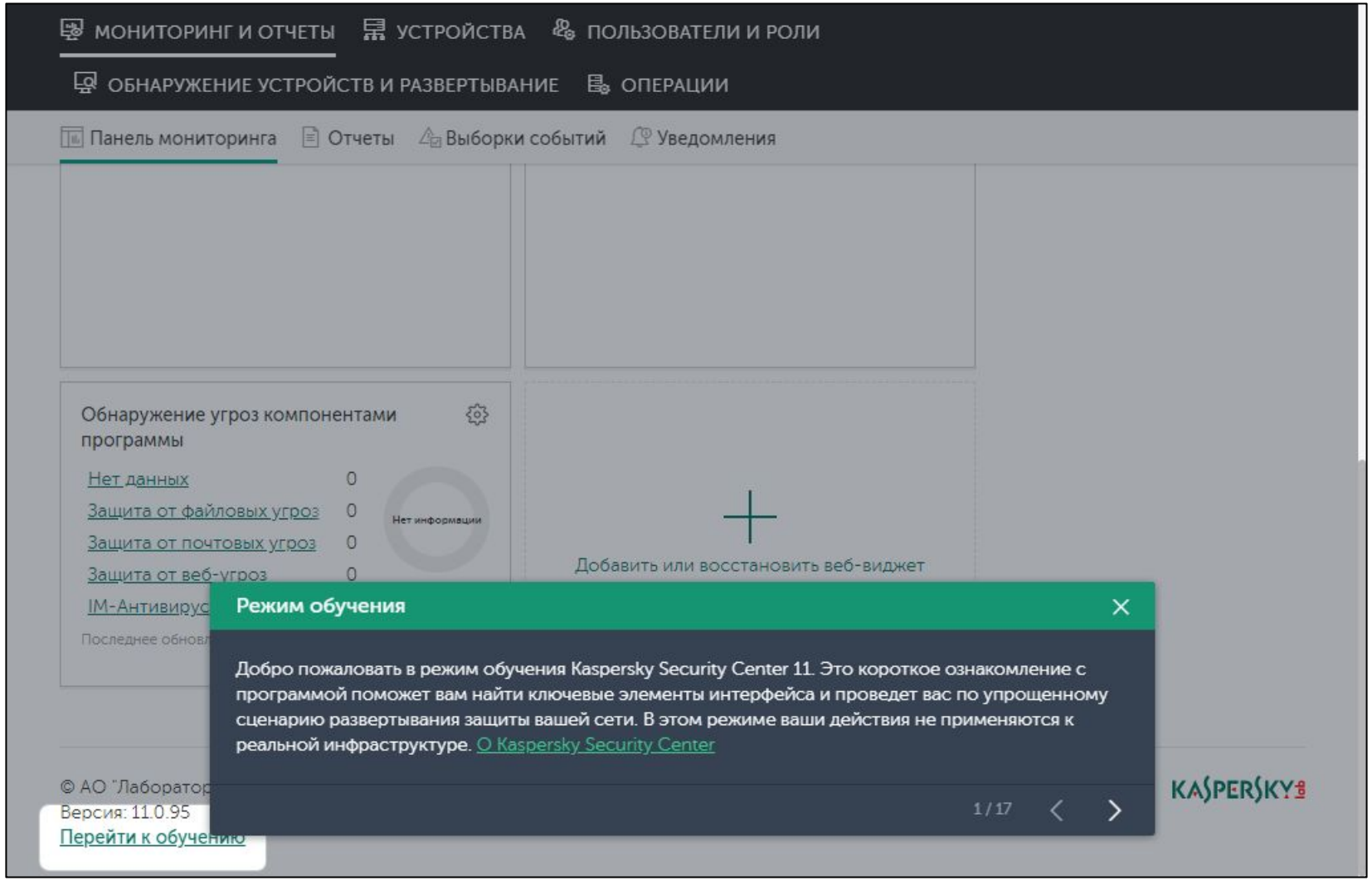
Требования к Серверу администрирования
Установка Сервера администрирования
Установка Kaspersky Security Center Web Console
Мастер первоначальной настройки

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Где что в Kaspersky Security Center Web Console?



При первом подключении к Web Console выскакивает **Режим обучения**

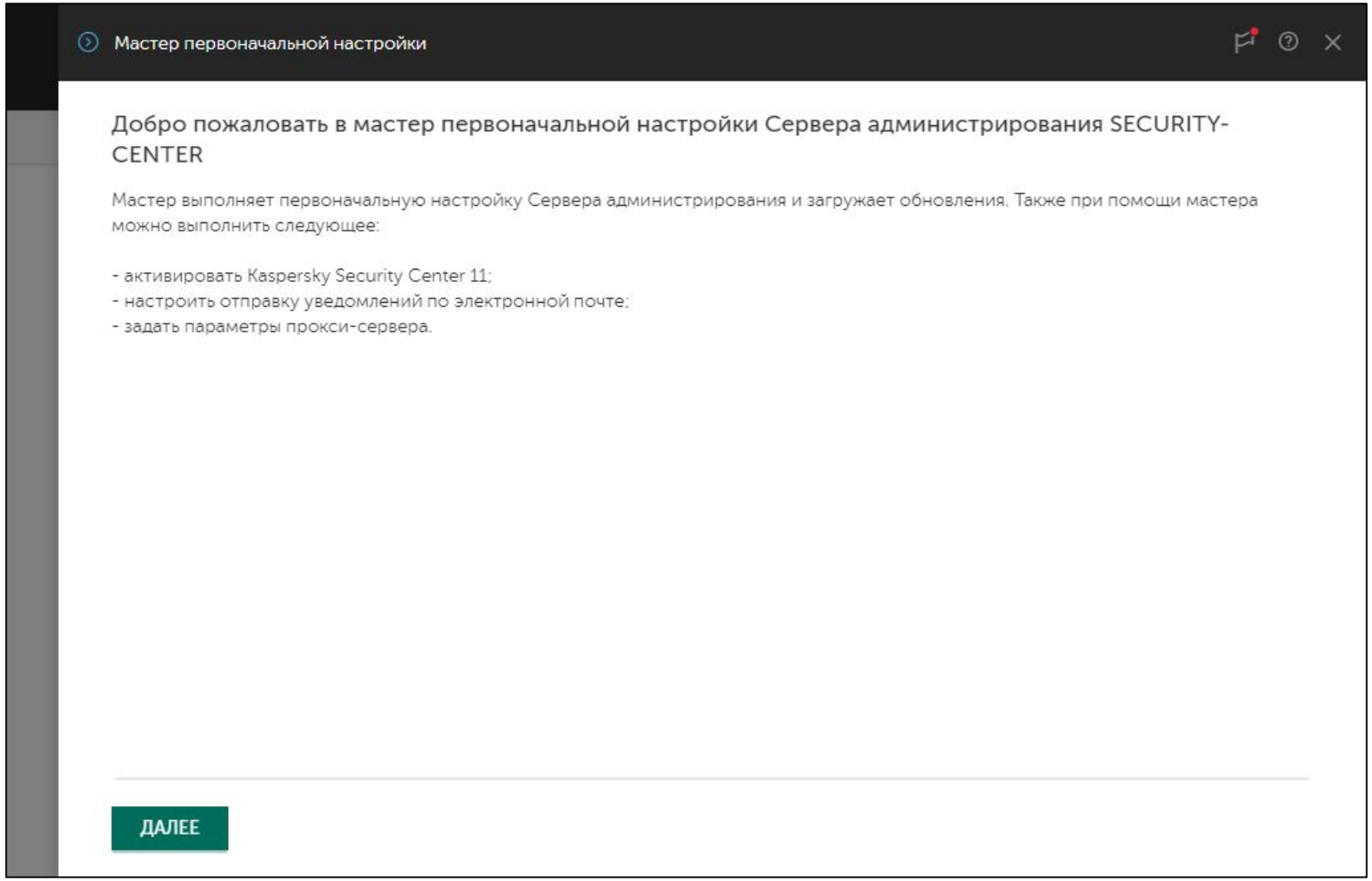
Это 17 шагов, которые рассказывают, где что находится в Web Console

Мы рекомендуем ознакомиться с этим **Режимом обучения**

Если вы случайно закрыли **Режим обучения** или хотите еще раз ознакомиться с ним, в главном окне внизу есть ссылка **Перейти к обучению**

При первом подключении после закрытия **Режима обучения** запускается **Мастер первоначальной настройки**

Мастер первоначальной настройки



Мастер первоначальной настройки запускается после первого подключения к серверу и готовит сервер к работе:

- Создает задачи и политики
- Загружает обновления в хранилище на Сервере администрирования

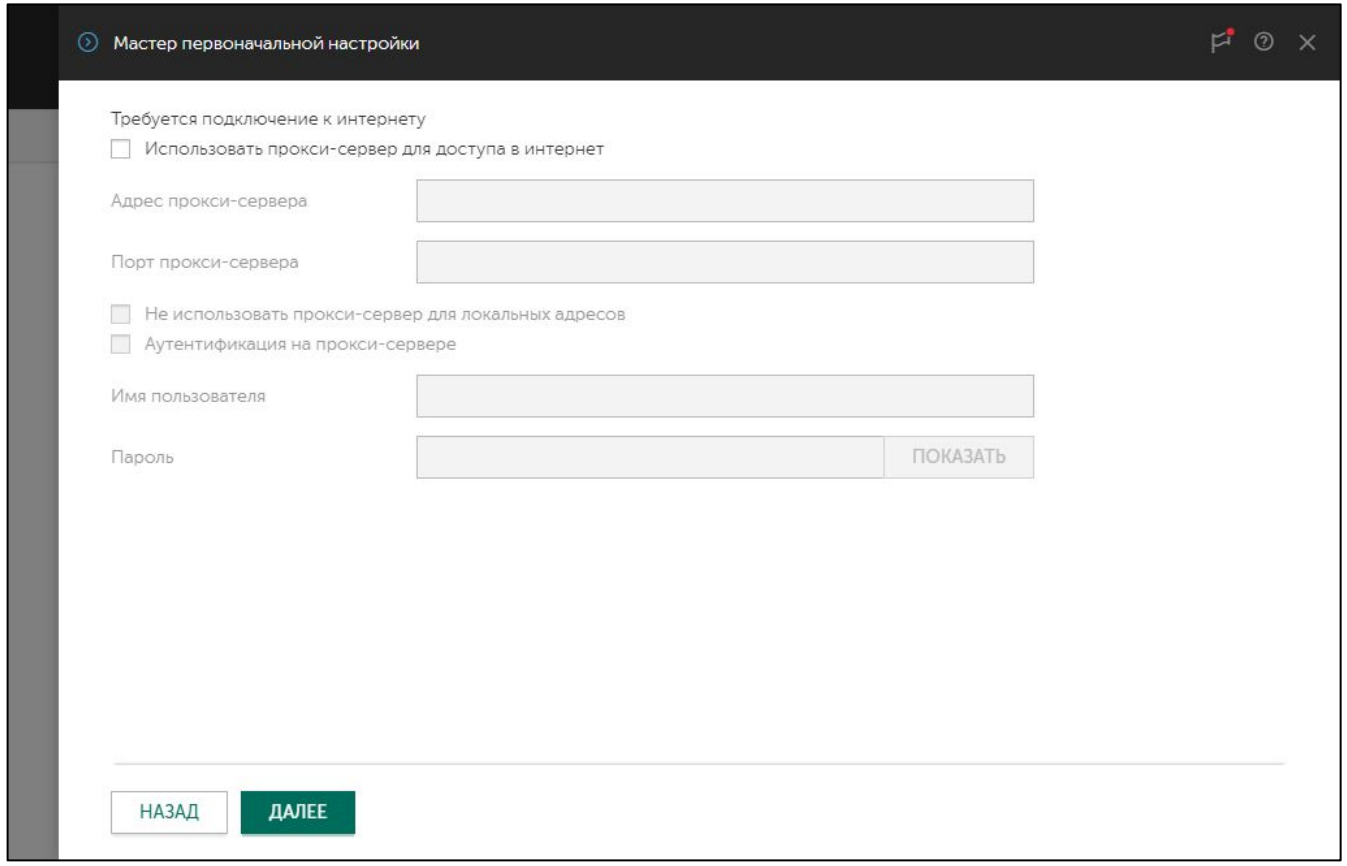
Мастер просит администратора:

- Настроить подключение к Интернет
- Добавить лицензию
- Принять соглашение Kaspersky Security Network
- Указать почтовый адрес, на который будут приходить отчеты и уведомления

Настройка доступа в Интернет

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты



Укажите параметры прокси-сервера для доступа в Интернет, или пропустите этот шаг, если для доступа в Интернет прокси-сервер не используется

Доступ в Интернет нужен:

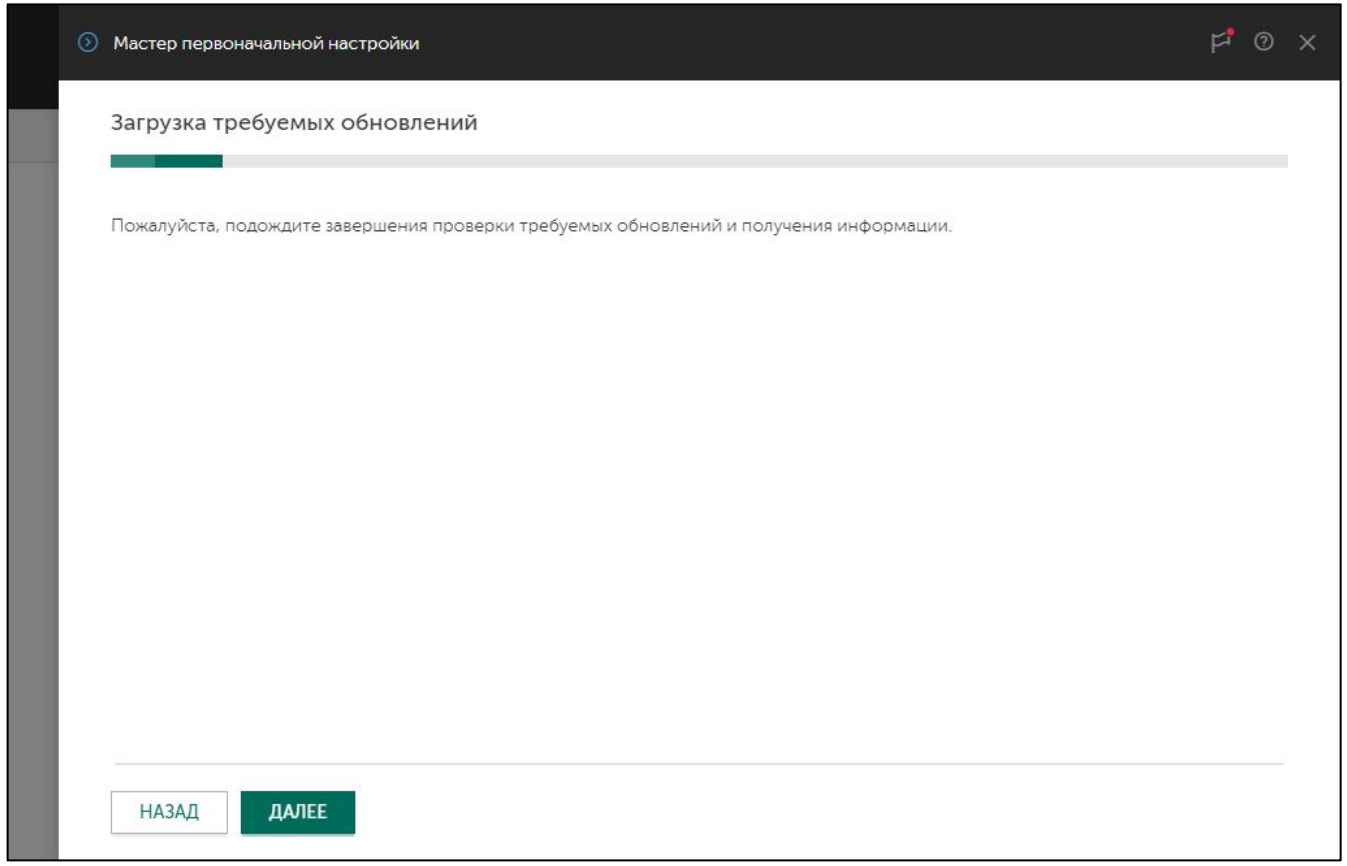
— Чтобы загружать обновления

— Чтобы перенаправлять запросы в Kaspersky Security Network от клиентских компьютеров, когда Сервер администрирования выступает в роли KSN-прокси

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Загрузка информации о плагинах

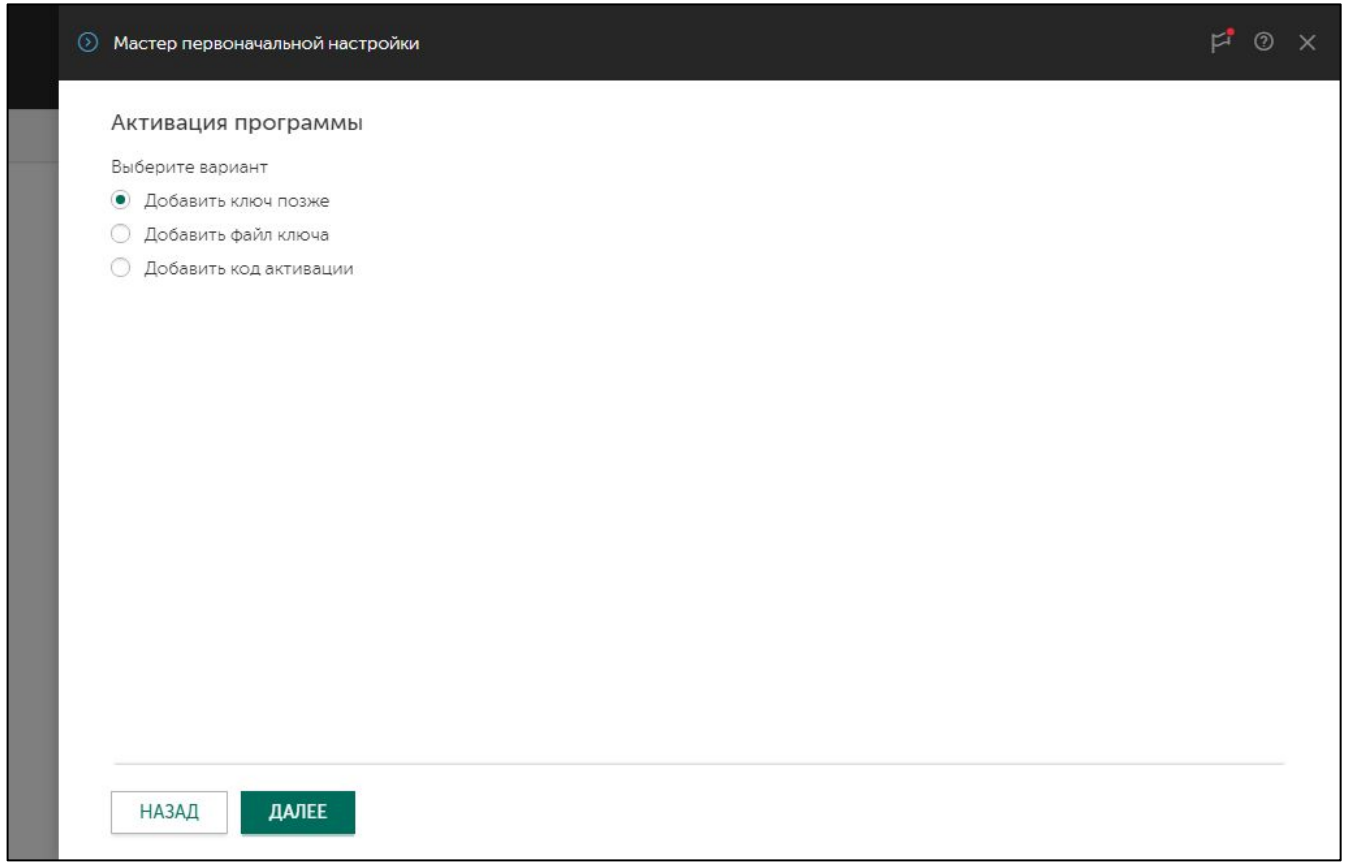


Мастер подключается к серверам Лаборатории Касперского и проверяет информацию о доступных плагинах для Web Console

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Выбор лицензии



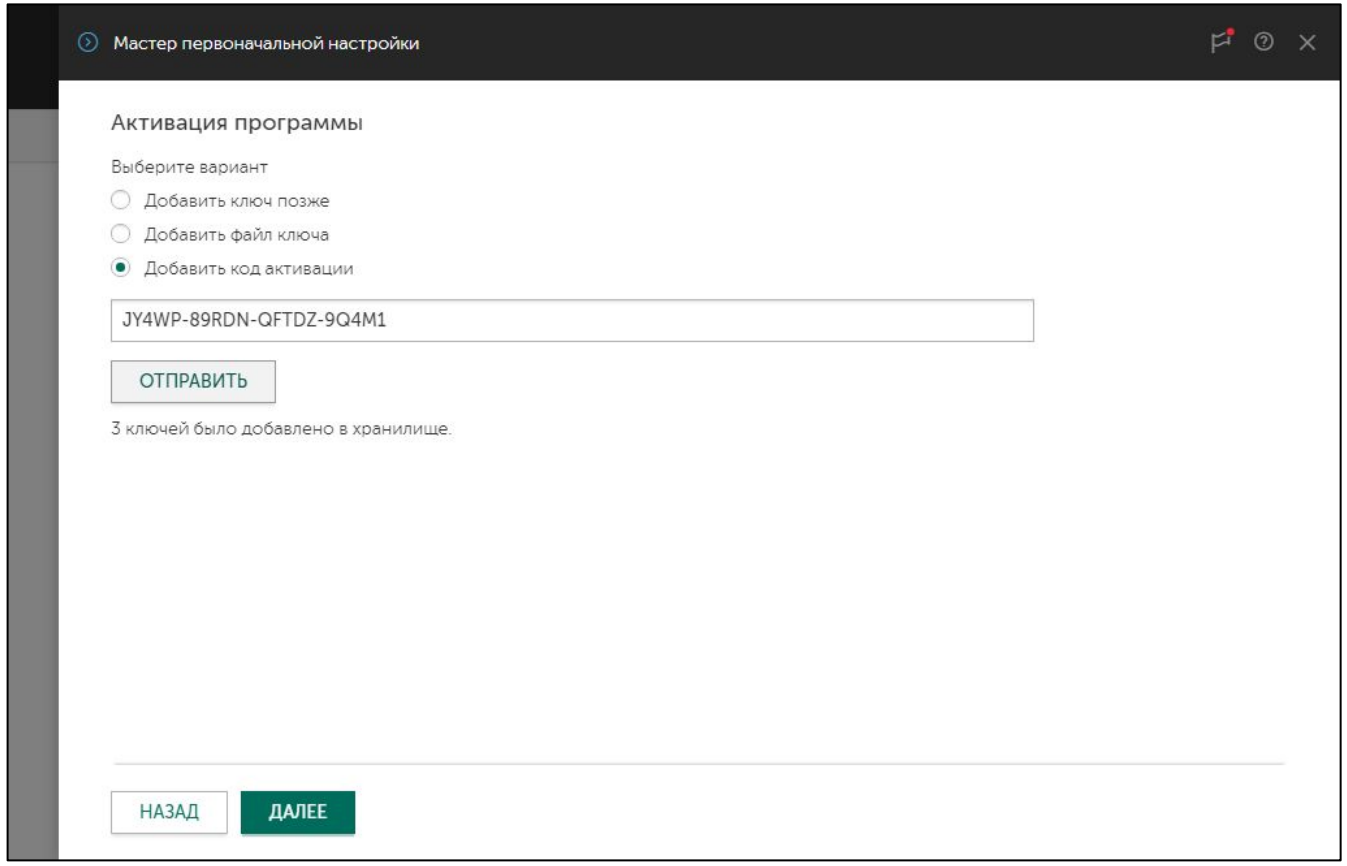
Добавьте лицензию на Сервер администрирования в виде кода активации или файла-ключа

Либо пропустите этот шаг и добавьте лицензию позже

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

Активация кодом



Для активации кодом нужен доступ в Интернет

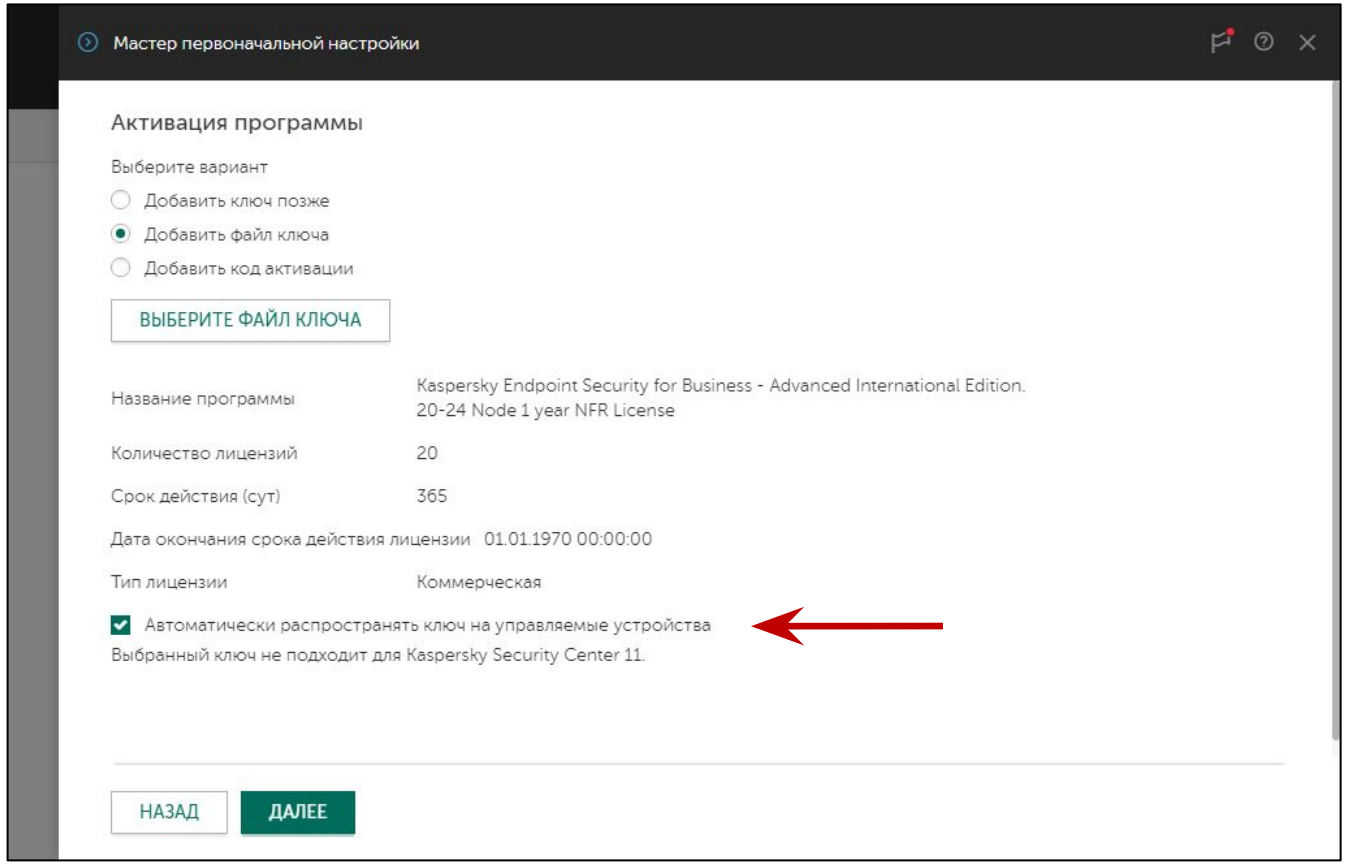
Кодом можно активировать сразу и Сервер администрирования и Kaspersky Endpoint Security на компьютерах

Опция автоматически распространять лицензию на клиентские устройства отсутствует, но ее можно указать позднее, чтобы не выбирать лицензию в задачах удаленной установки

Активация ключом

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты



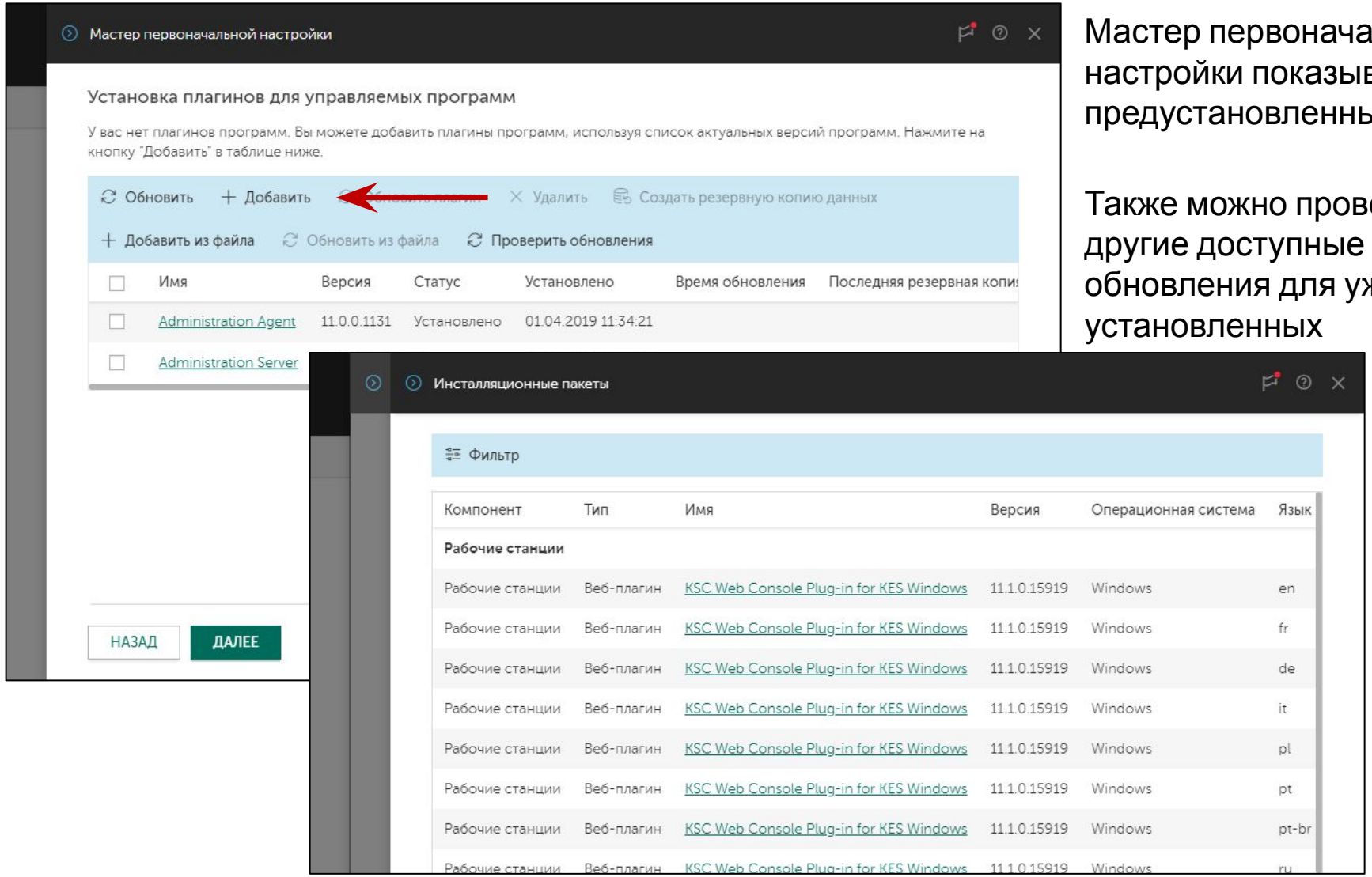
Используйте активацию ключом, если нет доступа в Интернет

В отличии от кода активации у ключа есть опция автоматического распространения

Список установленных плагинов

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты



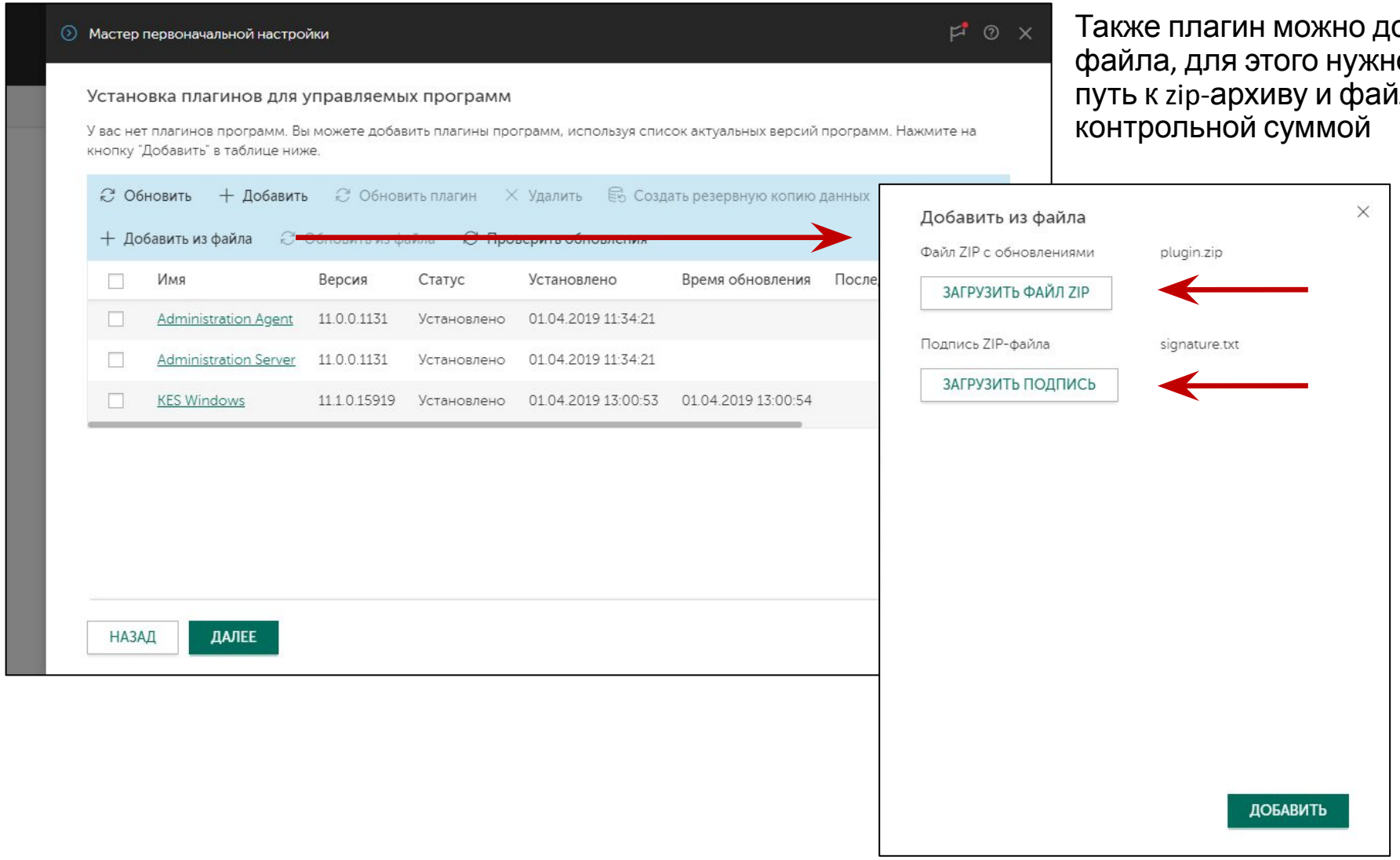
Мастер первоначальной настройки показывает список предустановленных плагинов

Также можно проверить есть ли другие доступные плагины или обновления для уже установленных

Загрузка плагинов из файла

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

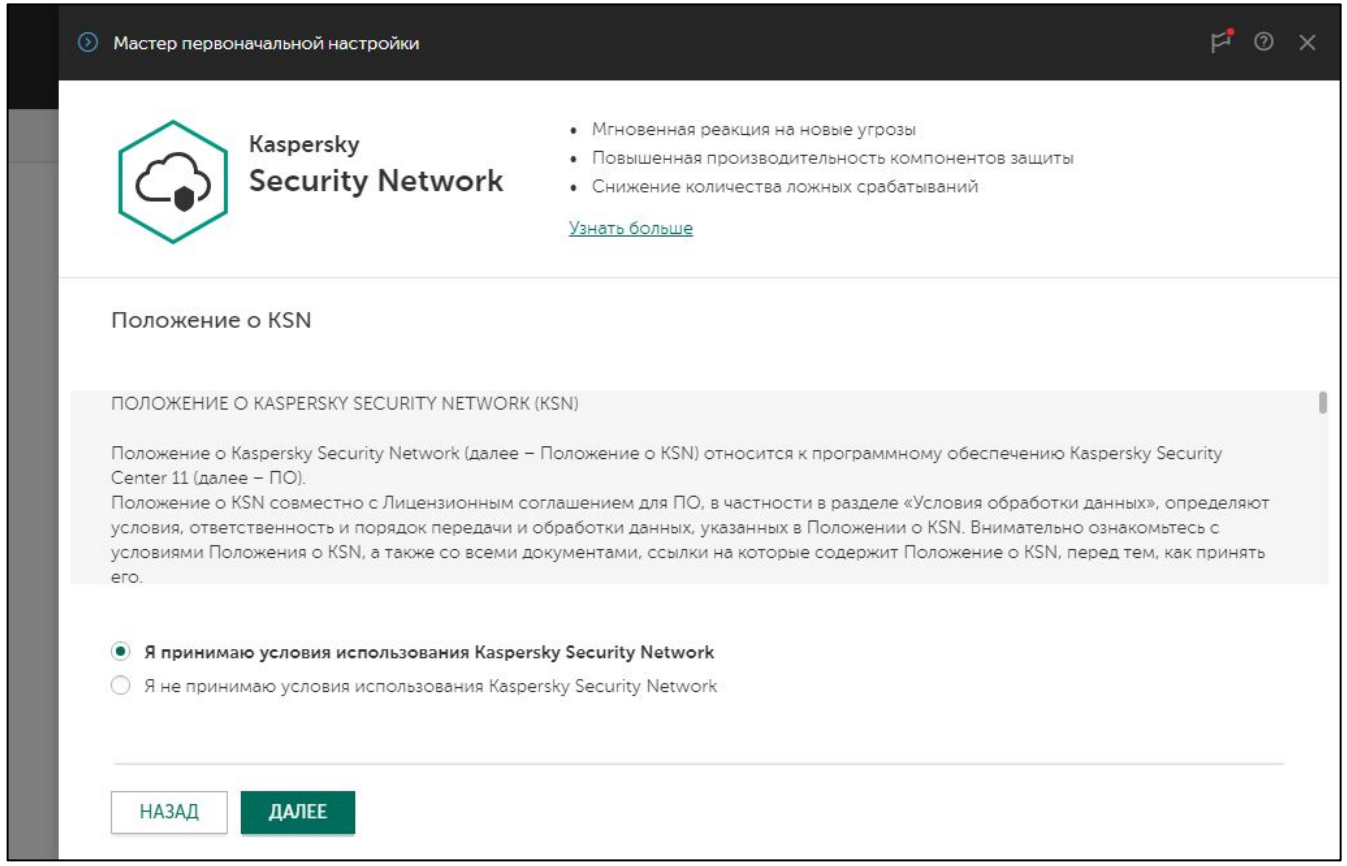


Также плагин можно добавить из файла, для этого нужно указать путь к zip-архиву и файлу с контрольной суммой

Kaspersky Security Network

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты



Kaspersky Security Network (KSN) это постоянно обновляемая онлайн-база (в «облаке») репутаций исполняемых файлов и веб-ресурсов

Kaspersky Endpoint Security получает из KSN самую свежую информацию об угрозах и о файлах, которым можно доверять

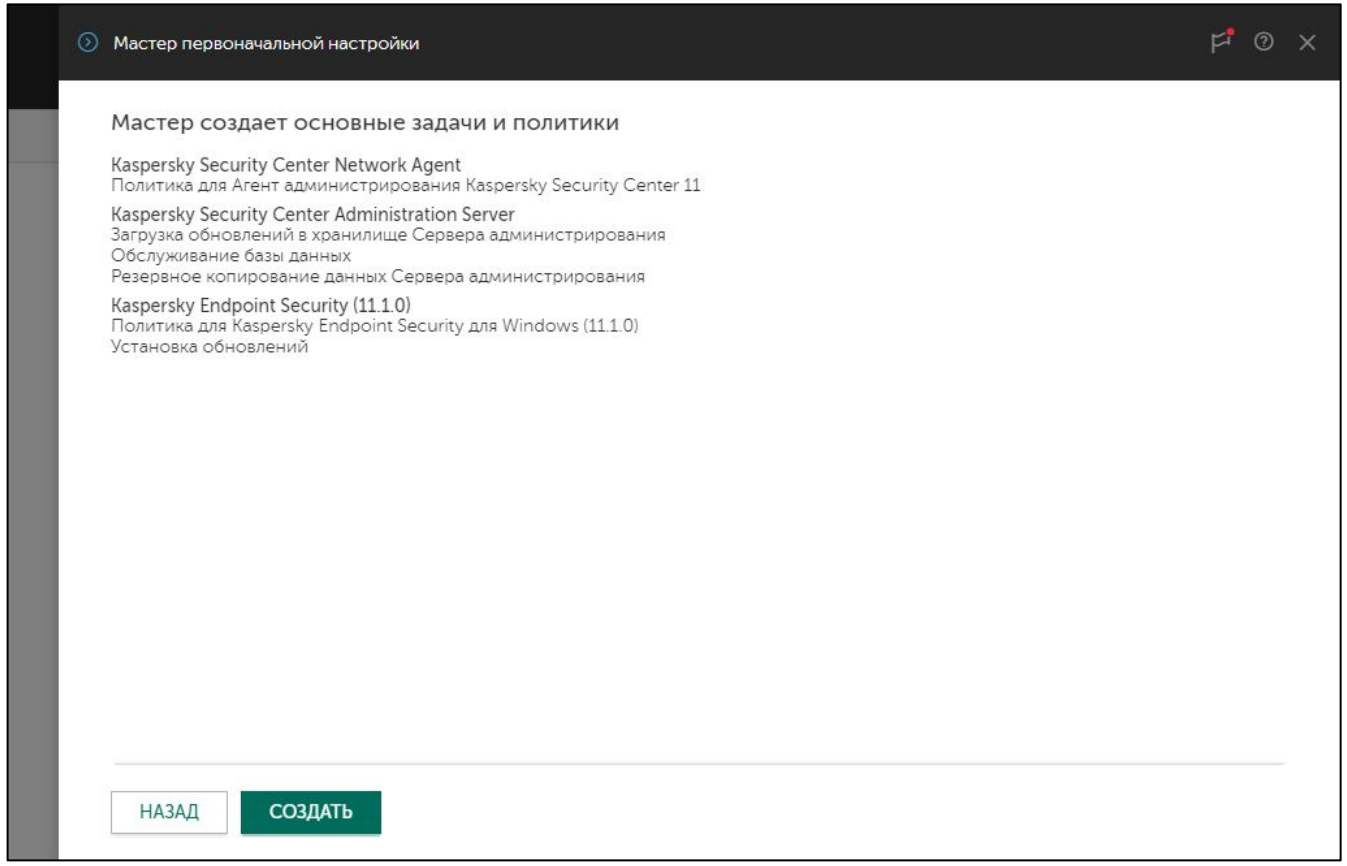
Принимая соглашение KSN, администратор включает KSN для Kaspersky Endpoint Security в политике по умолчанию и для KSC в свойствах сервера администрирования

Администратор всегда может включить или выключить KSN для любого продукта в настройках или политике продукта

Создание задач и политик

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты



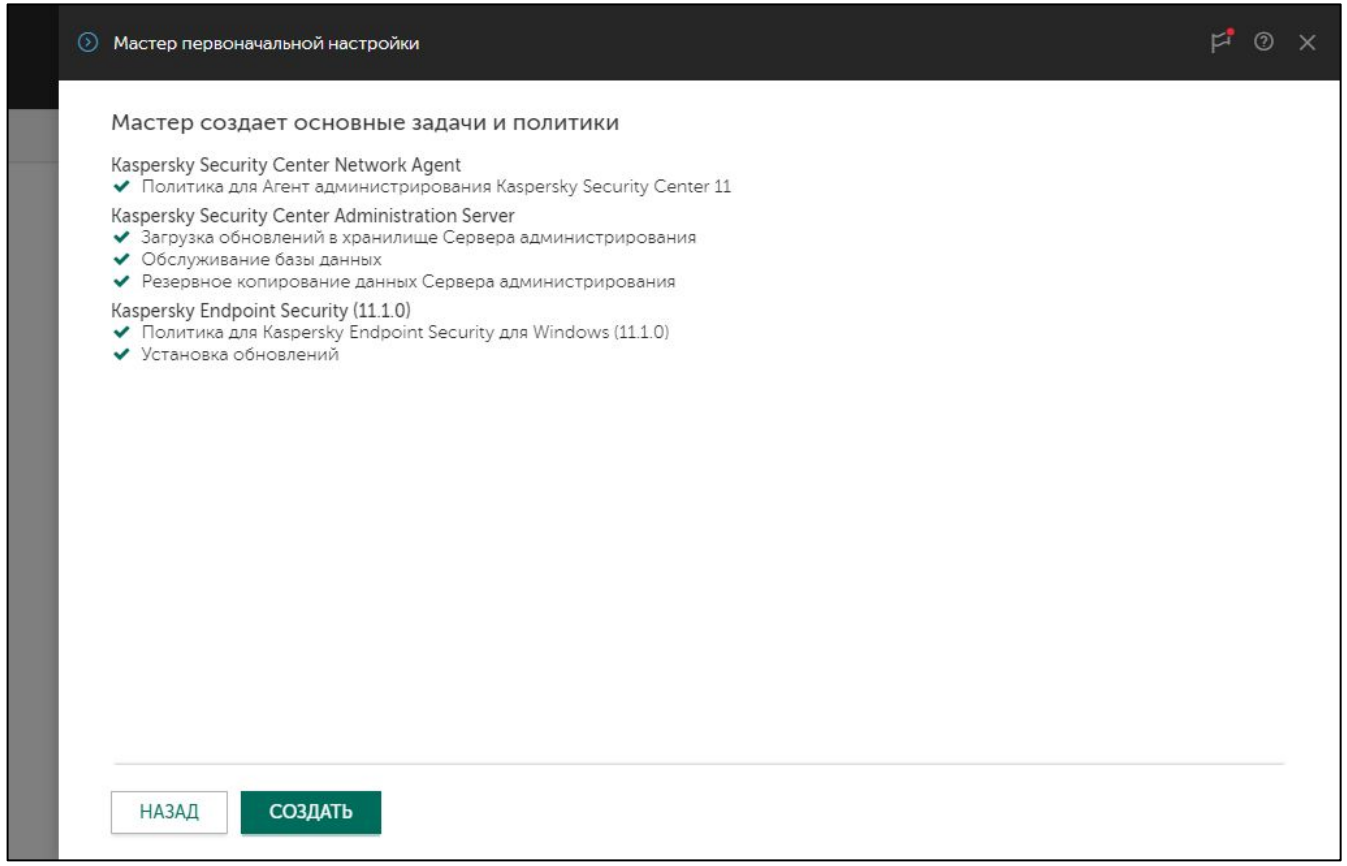
Мастер создает задачи Сервера администрирования:

- Загрузка обновлений в хранилище
- Обслуживание базы данных
- Резервное копирование данных Сервера администрирования

Создание задач и политик

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты



Мастер создает групповые политики:

— Агента администрирования KSC

— Kaspersky Endpoint Security для Windows

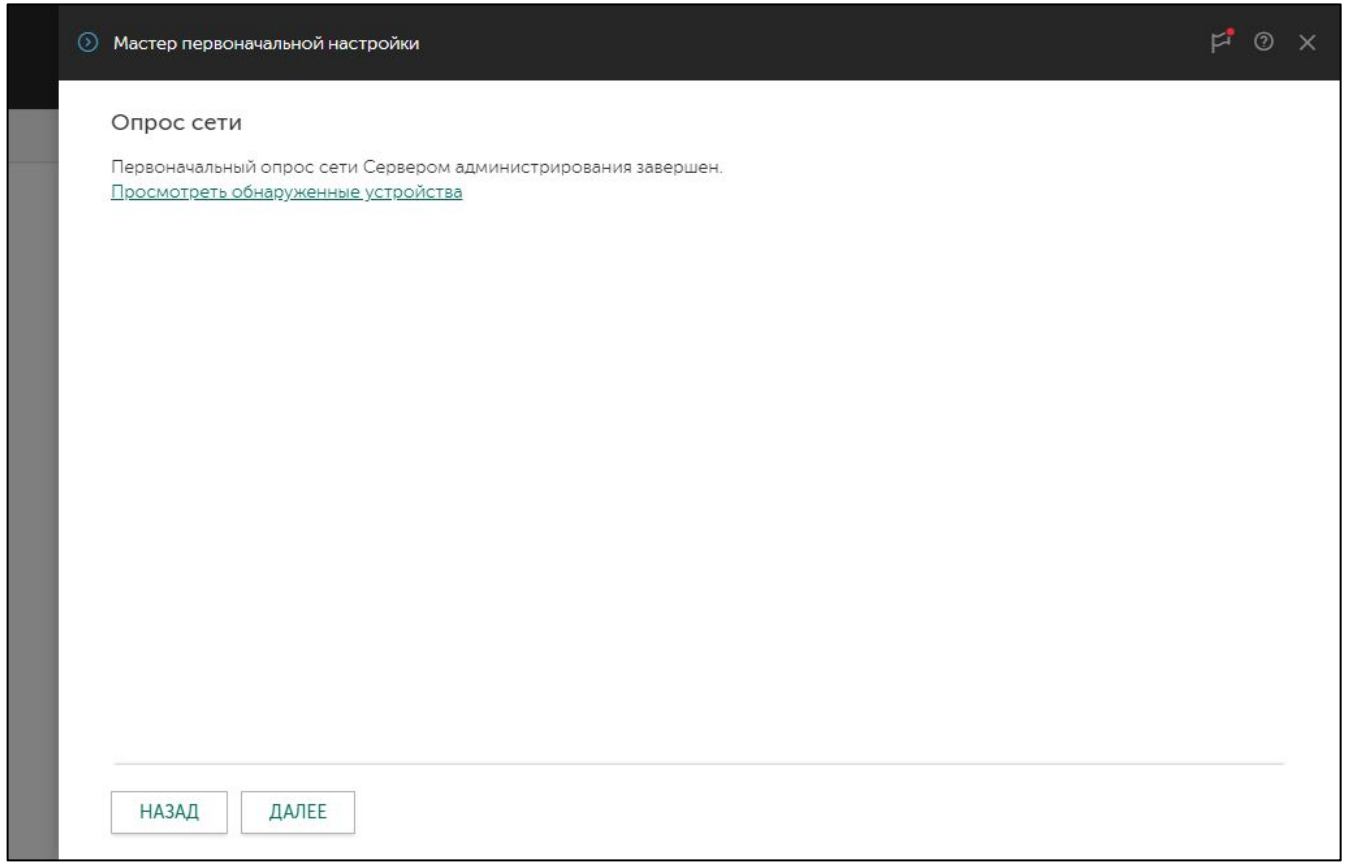
Групповые задачи:

— Установка обновлений

Сканирование сети

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты

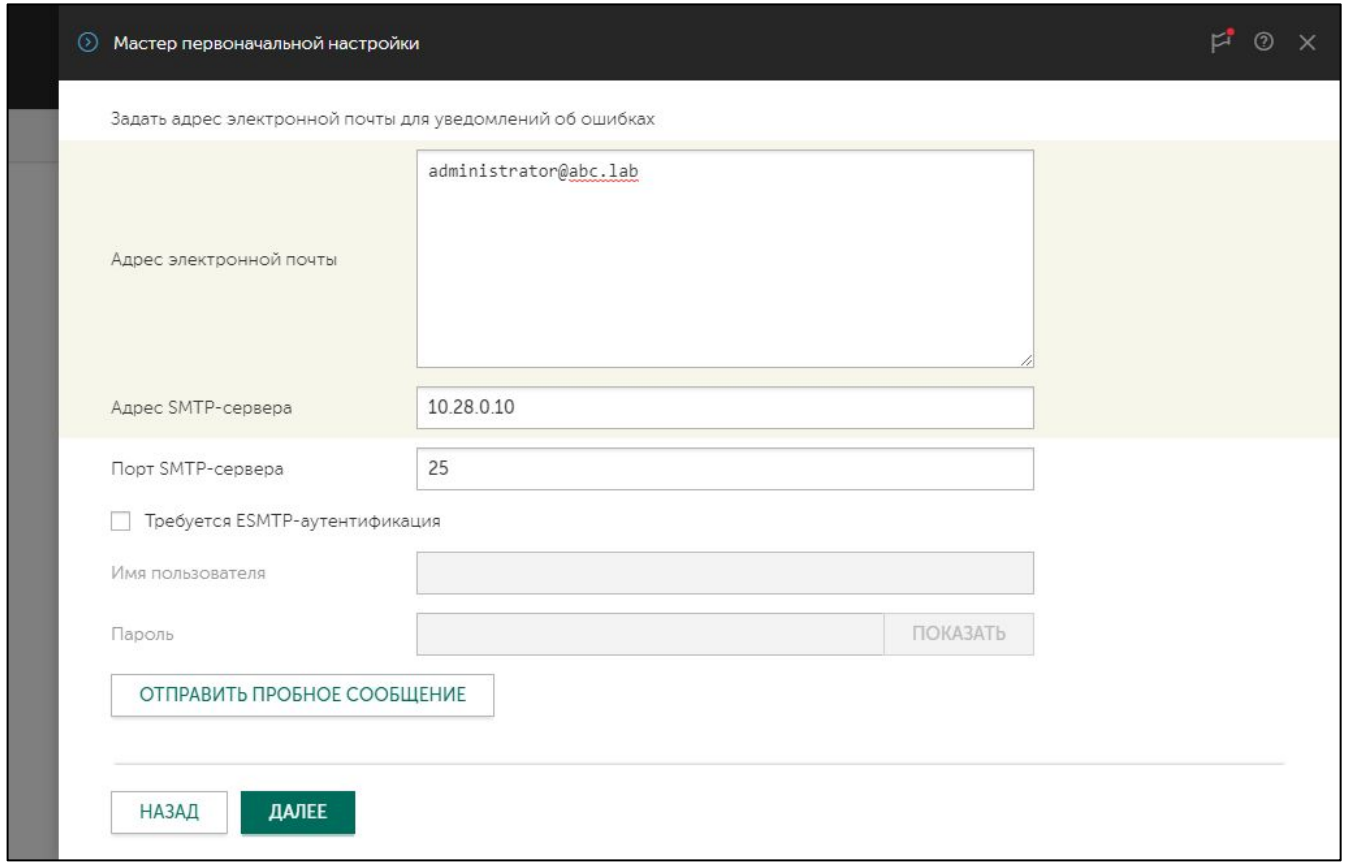


Мастер запускает сканирование сети средствами Microsoft Windows

Настройка доставки почтовых уведомлений

Мастер первоначальной настройки:

1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты



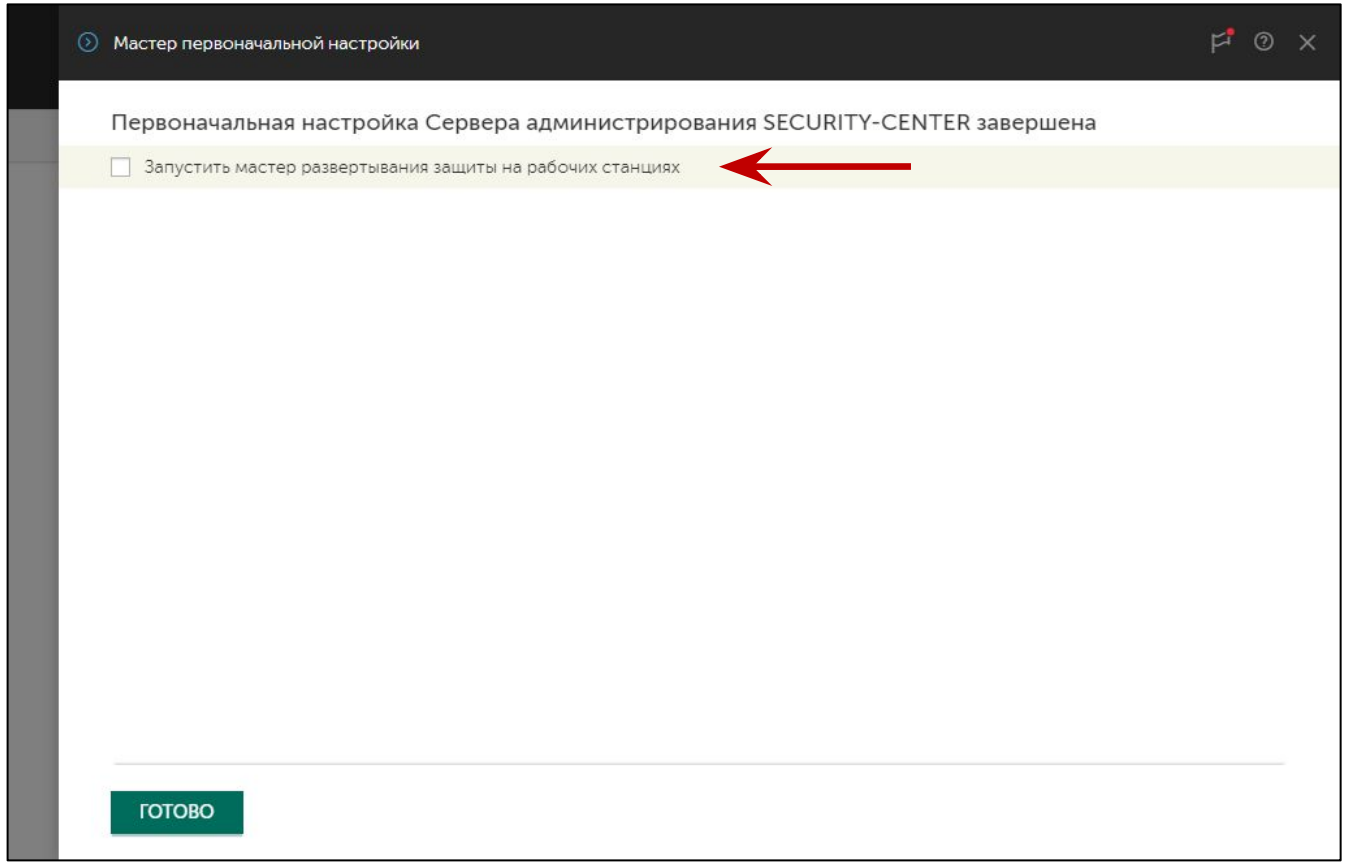
Параметры используются для доставки уведомлений и отчетов

Мастер не создает задачу рассылки отчетов, но ее можно создать вручную в любое время

Завершение первоначальной настройки

Мастер первоначальной настройки:

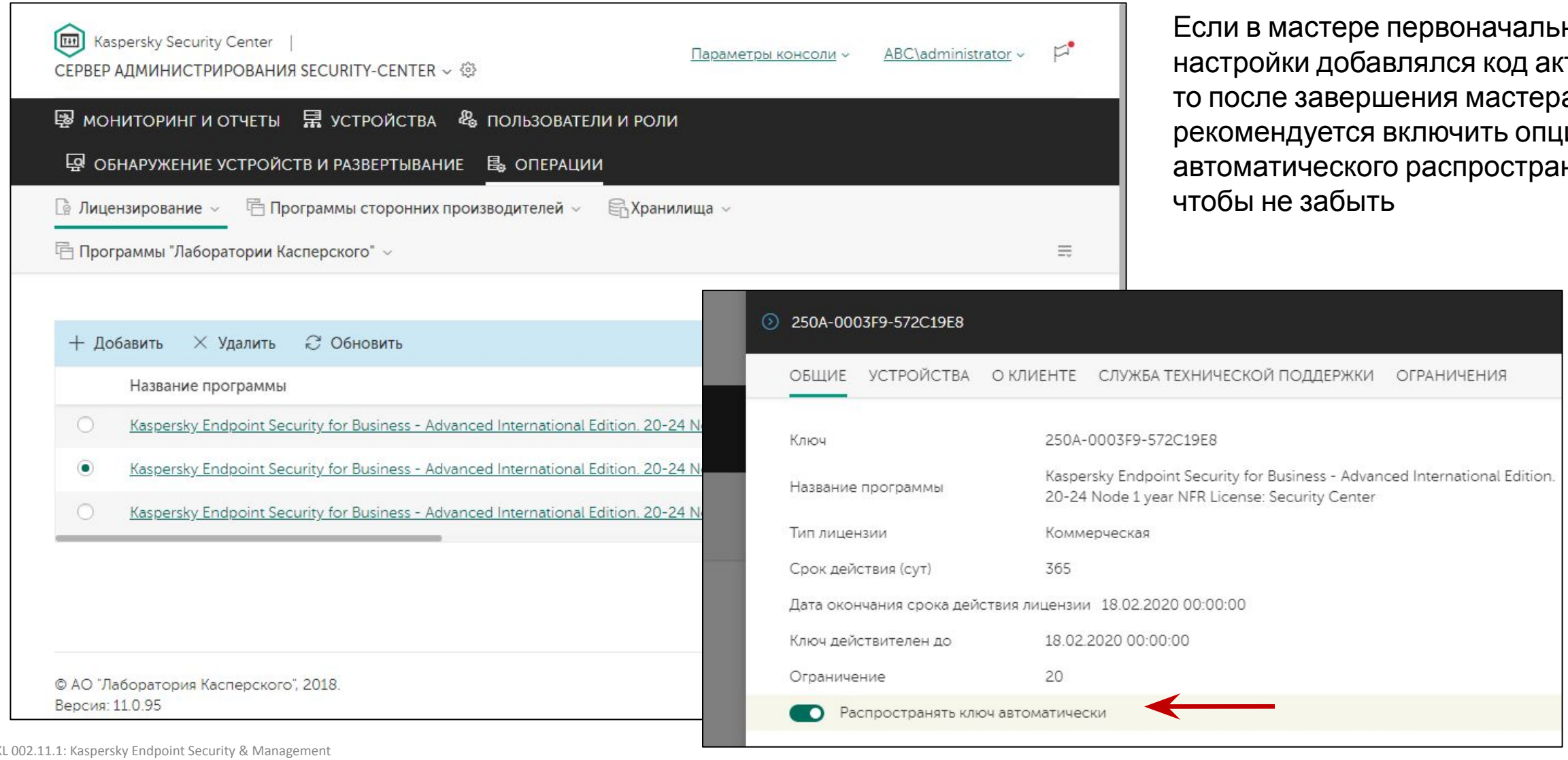
1. Настройте подключение к Интернет
2. Загрузите обновления
3. Добавьте лицензию
4. Загрузите новые плагины
5. Примите соглашение KSN
6. Дайте мастеру создать задачи и политики
7. Запустите сканирование сети
8. Укажите почтовый ящик для уведомлений и отчетов
9. Не запускайте мастер распространения защиты



Снимите отметку у параметра **Запускать мастер развертывания защиты**

Не начинайте разворачивать защиту, пока не подготовитесь

Автоматическое распространение лицензии

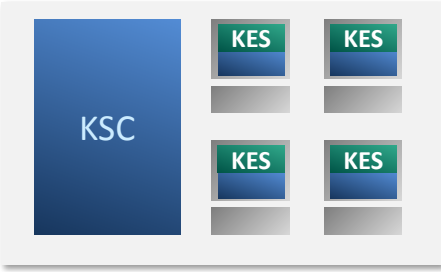


Если в мастере первоначальной настройки добавлялся код активации, то после завершения мастера рекомендуется включить опцию автоматического распространения, чтобы не забыть

Лабораторная работа №1

Как установить Kaspersky Security Center

1. Установите Сервер администрирования Kaspersky Security Center
2. Установите Kaspersky Secuirty Center Web Console
3. Пройдите мастер первоначальной настройки Сервера администрирования



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Требования к клиентским компьютерам

Как изменить состав компонентов KES
Как создать новый пакет установки
Как создать пакет KSWS
Какие есть методы установки
Как удаленно установить агент и KES
Как проще установить агент и KES локально
Как установить агент через Active Directory
Как удалить несовместимые программы

Требования для установки Kaspersky Endpoint Security 11.1 для Windows

- Клиентские операционные системы
  - Windows 10 x86 / x64 (все редакции вплоть до RS5)
    - Home / Pro / Education / Enterprise
  - Windows 8.1 x86 / x64
    - Enterprise
  - Windows 8 x86 / x64
    - Pro / Enterprise
  - Windows 7 SP1 x86 / x64
    - Professional / Enterprise / Ultimate

- Серверные операционные системы [1, 2]
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2012 R2
    - Foundation / Essentials / Standard
  - Microsoft Windows Server 2012 x64
    - Foundation / Essentials / Standard
  - Microsoft Small Business Server 2011 x64
    - Essentials / Standard
  - Microsoft Windows Server 2008 R2 SP1 x64
    - Standard / Enterprise
  - Microsoft Windows Server 2008 SP2 x86 / x64
    - Standard / Enterprise

[1] *Ограниченная поддержка ReFS*
[2] *Core mode, Nano mode и кластеры не поддерживаются*

Требования для установки Kaspersky Endpoint Security 11.1 для Windows

- Виртуальные платформы
  - VMware Workstation 14
  - VMware ESXi 6.5
  - Microsoft Hyper-V 2016
  - Citrix XenServer 7.2
  - Citrix XenDesktop 7.14
  - Citrix Provisioning Services 7.14 [1]

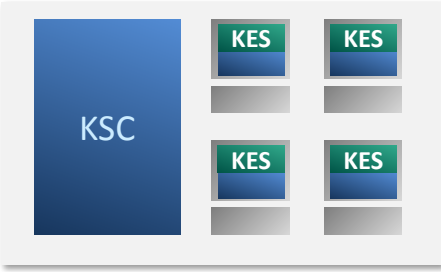
- Аппаратные требования:
  - CPU: 1 ГГц
  - Память — 1 ГБ для x86 / 2 ГБ для x64*
  - Место на диске — 2 ГБ

**В коде минимальное ограничение 768 МБ*

[1] *Для поддержки Citrix PVS, Kaspersky Endpoint Security 11.1 нужно устанавливать с параметром /pCITRIXCOMPATIBILITY=1 или с включенным параметром совместимости в свойствах инсталляционного пакета*

Требования для установки Агента администрирования

- Поддерживает все операционные системы, на которые можно установить Kaspersky Endpoint Security 11.1 для Windows
- Полный список совместимых систем: http://support.kaspersky.com/ksc11#requirements
- Чтобы установить Агент администрирования, нужны права администратора
- Аппаратные требования
  - Процессор:
    - 1.0 GHz для 32-bit систем
    - 1.4 GHz для 64-bit систем
  - Память — 512 МБ
  - Место на диске — 1 ГБ



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

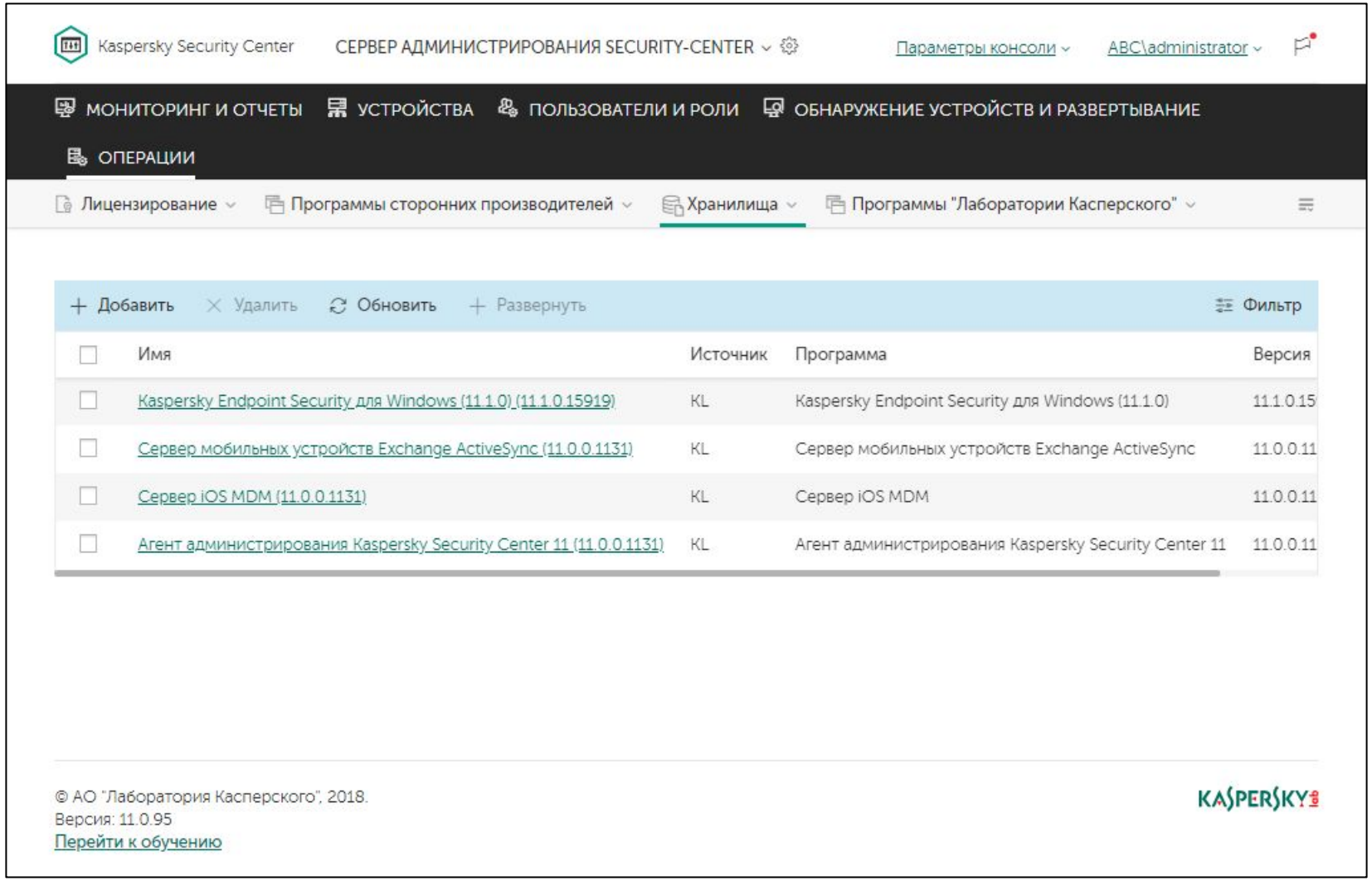
- Требования к клиентским компьютерам
- **Как изменить состав компонентов KES**
- Как создать новый пакет установки
- Как создать пакет KSWS
- Какие есть методы установки
- Как удаленно установить агент и KES
- Как проще установить агент и KES локально
- Как установить агент через Active Directory
- Как удалить несовместимые программы

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Инсталляционные пакеты



Пакеты нужны для:

- задач удаленной установки
- автономных пакетов установки

Пакет содержит:

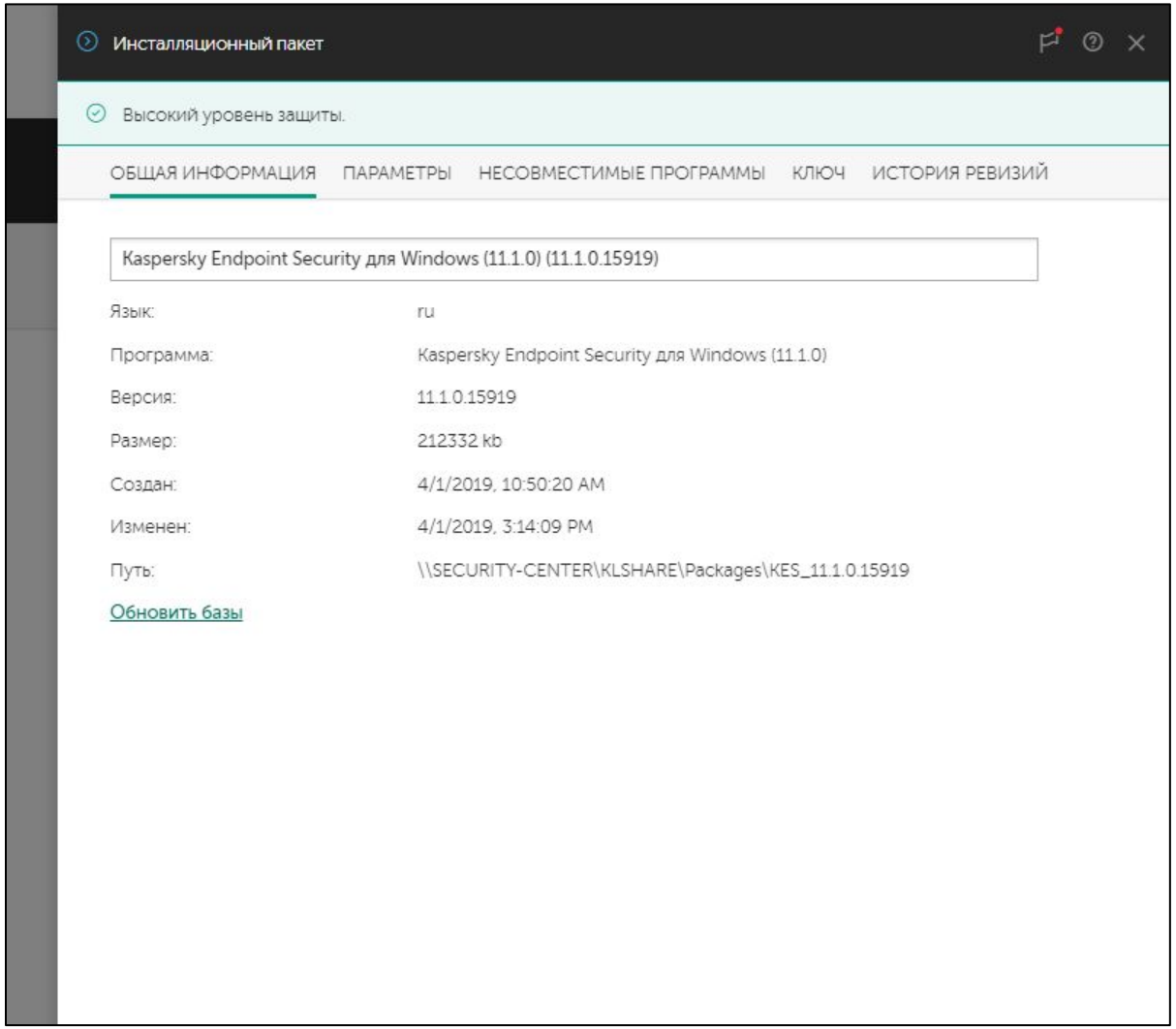
- инсталляционные файлы
- параметры установки

Пакеты можно изменять, удалять и создавать новые

Добраться до пакетов можно несколькими способами:

- Операции | Хранилища | Инсталляционные пакеты
- Обнаружение устройств и развертывание | Развертывание и назначение | Инсталляционные пакеты

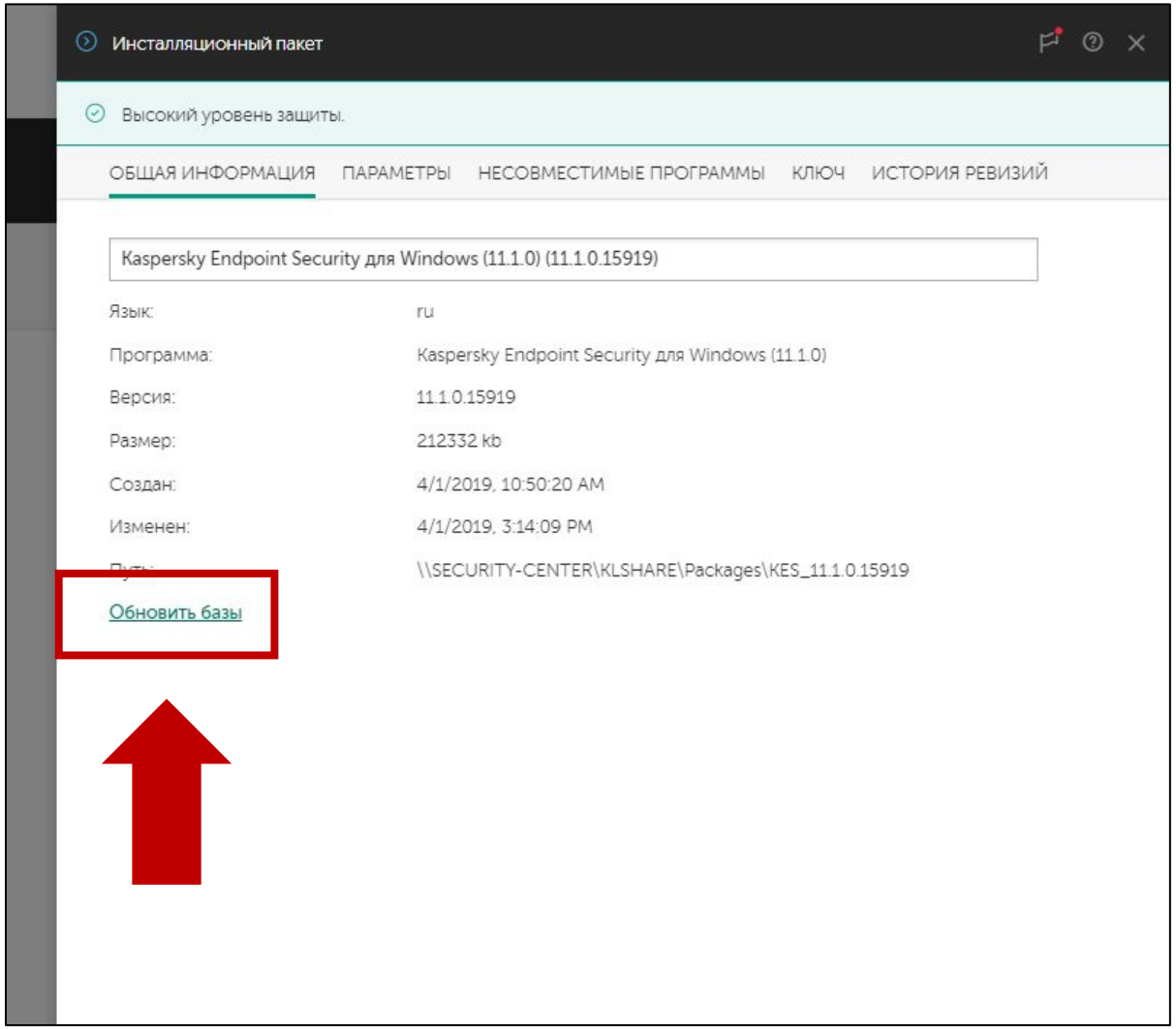
Общие сведения



На вкладке **Общая информация** можно найти

- Имя пакета
- Имя программы, которую устанавливает пакет
- Версию программы
- Дата, когда был создан пакет
- Папку, в которой хранятся файлы пакета (в общей папке Сервера администрирования)

Как обновить базы в пакете Kaspersky Endpoint Security



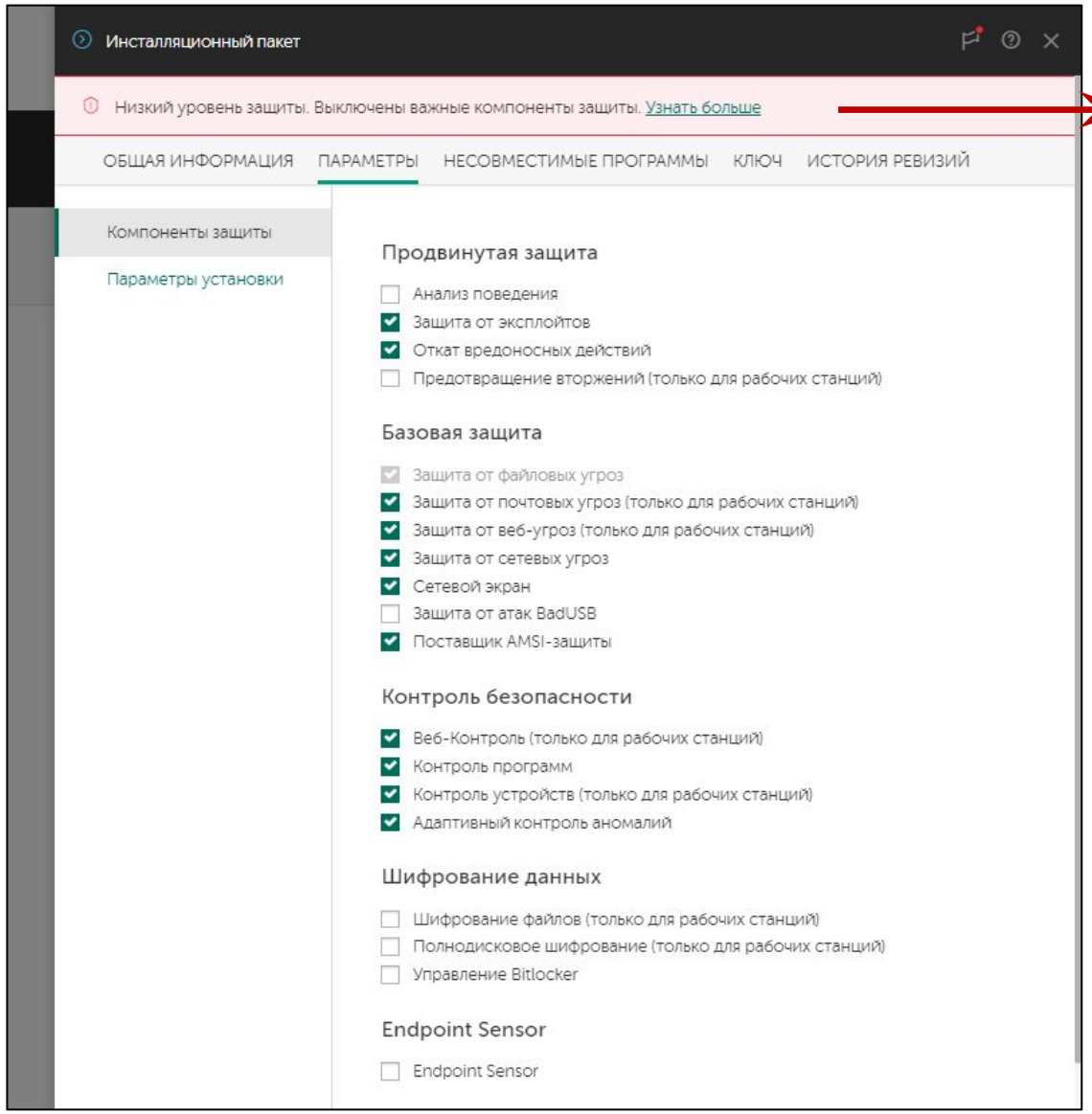
Если базы в пакете сильно устарели, Kaspersky Endpoint Security после установки загрузит почти всю базу сигнатур в виде обновлений

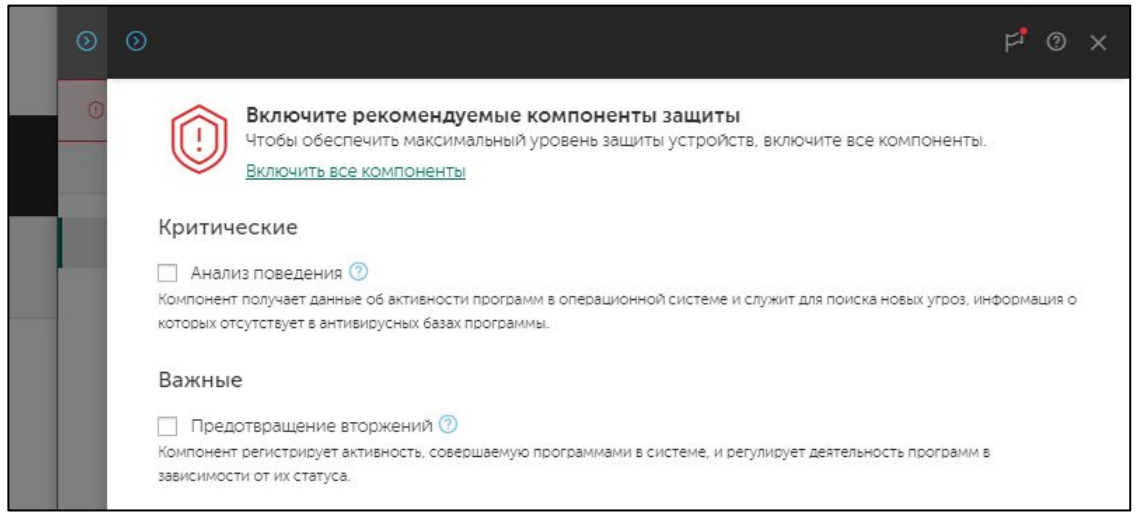
Чтобы уменьшить трафик первого обновления, обновите базы в пакете перед тем как запускать удаленную установку или создавать автономный пакет

Сервер администрирования автоматически обновляет базы в пакетах только один раз для каждого пакета, после этого базы в пакетах обновляет вручную администратор

К сожалению из Web Console нельзя узнать, какие сейчас базы в пакете

Состав установки Kaspersky Endpoint Security





Продвинутая защита

- Анализ поведения
- Защита от эксплойтов
- Откат вредоносных действий
- Предотвращение вторжений *

Базовая защита

- Защита от файловых угроз
- Защита от почтовых угроз *
- Защита от веб-угроз *
- Защита от сетевых угроз
- Сетевой экран
- Защита от атак BadUSB
- Поставщик AMSI-защиты

Контроль безопасности

- Веб-Контроль *
- Контроль программ
- Контроль устройств *
- Адаптивный контроль аномалий *

Шифрование данных

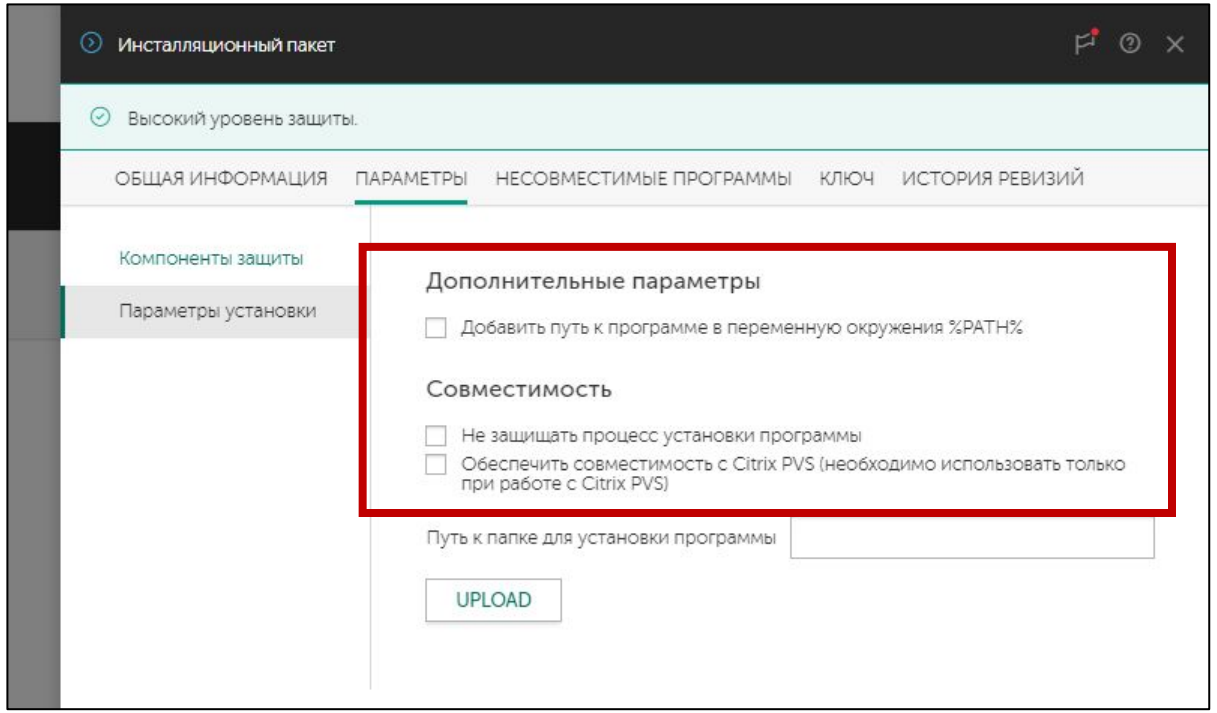
- Шифрование файлов *
- Полнодисковое шифрование *
- Управление Bitlocker

Endpoint Sensor

- Endpoint Sensor

*** Только для рабочих станций**

Параметры установки Kaspersky Endpoint Security



Добавить путь к программе в переменную окружения %PATH%

Позволяет запускать интерфейс командной строки **avp.exe** из любой папки. Через интерфейс командной строки можно запускать и останавливать задачи, смотреть статистику и т.п. (чтобы узнать подробности, запустите **avp.exe help**)

Не защищать процесс установки программы

Kaspersky Endpoint Security применяет самозащиту, чтобы не дать вредоносным программам повредить или изменить свои файлы

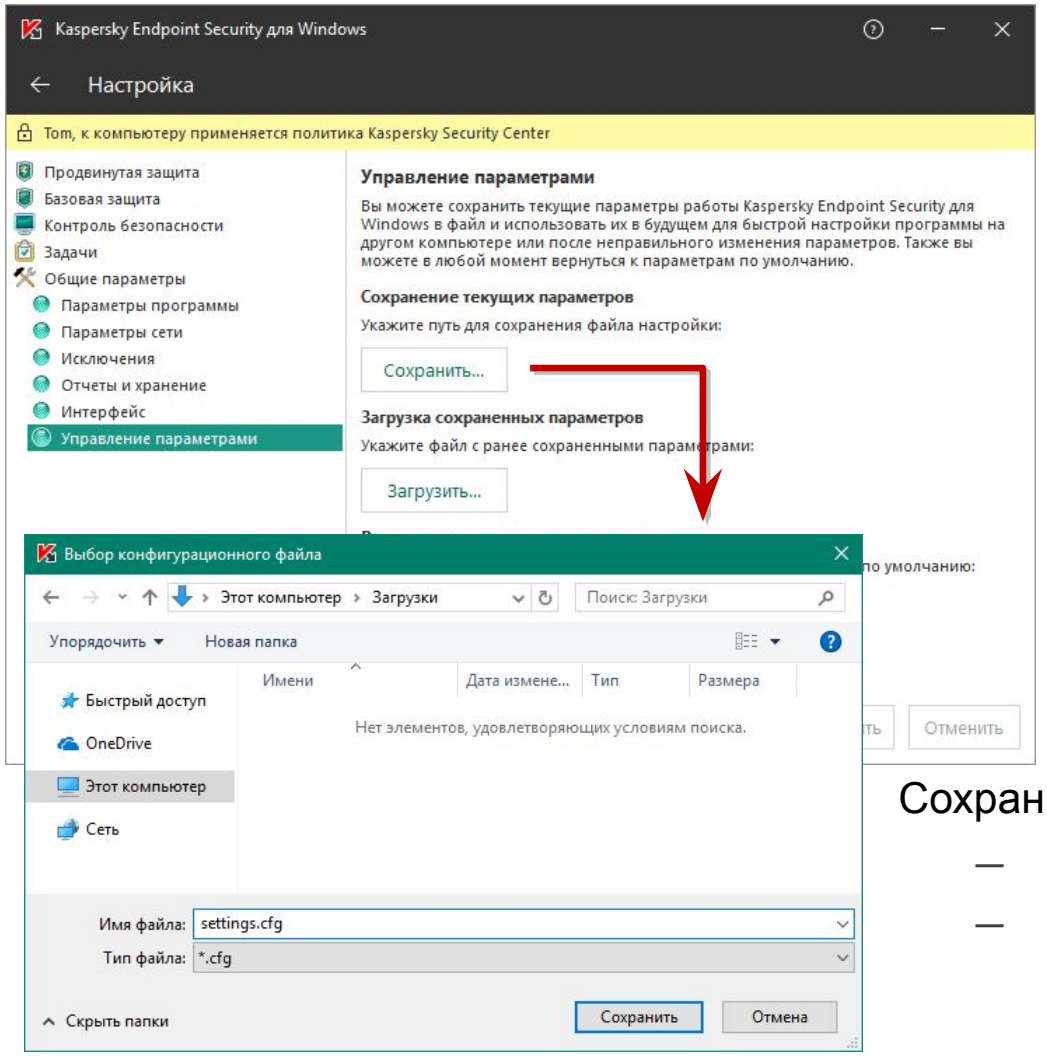
Если самозащита конфликтует с установленными программами, такими как агенты резервного копирования, которые следят за всеми файлами в системе, отключите ее во время установи, и настройте исключения для конфликтующих программ в политике

Обеспечить совместимость с Citrix PVS

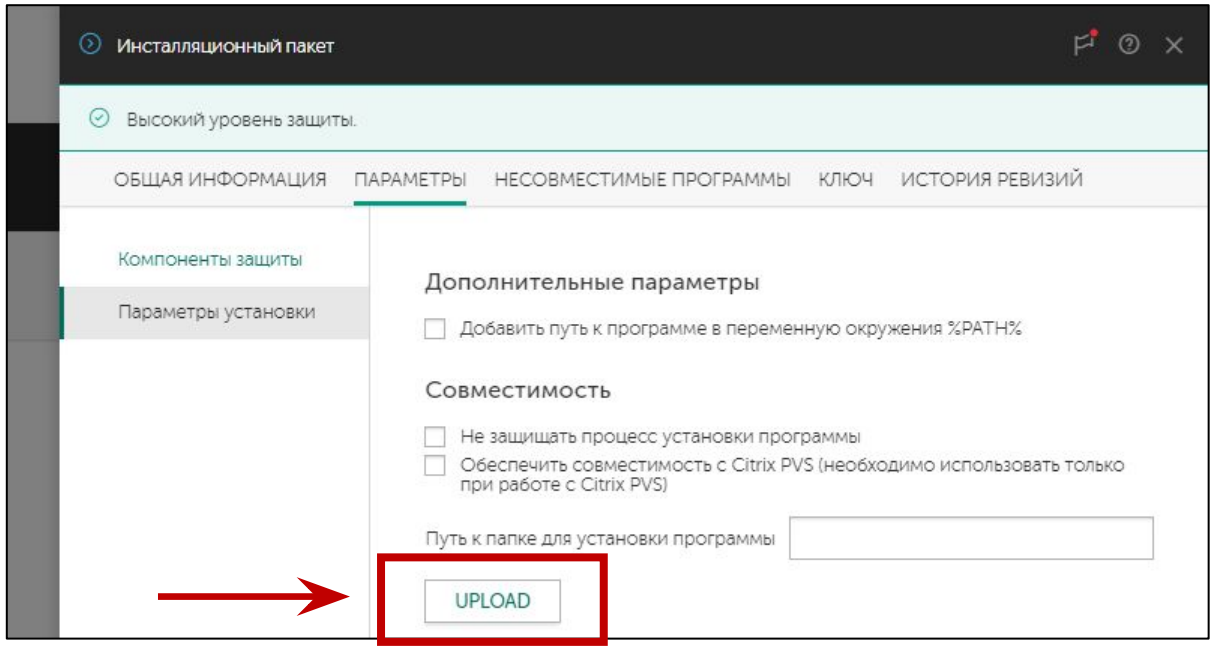
Citrix Provisioning Cervices это технология виртуализации, и подробнее рассматривается в курсе KL 031

Вы можете изменить путь установки, по умолчанию
—*%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows*

Конфигурационный файл Kaspersky Endpoint Security



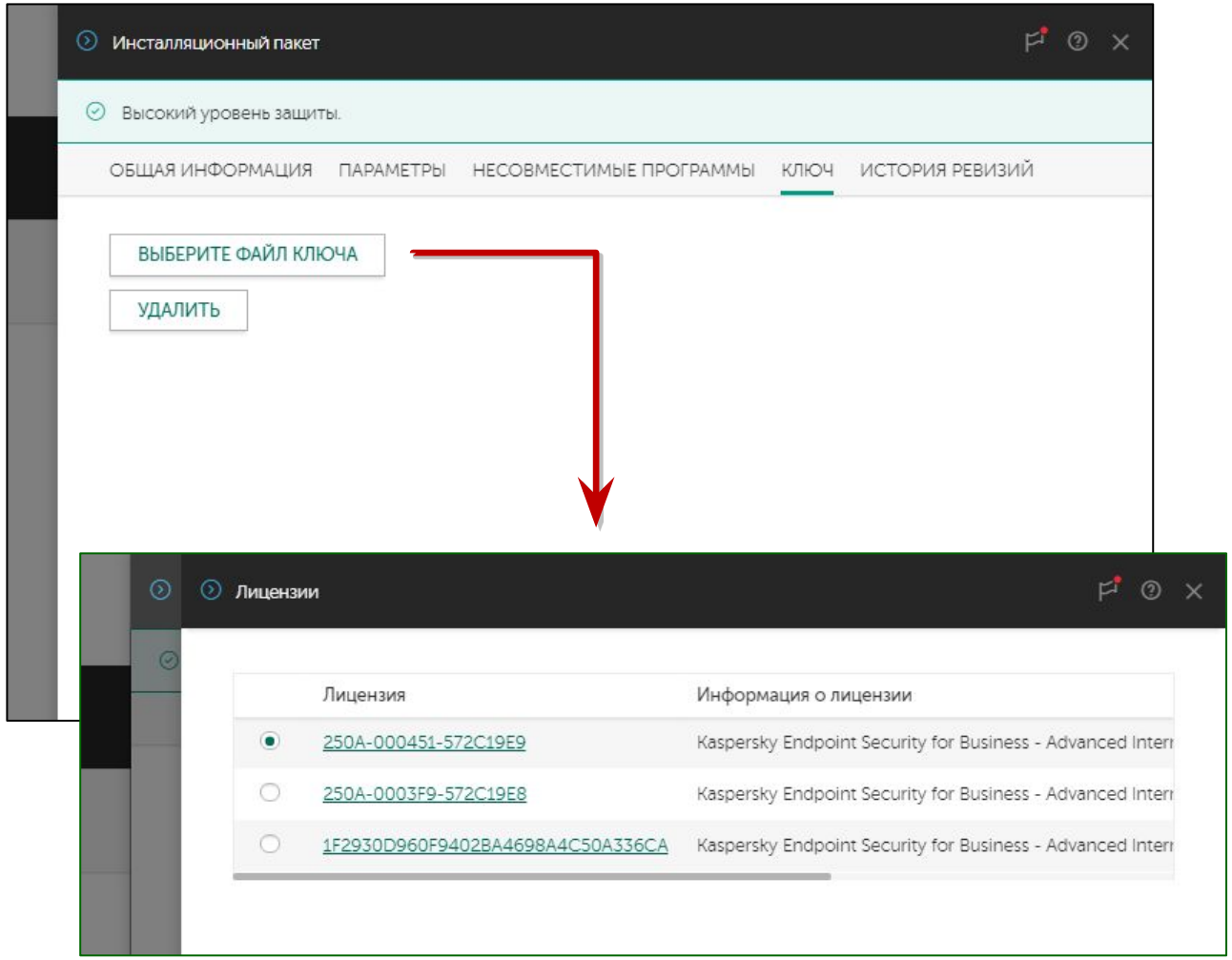
На компьютерах, подключенных к Серверу администрирования, настройки задает политика



Сохраните файл настроек в локальном интерфейсе, чтобы:

- распространить настройки на компьютеры, не подключенные к Серверу
- активировать важные исключения (или правила контроля для компонентов контроля) сразу после установки, а не спустя несколько минут, когда придет политика
- задать настройки, которых нет в политике (но есть в продукте), например, настройки локальных задач

Ключ Kaspersky Endpoint Security



По умолчанию в пакете нет ключа

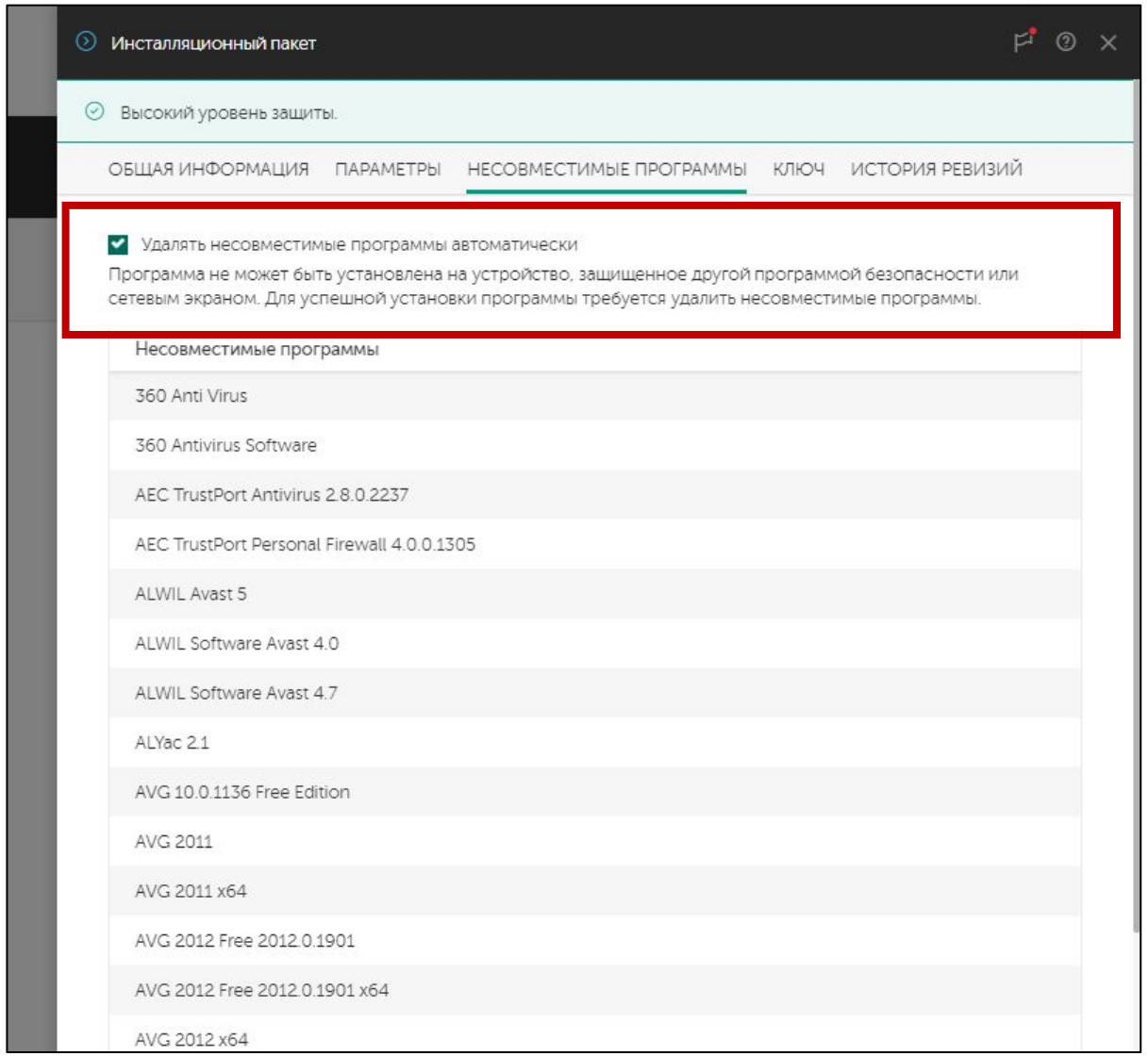
Ключ в пакете не нужен, если вы используете автоматическое распространение лицензии из хранилища или задачу установки ключа

Добавьте ключ в пакет, чтобы:

- Распространить ключ на компьютеры, не подключенные к серверу
- Активировать защиту сразу после установки, а не спустя несколько минут, когда Агент получит лицензию с сервера (автоматически или задачей)

Проверяйте, что добавляете подходящий и годный ключ. Окно свойств пакета не проверяет, годится ли ключ. Если вы ошиблись, узнаете об этом только после установки

Удаление несовместимых программ

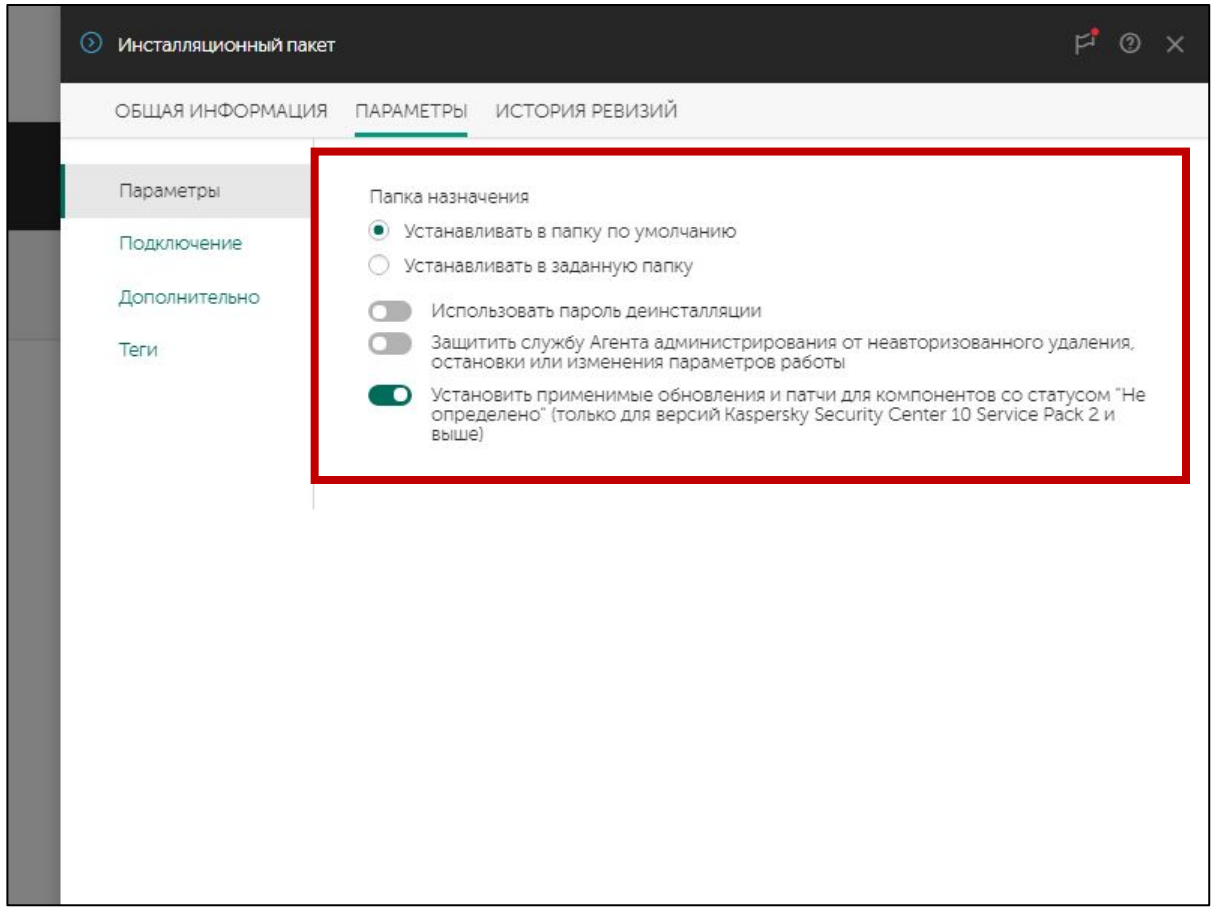


По умолчанию удаление несовместимых программ включено

Если автоматическое удаление включено, и инсталлятор обнаружил несовместимую программу, он ее удалит, установит Kaspersky Endpoint Security и попросит перезагрузить компьютер

Если автоматическое удаление выключено, и инсталлятор обнаружил несовместимую программу, установка завершится с ошибкой

Параметры установки Агента администрирования



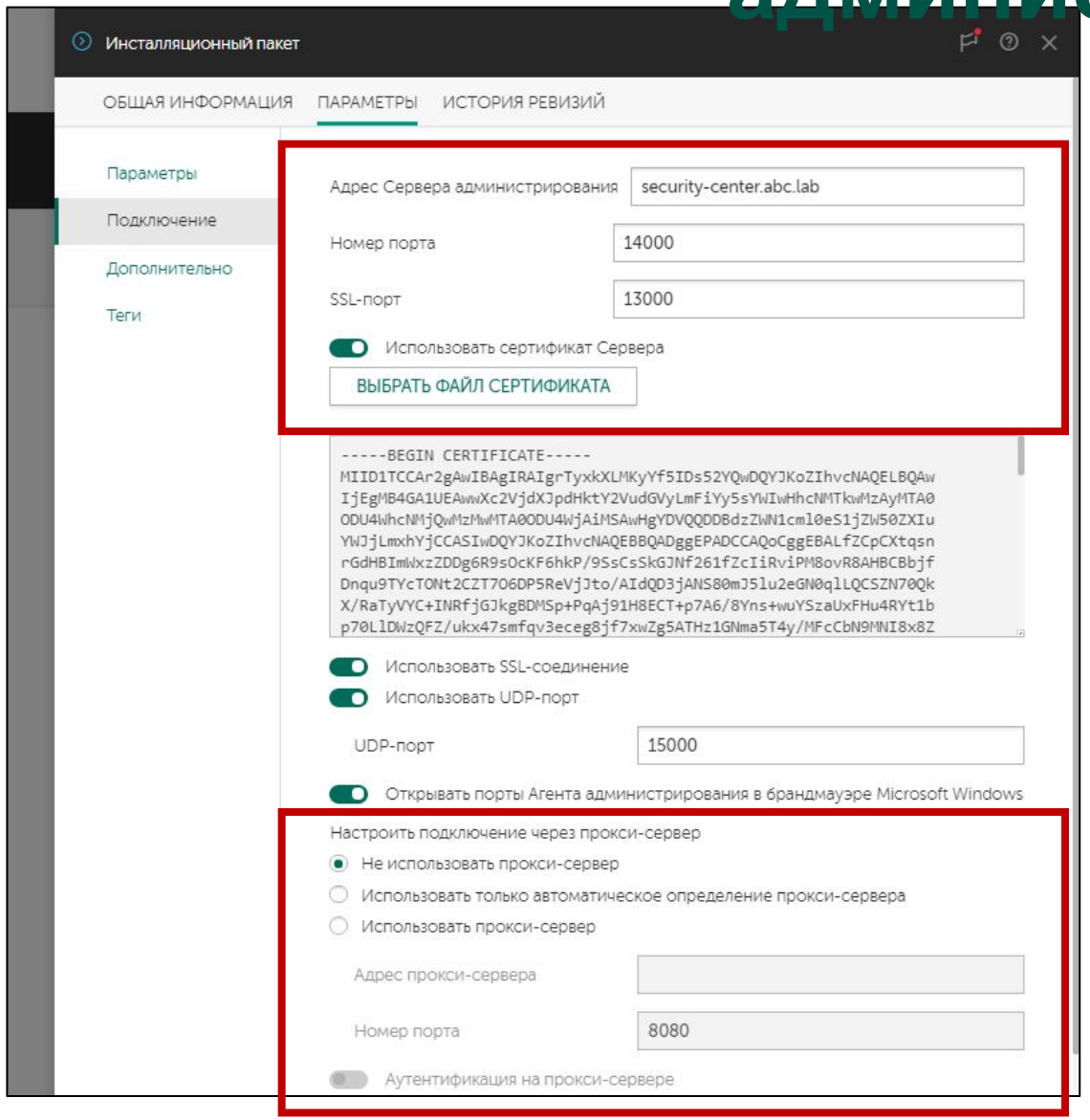
Параметры, которые можно изменить только перед установкой

- **Папка установки** — по умолчанию *%ProgramFiles(x86)%\Kaspersky Lab\NetworkAgent*
- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы** — по умолчанию выключен; включите, чтобы не дать пользователям (и сторонним программам) останавливать службу Агента

Параметры, которые можно изменить политикой

- **Пароль деинсталляции** — по умолчанию не задан; задайте пароль, чтобы пользователи не могли удалить Агент администрирования
- **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом «Не определено»** — по умолчанию включено. Отключите, если хотите вручную управлять установкой новых версий и обновлений Агента администрирования

Параметры подключения Агента администрирования

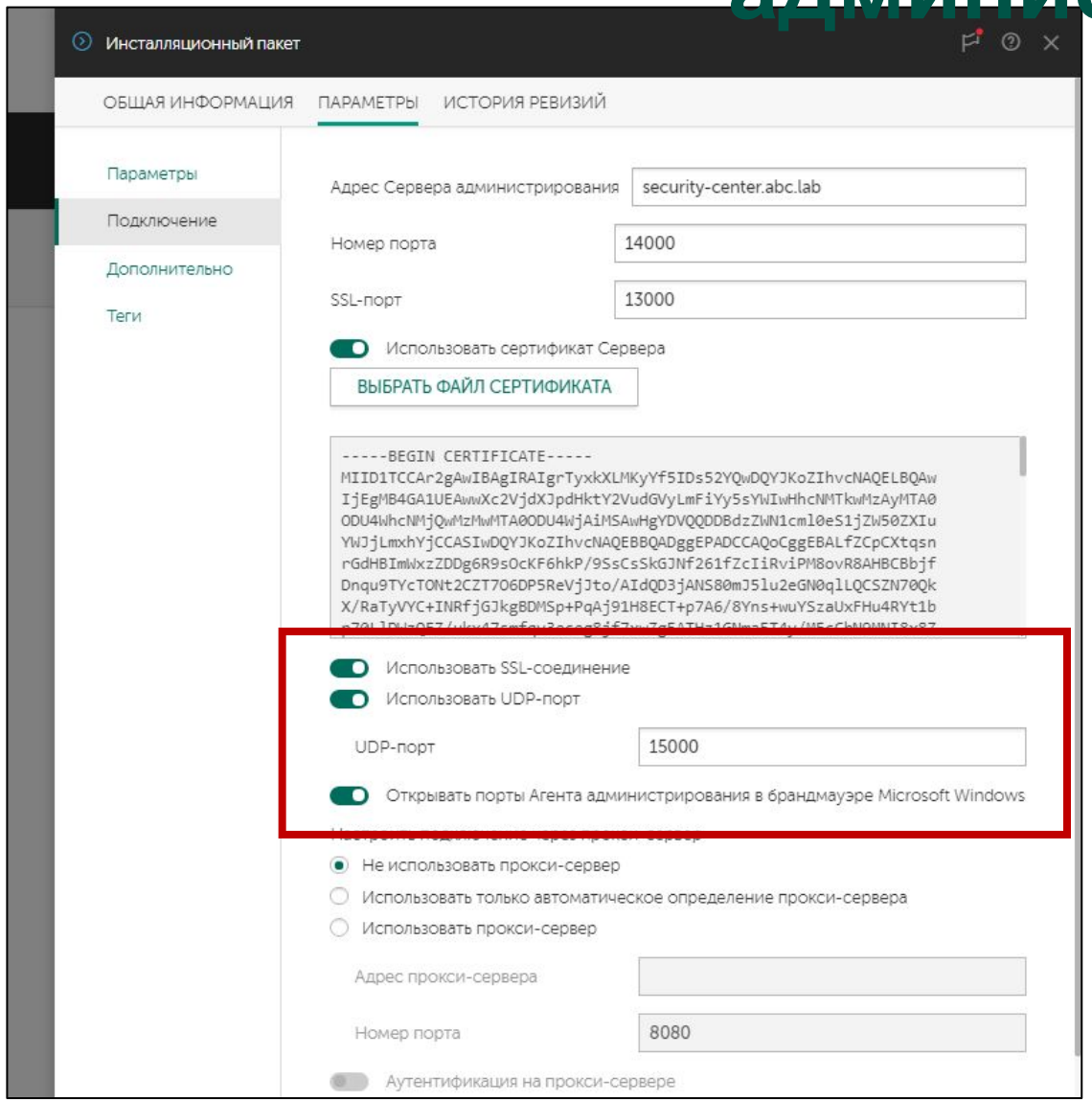


Параметры, которые можно задать только в пакете:

- **Адрес сервера, порт и SSL-порт** — по умолчанию соответствуют значениями, которые администратор выбрал при установке Сервера. Если вы решили изменить адрес или порты подключения Сервера администрирования, измените их и в свойствах пакета перед установкой Агентов
- **Использовать сертификат сервера** — по умолчанию включено и выбран сертификат Сервера администрирования. Как правило, этот параметр менять не нужно
- **Настроить подключение через прокси-сервер** — по умолчанию не настроены; настройте, если компьютеры подключаются к Серверу через Интернет и для выхода в Интернет используют прокси-сервер

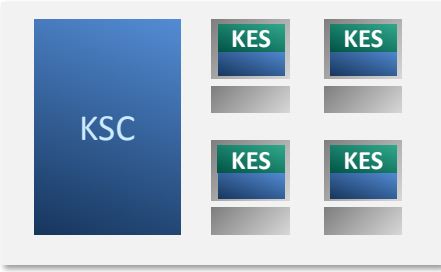
Если в инсталляционном пакете заданы неверные параметры подключения к Серверу администрирования, Агенты администрирования не подключатся к Серверу, и администратор не сможет управлять компьютерами

Параметры подключения Агента администрирования



Параметры, которые можно изменить в политике:

- **Использовать SSL-соединение** — по умолчанию включено, отключайте для поиска неполадок
- **Использовать UDP-порт** и **Номер UDP-порта** — по умолчанию включено и номер порта равен 15000; на этот порт Агент ожидает сигналы от Сервера
- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** — по умолчанию включено, чтобы Агент мог принимать сигналы от Сервера



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Требования к клиентским компьютерам

Как изменить состав компонентов KES

Как создать новый пакет установки

Как создать пакет KSWS

Какие есть методы установки

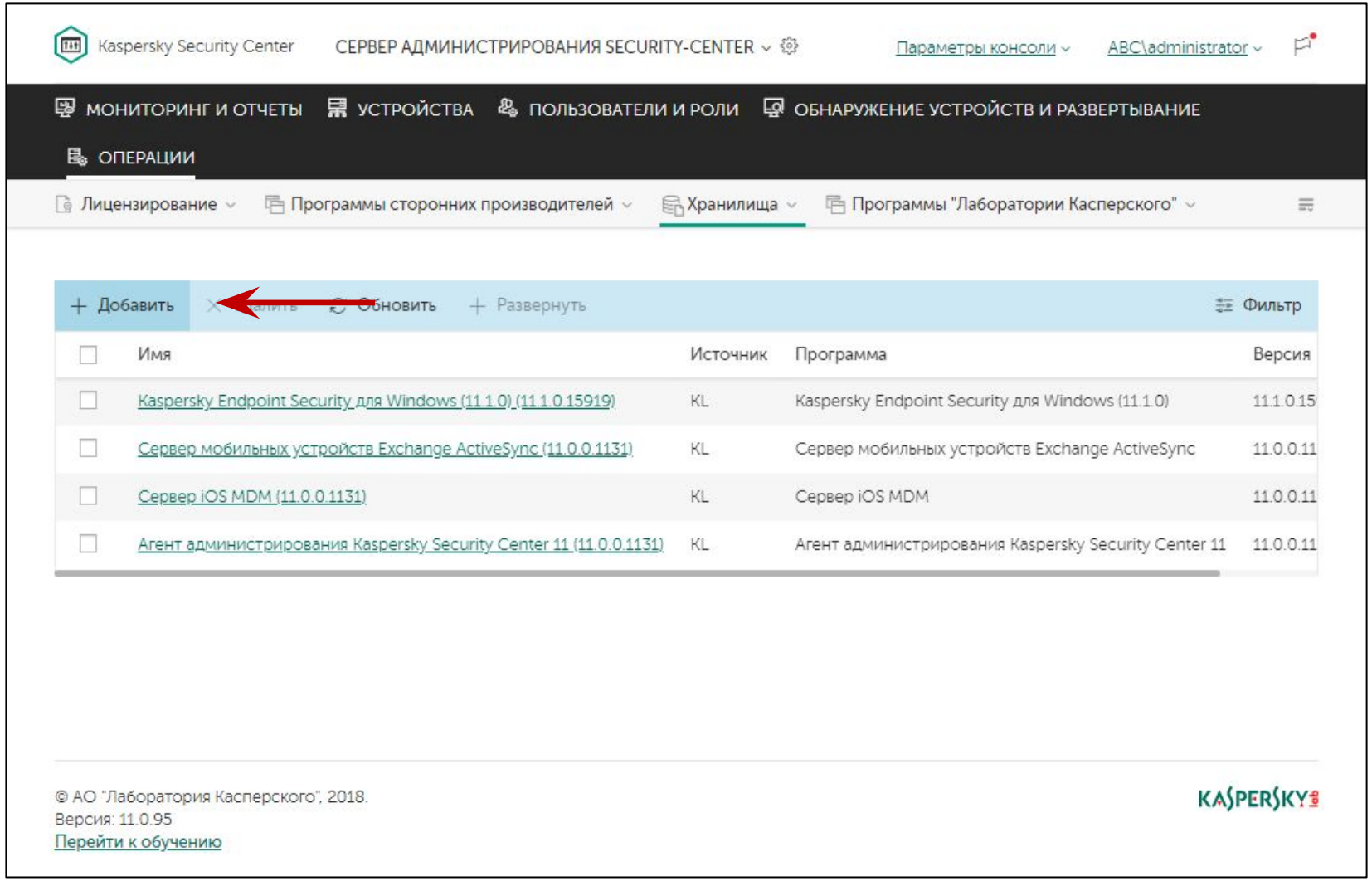
Как удаленно установить агент и KES

Как проще установить агент и KES локально

Как установить агент через Active Directory

Как удалить несовместимые программы

Создание инсталляционных пакетов



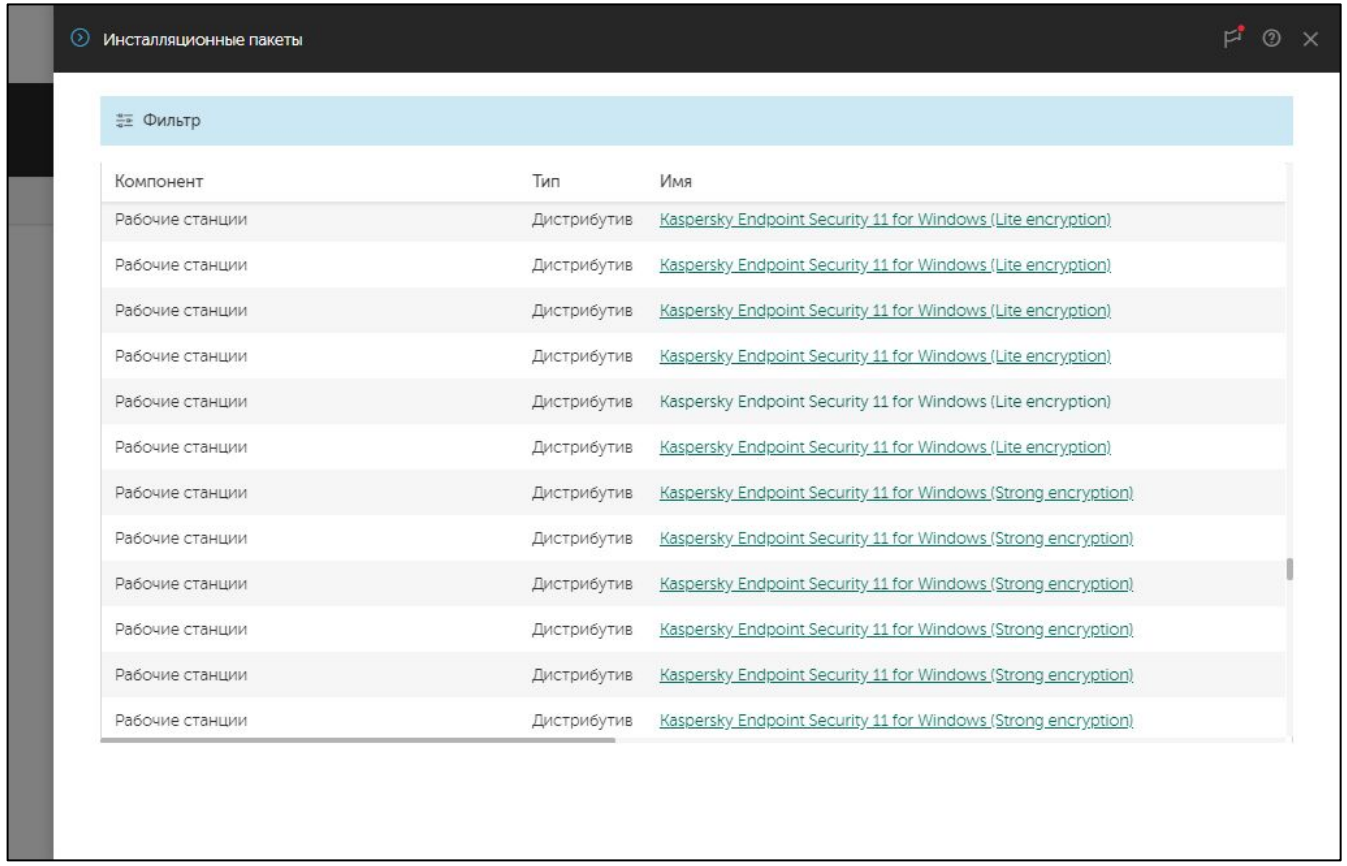
Создавайте пакеты:

- Чтобы устанавливать Kaspersky Endpoint Security или Агент администрирования с разными настройками на разные компьютеры
- Чтобы устанавливать другие программы Лаборатории Касперского, например, Kaspersky Security для Windows Servers
- Чтобы устанавливать другие версии программ Лаборатории Касперского, например, Kaspersky Endpoint Security 10 SP2

Выбор пакета

Пакет установки:

1. Выберите пакет среди доступных
2. Примите лицензионное соглашение
3. Подождите пока мастер загрузит файлы в хранилище



Web Console не позволяет создать свой инсталляционный пакет, можно выбрать только среди доступных

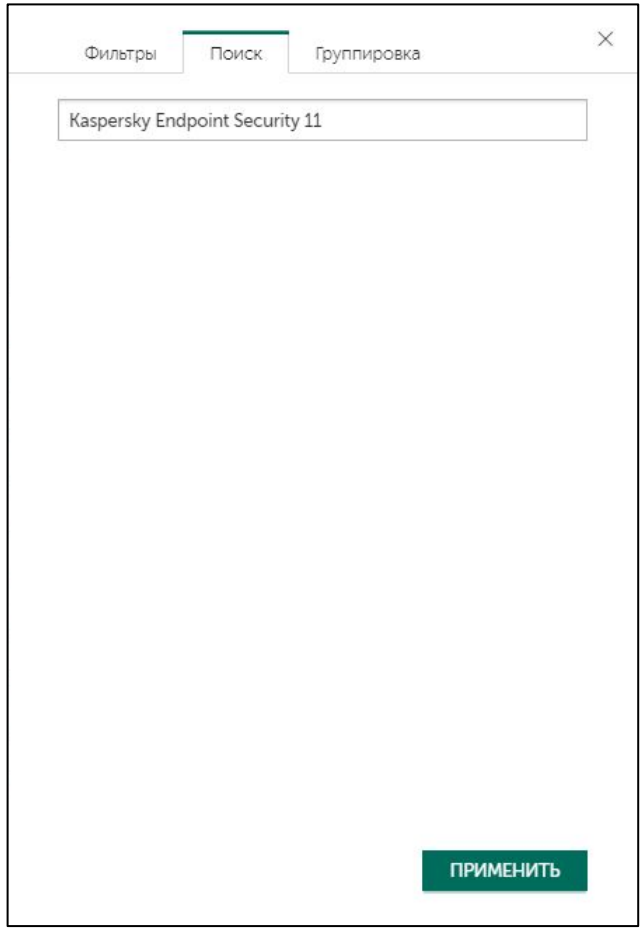
Администратор может загрузить:

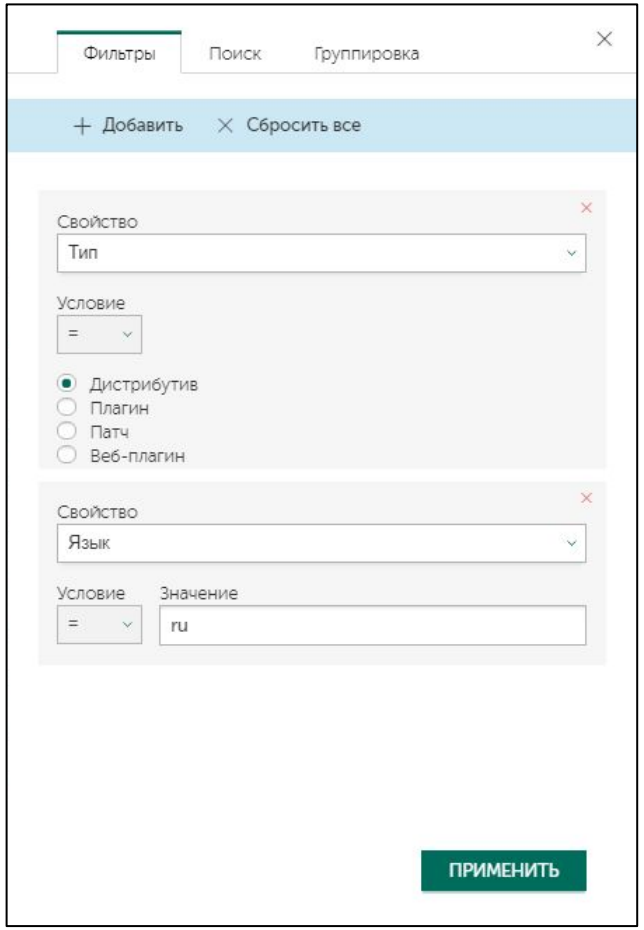
- инсталляционные пакеты (новые версии, старые версии, другие языки)
- плагины управления
- новые версии компонентов Kaspersky Security Center (Веб-Консоль)

Выбор пакета

Пакет установки:

1. Выберите пакет среди доступных
2. Примите лицензионное соглашение
3. Подождите пока мастер загрузит файлы в хранилище





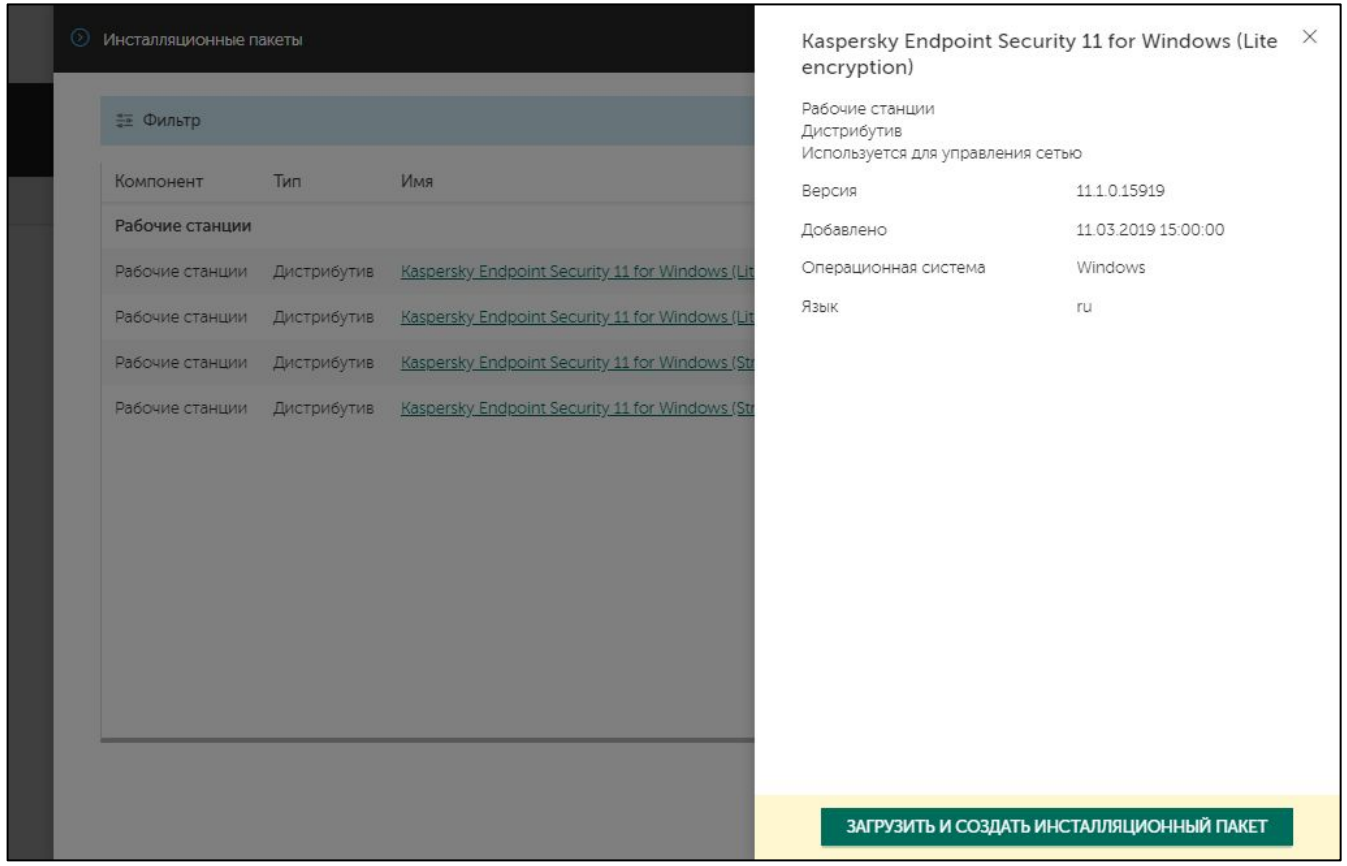
Для того, чтобы найти нужное приложение, используйте фильтр

Например, можно в явном виде указать название приложения, а также добавить тип пакета и локализацию

Выбор пакета

Пакет установки:

1. Выберите пакет среди доступных
2. Примите лицензионное соглашение
3. Подождите пока мастер загрузит файлы в хранилище

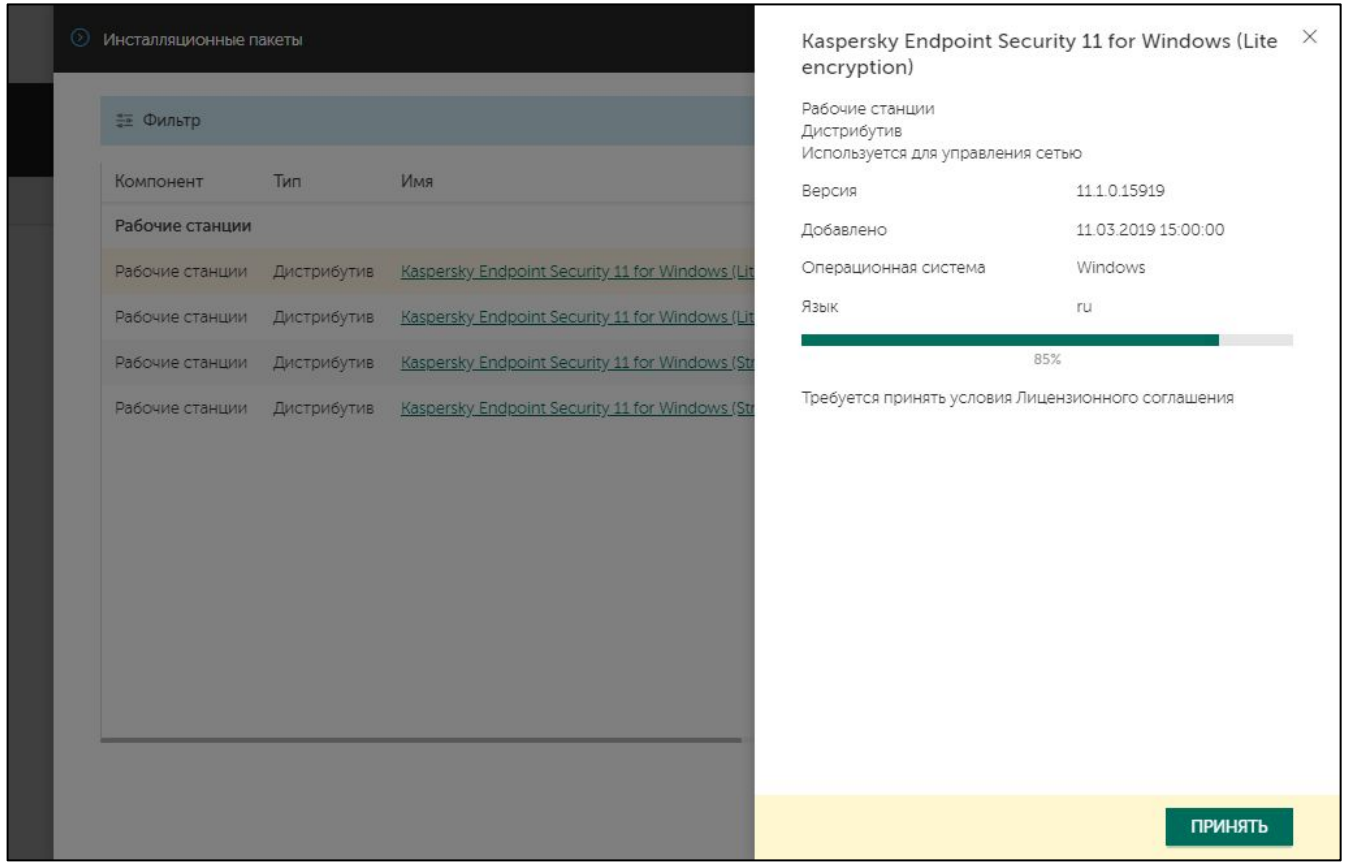


Затем нажимаете на пакет и выбираете **Загрузить и создать инсталляционный пакет**

Лицензионное соглашение

Пакет установки:

1. Выберите пакет среди доступных
2. Примите лицензионное соглашение
3. Подождите пока мастер загрузит файлы в хранилище



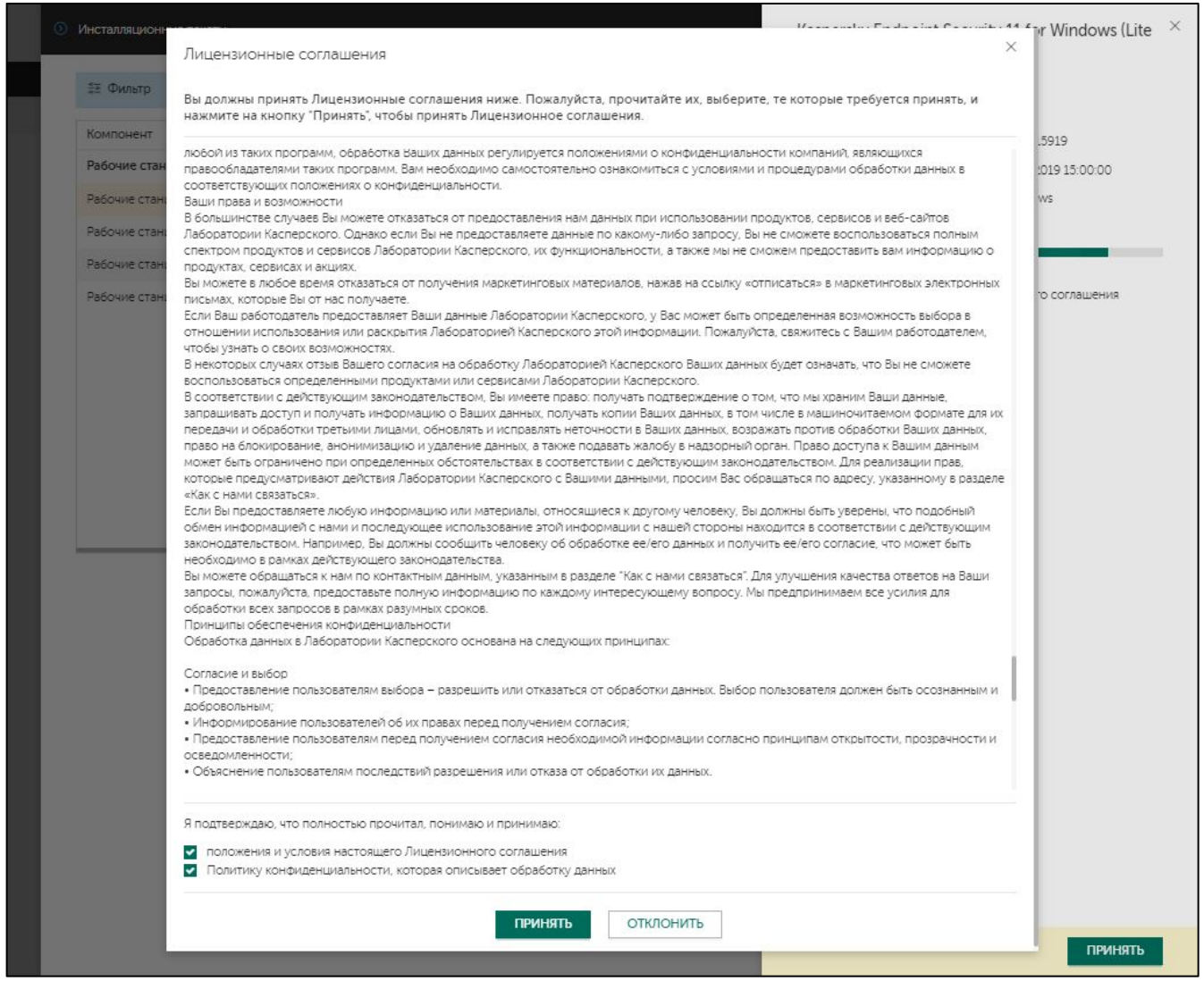
В процессе создания пакета нужно будет принять лицензионное соглашение

Мастер остановится и будет ждать действия пользователя

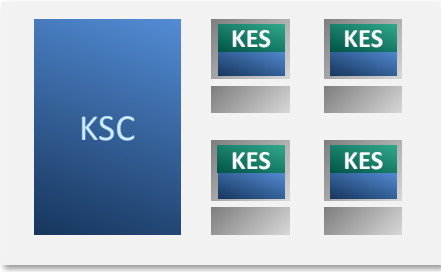
Лицензионное соглашение

Пакет установки:

1. Выберите пакет среди доступных
2. Примите лицензионное соглашение
3. Подождите пока мастер загрузит файлы в хранилище



Кнопка **Принять** по умолчанию тусклая, чтобы она стала яркой нужно прокрутить лицензионное соглашение до самого конца



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Требования к клиентским компьютерам
Как изменить состав компонентов KES
Как создать новый пакет установки

Как создать пакет KSWS

Какие есть методы установки
Как удаленно установить агент и KES
Как проще установить агент и KES локально
Как установить агент через Active Directory
Как удалить несовместимые программы

Какие еще есть приложения для защиты Windows Servers

- Kaspersky Security 10.1 for Windows Server
  - Защищает серверную файловую систему
  - Контролирует запуск программ на сервере
  - Контролирует подключения сторонних устройств к серверу
  - Защищает сеансы удаленного рабочего стола
  - Защищает системы хранения данных от вредоносных программ и шифровальщиков-вымогателей
  - Анализирует журналы операционной системы и мониторит файловые операции
  - Отправляет события в SIEM

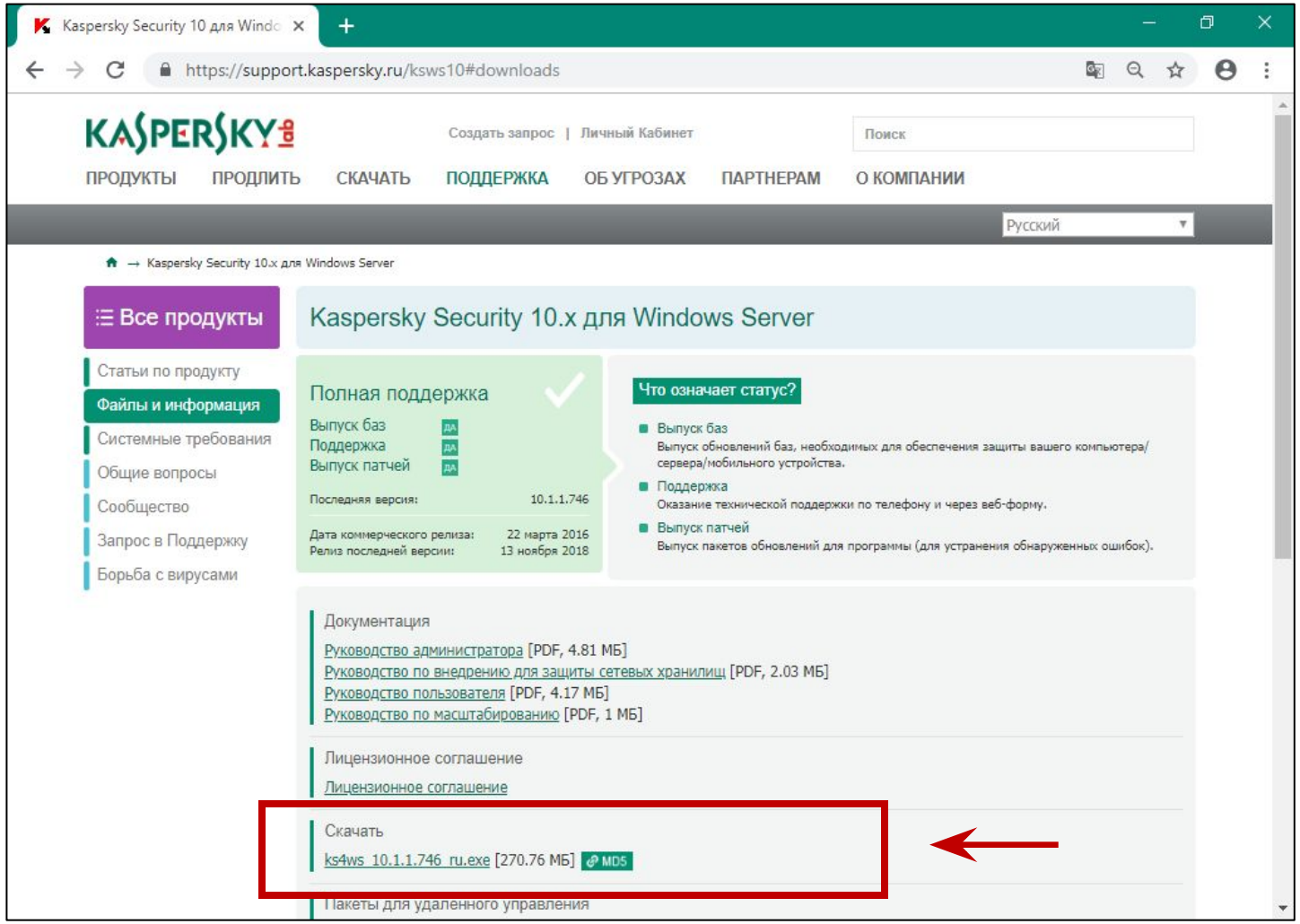
Достоинства Kaspersky Security 10.1 for Windows Server

- Стабильность
  - KSWS 10.1 оптимизирован и тестируется только на серверных ОС
  - Сертификаты Microsoft®, Citrix®, VMware®
  - Не требует перезагрузку при установке и обновлении версии
- Производительность
  - Набор компонентов оптимизирован для защиты сервера от современных угроз
  - Оптимизация под серверные операционные системы
  - Гибкие настройки защиты
- Поддержка различных корпоративных сценариев
  - Установка на Windows Server в режиме Core
  - Прозрачная работа на терминальном сервере
  - Работа на отказоустойчивом кластере
  - Защита Систем Хранения Данных
  - Поддержка SNMP

Особенности Kaspersky Security 10.1 for Windows Server

- Установка на Windows Server в режиме Core
- Отслеживание вредоносного шифрования в папках общего доступа и системах хранения данных
- Блокировка сессий пользователей при обнаружении вредоносной активности в папках общего доступа
- Уведомление пользователей в терминальных сессиях о вредоносных объектах
- Поддержка отказоустойчивого кластера

Где скачать дистрибутив KSWS 10.1



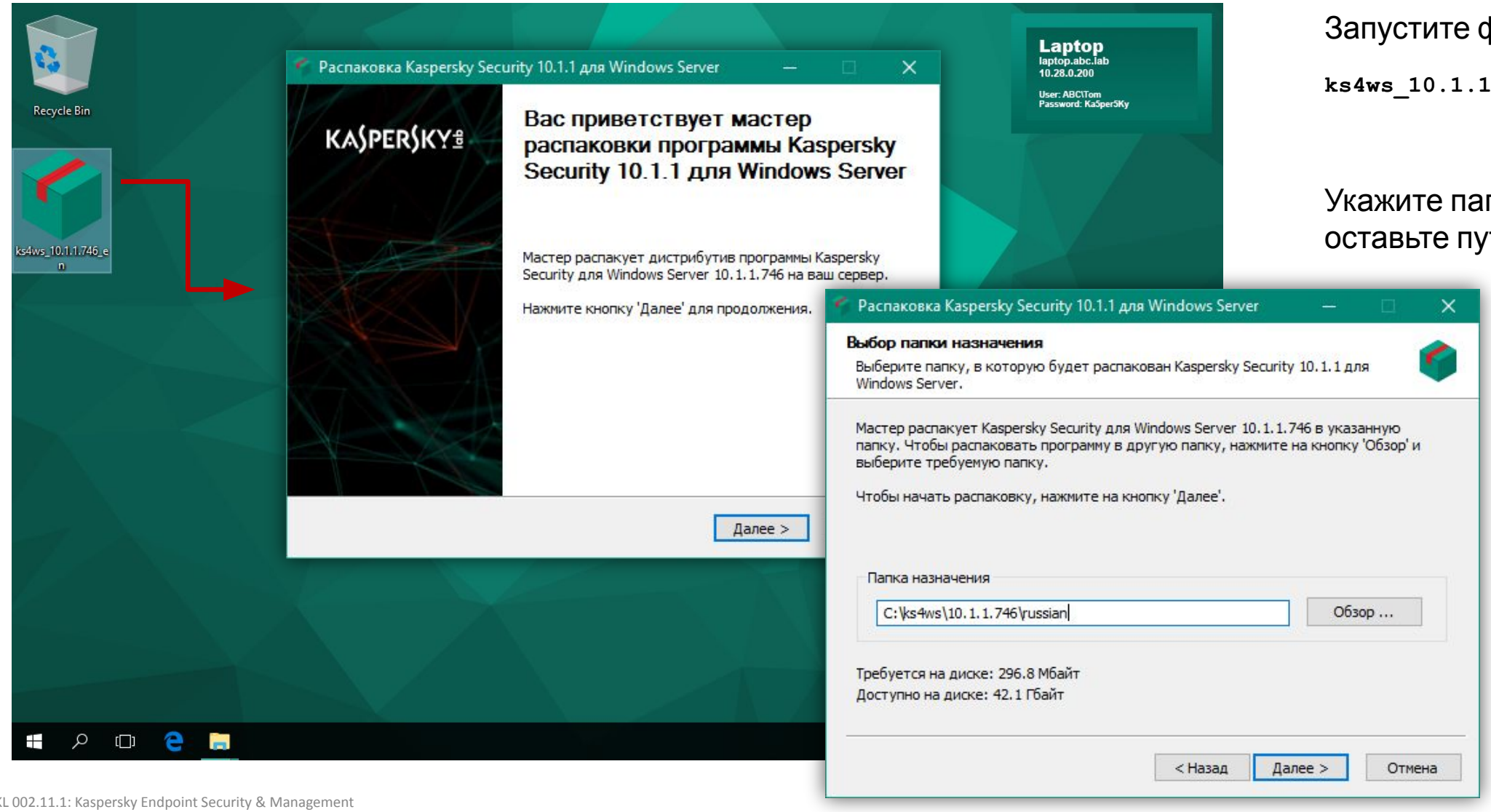
Существует несколько локализаций Kaspersky Security для Windows Server

- English
- Russian
- German
- French
- Japanese
- Chinese

Также на сайте можно скачать документацию к Kaspersky Security для Windows Server на разных языках

https://support.kaspersky.com/ksws10#downloads

Как распаковать дистрибутив KSWS 10.1

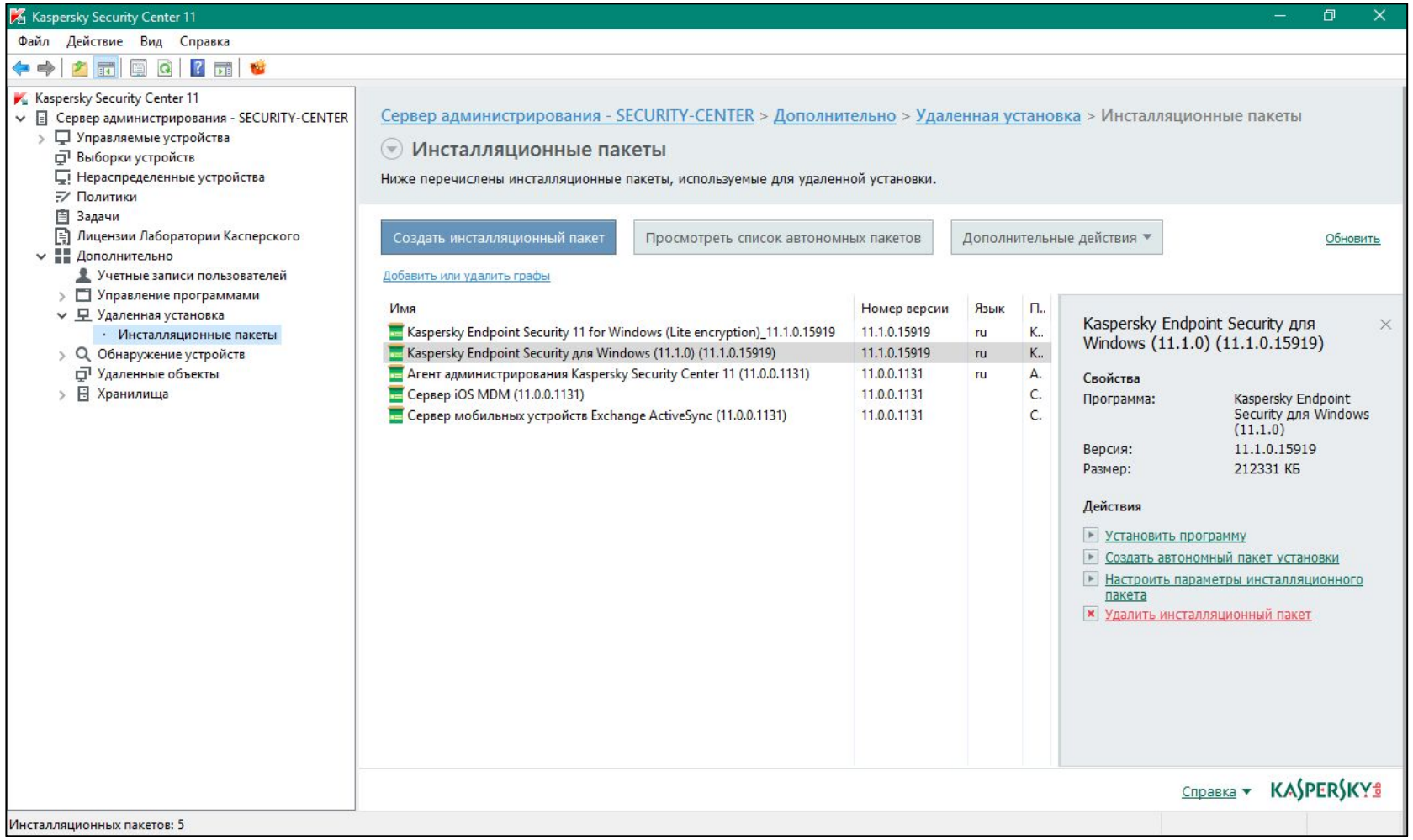


Запустите файл –

`ks4ws_10.1.1.746_ru.exe`

Укажите папку назначения или оставьте путь по умолчанию

Как создать инсталляционный пакет KSWS 10.1



Инсталляционный пакет можно создать как из MMC, так и из Web Console, но управлять можно только из MMC

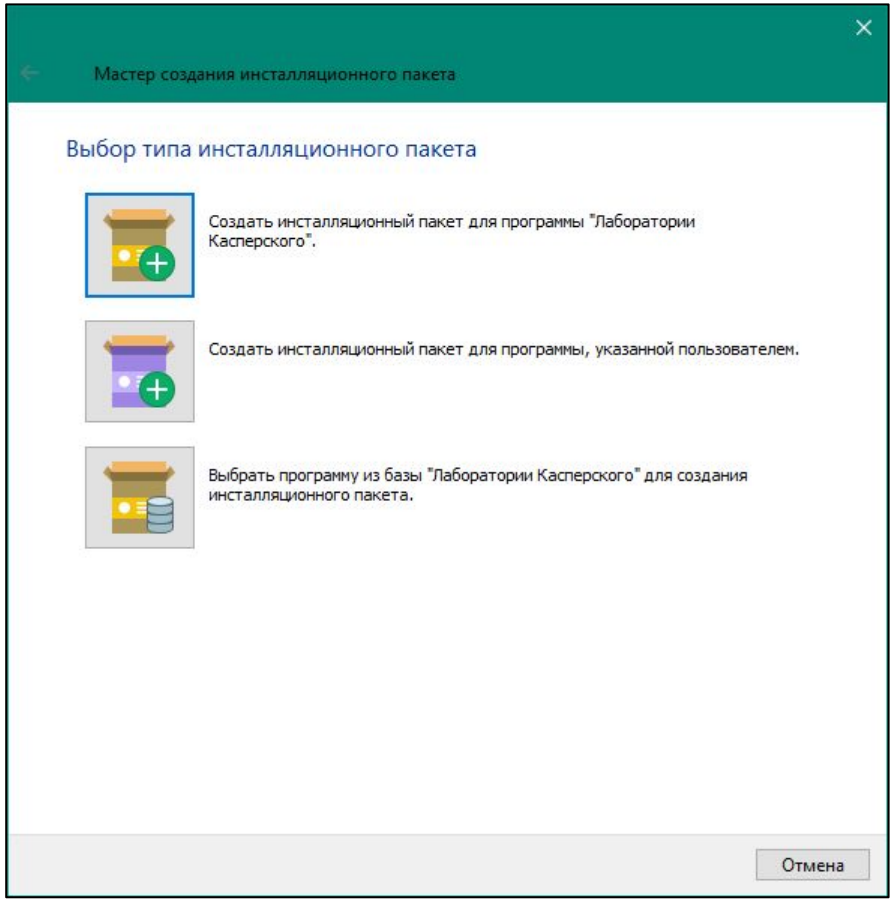
На компьютере, где установлена Консоль KSC, необходимо иметь дистрибутив KSWS в распакованном виде

Запустите Мастер создания инсталляционного пакета

Тип пакета

Мастер создания установочного пакета:

1. Выберите тип пакета
2. Назовите пакет
3. Укажите исходные файлы для установки
4. Примите условия лицензионного соглашения
5. Завершите автоматическую установку плагина
6. Подождите пока мастер загрузит файлы в хранилище



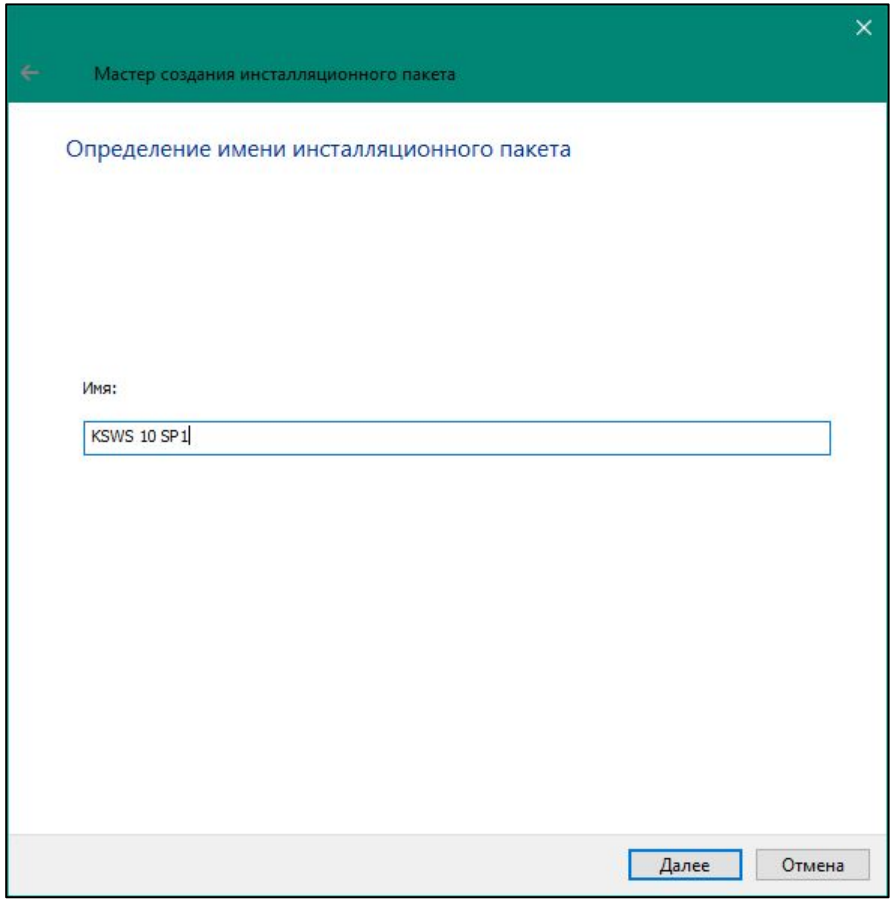
Существует 3 типа инсталляционных пакетов в Kaspersky Security Center:

- Пакеты для программ Лаборатории Касперского — требуют плагин программы, чтобы показать свойства пакета; могут содержать настройки установки или настройки программы
- Пакеты для исполняемых файлов — запускают на компьютерах выбранный исполняемый файл; допускают задать параметры командной строки
- Пакеты для программ из базы обновляемых программ Лаборатории Касперского; требуют лицензию KESB расширенный

Мастер создания установочного пакета:

1. Выберите тип пакета
2. Назовите пакет
3. Укажите исходные файлы для установки
4. Примите условия лицензионного соглашения
5. Завершите автоматическую установку плагина
6. Подождите пока мастер загрузит файлы в хранилище

Имя пакета



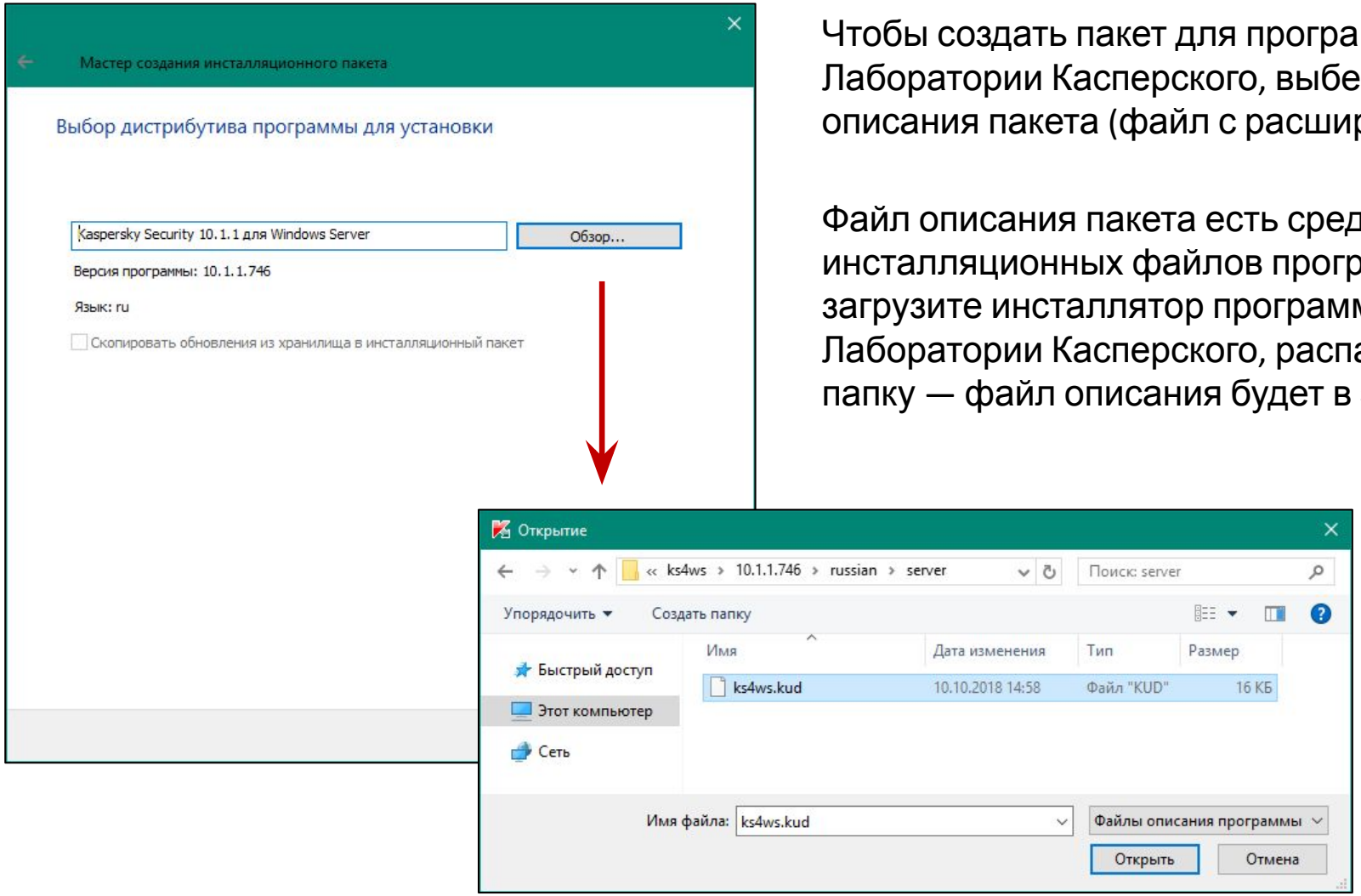
Вы можете выбрать произвольное имя для пакета

Имеет смысл выбирать имя, которое отражает особенности настроек пакета, например KSWS 10.1 без мониторинга скриптов

Файлы для создания инсталляционного пакета

Мастер создания установочного пакета:

1. Выберите тип пакета
2. Назовите пакет
3. Укажите исходные файлы для установки
4. Примите условия лицензионного соглашения
5. Завершите автоматическую установку плагина
6. Подождите пока мастер загрузит файлы в хранилище



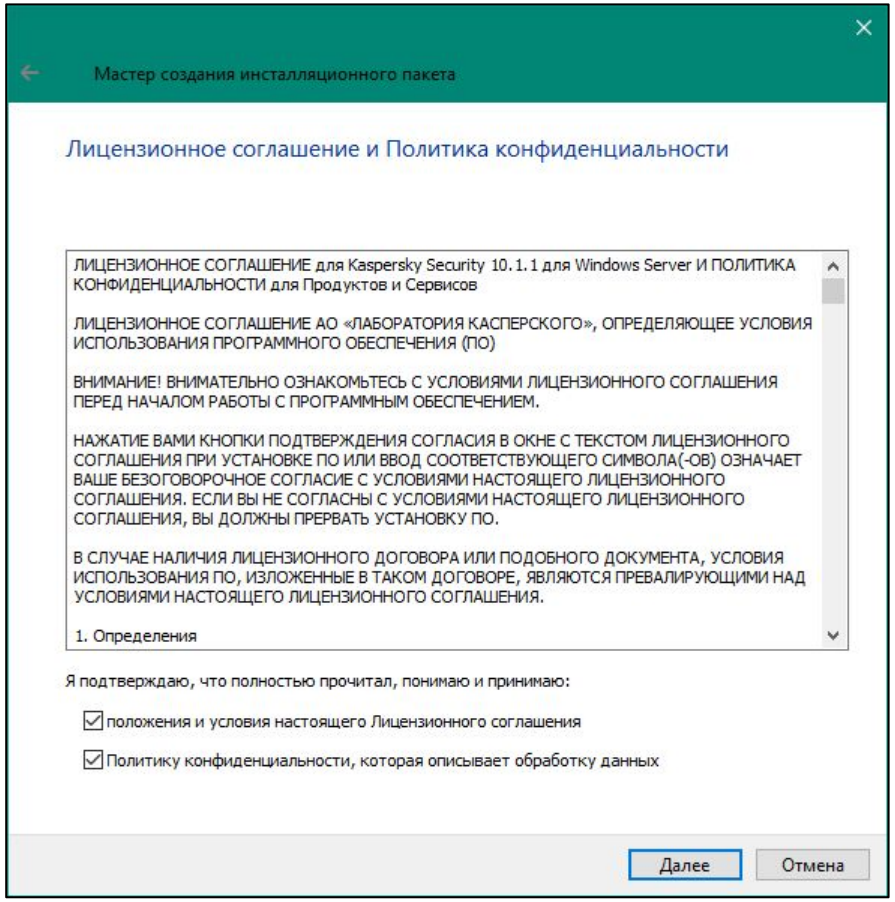
Чтобы создать пакет для программы Лаборатории Касперского, выберите файл описания пакета (файл с расширением ***.kud**)

Файл описания пакета есть среди инсталляционных файлов программы: загрузите инсталлятор программы с веб-сайта Лаборатории Касперского, распакуйте его в папку — файл описания будет в этой папке

Мастер создания установочного пакета:

1. Выберите тип пакета
2. Назовите пакет
3. Укажите исходные файлы для установки
4. Примите условия лицензионного соглашения
5. Завершите автоматическую установку плагина
6. Подождите пока мастер загрузит файлы в хранилище

Лицензионное соглашение

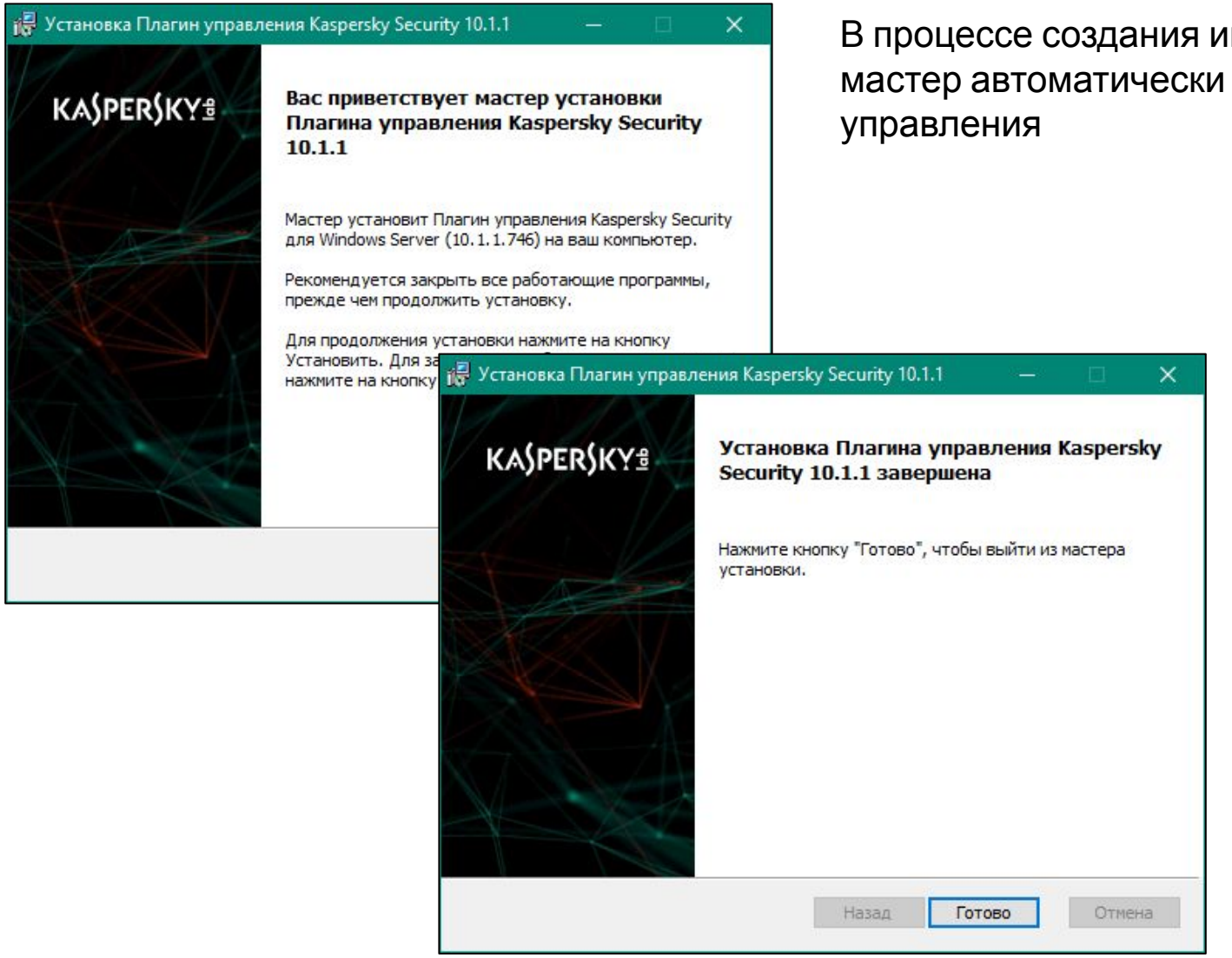


Чтобы создать пакет, примите лицензионное соглашение

Автоматическая установка плагина управления KSWS 10.1

Мастер создания установочного пакета:

1. Выберите тип пакета
2. Назовите пакет
3. Укажите исходные файлы для установки
4. Примите условия лицензионного соглашения
5. Завершите автоматическую установку плагина
6. Подождите пока мастер загрузит файлы в хранилище

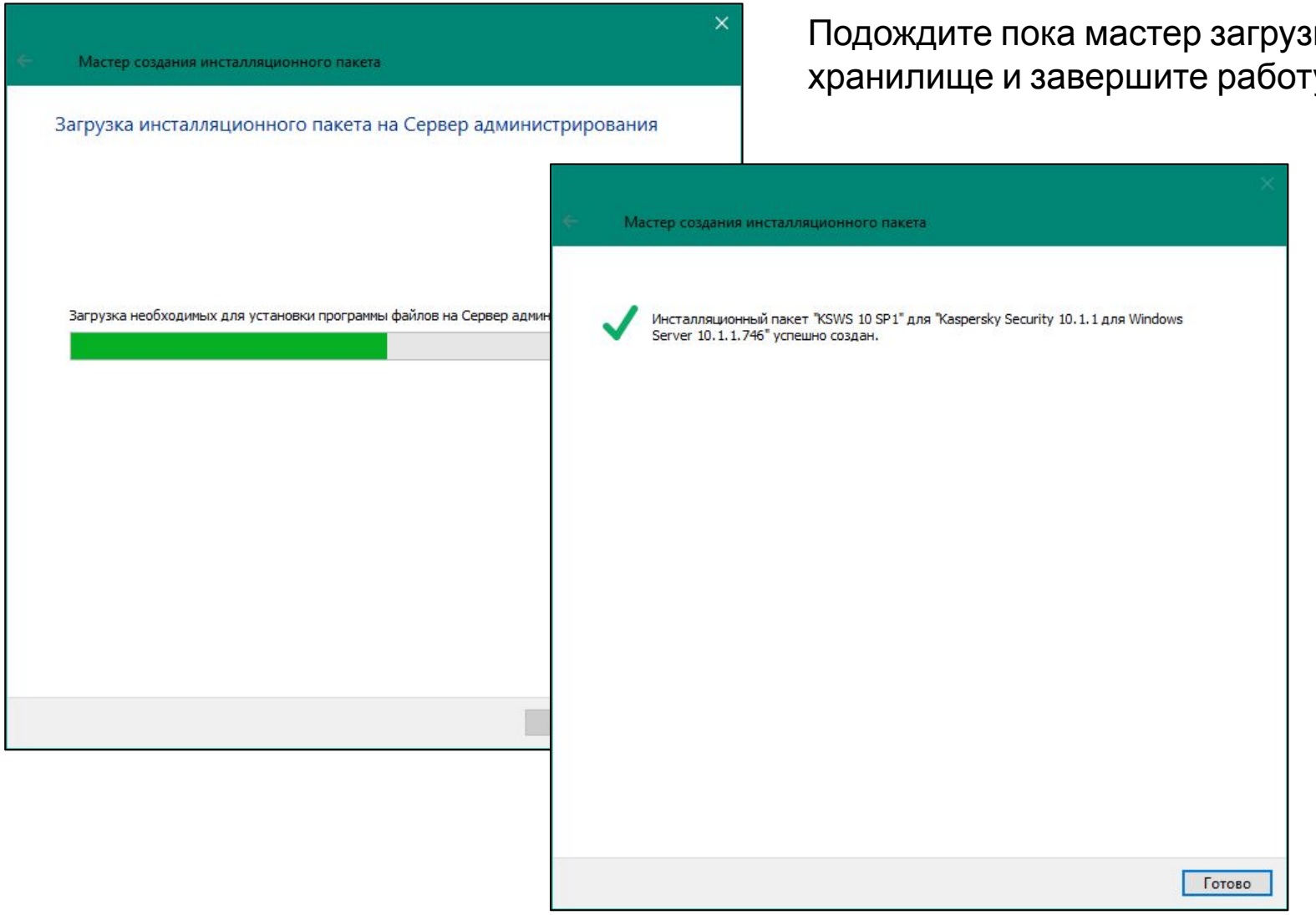


В процессе создания инсталляционного пакета, мастер автоматически установит и плагин управления

Мастер создания установочного пакета:

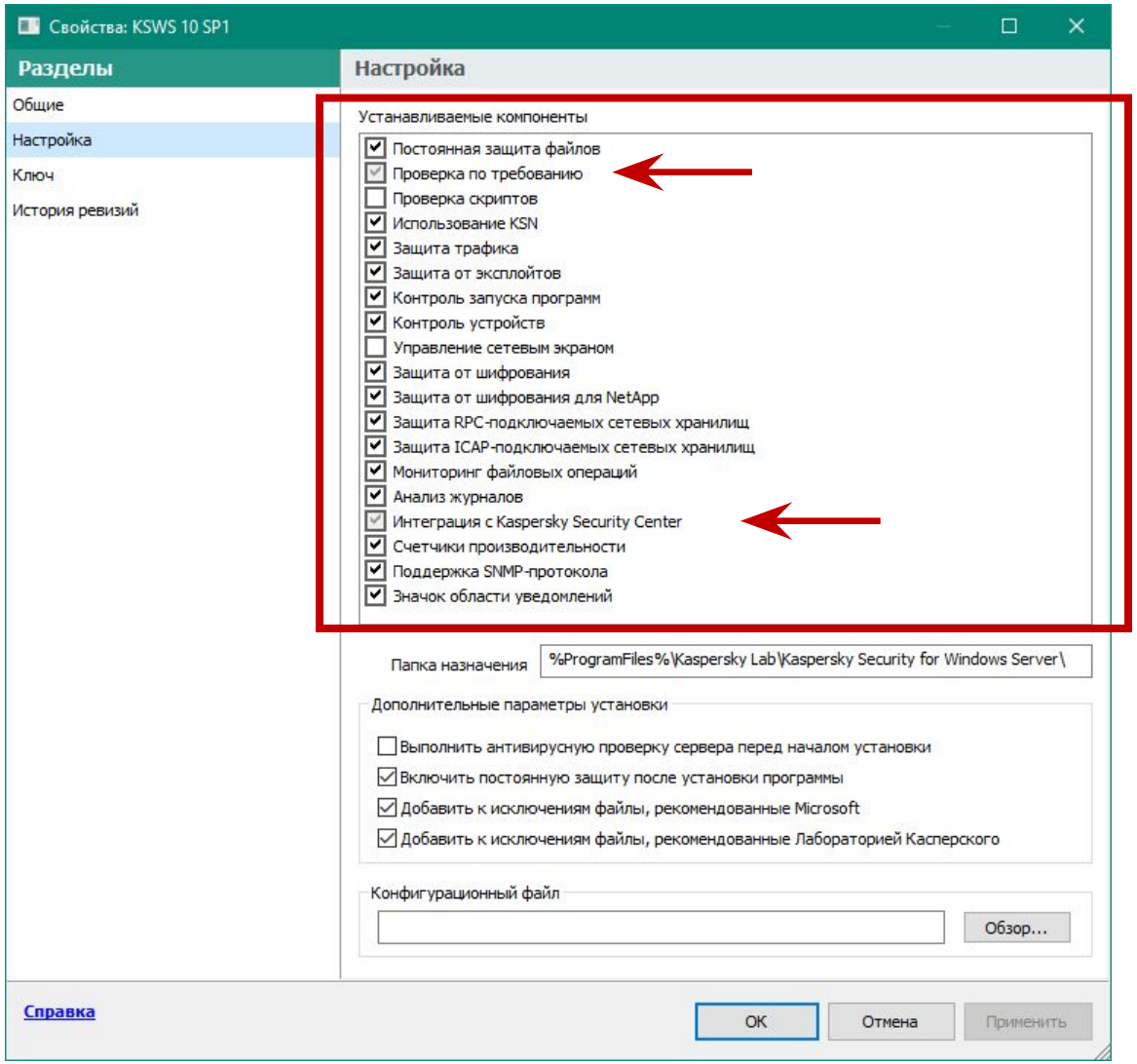
1. Выберите тип пакета
2. Назовите пакет
3. Укажите исходные файлы для установки
4. Примите условия лицензионного соглашения
5. Завершите автоматическую установку плагина
6. Подождите пока мастер загрузит файлы в хранилище

Загрузка пакета в хранилище



Подождите пока мастер загрузит файлы в хранилище и завершите работу мастера

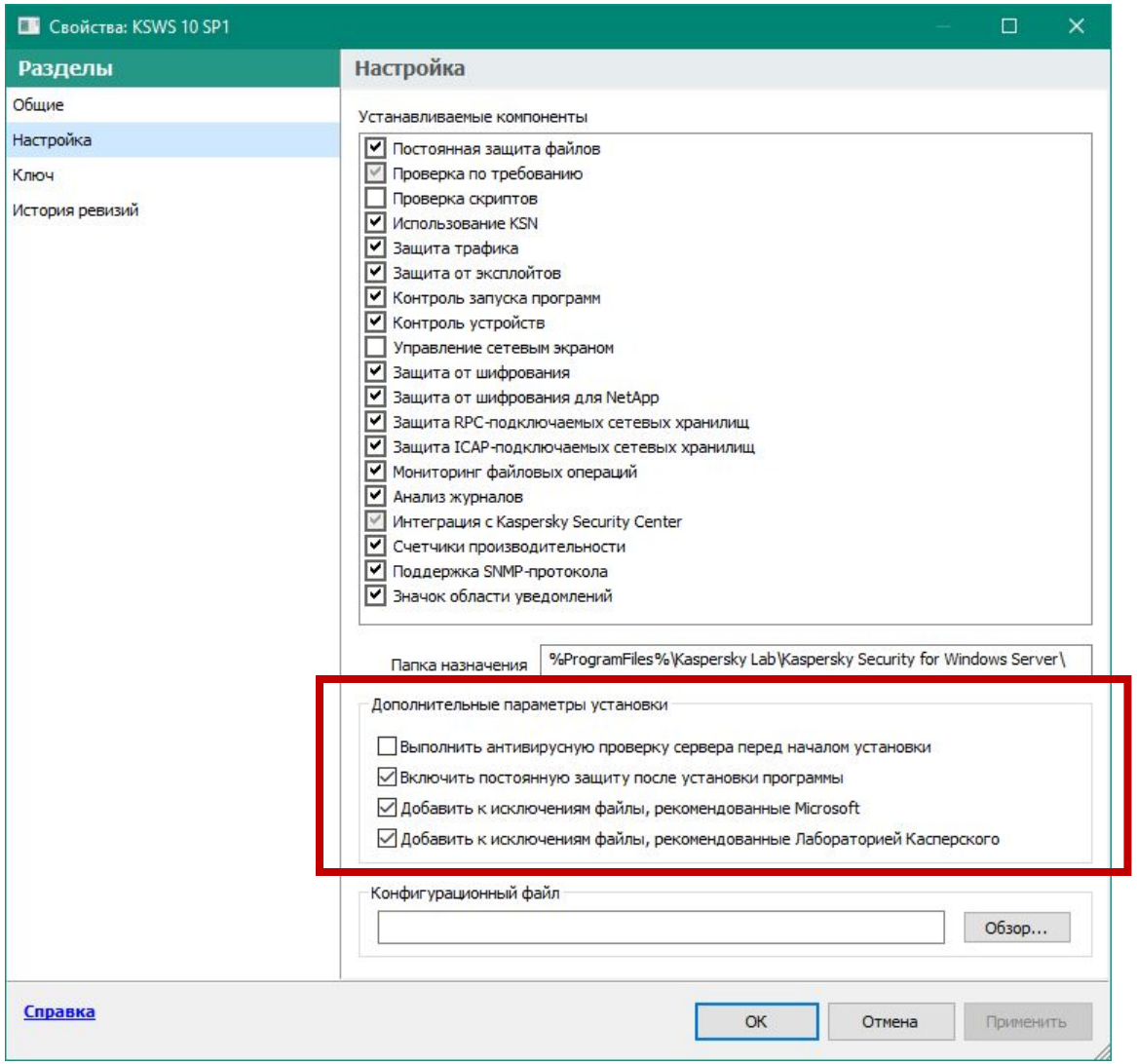
Выберите компоненты KSWS 10.1 (опционально)



Есть только два обязательных компонента при установке через Kaspersky Security Center

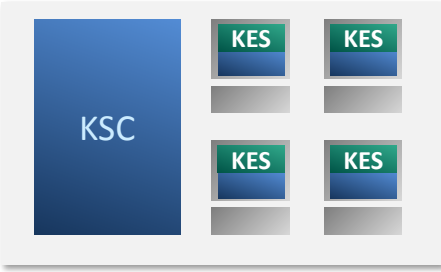
- Проверка по требованию
- Интеграция с Kaspersky Security Center

Измените дополнительные настройки KSWS 10.1 (опционально)



В свойствах пакета можно изменить дополнительные параметры, которые будут использоваться при установке через Kaspersky Security Center:

- Сканировать ли системную память перед установкой
- Включить ли постоянную защиту сразу после установки
- Добавлять ли рекомендуемые исключения



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Требования к клиентским компьютерам
Как изменить состав компонентов KES
Как создать новый пакет установки
Как создать пакет KSWS

Какие есть методы установки

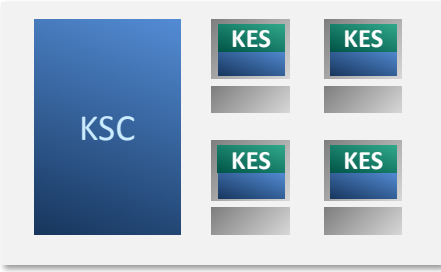
Как удаленно установить агент и KES
Как проще установить агент и KES локально
Как установить агент через Active Directory
Как удалить несовместимые программы

Что сделать перед установкой

- Дайте серверу время обнаружить компьютеры
- Подготовьте независимый список компьютеров, если у вас он есть, с адресами компьютеров и паролями администраторов, если компьютеры не в домене
- Выясните, включен ли на компьютерах сетевой экран, и есть ли доступ к общим папкам
- Выясните, есть ли на компьютерах другие антивирусы
- Если компьютеров много, разбейте их на группы и этапы установки
- Попробуйте разные методы установки в тестовой среде и решите, какие и как будете использовать
- Приступайте

Какие есть методы установки

Метод	Особенности
Удаленная установка	Нужно имя и пароль администратора Нужен доступ к общим папкам компьютера по сети Иногда нужно знать адрес (или имя) компьютера
Автономные пакеты	Локальная установка Нужны права администратора Не нужен доступ к компьютеру по сети
Установка через Active Directory	Нужны права администратора домена Не нужны права на компьютере и доступ к компьютеру Компьютер должен быть в домене Установка выполняется во время перезагрузки
Установка сторонними средствами	Зависят от стороннего средства



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса
Глава 2. Как установить Kaspersky Security Center
Глава 3. Как установить Kaspersky Endpoint Security на компьютеры
Глава 4. Как организовать компьютеры в группы

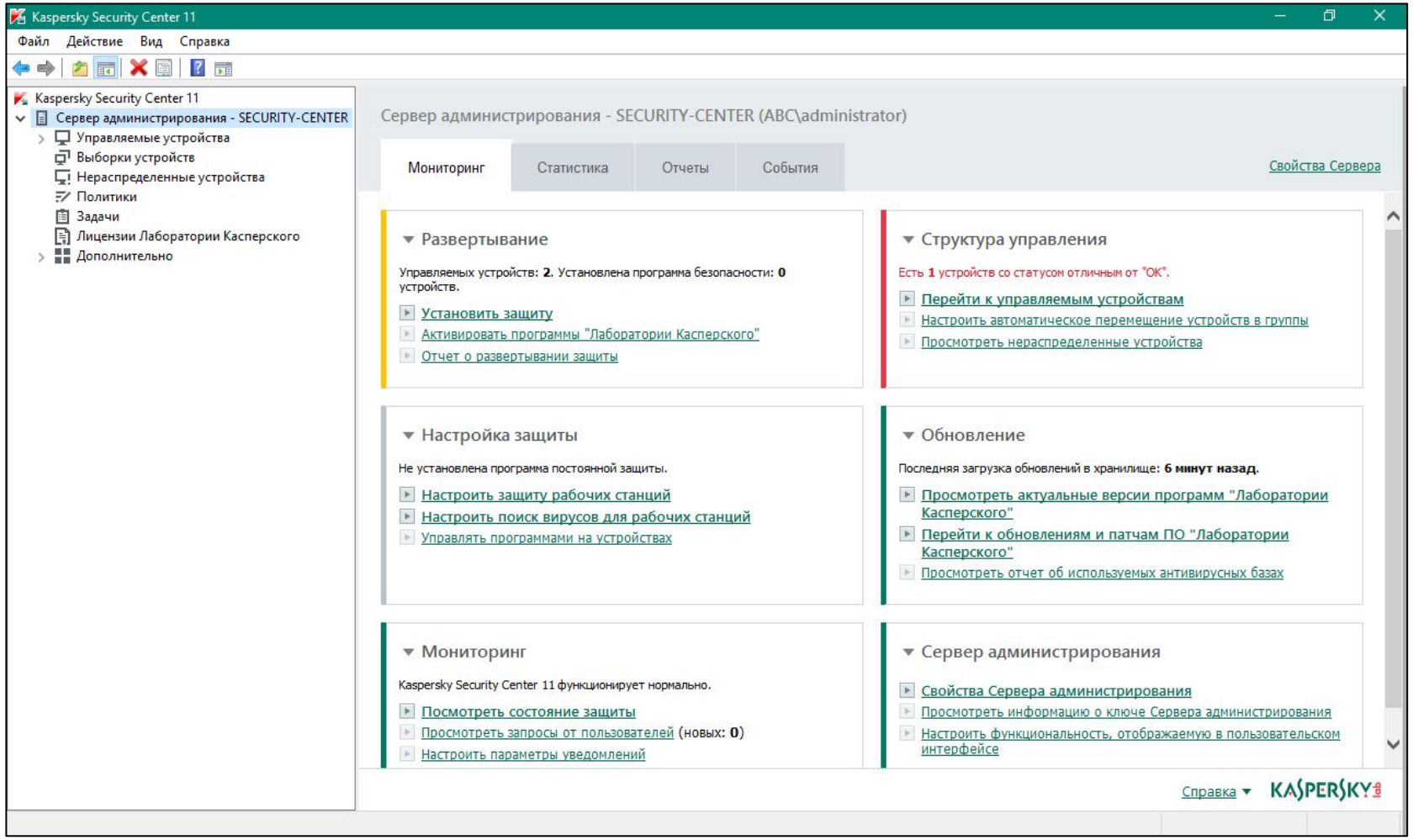
Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Требования к клиентским компьютерам
Как изменить состав компонентов KES
Как создать новый пакет установки
Как создать пакет KSWS
Какие есть методы установки
Как удаленно установить агент и KES
Как проще установить агент и KES локально
Как установить агент через Active Directory
Как удалить несовместимые программы

Запуск мастера удаленной установки



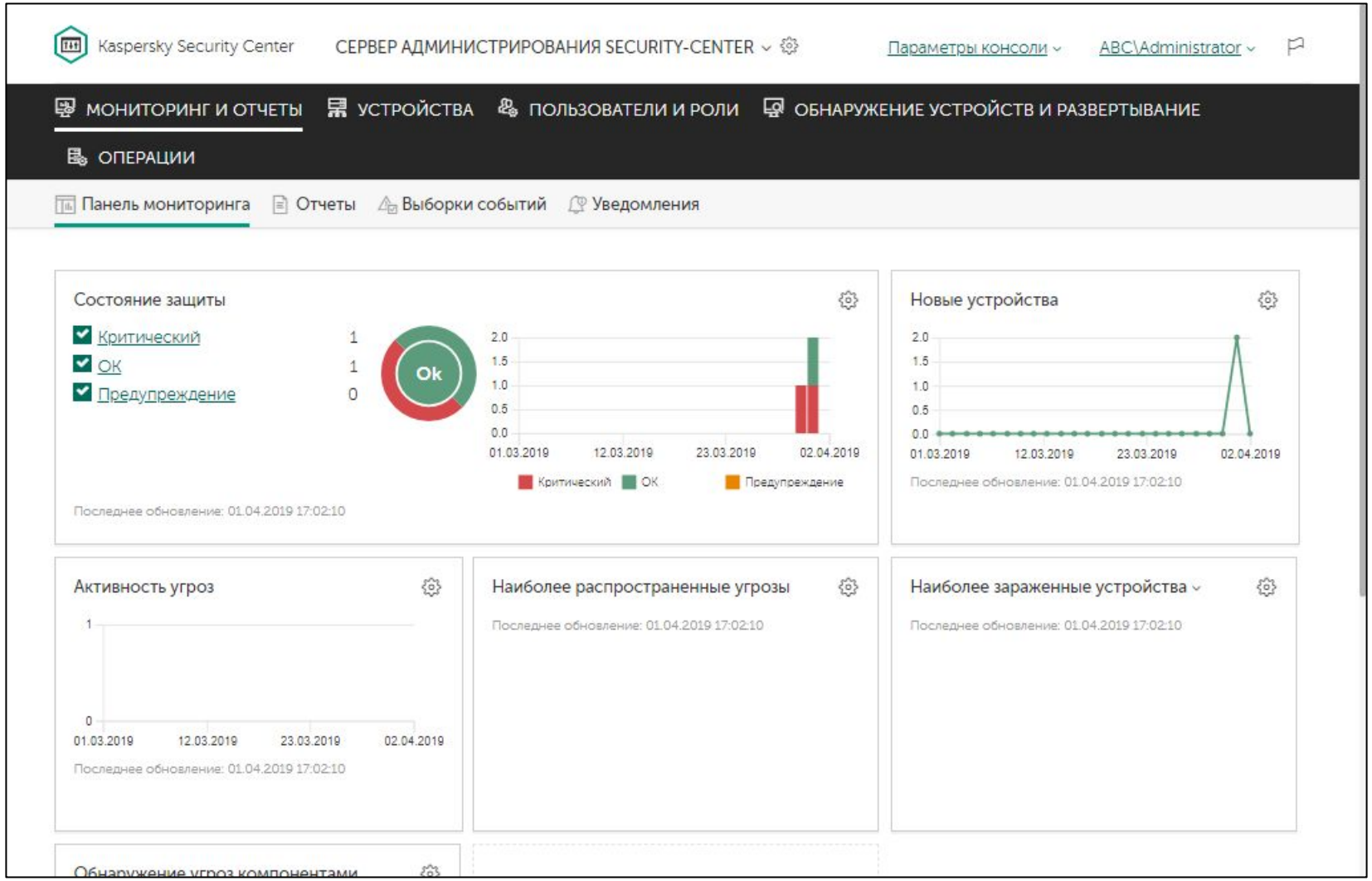
Страница **Мониторинг** предлагает начать развертывание продукта с помощью специального мастера установки

Установить защиту читайте как *установить программы для защиты от угроз*, например, Kaspersky Endpoint Security для Windows

Кроме мастера установки вы можете использовать:

- Задачи удаленной установки
- Режим автоматической установки в группах администрирования

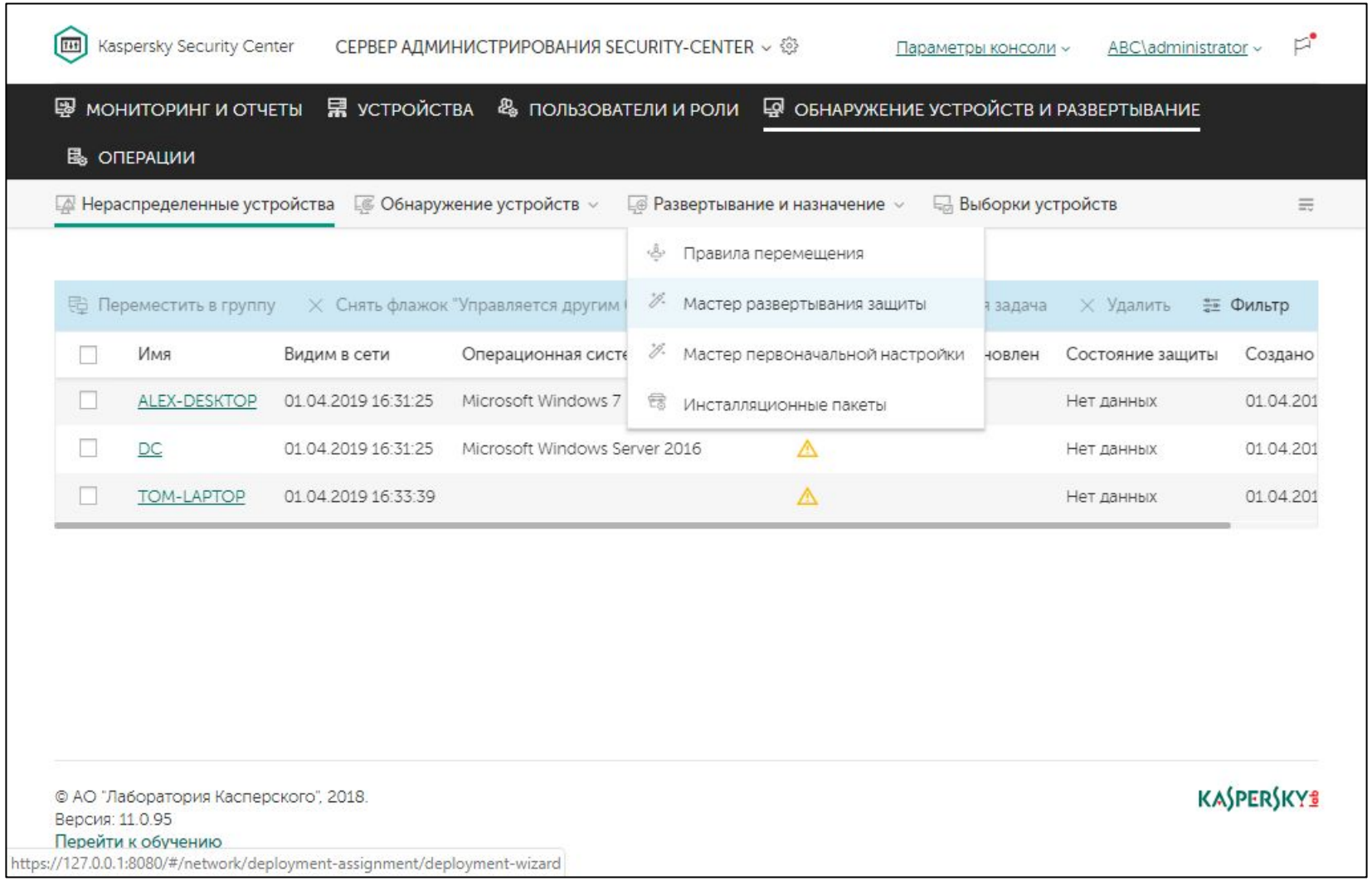
Запуск мастера удаленной установки



К сожалению, в главном окне не показывается в явном виде, где установлена защита, а где нет

Также в главном окне не показывается сколько устройств находится в списке нераспределенных

Запуск мастера удаленной установки



Запустить мастер удаленной установки можно разными способами:

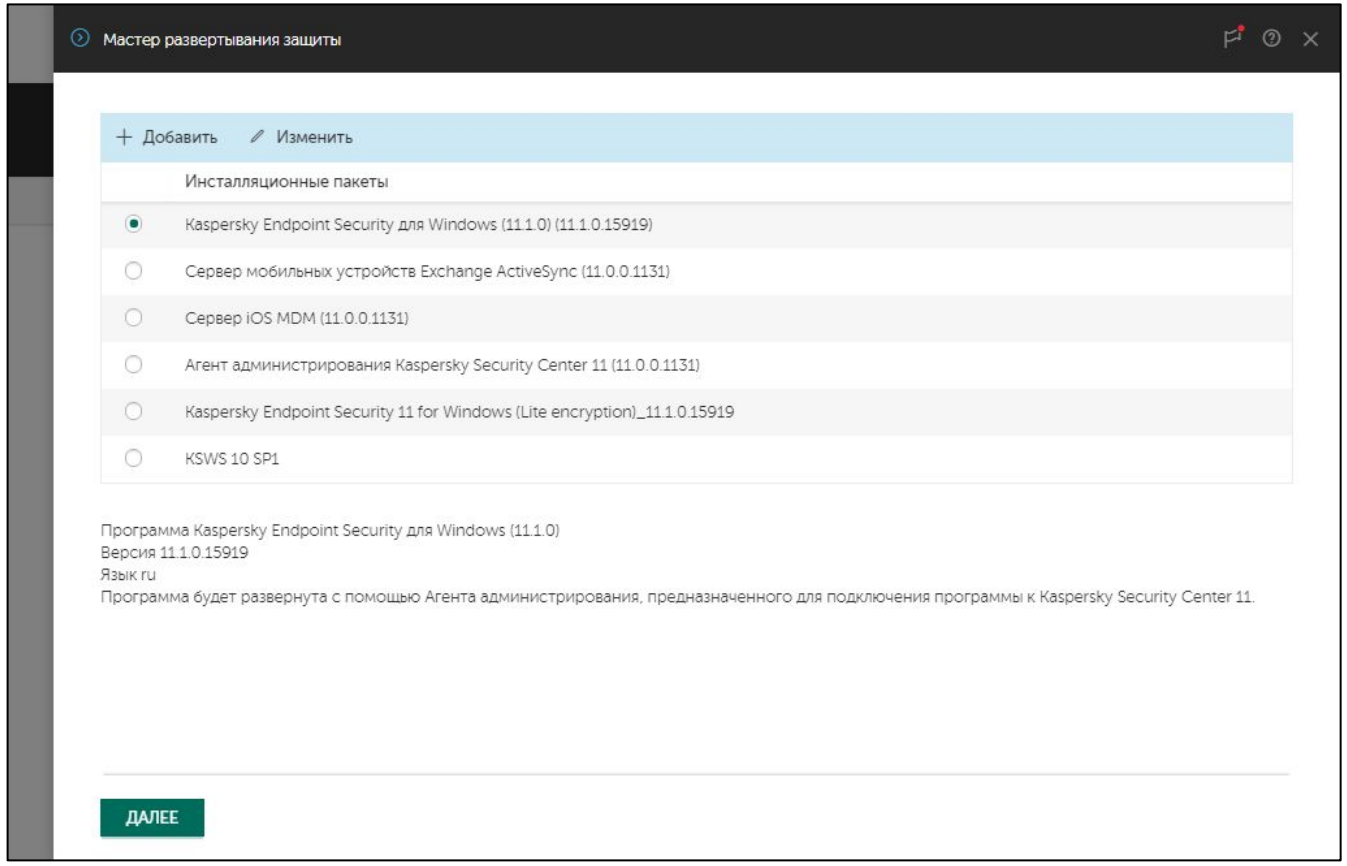
- **Обнаружение устройств и развертывание | Развертывание и назначение | Мастер первоначальной настройки**
- Перейти в **Обнаружение устройств и развертывание | Развертывание и назначение | Инсталляционные пакеты**, выбрать нужный пакет и нажать **Развернуть**
- Создать задачу удаленной установки

Кроме мастера можно воспользоваться режимом автоматической установки в группах администрирования

Выбор пакета установки

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



Установка Kaspersky Security Center содержит инсталляционные пакеты Агента администрирования и Kaspersky Endpoint Security

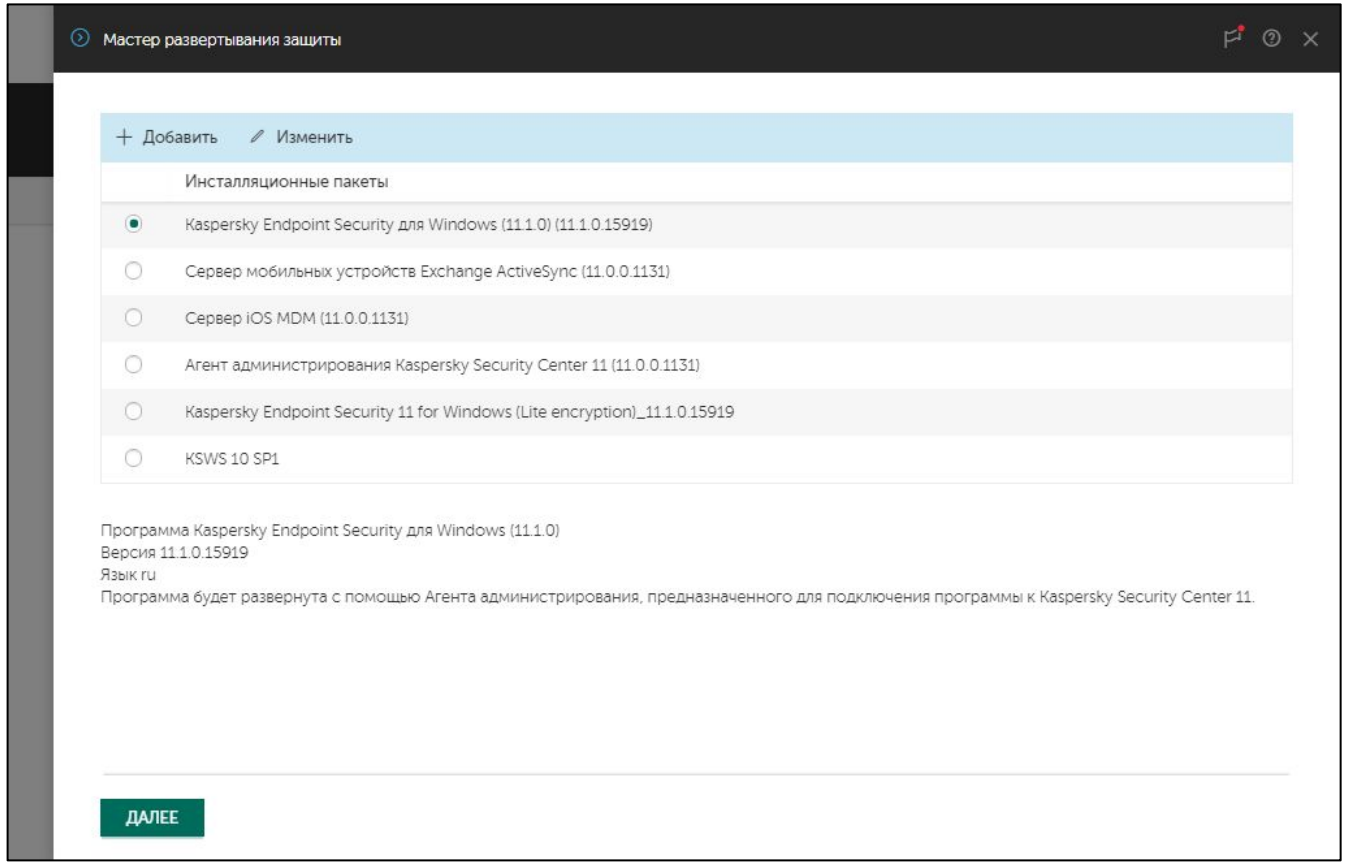
В пакете Kaspersky Endpoint Security выбраны для установки все компоненты, кроме шифрования, Endpoint Sensor и защиты от атак BadUSB

Администратор может ничего не менять и сразу подключать компьютеры к серверу и защищать их от угроз

Выбор пакета установки

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



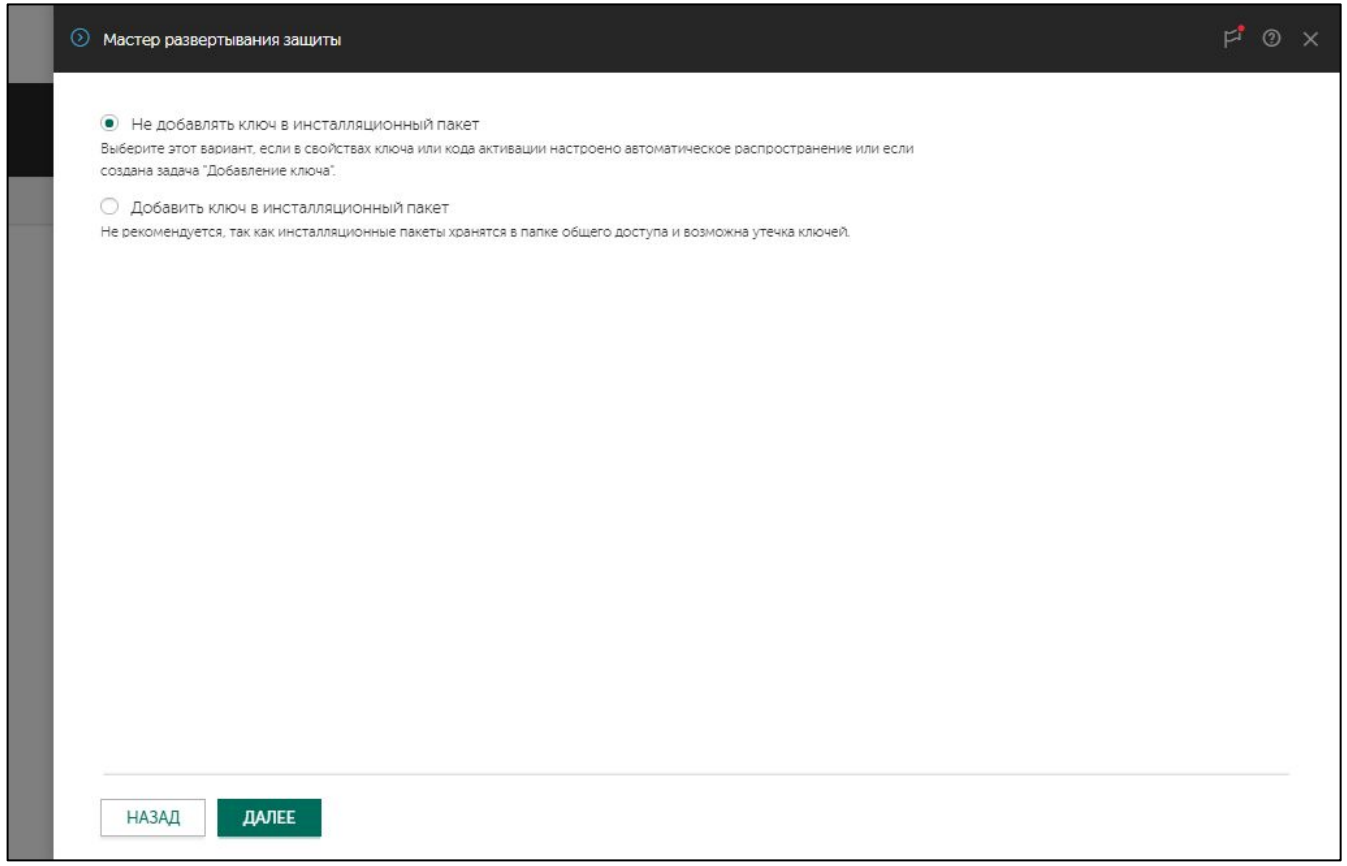
Инсталлятор Kaspersky Endpoint Security 11.1 для Windows поддерживает разные архитектуры (x86/x64) и операционные системы

Мастер удаленной установки автоматически устанавливает Агент администрирования вместе с Kaspersky Endpoint Security (а также и вместе с другими программами)

Выбор ключа

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



Активировать Kaspersky Endpoint Security можно тремя способами:

— Включить в свойствах ключа автоматическое распространение (рекомендуется)

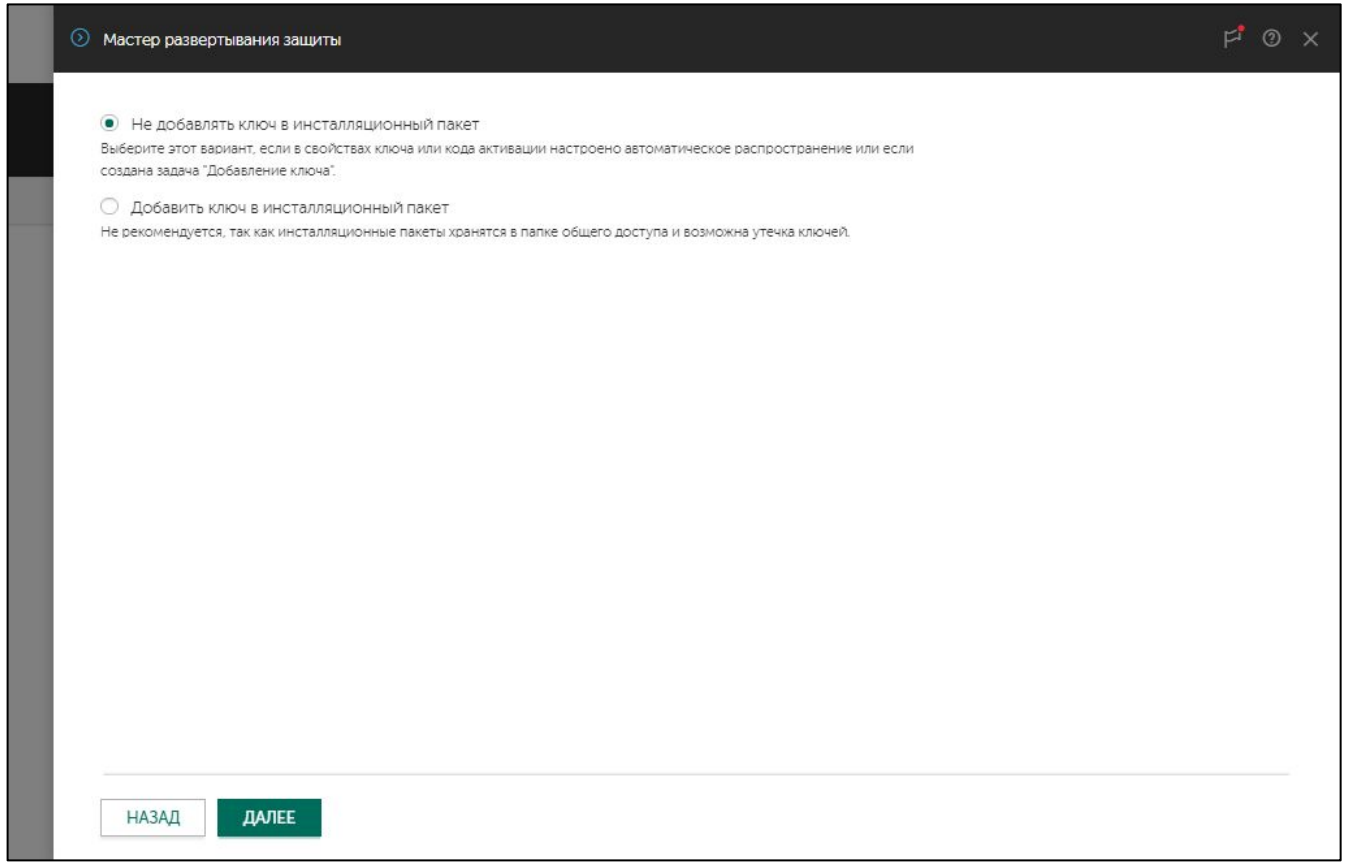
— Добавить лицензионный ключ в пакет установки

— Создать задачу установки лицензии

Выбор ключа

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



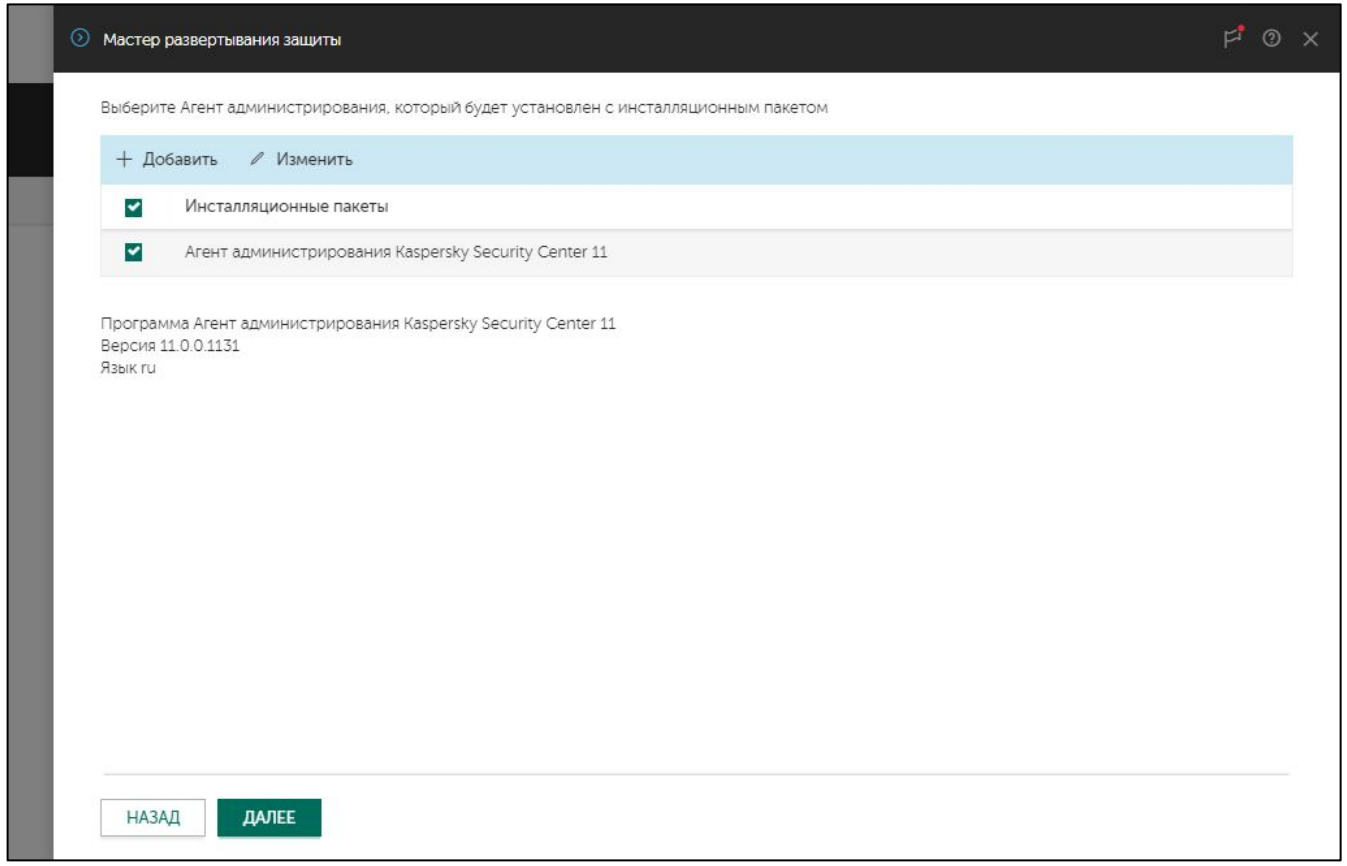
Если есть лицензия и она распространяется автоматически, выберите опцию **Не добавлять ключ…**

Если вы хотите активировать защиту сразу после установки (а не после первой синхронизации), выберите опцию **Добавить ключ…**

Выбор пакета установки Агента

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



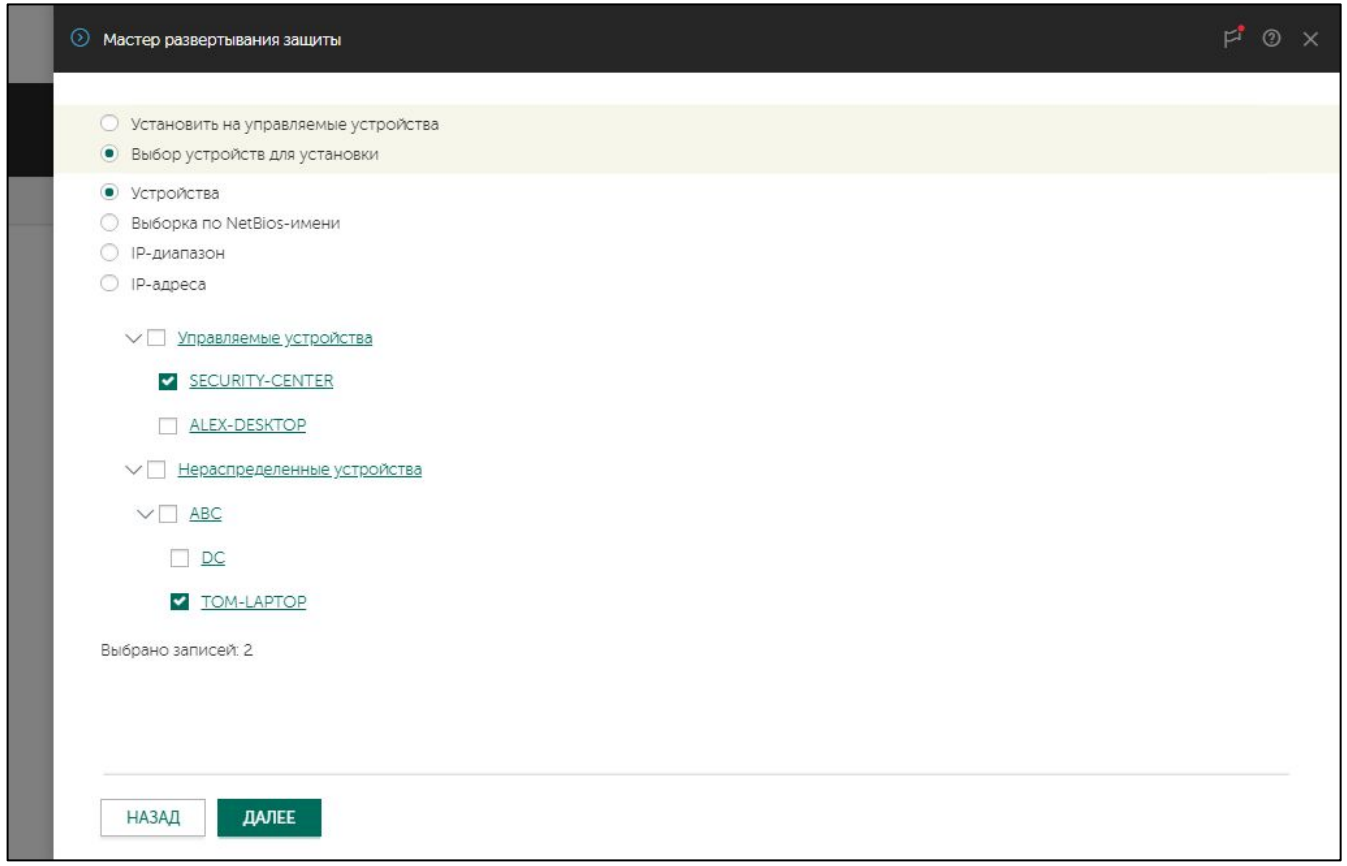
Выбор инсталляционного пакета Агента администрирования это обязательный шаг и его нельзя пропустить

Однако если Агент уже установлен, то повторно он не переустановится

Выбор компьютеров

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



Первая опция позволяет установить на компьютеры, которые уже добавлены в выбранную группу

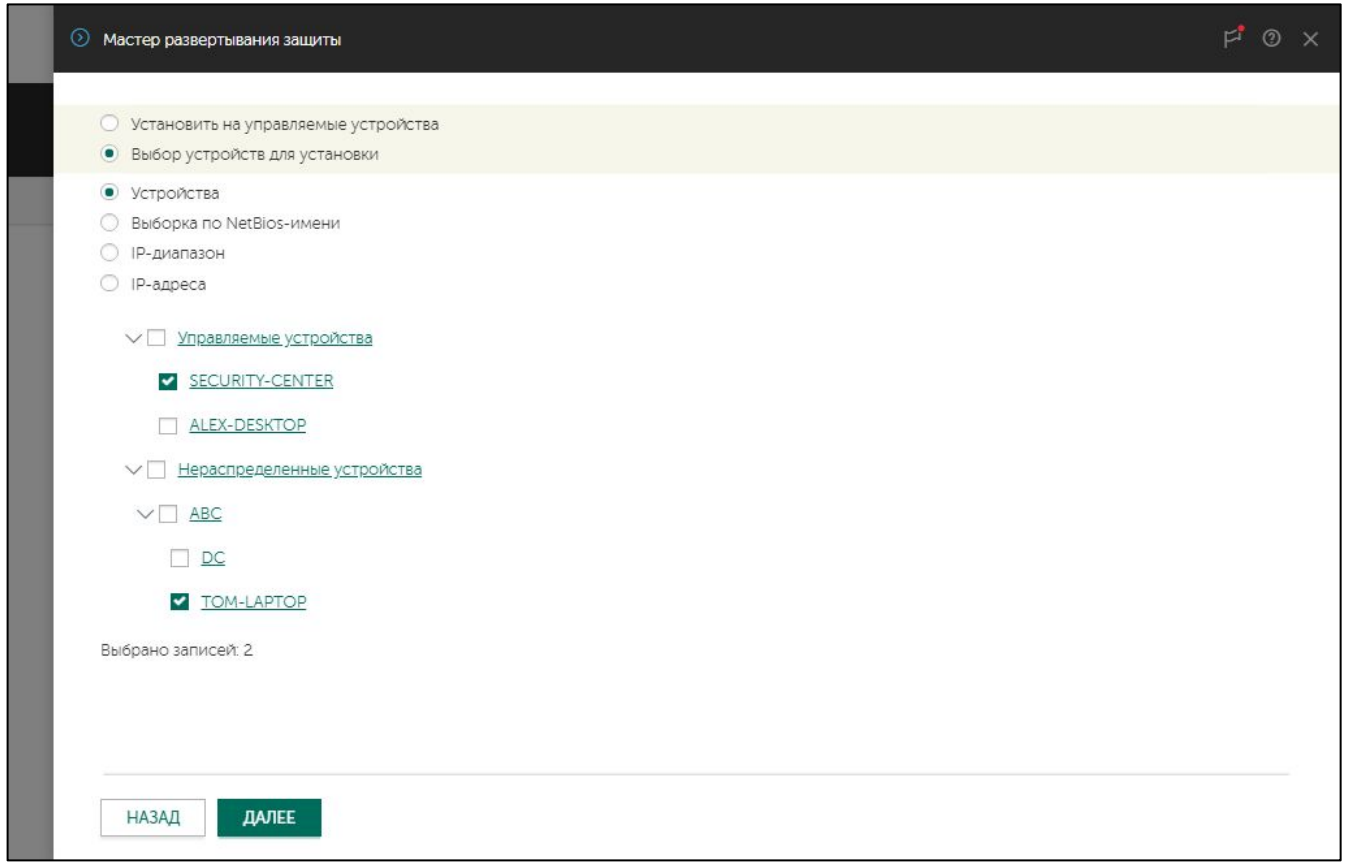
Вторая опция позволяет выбрать нераспределенные компьютеры или отдельные компьютеры из разных групп

В результате мастер создаст задачу для наборов компьютеров

Выбор компьютеров

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



Сервер администрирования автоматически обнаруживает компьютеры

Нераспределенные компьютеры структурированы по доменам и рабочим группам

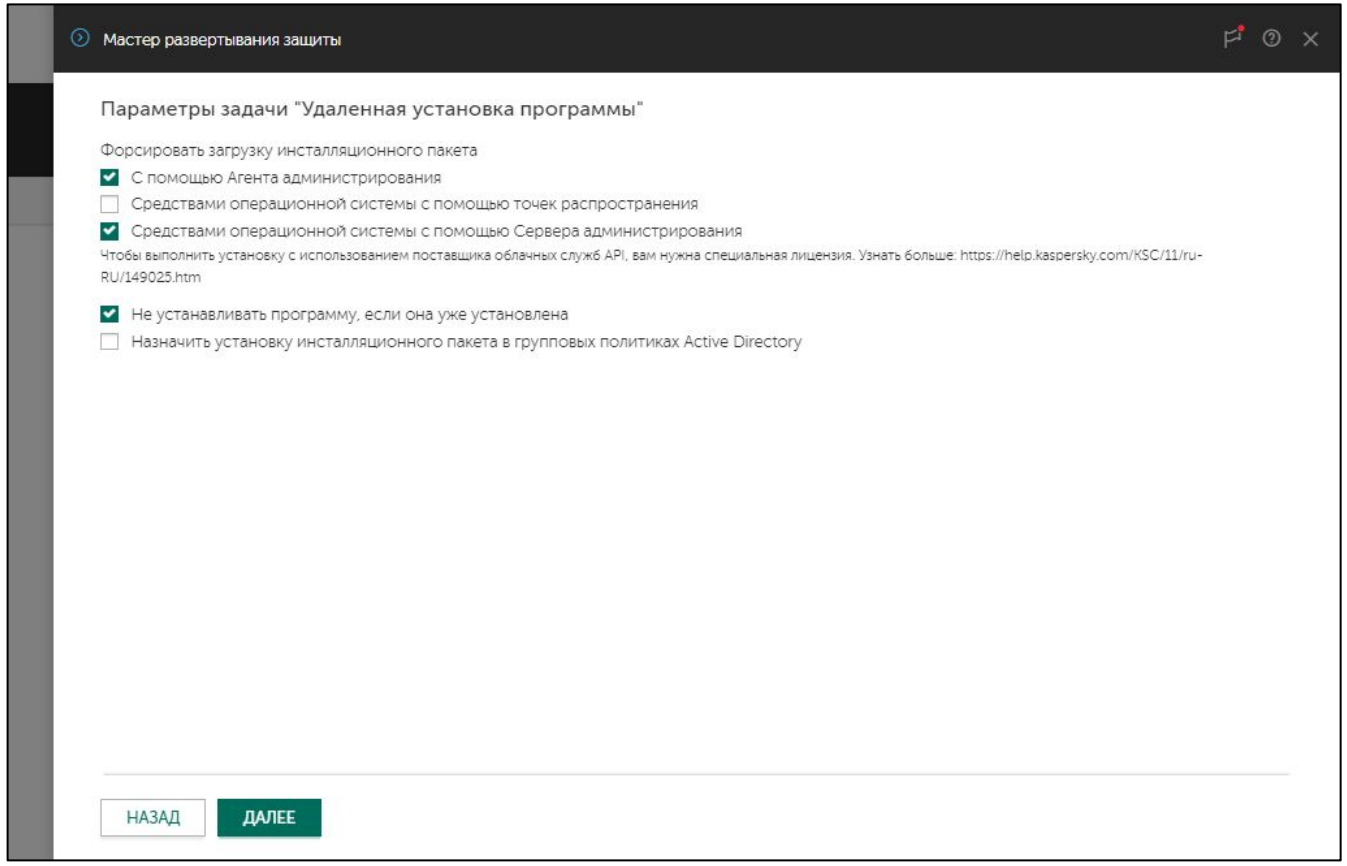
Компьютеры, которые Сервер администрирования не обнаружил, можно добавить по именам или IP-адресам

Список имен или адресов можно импортировать из файла, но только в MMC-консоли

Способ установки

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



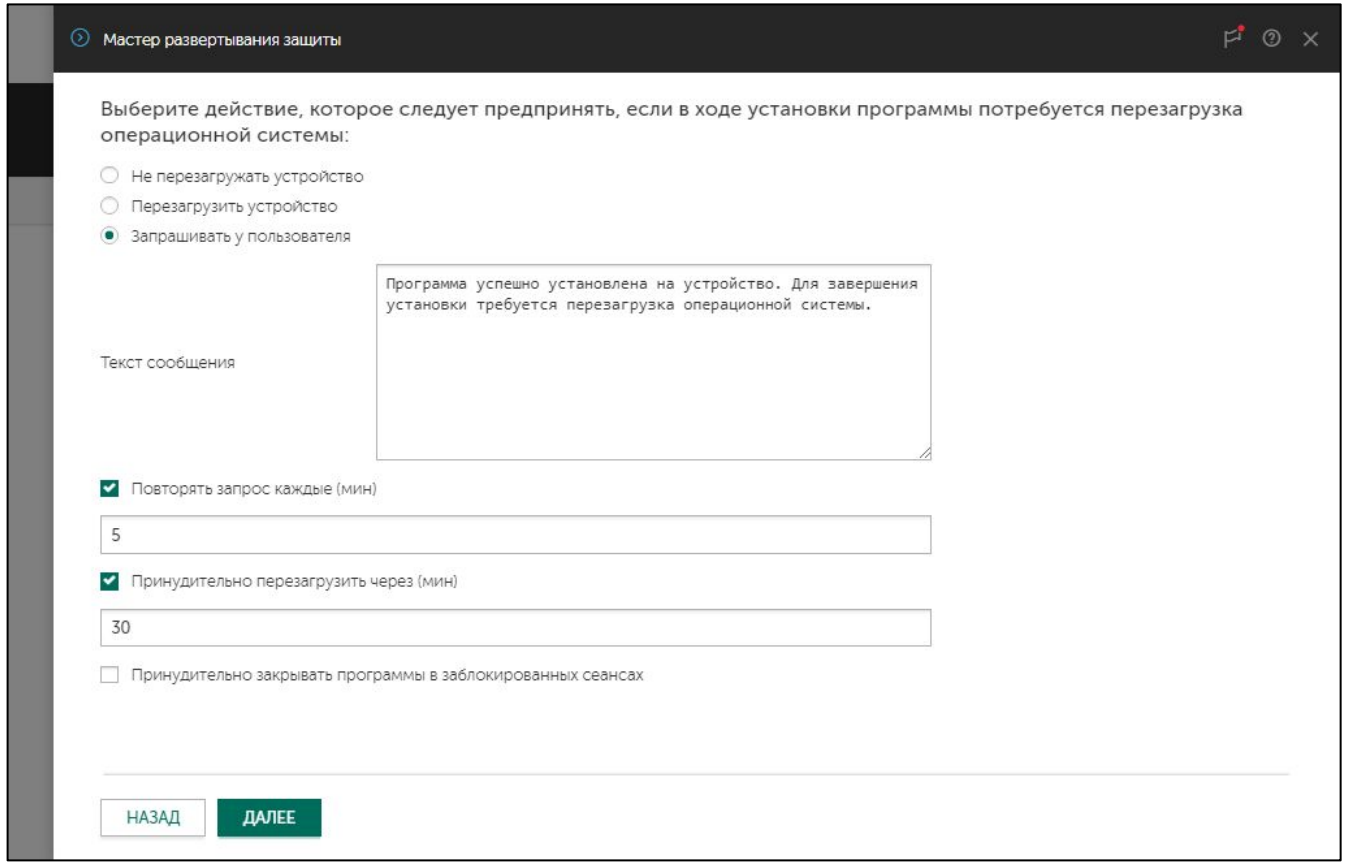
Установка по умолчанию — с помощью Агента

Если Агента нет — средствами Windows

Перезагрузка компьютера

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



При установке на незащищенный компьютер перезагрузка не требуется

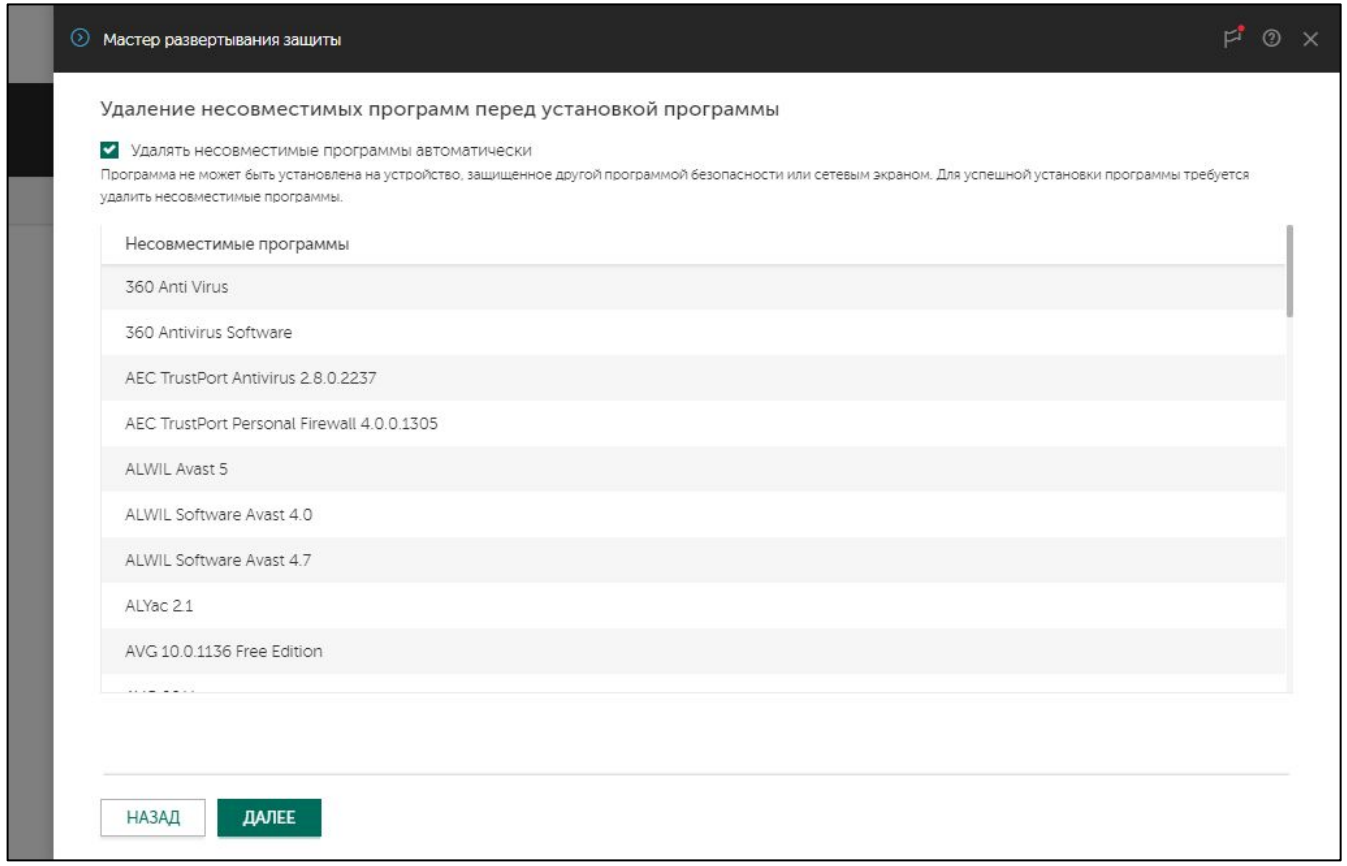
Перезагрузка может потребоваться если компьютер уже защищен Kaspersky Endpoint Security или другим средством

При установке на сервера спросить будет не у кого — лучше выбрать Не перезагружать компьютер

Удаление несовместимых программ

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



Инсталлятор Kaspersky Endpoint Security 11 для Windows автоматически обнаруживает и пытается удалить сторонние средства защиты (и при этом требует перезагрузить компьютер)

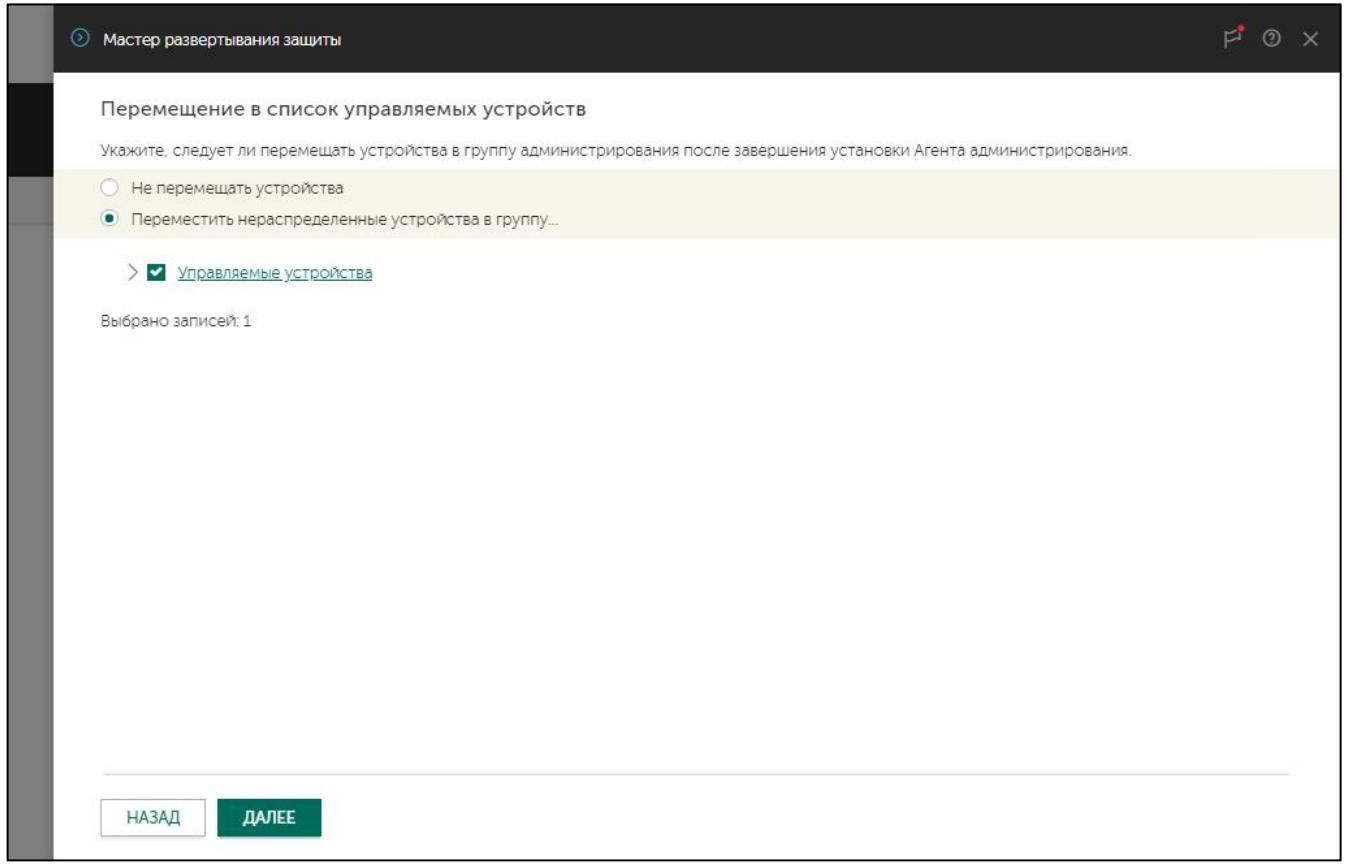
При выключенном параметре Удалять несовместимые программы автоматически, задача установки завершится с ошибкой, если обнаружит сторонние средства защиты

Обнаруживать и удалять несовместимые программы можно также с помощью Агента администрирования

Перемещение нераспределенных компьютеров

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



Если ранее вы выбрали для установки нераспределенные компьютеры, укажите в какую группу их переместить после установки

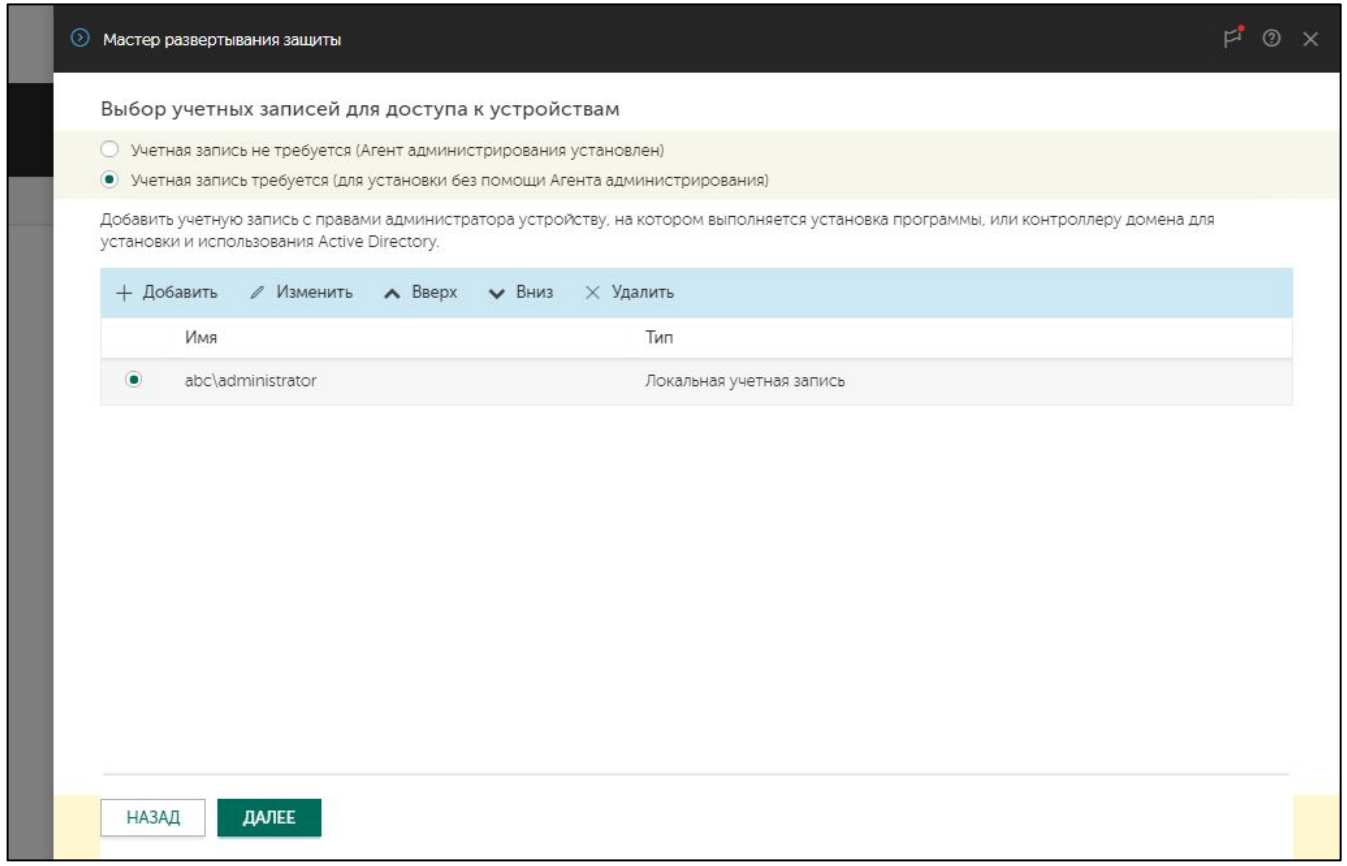
Нераспределенные компьютеры не управляются политиками и не сообщают о событиях

Сервер администрирования переместит компьютеры после того как Агенты администрирования выйдут на связь, независимо от результата установки Kaspersky Endpoint Security

Выбор учетной записи

Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



Добавьте учетную запись с правами администратора на выбранных компьютерах

Если у разных компьютеров разные администраторы, добавьте несколько записей

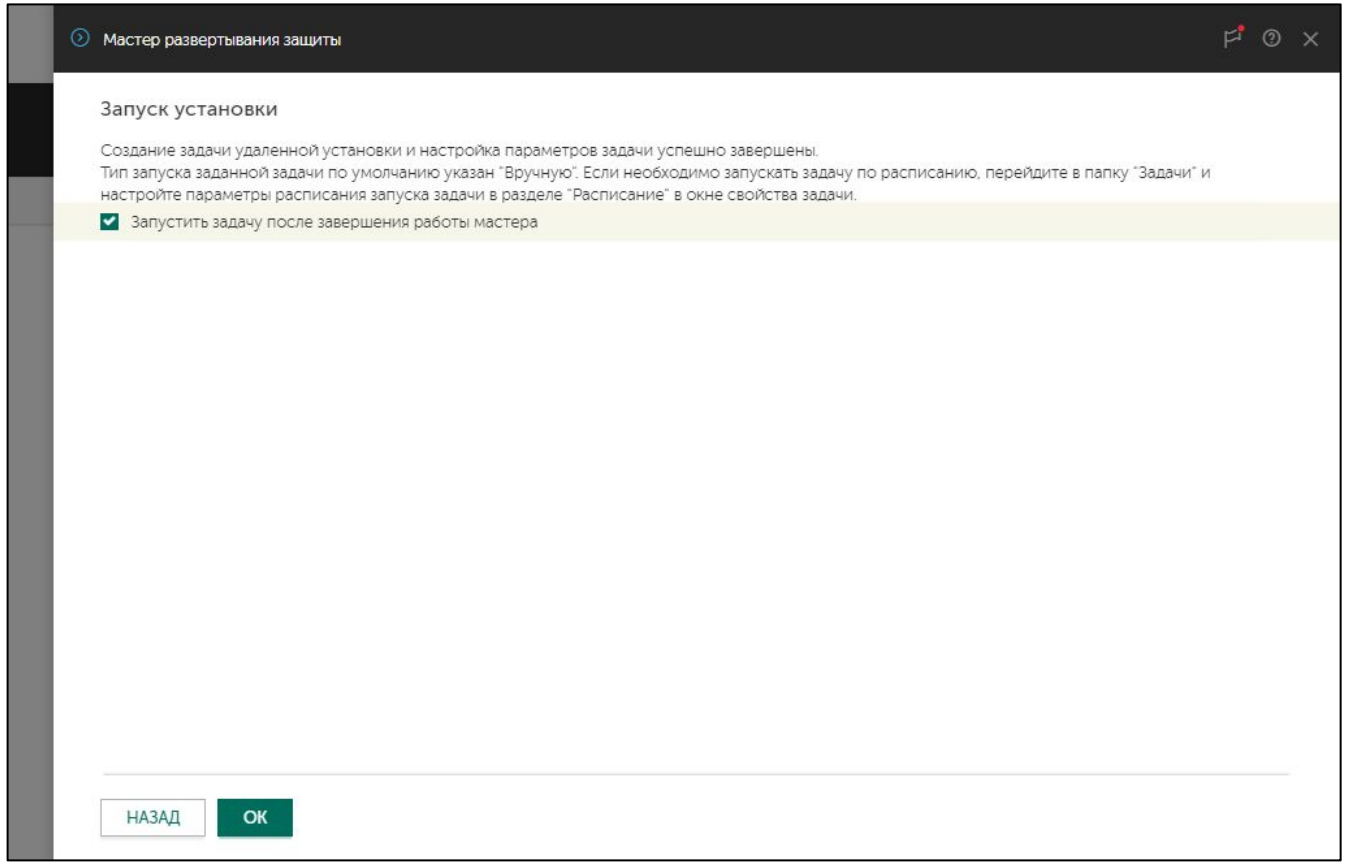
Перед тем, как пробовать учетные записи из списка, задача пытается выполнить установку от имени учетной записи службы Сервера администрирования

Учетная запись **KL-AK-*** не имеет прав на удаленных компьютерах и не годится для удаленной установки

Завершение мастера

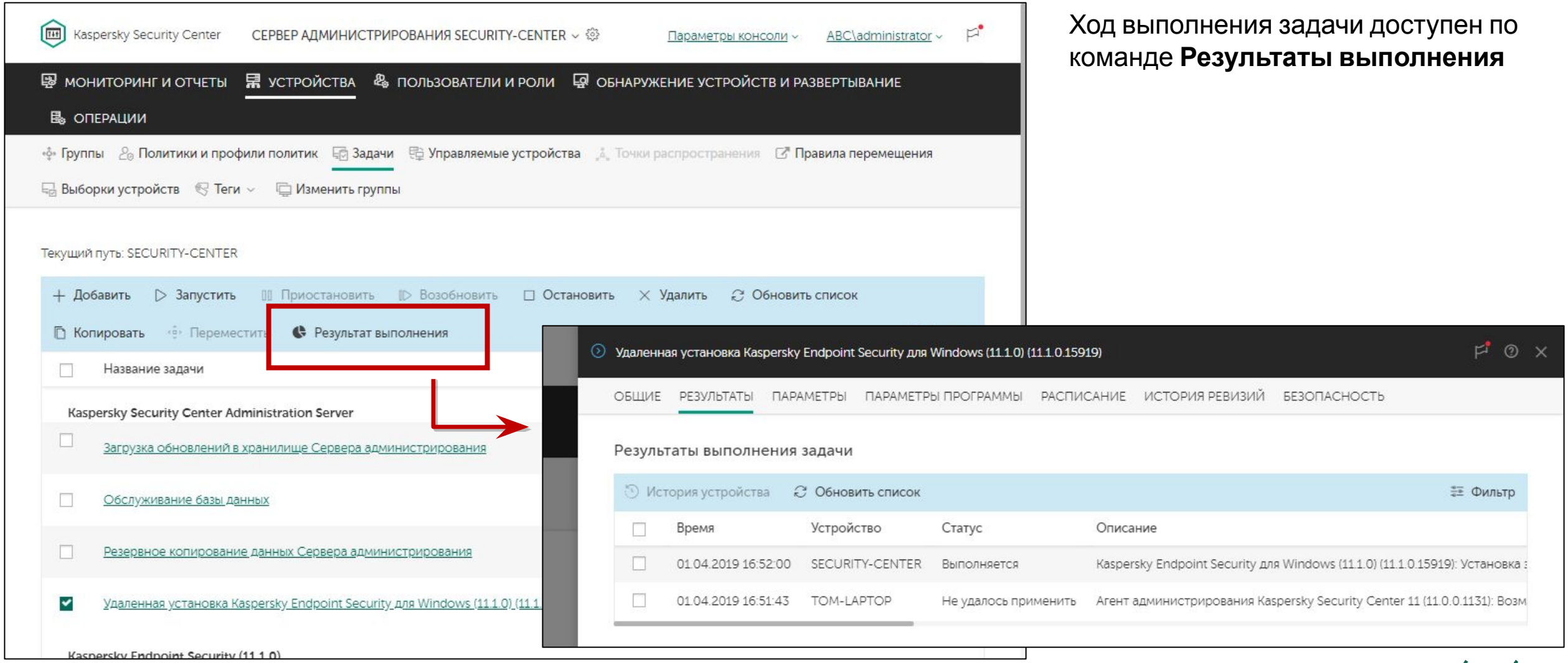
Мастер удаленной установки:

1. Выберите программу (Kaspersky Endpoint Security)
2. Выберите лицензию
3. Выберите инсталляционный пакет Агента
4. Выберите компьютеры
5. Выберите, как устанавливать
6. Укажите, как перезагружать компьютеры
7. Соглашайтесь удалять несовместимые программы
8. Выберите группу, в которую попадут компьютеры
9. Добавьте учетные записи с правами администратора на выбранных компьютерах
10. Завершите мастер



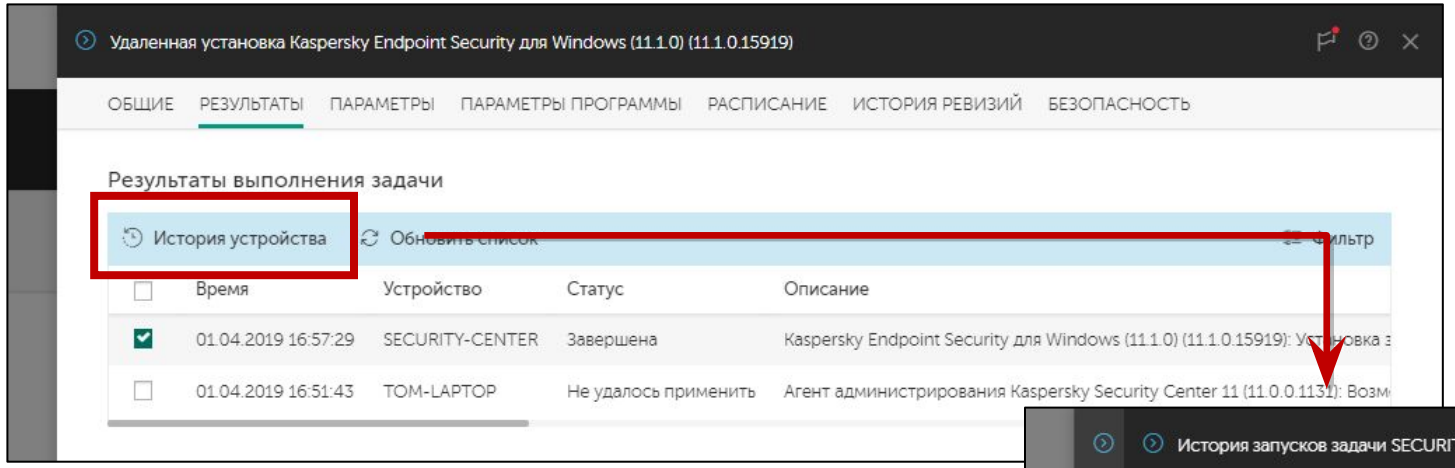
Мастер создает задачу удаленной установки и по желанию может сразу же ее запустить

Задача установки



Ход выполнения задачи доступен по команде **Результаты выполнения**

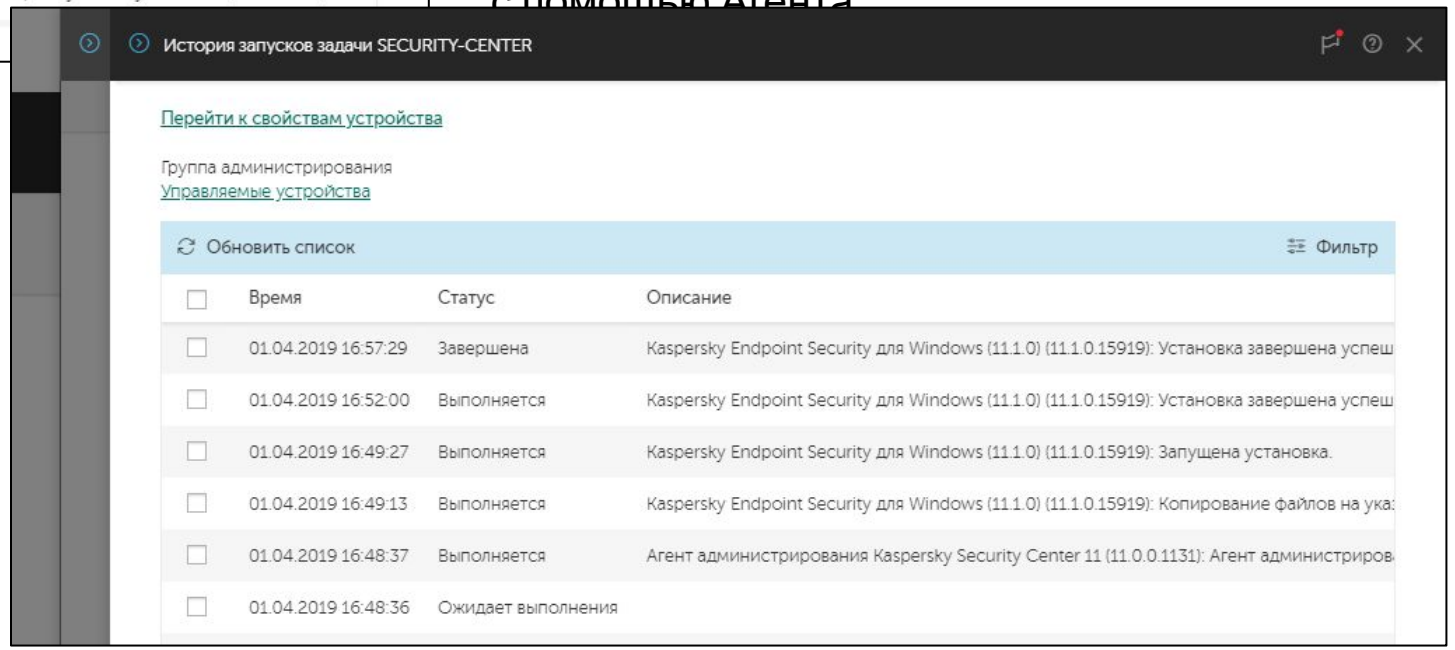
Ход установки



Чтобы посмотреть ход выполнения на каждом отдельном компьютере есть команда **История устройства**

Сначала Агент устанавливается средствами Windows

Затем Kaspersky Endpoint Security устанавливается с помощью Агента



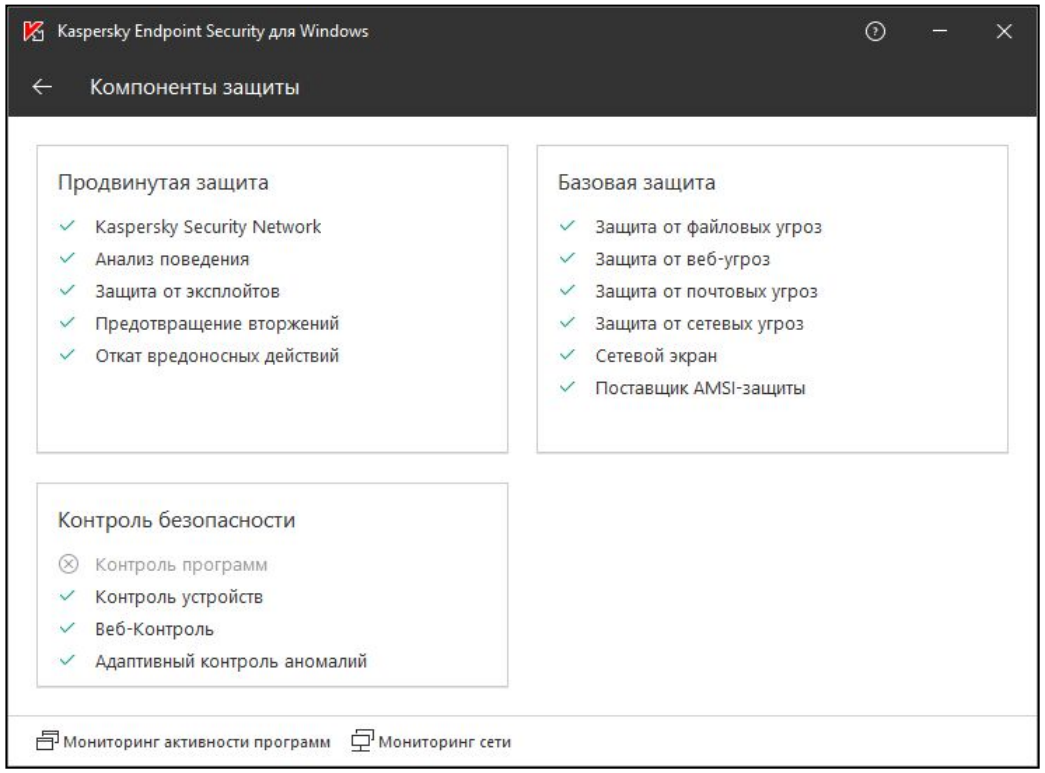
Журналы установки в *Windows\Temp*:

- *$klnagent-< дата и время >.log*
- *$klnagent-setup-< дата и время >.log*
- *kl-install-<дата и время>.log*
- *kl-setup-<дата и время>.log*
- *ucaevents.log*

Подробности в курсе KL 016.03 Troubleshooting

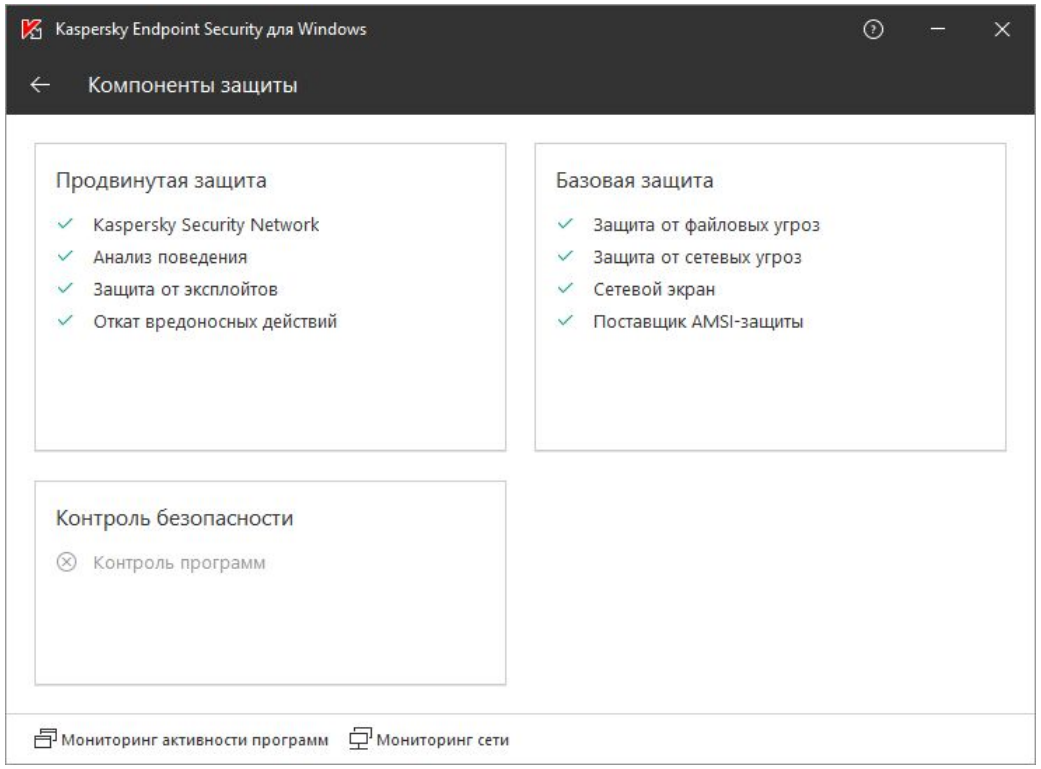
Результаты установки

Рабочие станции



По умолчанию мастер устанавливает стандартный набор компонентов: компоненты расширенной и базовой защиты, а также компоненты контроля

Серверы



На серверных операционных системах не устанавливаются:

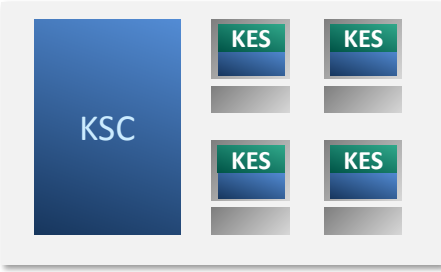
—Защита от почтовых угроз
—Защита от веб-угроз
—Предотвращение вторжений

—Веб-Контроль

Лабораторная работа №2

Внедрение Kaspersky Endpoint Security

1. Установите Kaspersky Endpoint Security 11.1 для Windows на рабочую станцию и Сервер администрирования
2. Создайте автономный пакет установки Kaspersky Endpoint Security
3. Установите автономный пакет Kaspersky Endpoint Security 11.1 для Windows на ноутбук
4. Изучите результаты установки



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

- Требования к клиентским компьютерам
- Как изменить состав компонентов KES
- Как создать новый пакет установки
- Как создать пакет KSWS
- Какие есть методы установки
- Как удаленно установить агент и KES
- **Как проще установить агент и KES локально**
- Как установить агент через Active Directory
- Как удалить несовместимые программы

Часть II. Управление защитой

Часть III. Контроль

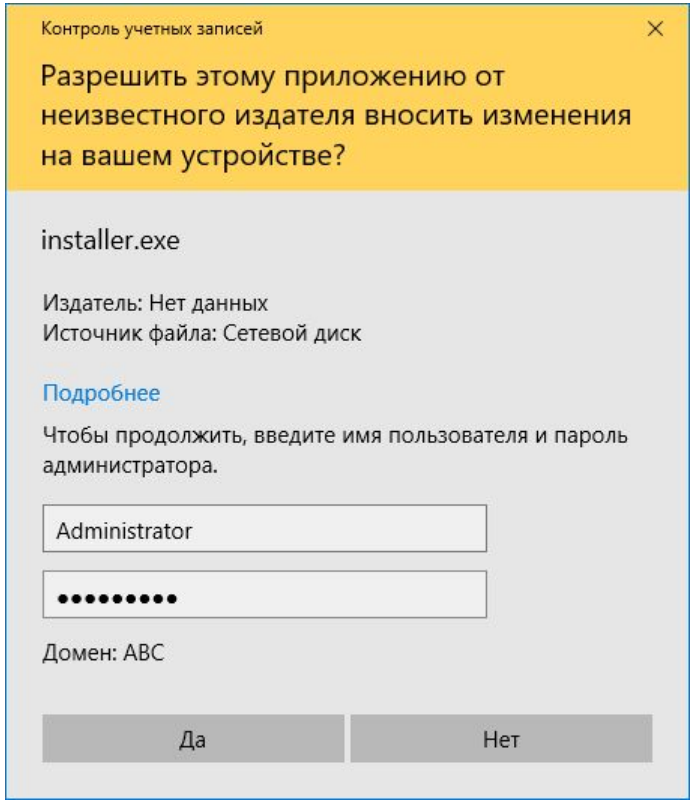
Часть IV. Сопровождение

Автономный пакет

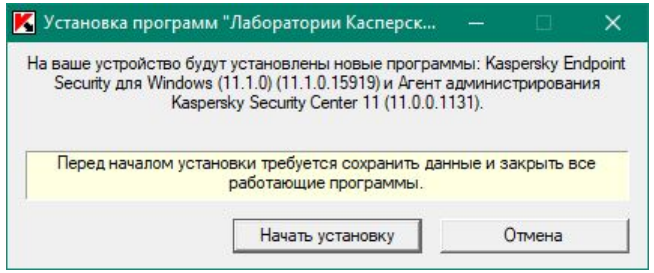
1 файл
installer.exe

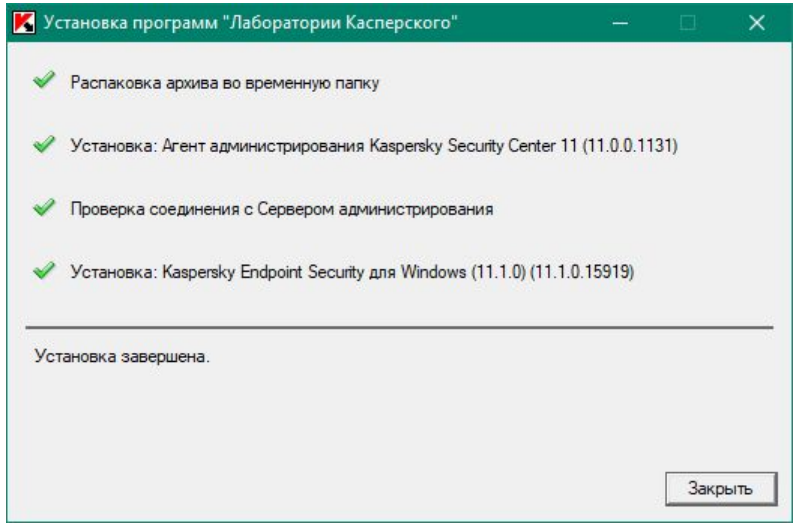
Содержит:

- Инсталляционные файлы Kaspersky Endpoint Security для Windows
- Параметры установки Kaspersky Endpoint Security для Windows
- Инсталляционные файлы Агента администрирования (опционально)
- Параметры подключения Агента к Серверу



Предназначен для локальной установки с правами администратора

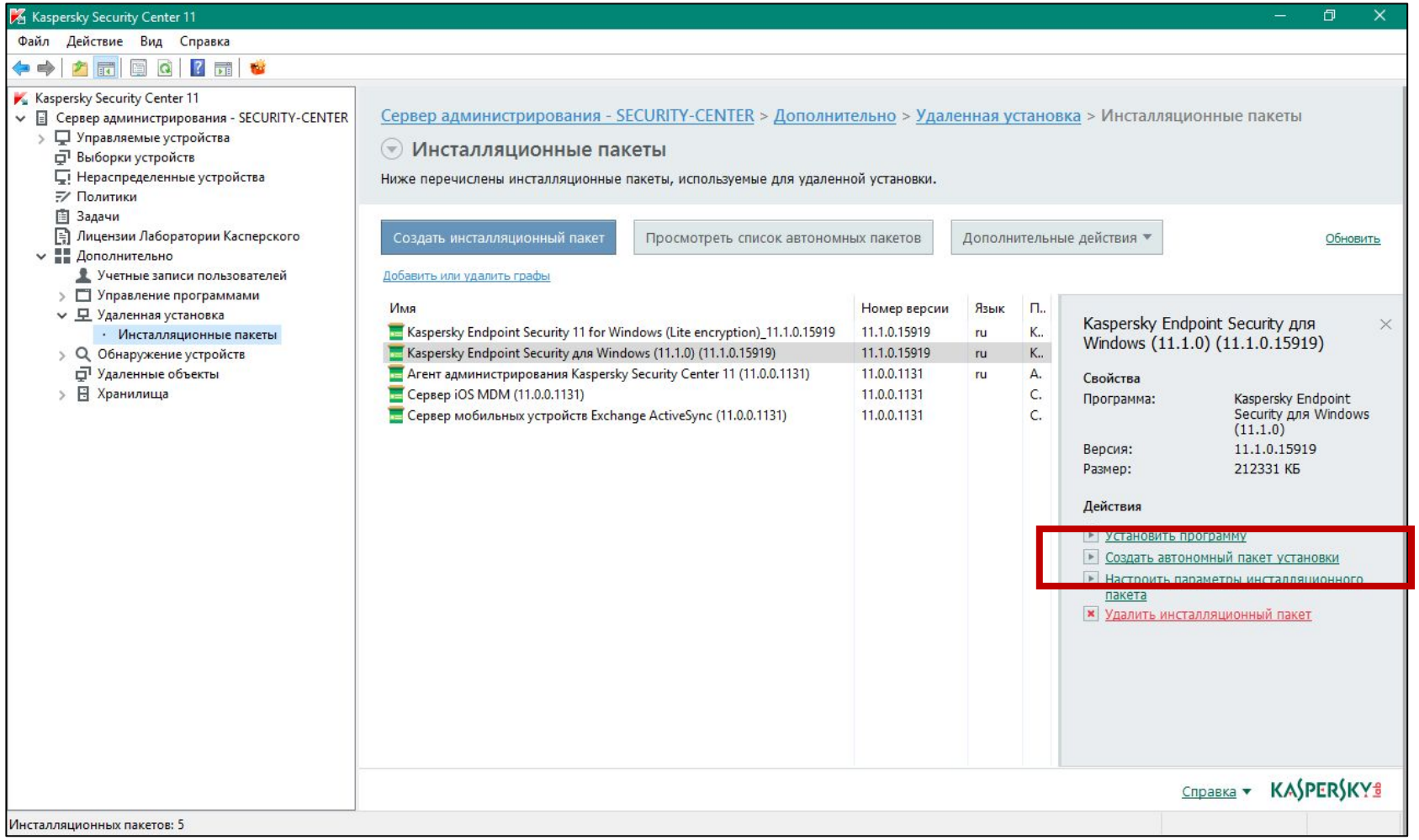




Не задает вопросов и не требует принимать решения

Чтобы выполнить установку вообще без окон, запускайте **installer.exe** с параметром **/s**

Создание автономного пакета



Автономные пакеты можно создавать только из MMC-консоли

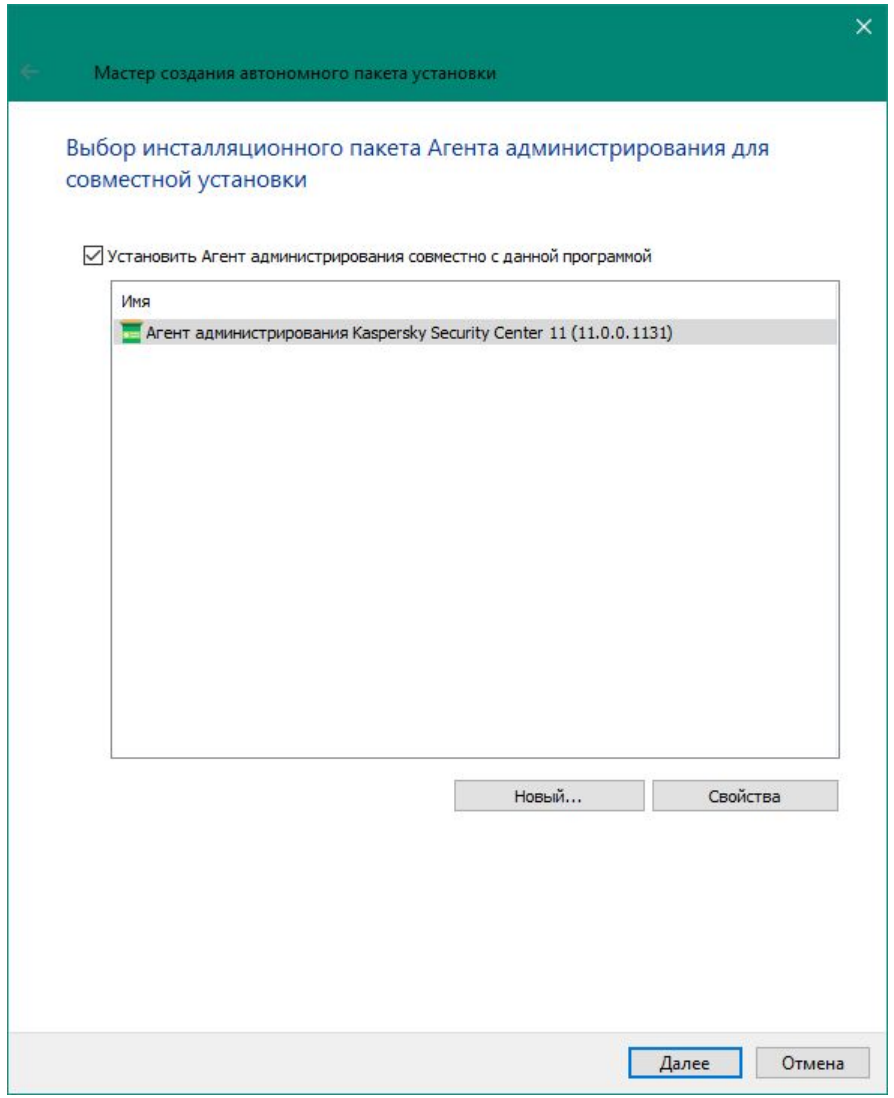
Автономные пакеты создаются из обычных

Параметры установки нужно предварительно задать в свойствах обычного пакета

Добавление Агента администрирования

Автономный пакет:

1. Добавьте Агент администрирования
2. Укажите, в какую группу поместить компьютеры
3. Скопируйте пакет на внешний диск или отправьте по почте

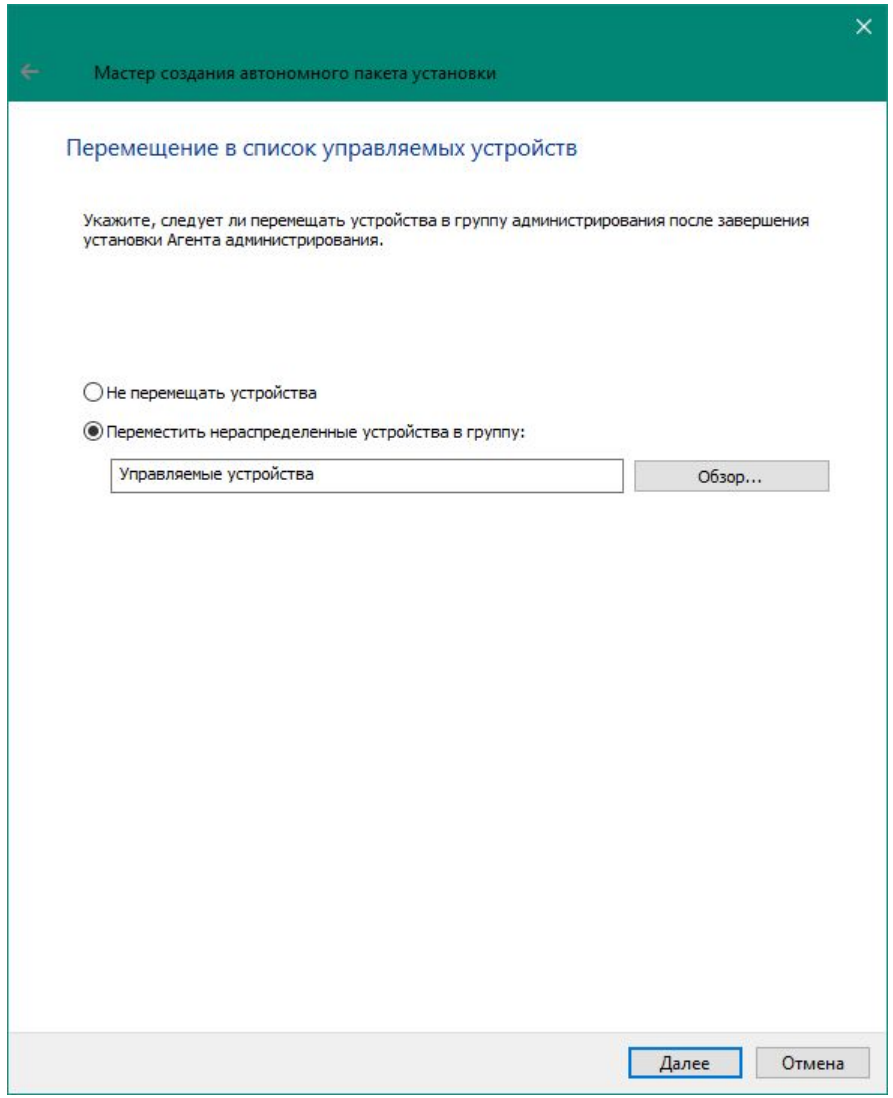


По умолчанию мастер создания автономного пакета Kaspersky Endpoint Security предлагает включить в него установку Агента администрирования

Перемещение компьютеров в группы

Автономный пакет:

1. Добавьте Агент администрирования
2. Укажите, в какую группу поместить компьютеры
3. Скопируйте пакет на внешний диск или отправьте по почте



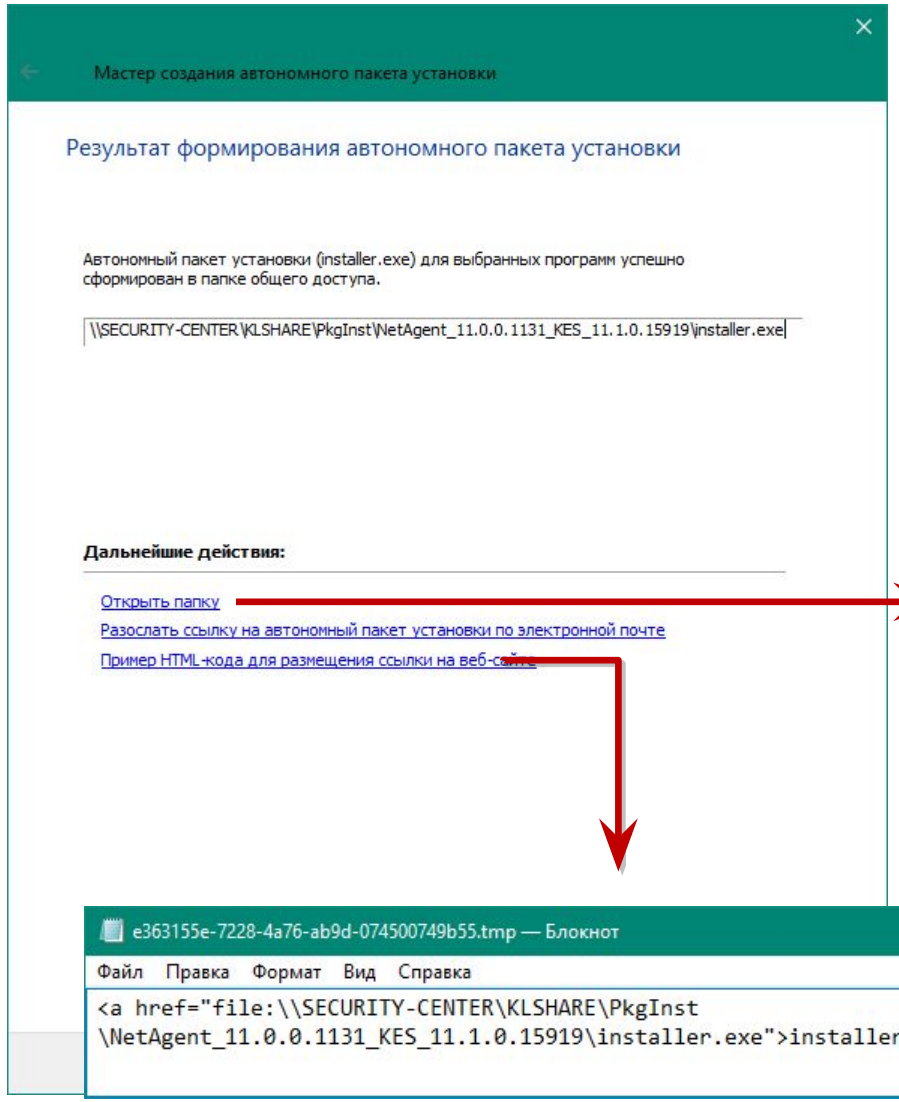
Если вы добавили в пакет установку Агента администрирования, выберите, в какую группу переместить компьютеры после установки Агента

Перемещение выполняется после установки Агента администрирования, даже если установка Kaspersky Endpoint Security завершается с ошибкой

Завершение создания автономного пакета

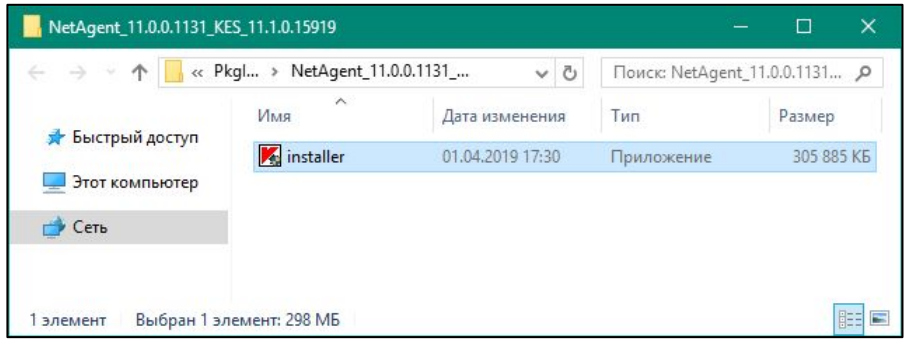
Автономный пакет:

1. Добавьте Агент администрирования
2. Укажите, в какую группу поместить компьютеры
3. Скопируйте пакет на внешний диск или отправьте по почте



Пакет доступен в общей папке Сервера администрирования *<адрес сервера>*\KLSHARE\PkgInst*<имя пакета>*\installer.exe

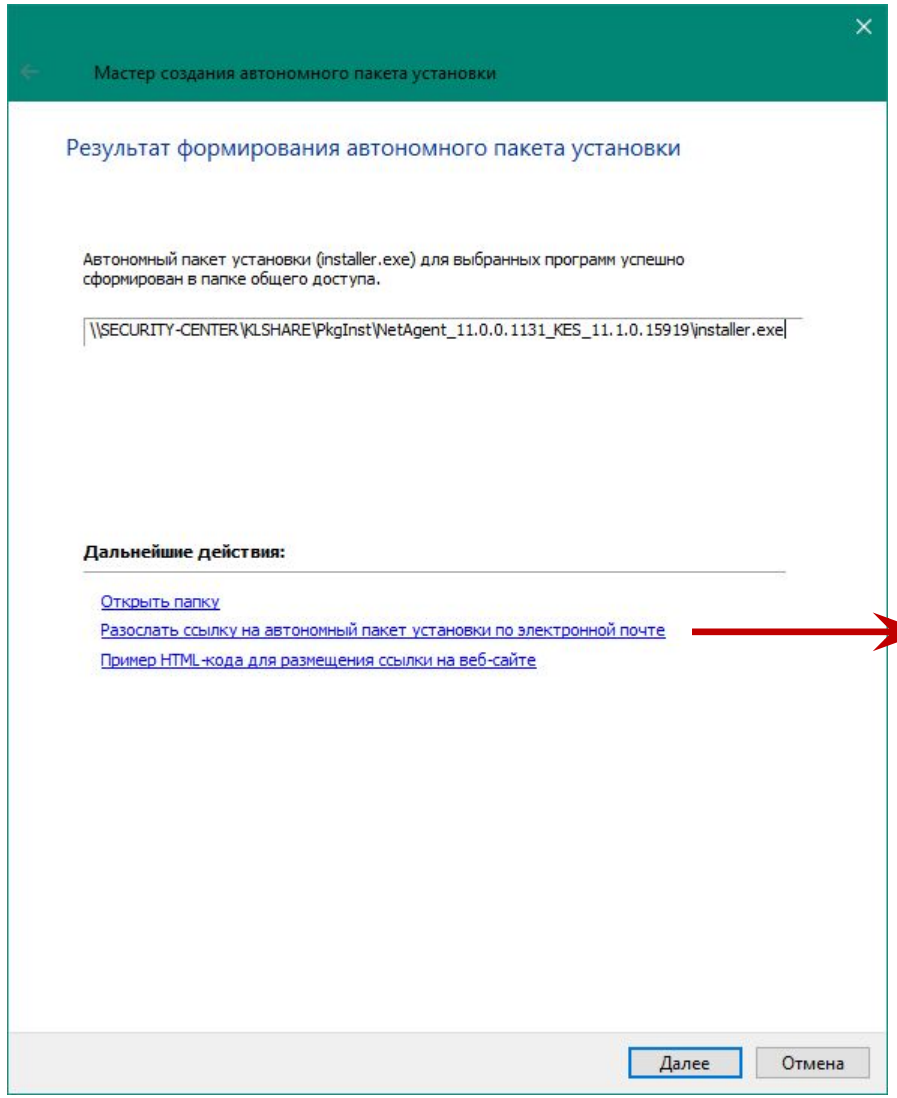
Имя пакета состоит из имен и версий программ, которые он устанавливает, например, *NetAgent_11.0.0.1131_KES_11.1.0.15919*



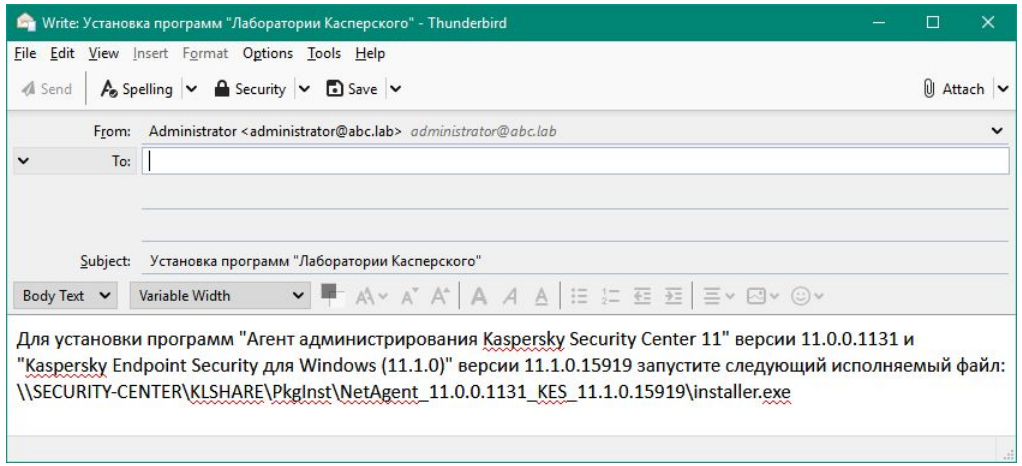
Завершение создания автономного пакета

Автономный пакет:

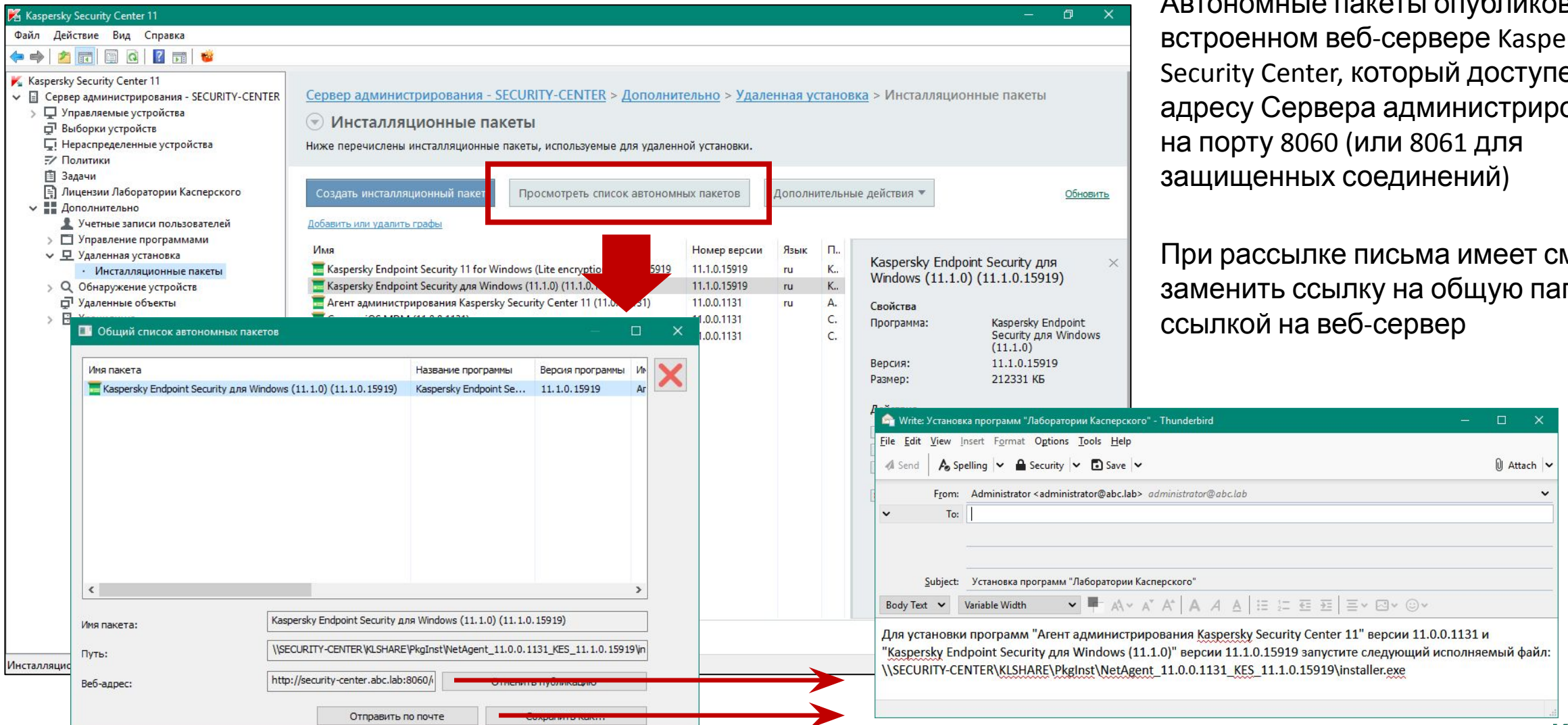
1. Добавьте Агент администрирования
2. Укажите, в какую группу поместить компьютеры
3. Скопируйте пакет на внешний диск или отправьте по почте



Команда ***Разослать ссылку…*** открывает почтовый клиент по умолчанию с готовым текстом письма и ссылкой на пакет в общей папке Сервера администрирования

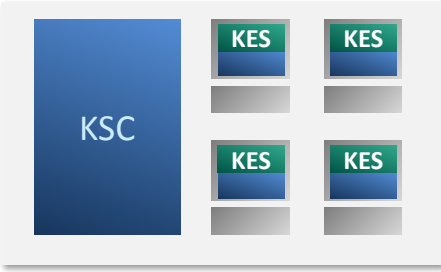


Список имеющихся автономных пакетов



Автономные пакеты опубликованы на встроенном веб-сервере Kaspersky Security Center, который доступен по адресу Сервера администрирования на порту 8060 (или 8061 для защищенных соединений)

При рассылке письма имеет смысл заменить ссылку на общую папку ссылкой на веб-сервер



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

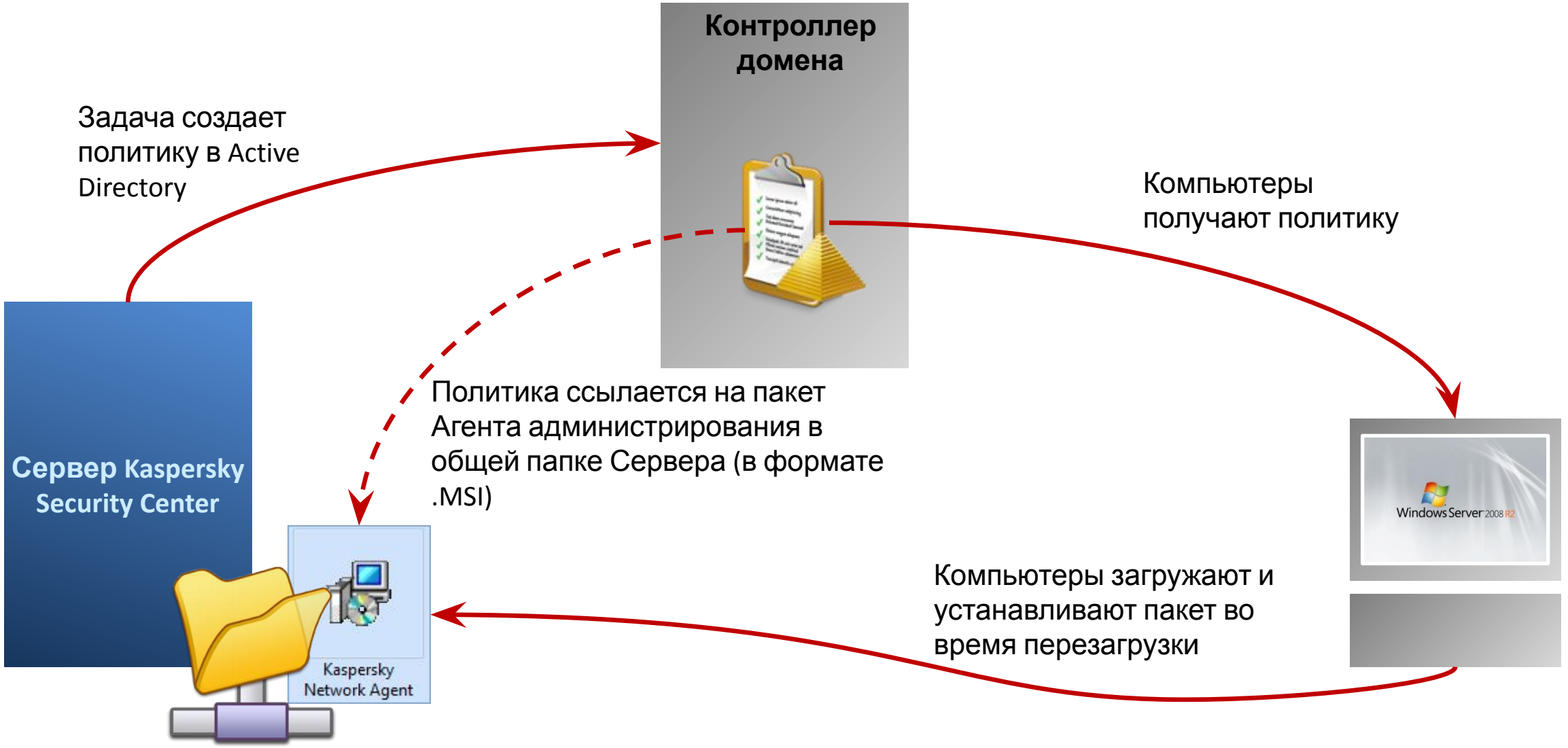
- Требования к клиентским компьютерам
- Как изменить состав компонентов KES
- Как создать новый пакет установки
- Как создать пакет KSWS
- Какие есть методы установки
- Как удаленно установить агент и KES
- Как проще установить агент и KES локально
- **Как установить агент через Active Directory**
- Как удалить несовместимые программы

Часть II. Управление защитой

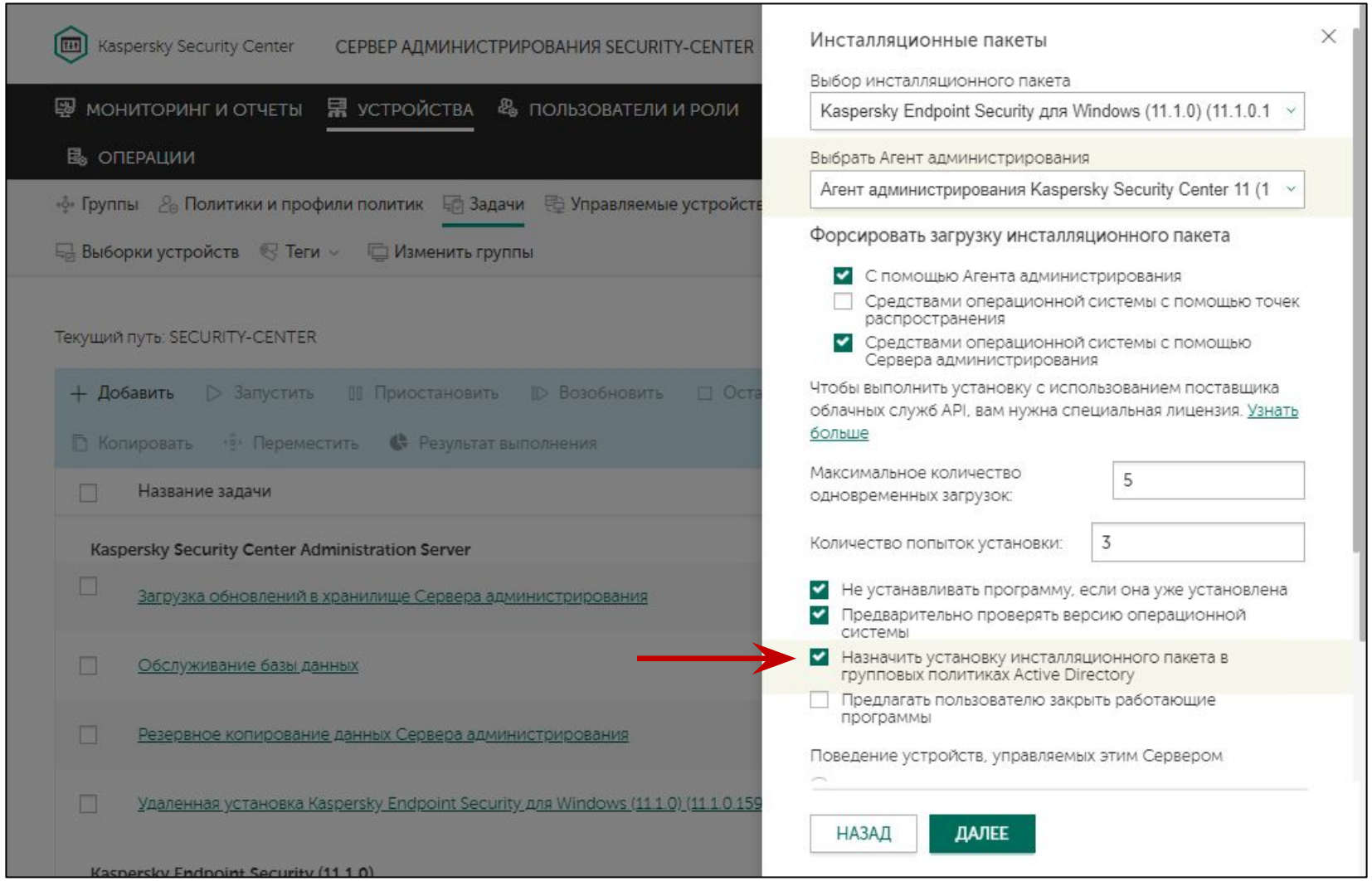
Часть III. Контроль

Часть IV. Сопровождение

Установка с помощью групповых политик



Установка с помощью групповых политик



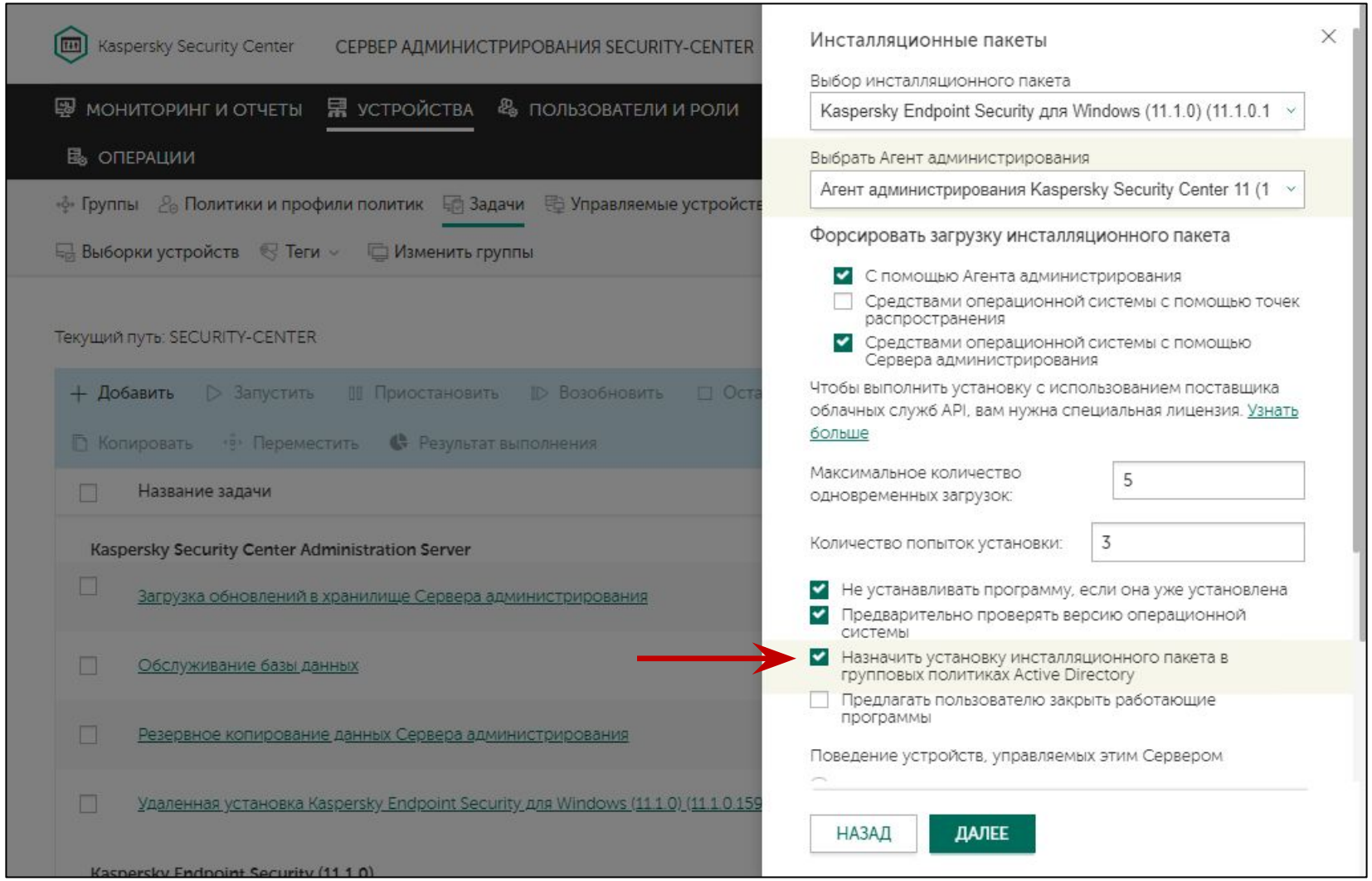
Kaspersky Security Center поддерживает публикацию в Active Directory только пакетов Агента администрирования

Другие пакеты (например, Kaspersky Endpoint Security 11) администратор может опубликовать вручную

Если задача вместе с Агентом администрирования устанавливает еще один пакет, то:

- Сначала Агент устанавливается средствами AD
- Затем Агент администрирования устанавливает второй пакет из задачи

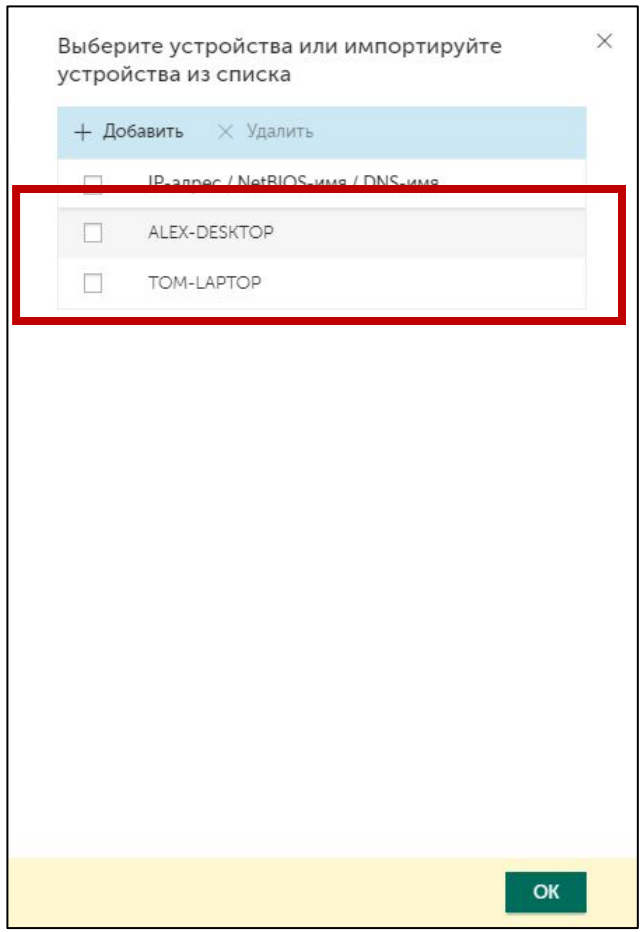
Установка с помощью групповых политик



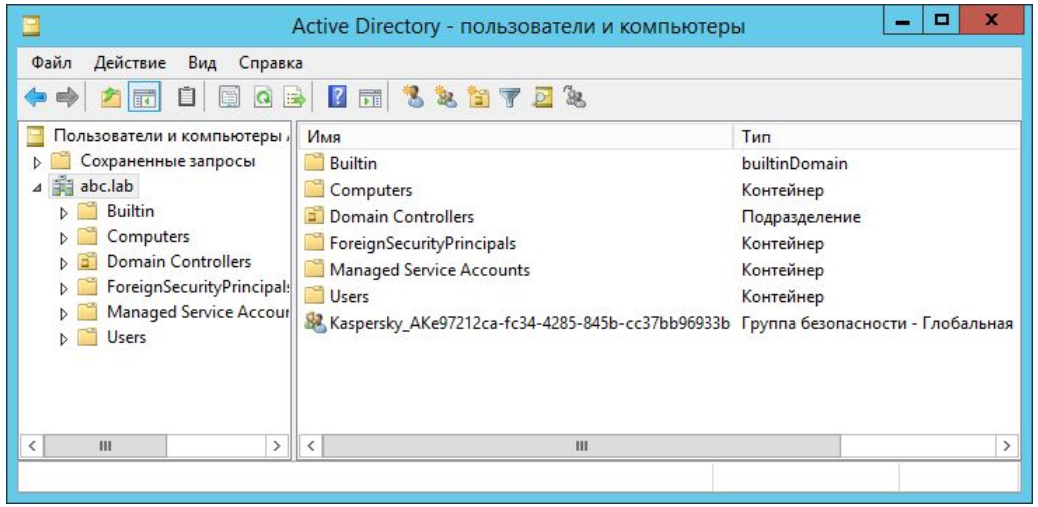
Установка с помощью групповых политик AD выполняется во время перезагрузки

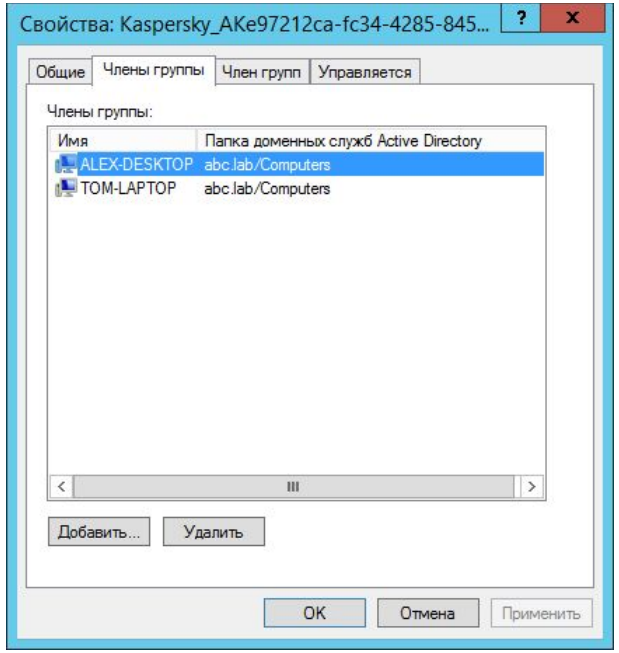
Чтобы задача внесла изменения в Active Directory, добавьте пользователя с правами администратора домена в раздел **Учетная запись**

Целевые компьютеры в Active Directory

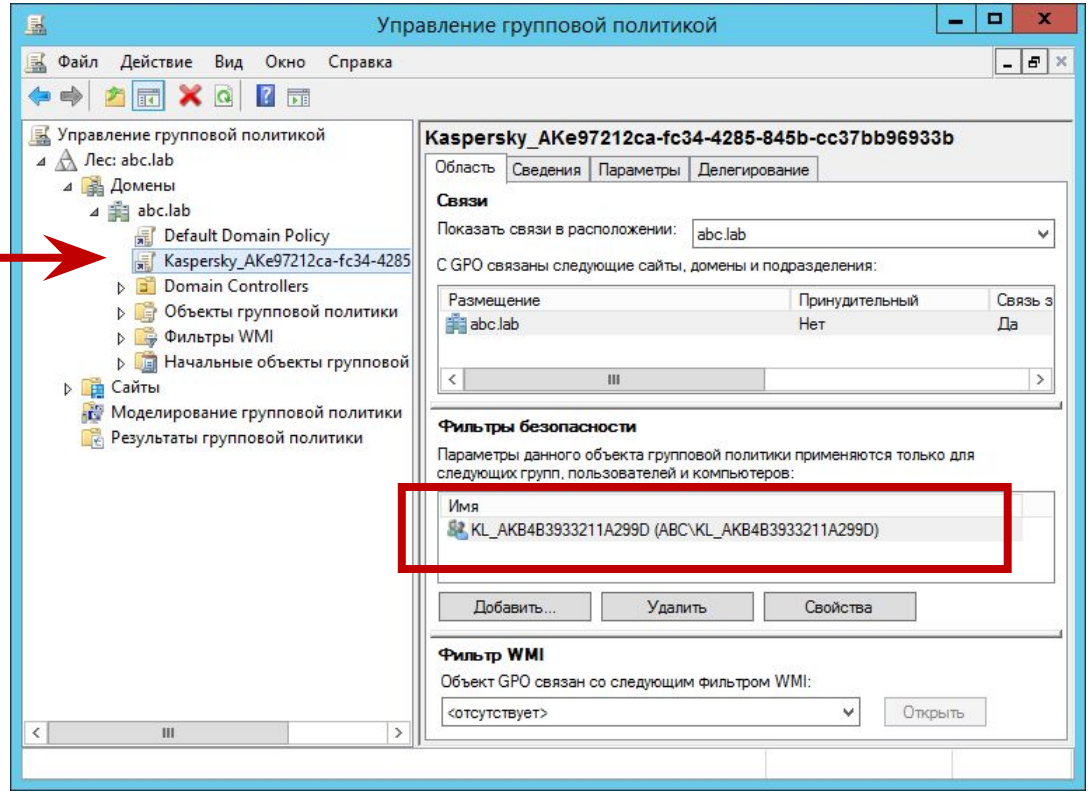


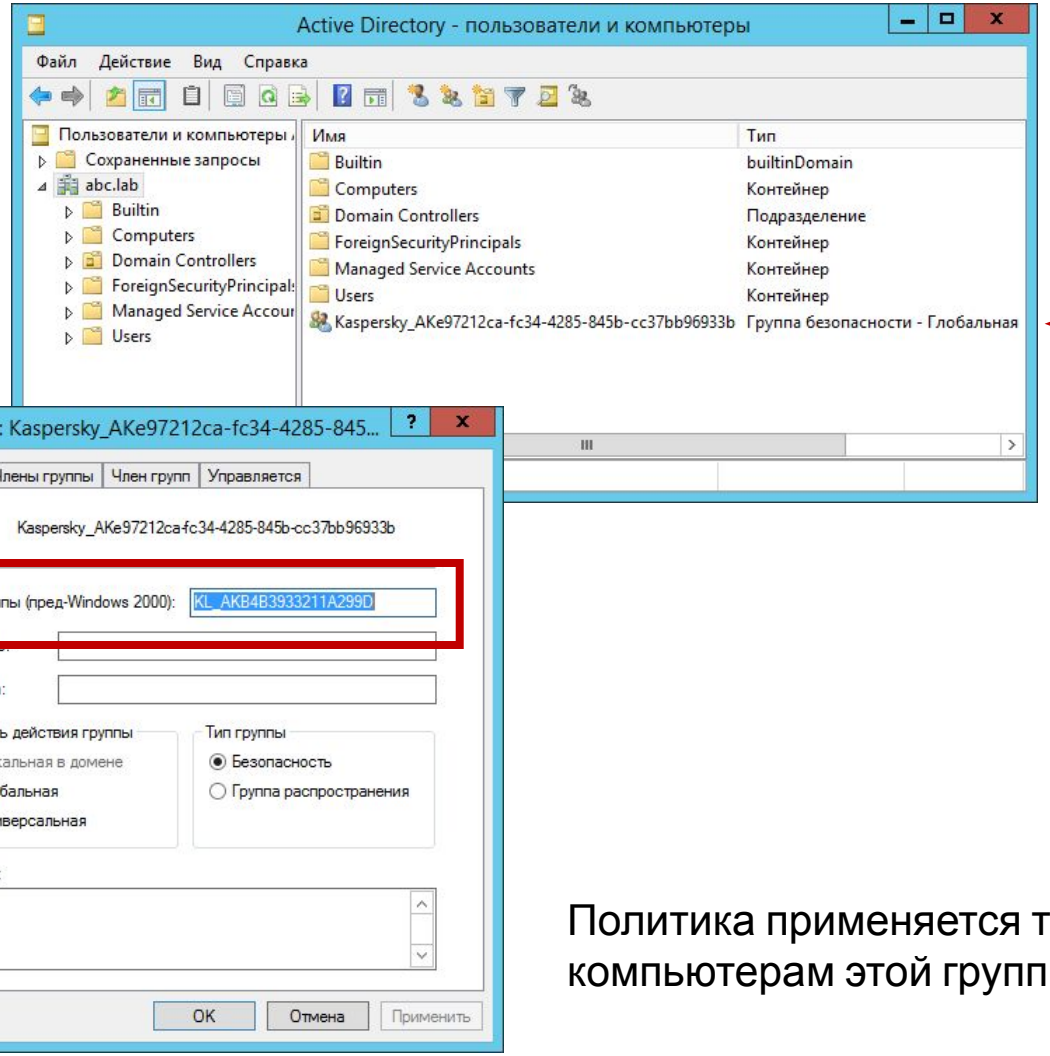
Задача создает в Active Directory новую группу с именем ***Kaspersky_AK{GUID}*** и добавляет в нее учетные записи целевых компьютеров





Целевые компьютеры в Active Directory

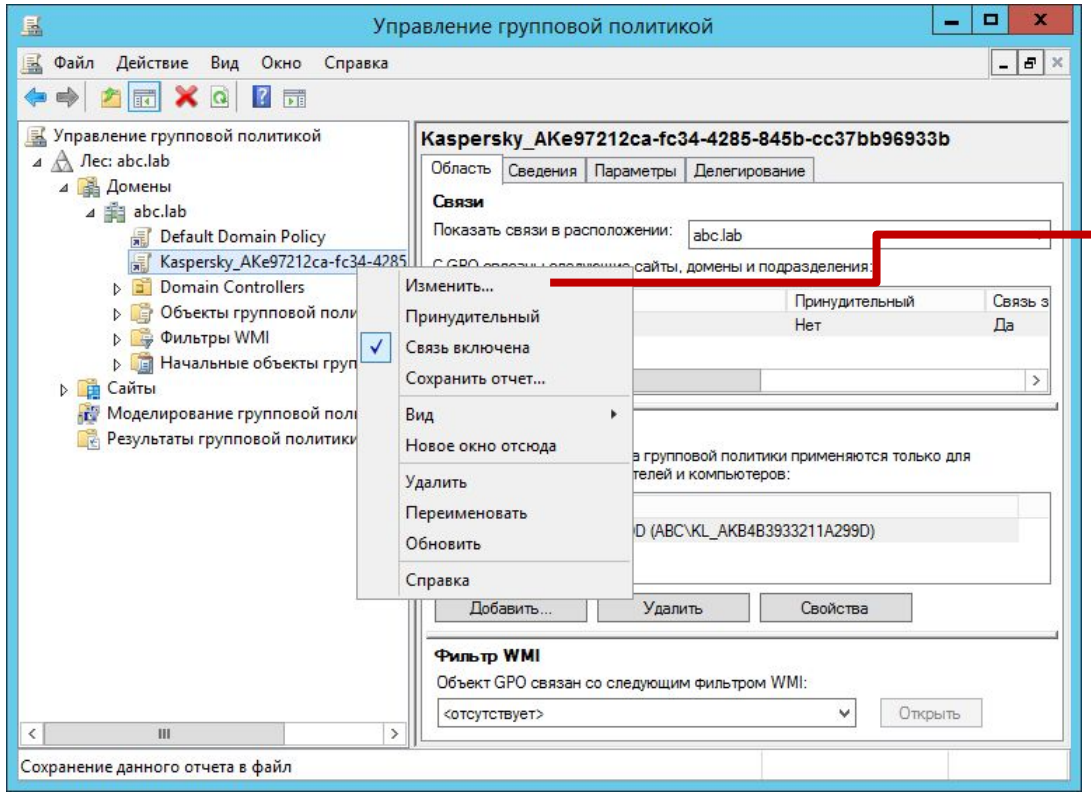


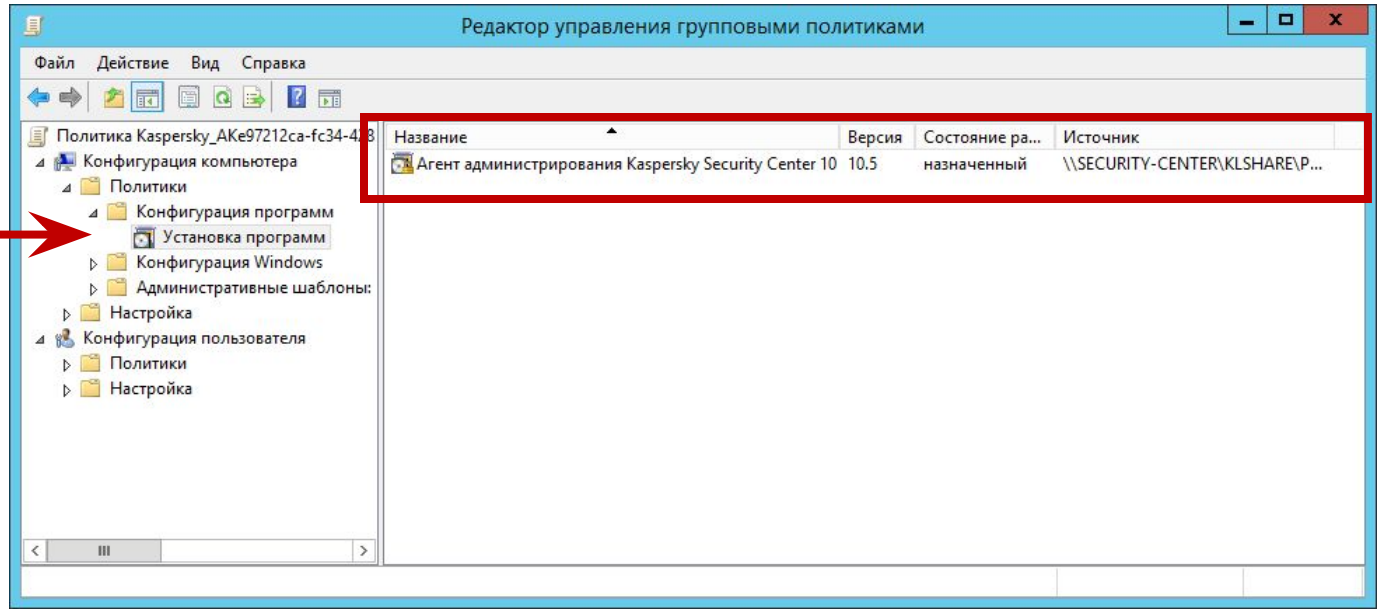


Задача создает в Active Directory групповую политику с таким же именем ***Kaspersky_AK****{GUID}*, как и у группы целевых компьютеров

Политика применяется только к компьютерам этой группы

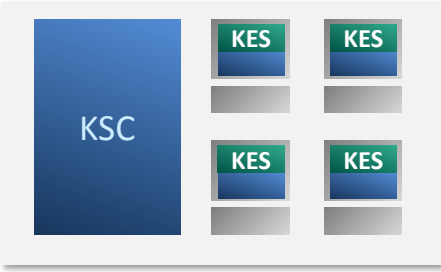
Параметры установки в объекте групповой политики





Чтобы удалить из Active Directory группу и объект групповой политики, отключите в задаче установки параметр **Назначить установку Агента администрирования в групповых политиках Active Directory** или удалите задачу

Групповая политика назначает установку MSI-пакета Агента администрирования, расположенного в общей папке Сервера — *\\<имя сервера>\KLSHARE*



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

- Требования к клиентским компьютерам
- Как изменить состав компонентов KES
- Как создать новый пакет установки
- Как создать пакет KSWS
- Какие есть методы установки
- Как удаленно установить агент и KES
- Как проще установить агент и KES локально
- Как установить агент через Active Directory
- **Как удалить несовместимые программы**

Часть II. Управление защитой

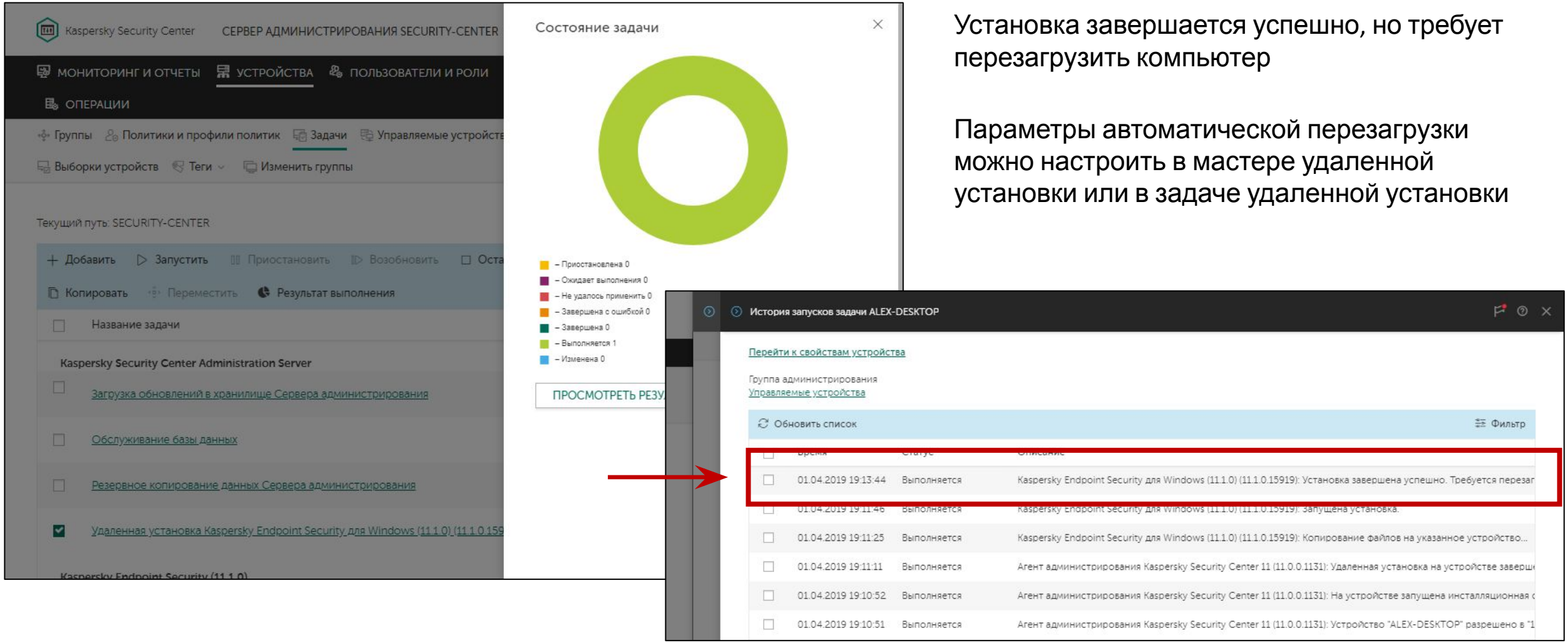
Часть III. Контроль

Часть IV. Сопровождение

Что такое несовместимые программы

- Какие программы не совместимы с Kaspersky Endpoint Security?
  - Сторонние программы для защиты компьютера: антивирусы, сетевые экраны и т. п.
- Какие программы несовместимы с Агентом администрирования KSC?
  - Официально таких нет
- Что будет если не удалить несовместимые программы?
  - Компьютер будет больше «тормозить», чаще сбоить, зависать и перезагружаться
- Как лучше удалить несовместимые программы?
  - Программы с централизованным управлением лучше удалять их же собственными средствами
  - Инсталлятор Kaspersky Endpoint Security автоматически удаляет многие несовместимые программы
  - Администратор может удалить несовместимые программы задачей для Агентов

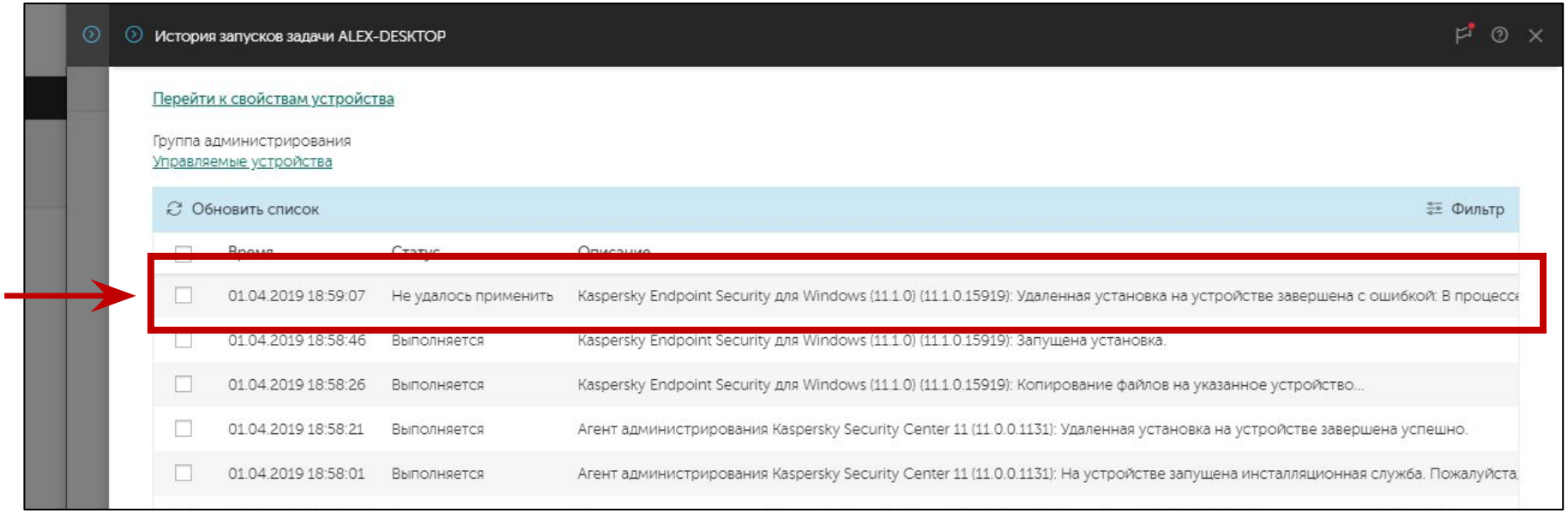
Если инсталлятор KES нашел и удалил несовместимые программы

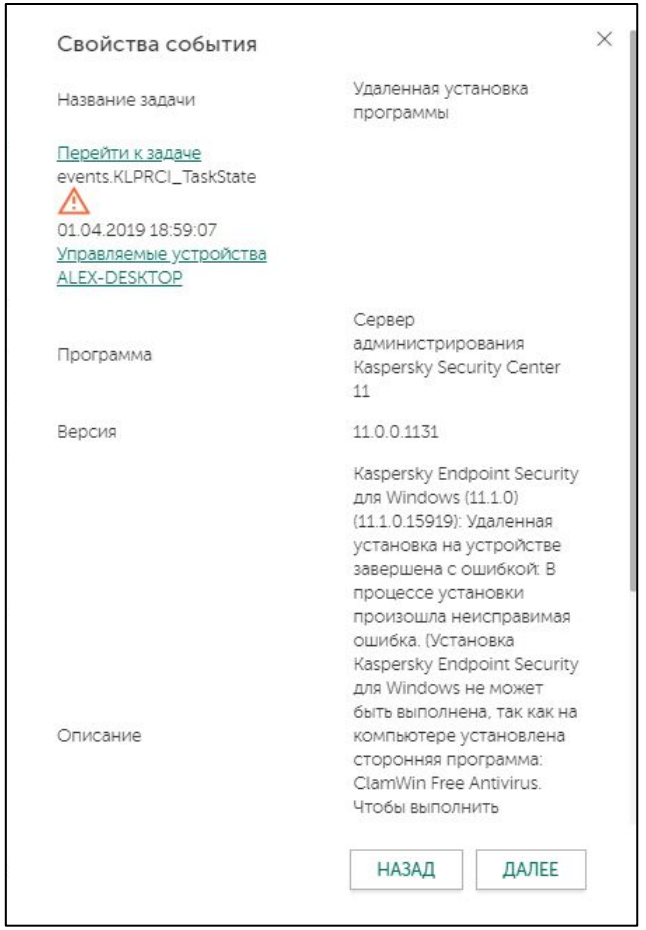


Установка завершается успешно, но требует перезагрузить компьютер

Параметры автоматической перезагрузки можно настроить в мастере удаленной установки или в задаче удаленной установки

Если инсталлятор нашел, но не удалил несовместимые программы



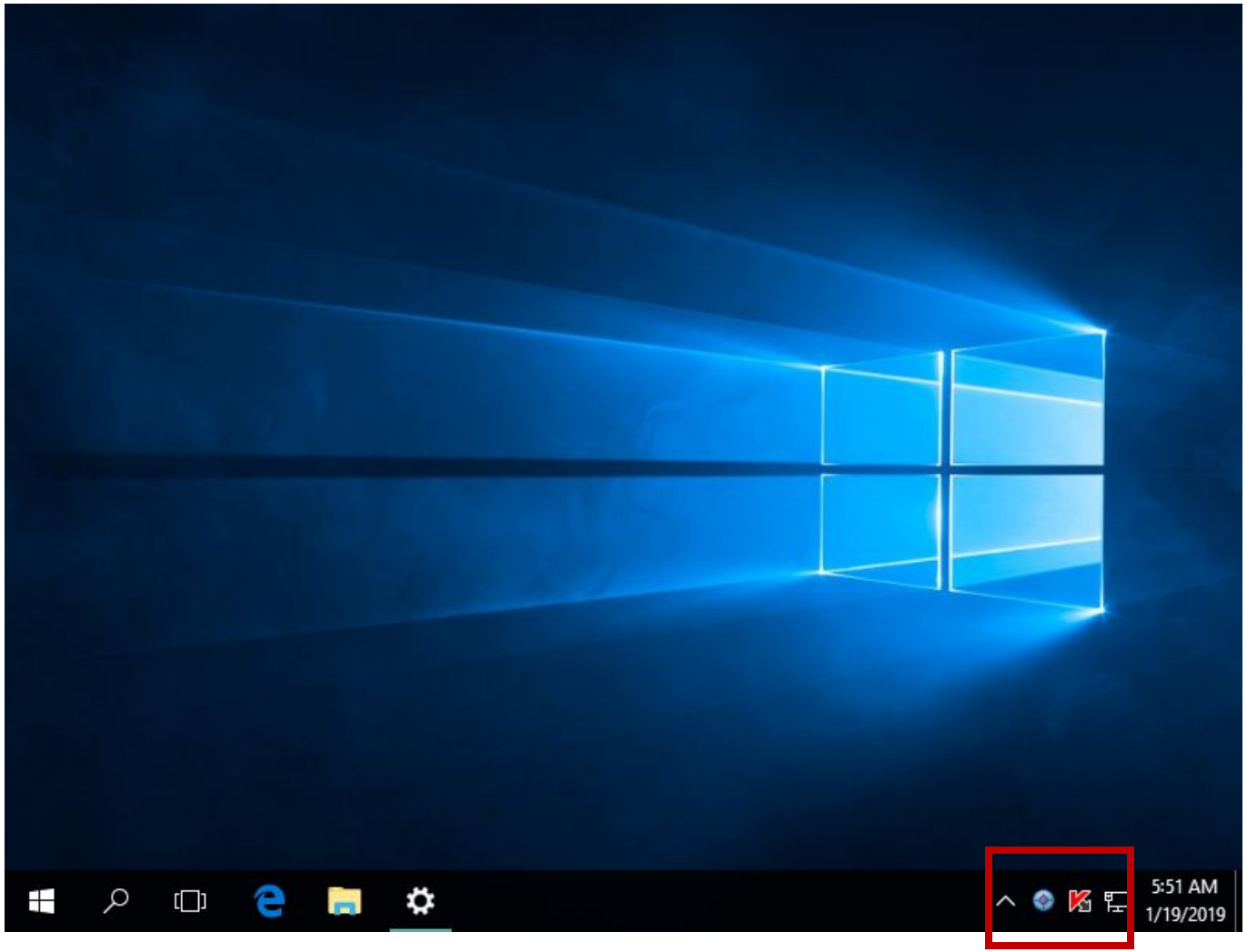


Установка Kaspersky Endpoint Security завершается с ошибкой и требует удалить несовместимую программу вручную

Установка Агента администрирования при этом завершается успешно, и компьютер попадает в группу управляемых компьютеров

Администратор может удалить несовместимые программы удаленно с помощью уже установленного Агента администрирования

Если инсталлятор не нашел и не удалил несовместимые программы



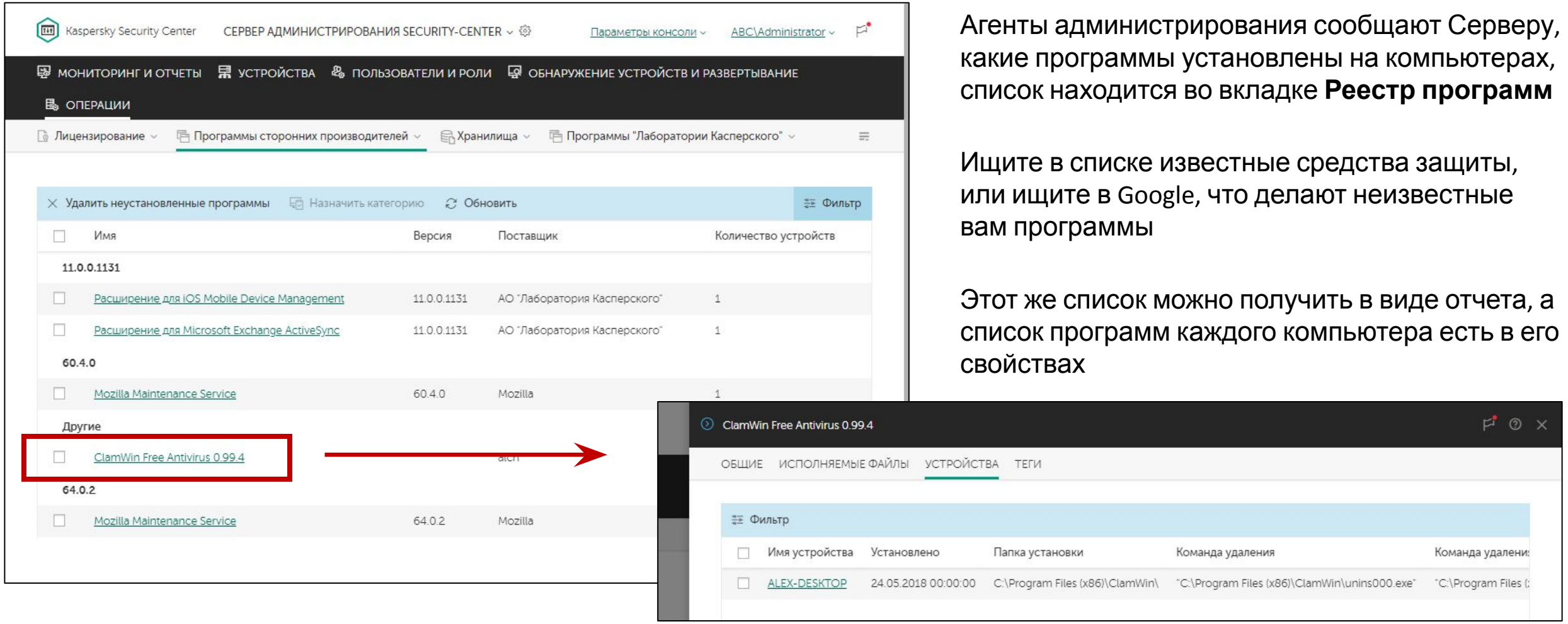
Установка Kaspersky Endpoint Security завершается успешно, но на компьютере теперь два «антивируса» со всеми сопутствующими рисками

- Замедление
- Сбои
- Перезагрузки

Чем больше таких компьютеров, тем больше проблем

Пострадает отчетность — угрозы, заблокированные сторонним антивирусом, не попадут в базу событий и в отчеты Kaspersky Security Center

Как узнать, что есть необнаруженные несовместимые программы



Агенты администрирования сообщают Серверу, какие программы установлены на компьютерах, список находится во вкладке **Реестр программ**

Ищите в списке известные средства защиты, или ищите в Google, что делают неизвестные вам программы

Этот же список можно получить в виде отчета, а список программ каждого компьютера есть в его свойствах

Как удалить необнаруженные несовместимые программы

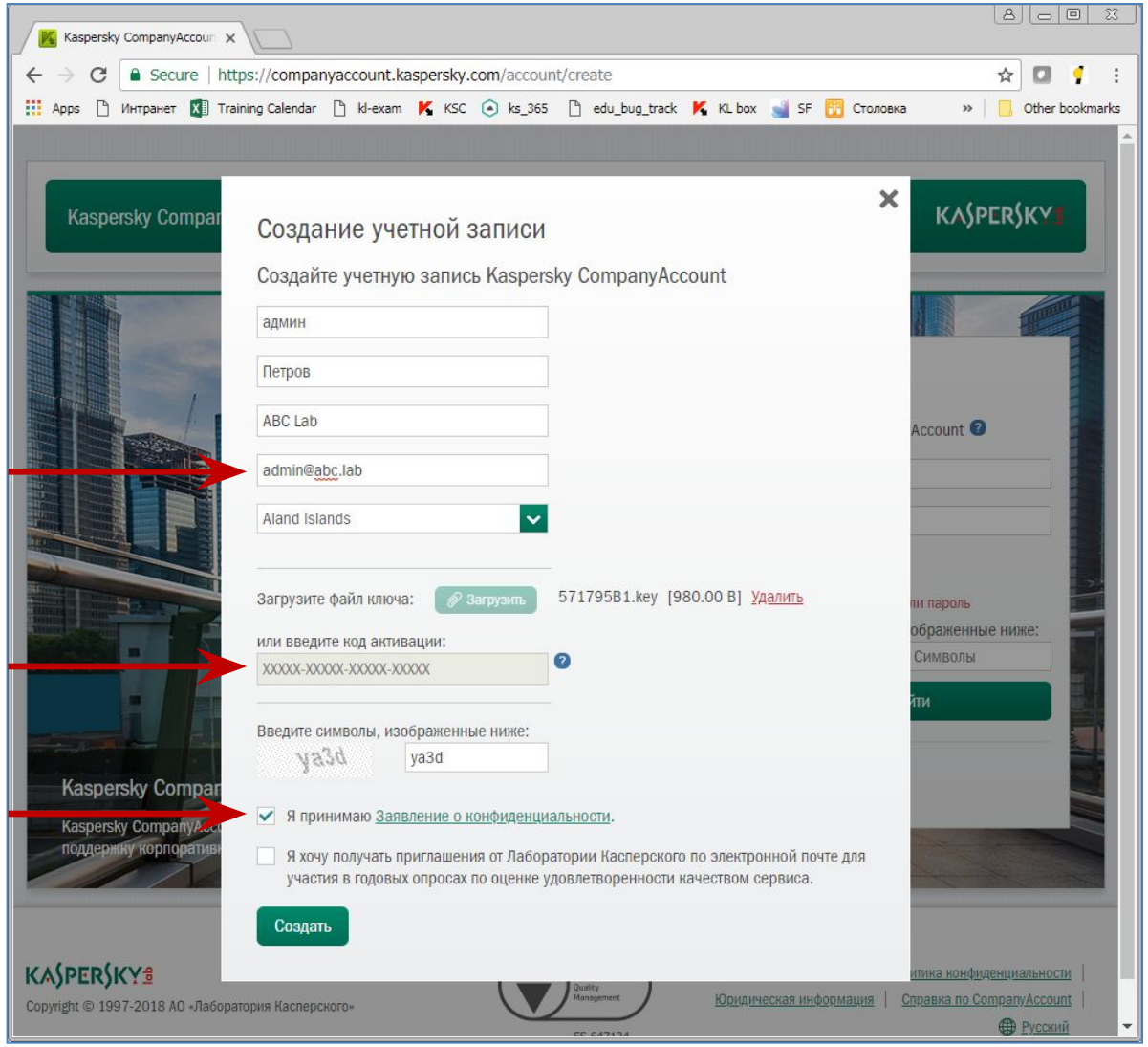
1. Запросите в технической поддержке ini-файл для задачи деинсталляции; приложите к запросу дистрибутив программы, которую нужно удалить

2. Получите .ini-файл, скопируйте его в папку *%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Data\Cleaner* на Сервере администрирования и перезагрузите службу Сервера администрирования

3. Опционально: создайте выборку компьютеров, на которых есть несовместимая программа

4. Создайте задачу удаления несовместимых программ, выберите из списка нужную программу, запустите задачу на всех компьютерах или на компьютерах выборки

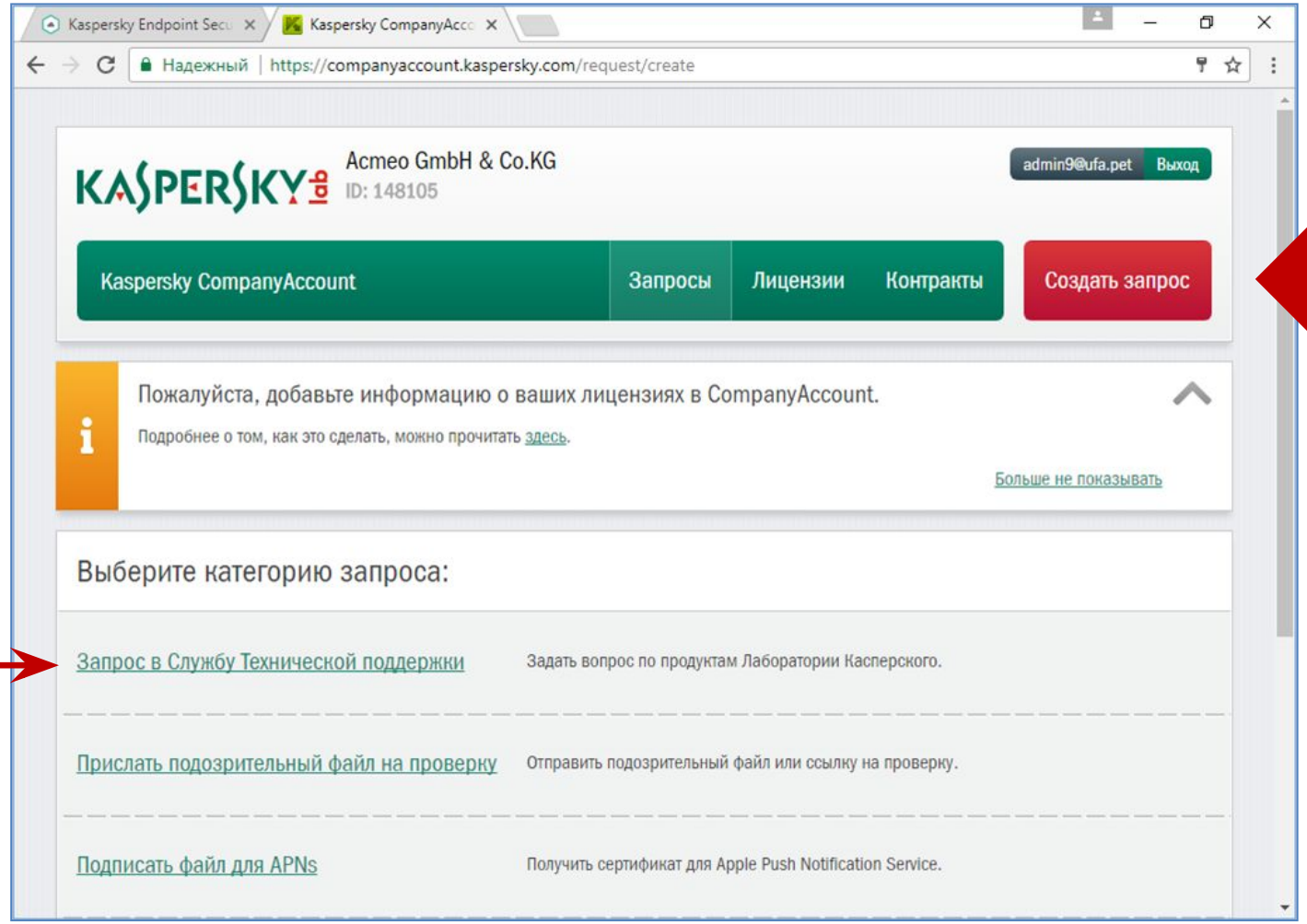
Как запросить .ini-файл у технической поддержки



Чтобы запросить у техподдержки ini-файл, зарегистрируйте личный кабинет на портале *companyaccount.kaspersky.com*

Укажите имя, название компании, почтовый адрес и, самое главное, лицензию: код или ключ

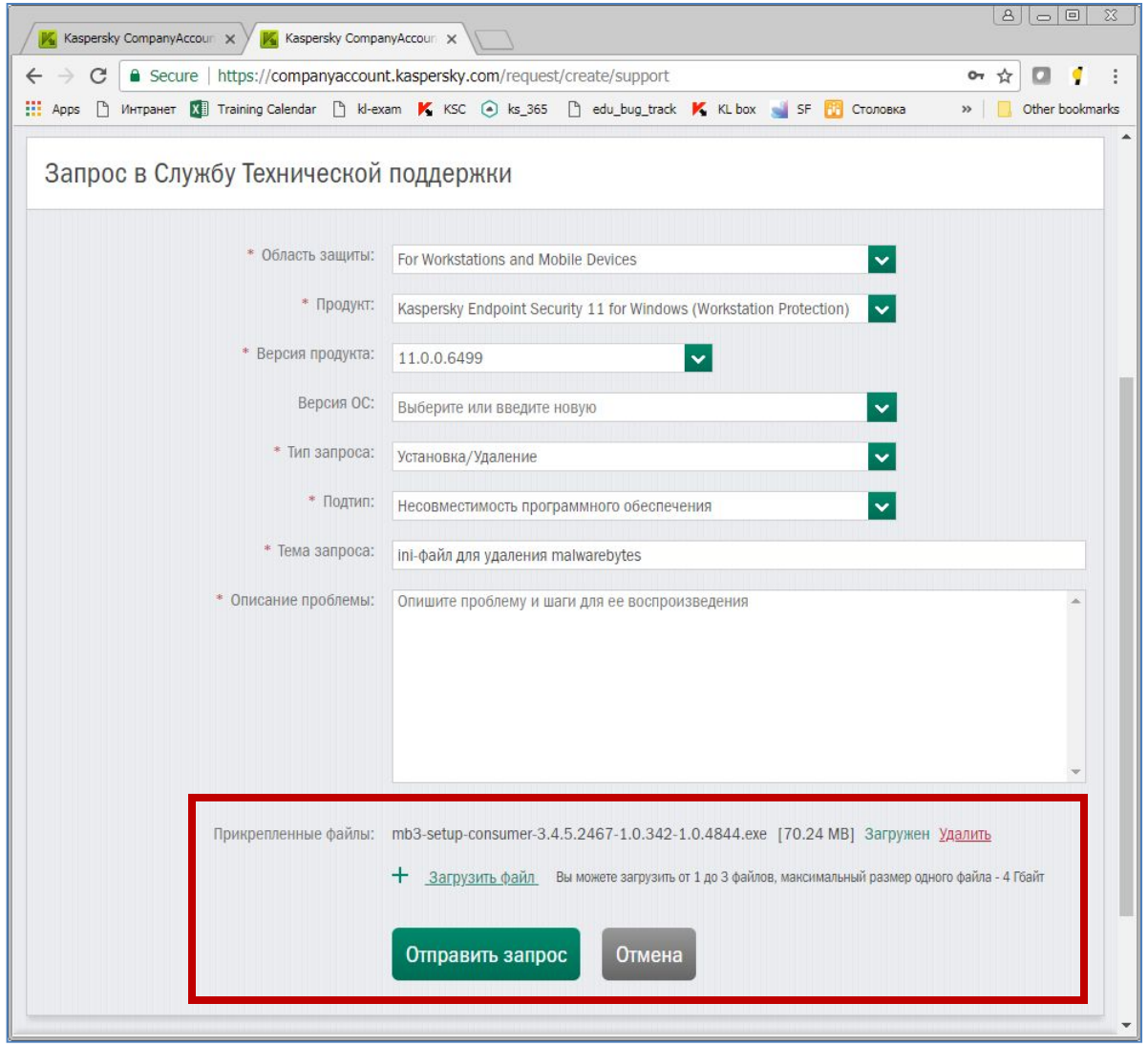
Как запросить .ini-файл у технической поддержки



Нажмите красную кнопку **Создать запрос**

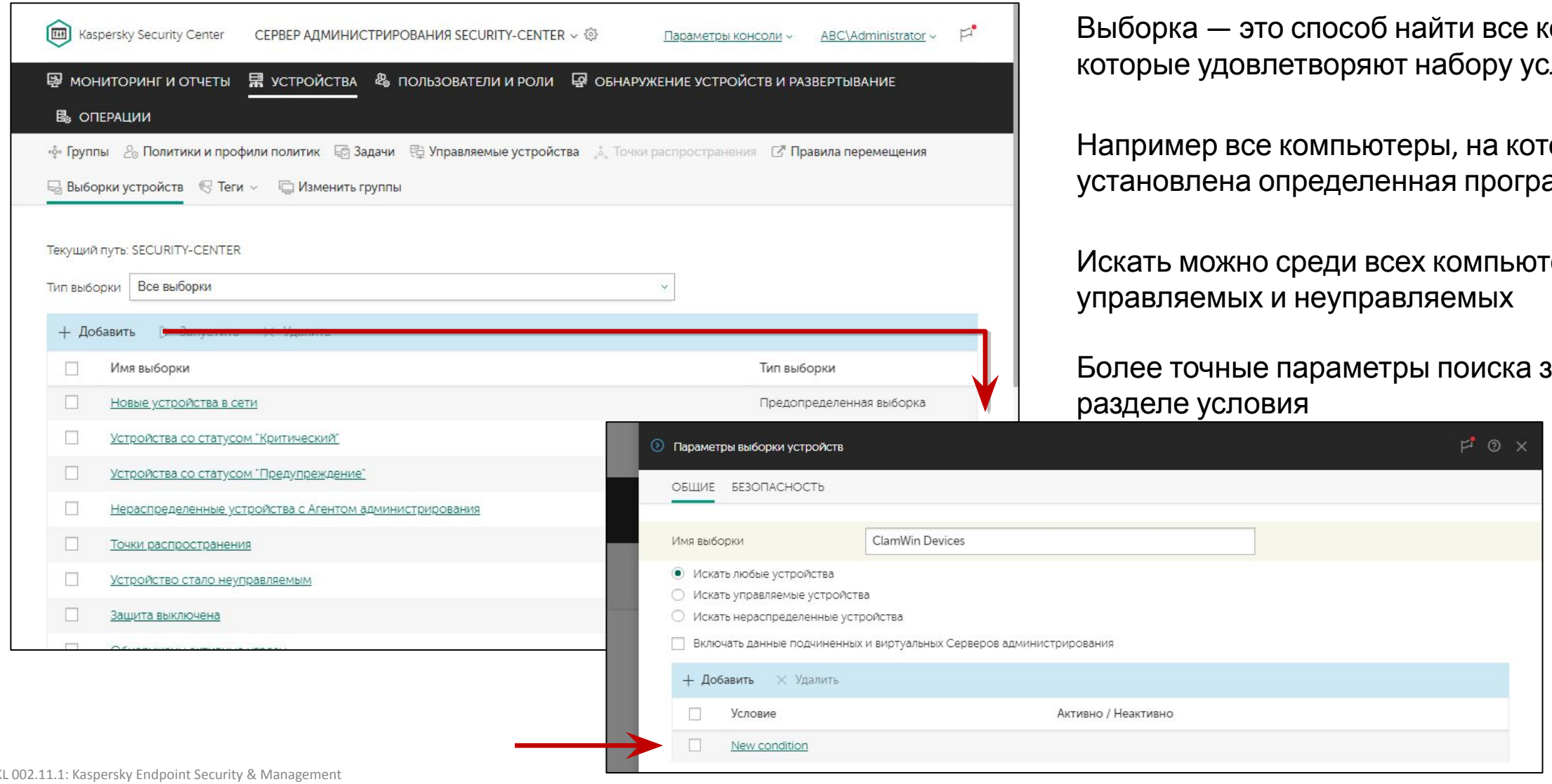
Выберите категорию **Запрос в Службу Технической поддержки**

Как запросить .ini-файл у технической поддержки



1. Выберите
   - Область For Workstations and Mobile Devices
   - Продукт Kaspersky Endpoint Security 11 для Windows
   - Тип запроса Установка/Удаление
   - Подтип Несовместимость программного обеспечения
2. Укажите имя несовместимой программы в теме
3. Прикрепите к запросу инсталлятор несовместимой программы
4. Дождитесь ответа от технической поддержки
5. Загрузите ini-файл, скопируйте его в папку *%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Data\Cleaner* и перезагрузите службу Сервера администрирования

Как сделать выборку компьютеров с несовместимой программой



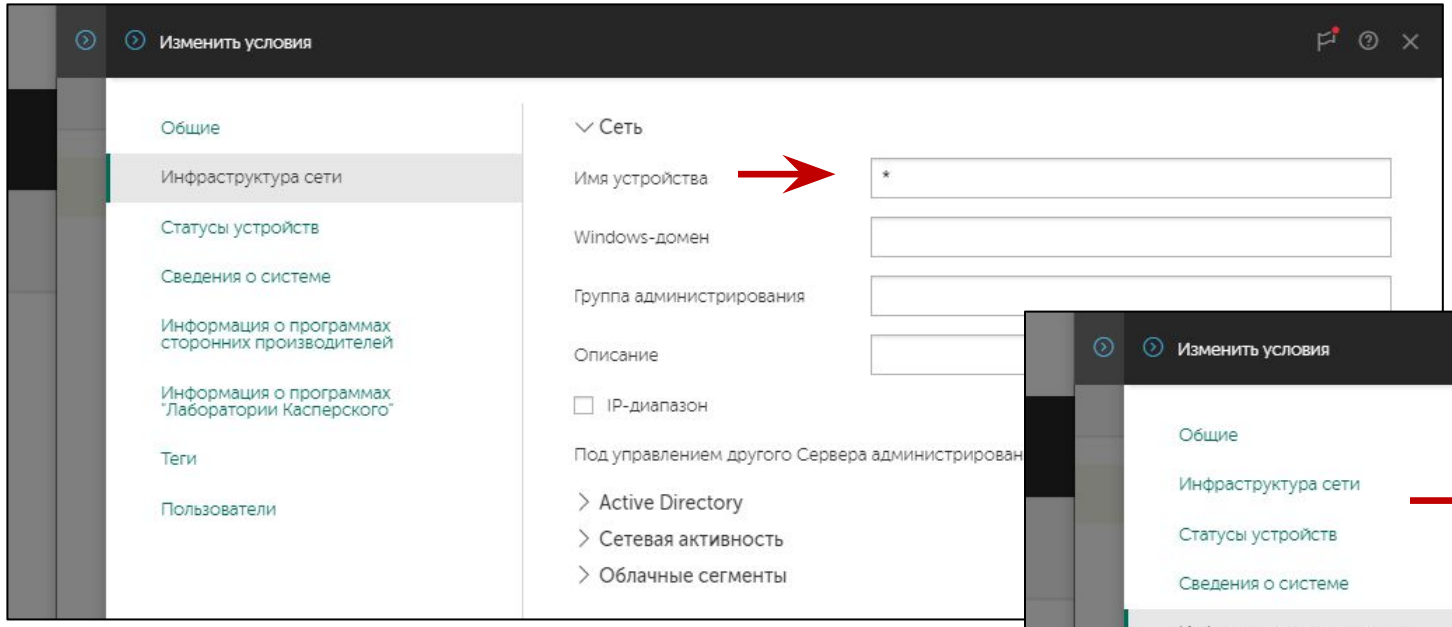
Выборка — это способ найти все компьютеры, которые удовлетворяют набору условий

Например все компьютеры, на которых установлена определенная программа

Искать можно среди всех компьютеров, управляемых и неуправляемых

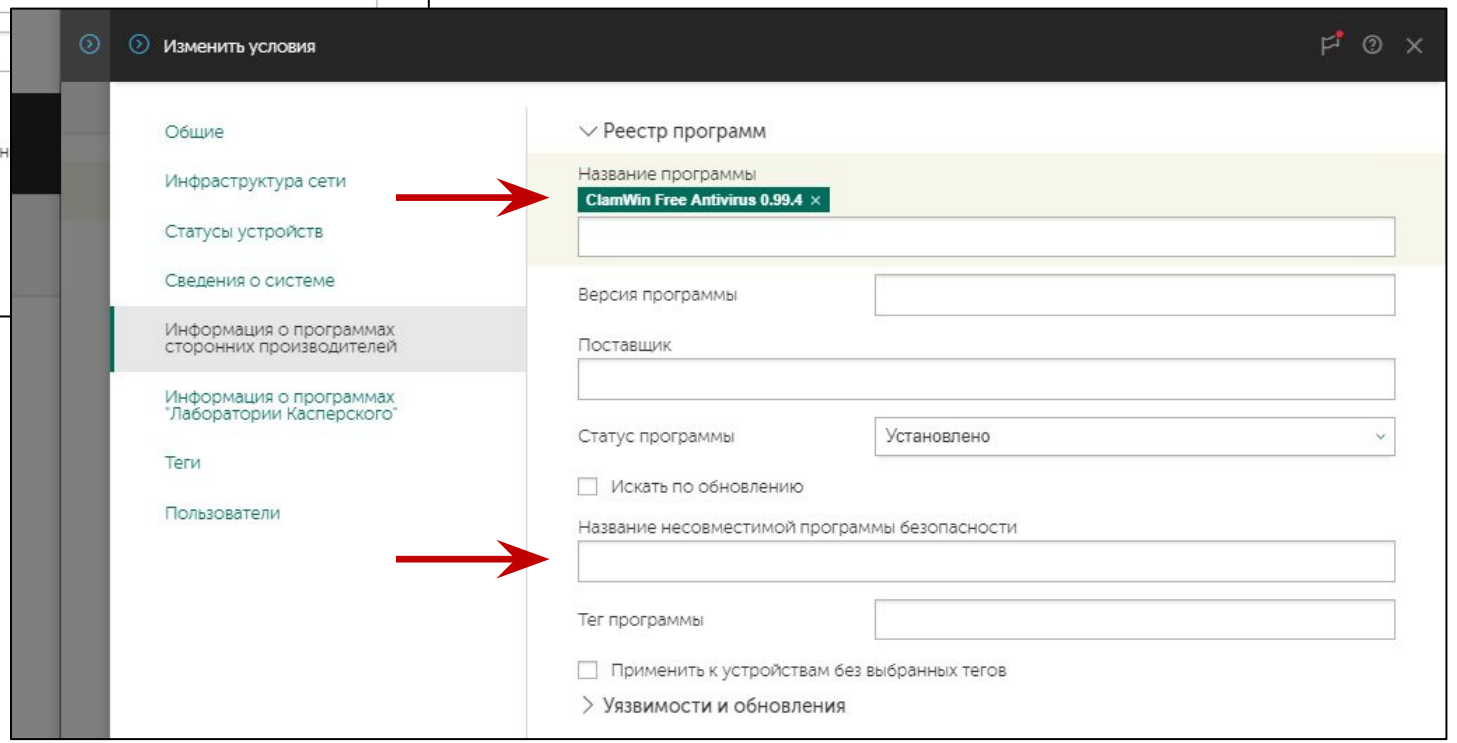
Более точные параметры поиска задайте в разделе условия

Компьютеры с несовместимыми программами



По умолчанию новая выборка ищет все компьютеры по условию: *имя устройства=«*»*

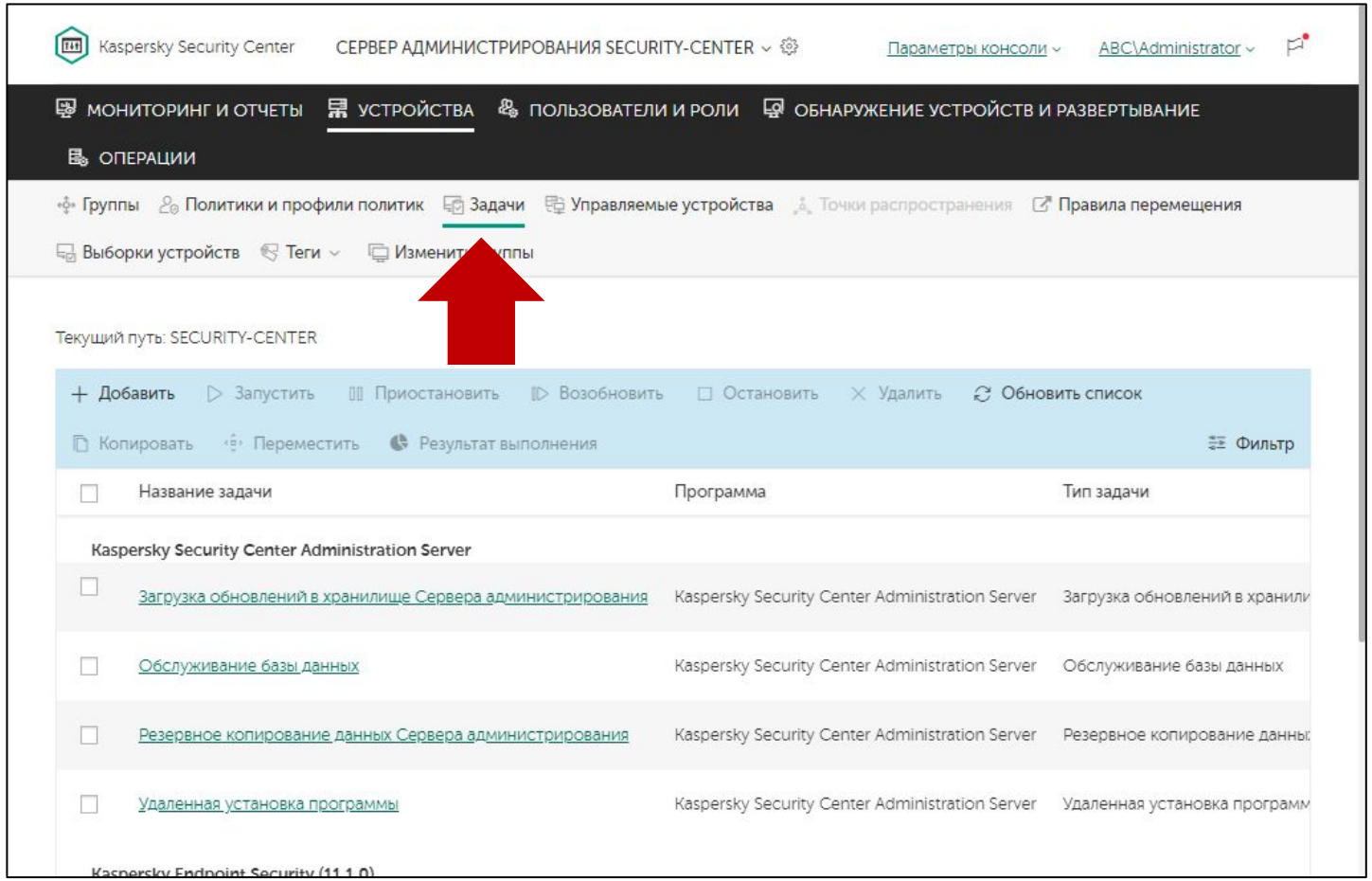
Имя программы настраивается в параметрах условий в свойствах выборки



Имена несовместимых программ нужно брать из отчета или реестра программ

Чтобы собрать в одной выборке компьютеры с разными несовместимыми программами, добавьте в выборку по одному условию для каждой несовместимой программы

Как создать задачу, чтобы удалить несовместимые программы



Одноразовые задачи создавайте в узле **Задачи**

Здесь собраны все задачи, включая

- групповые задачи
- задачи для наборов компьютеров
- задачи Сервера администрирования

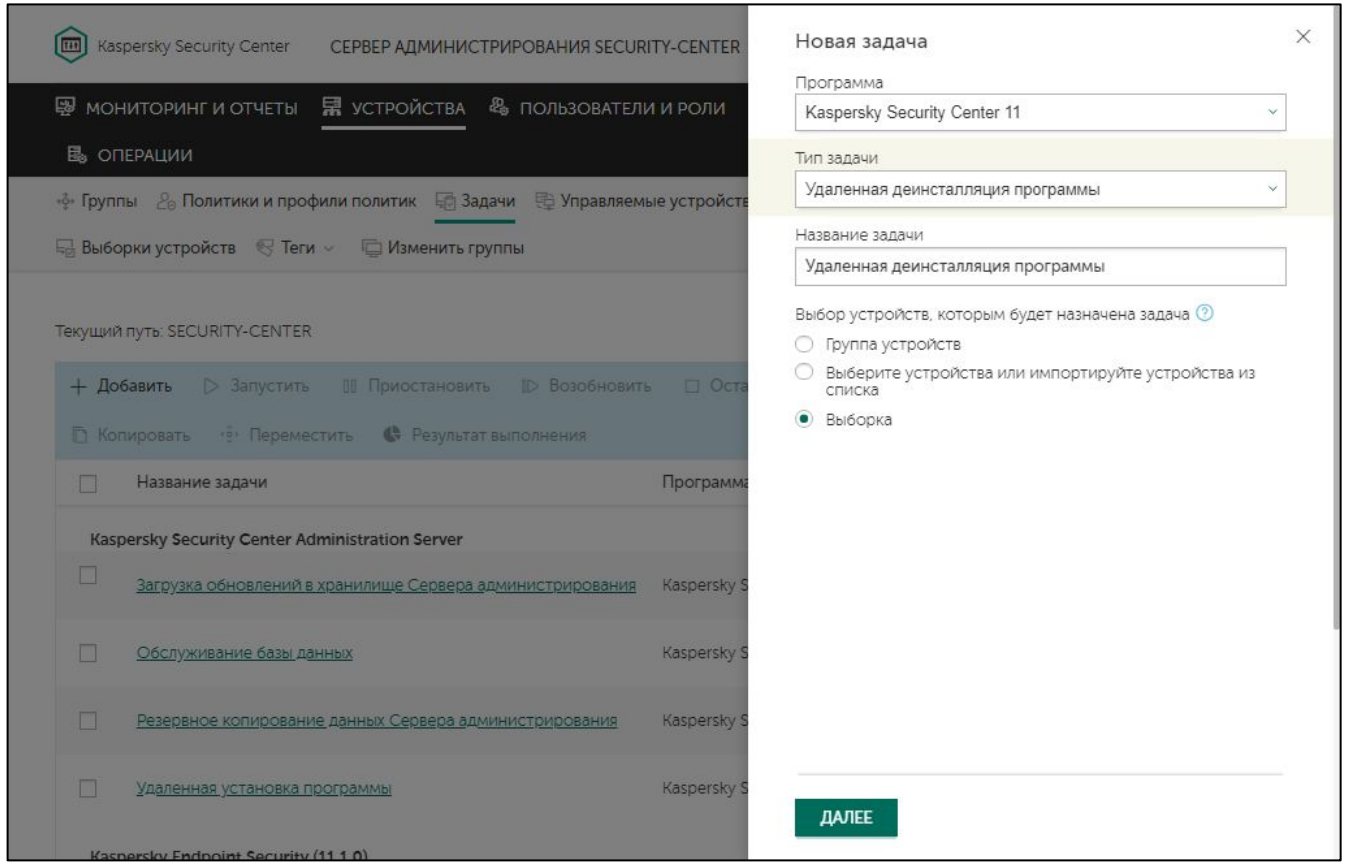
Чтобы удалить несовместимые программы, создайте задачу для наборов компьютеров

Групповые задачи создавайте для рутинных операций: загрузки обновлений, поиска вирусов, и т. п.

Удаленная деинсталляция программы

Задача деинсталляции:

1. Выберите тип задачи, укажите имя задачи и устройства
2. Укажите выборку
3. Укажите несовместимые программы
4. (Не обязательно) Задайте имя и пароль администратора
5. Создайте задачу



Задача деинсталляции относится к задачам Сервера администрирования Kaspersky Security Center

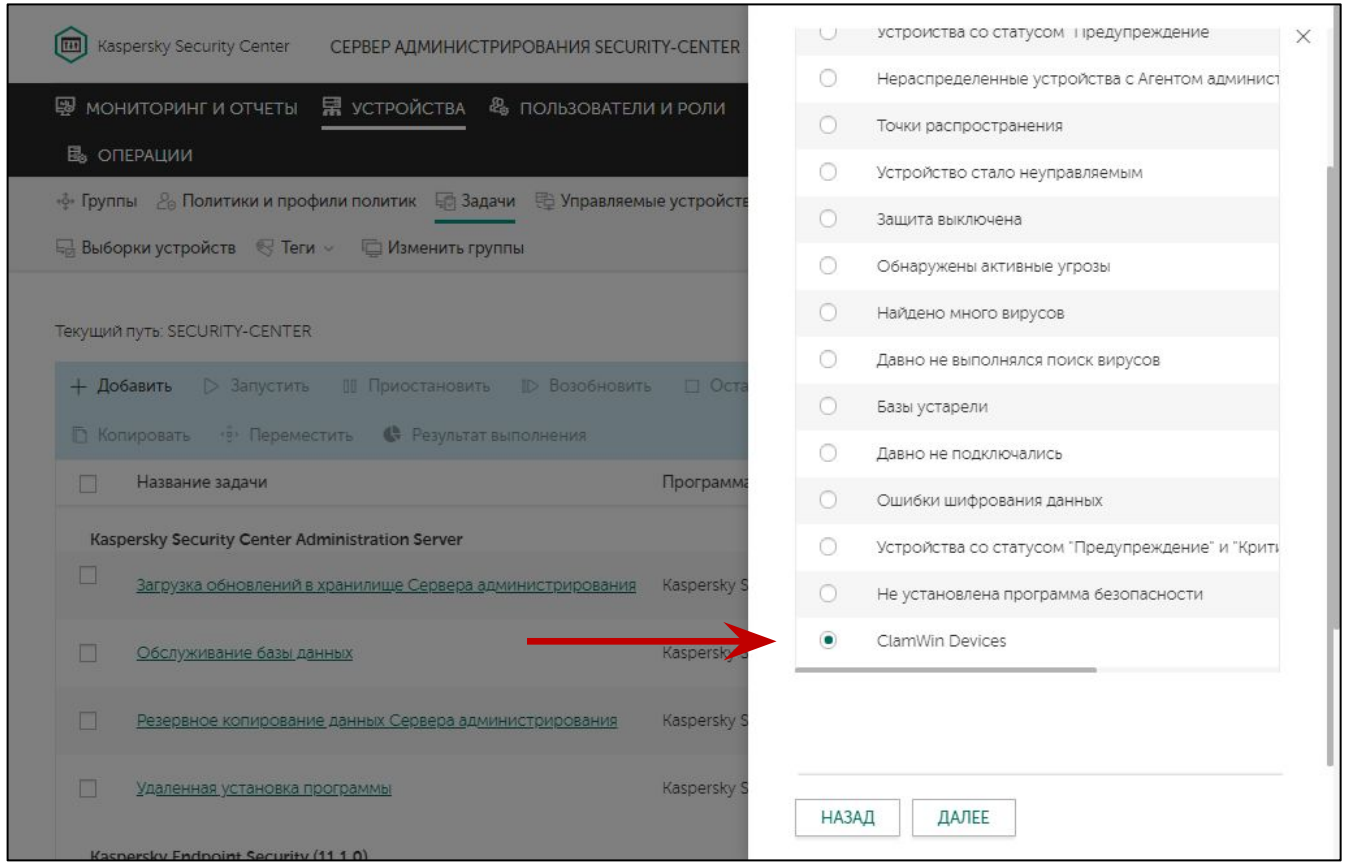
Есть три способа выбрать компьютеры для задачи:

- Указать группу администрирования
- Отметить компьютеры в списке обнаруженных
- **Указать выборку компьютеров**

Выборка

Задача деинсталляции:

1. Выберите тип задачи, укажите имя задачи и устройства
2. Укажите выборку
3. Укажите несовместимые программы
4. (Не обязательно) Задайте имя и пароль администратора
5. Создайте задачу

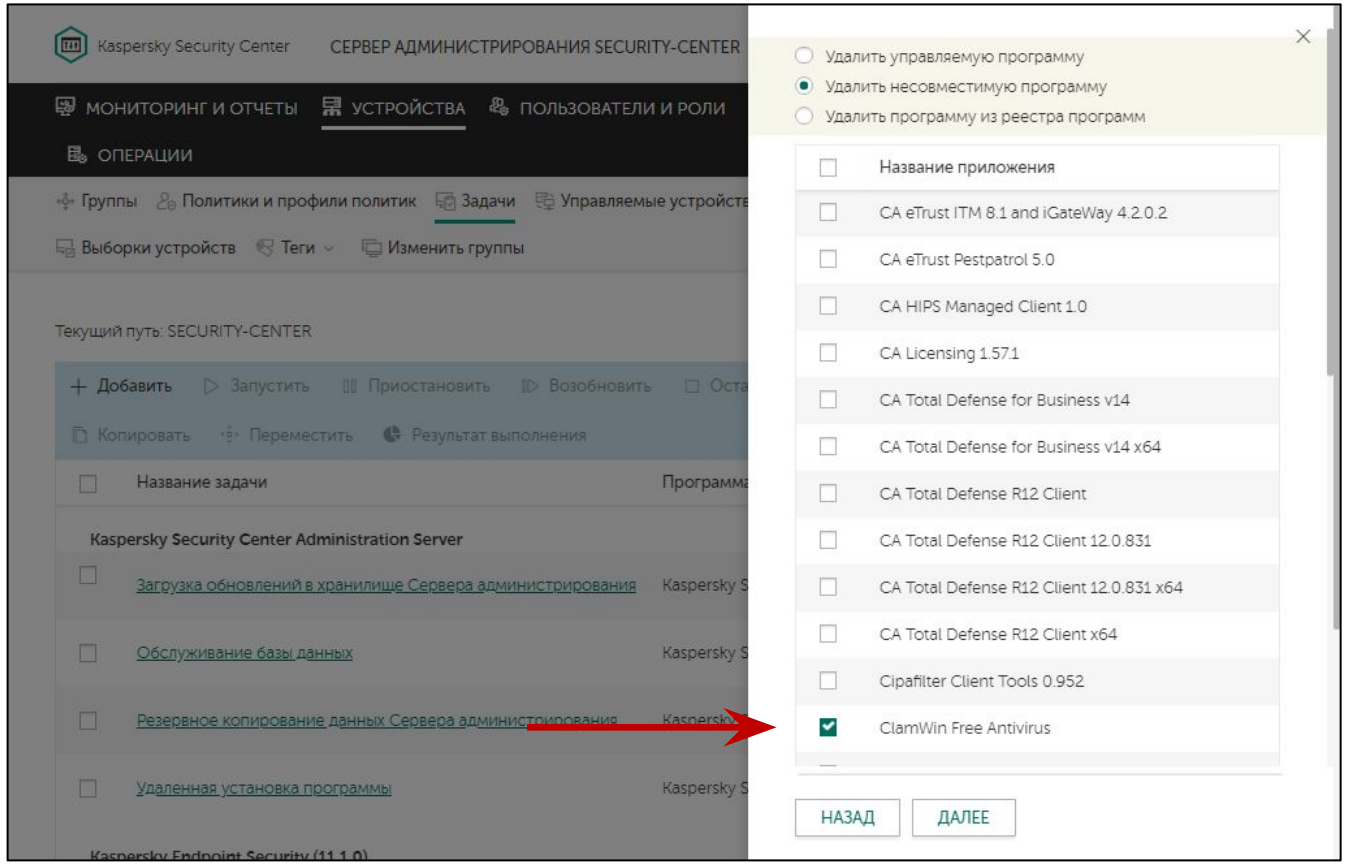


Отметьте нужную выборку в списке

Что деинсталлировать?

Задача деинсталляции:

1. Выберите тип задачи, укажите имя задачи и устройства
2. Укажите выборку
3. Укажите несовместимые программы
4. (Не обязательно) Задайте имя и пароль администратора
5. Создайте задачу



Задача деинсталляции может удалить:

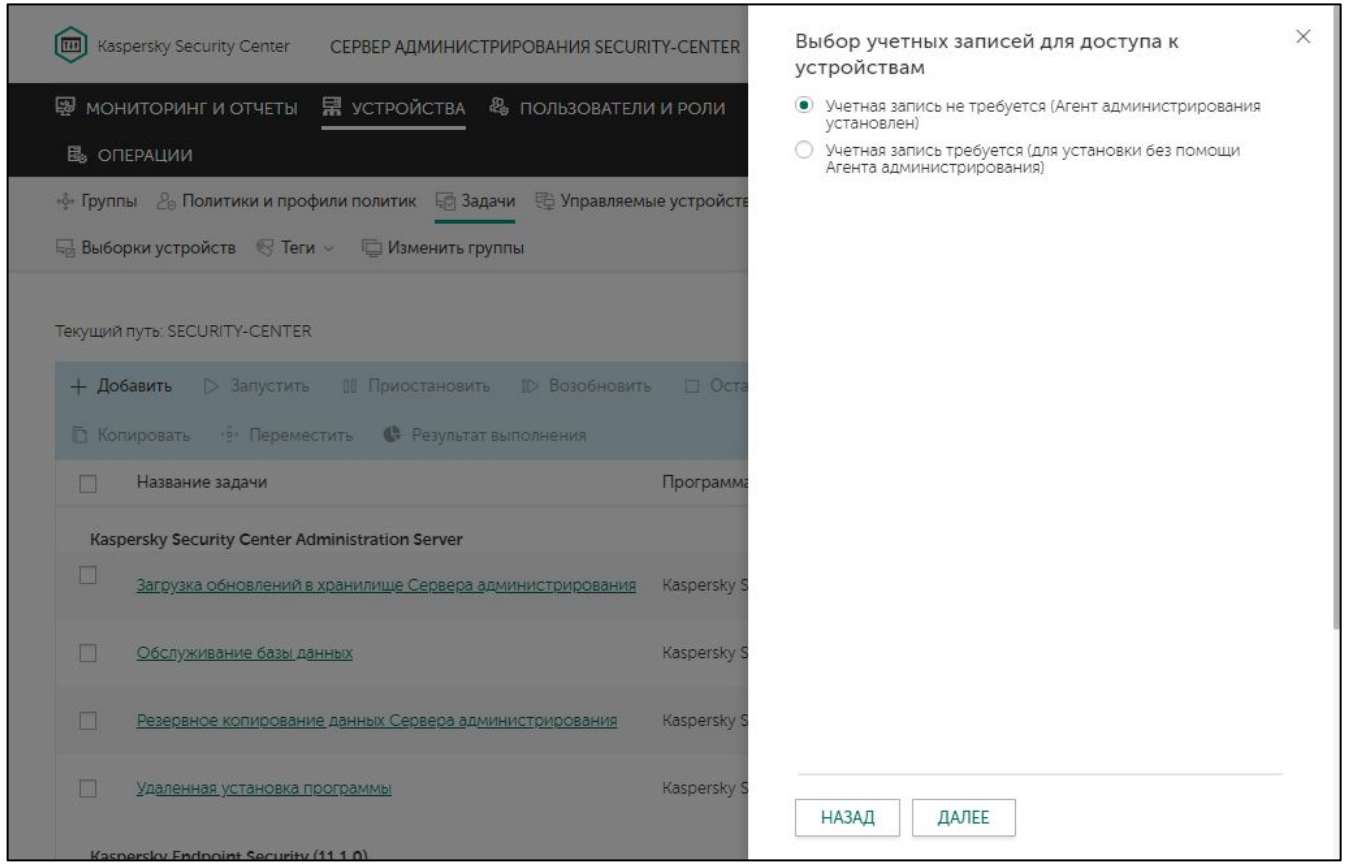
- Управляемые программы (например, Kaspersky Endpoint Security)
- **Несовместимые программы (то, что нам нужно)**
- Программы из реестра (в таких случаях администратор иногда должен сам ввести команду деинсталляции)

Задача может удалить несколько или даже все несовместимые приложения

Учетная запись

Задача деинсталляции:

1. Выберите тип задачи, укажите имя задачи и устройства
2. Укажите выборку
3. Укажите несовместимые программы
4. (Не обязательно) Задайте имя и пароль администратора
5. Создайте задачу



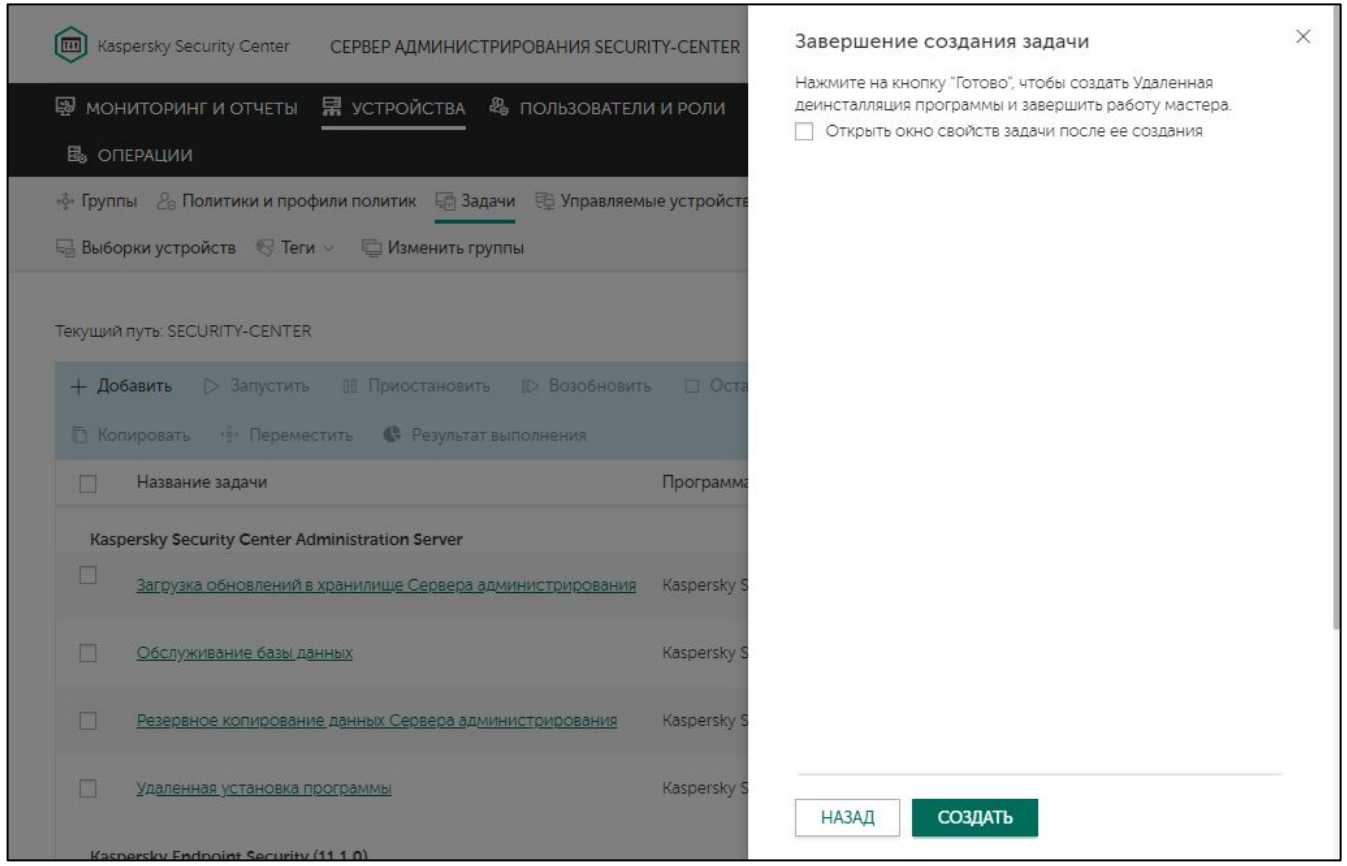
Задаче деинсталляции нужны права, чтобы скопировать и запустить скрипт удаления программы (такие же, как и задаче установки)

Если Агент администрирования уже установлен на компьютерах, учетную запись указывать не нужно

Создание задачи

Задача деинсталляции:

1. Выберите тип задачи, укажите имя задачи и устройства
2. Укажите выборку
3. Укажите несовместимые программы
4. (Не обязательно) Задайте имя и пароль администратора
5. Создайте задачу



Мастер создает задачу, но не запускает ее

Можно открыть свойства задачи сразу после ее создания и еще раз убедиться в правильности настроек

Расписание запуска у задачи – **Вручную**

Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса
Глава 2. Как установить Kaspersky Security Center
Глава 3. Как установить Kaspersky Endpoint Security на компьютеры
Глава 4. Как организовать компьютеры в группы

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Как понять, что установка окончена

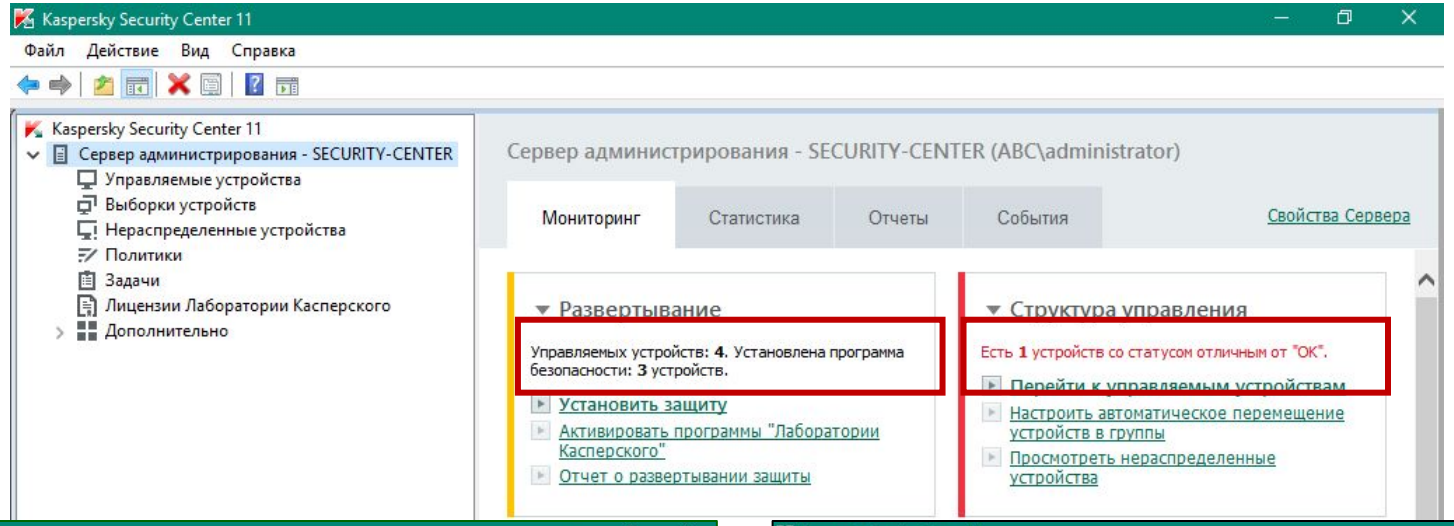
Как Сервер администрирования ищет компьютеры
Как создать или импортировать группы
Как автоматически распределить компьютеры по группам

Средства мониторинга внедрения

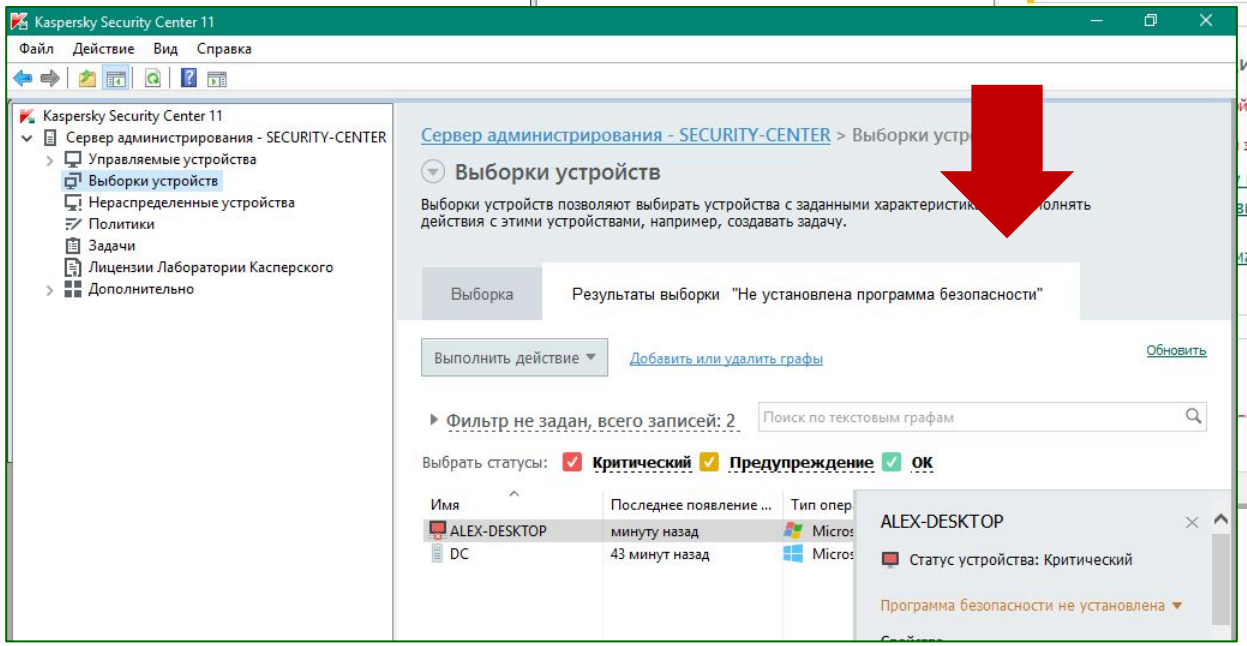
- Отчеты
  - Отчет о несовместимых программах
  - Отчет о развертывании защиты
  - Отчет о версиях приложений Лаборатории Касперского
- Выборки компьютеров
  - Новые компьютеры в сети
  - Нераспределенные компьютеры с Агентом администрирования
  - Не установлено средство защиты
- Дэшборды
  - Развертывание
- События
  - Найден новый клиентский компьютер

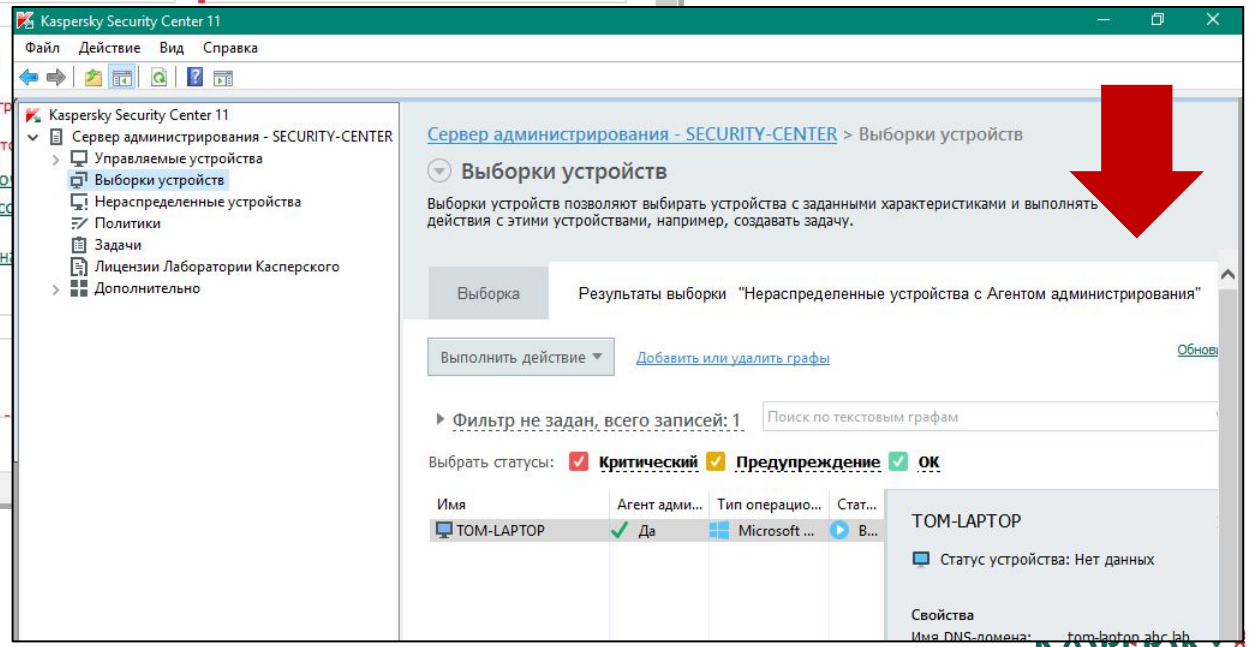
Информация на экране Мониторинг

Секция **Развертывание** показывает управляемые компьютеры без защиты

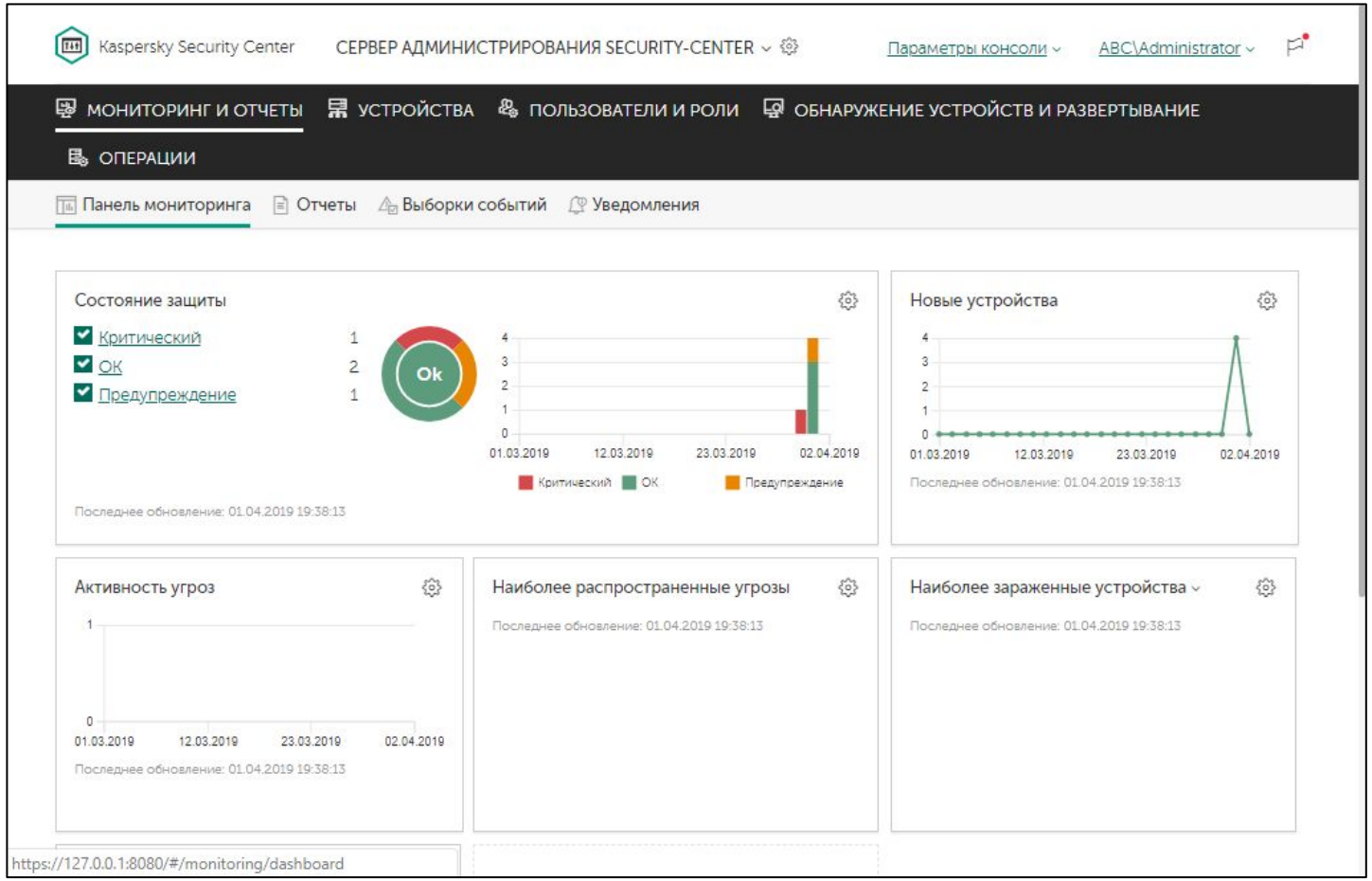


Секция **Структура управления** показывает неуправляемые компьютеры с Агентом администрирования





Информация на главном экране Web Console

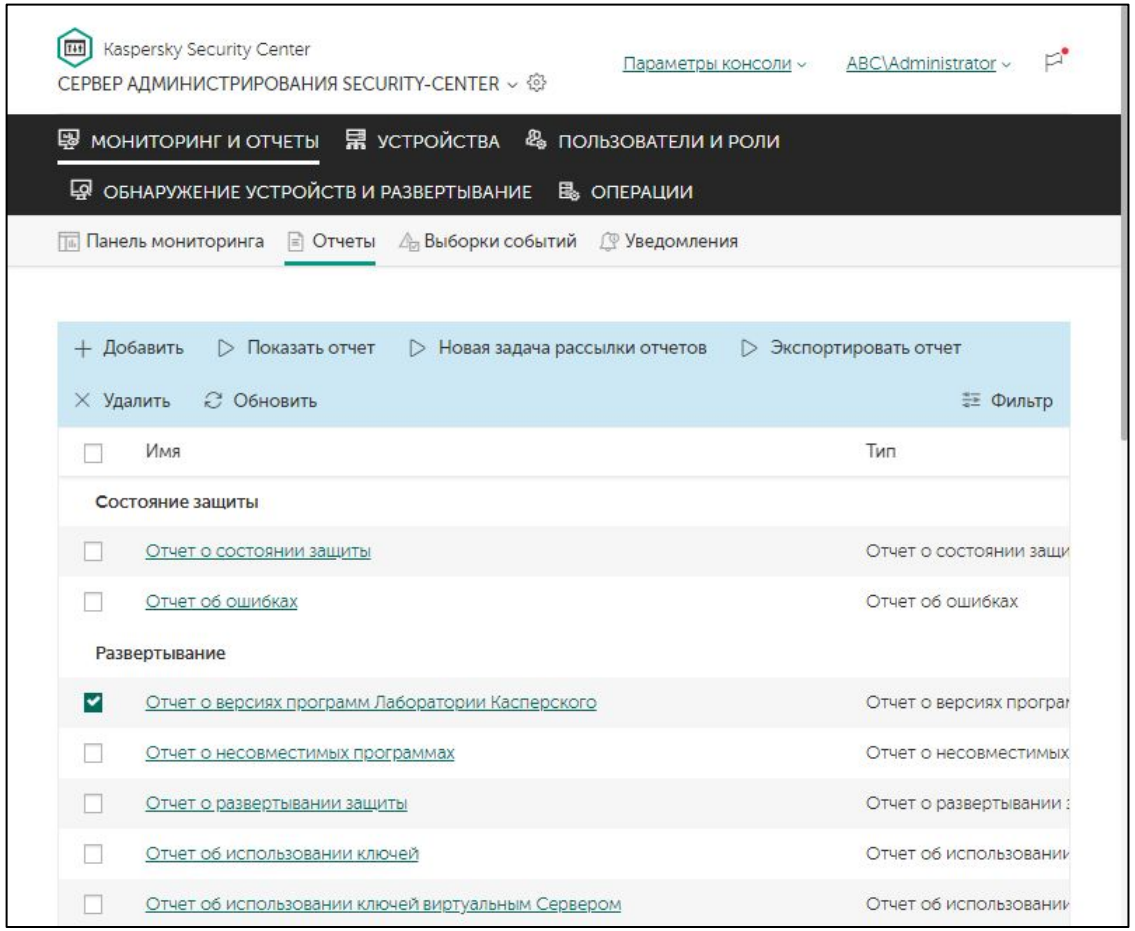


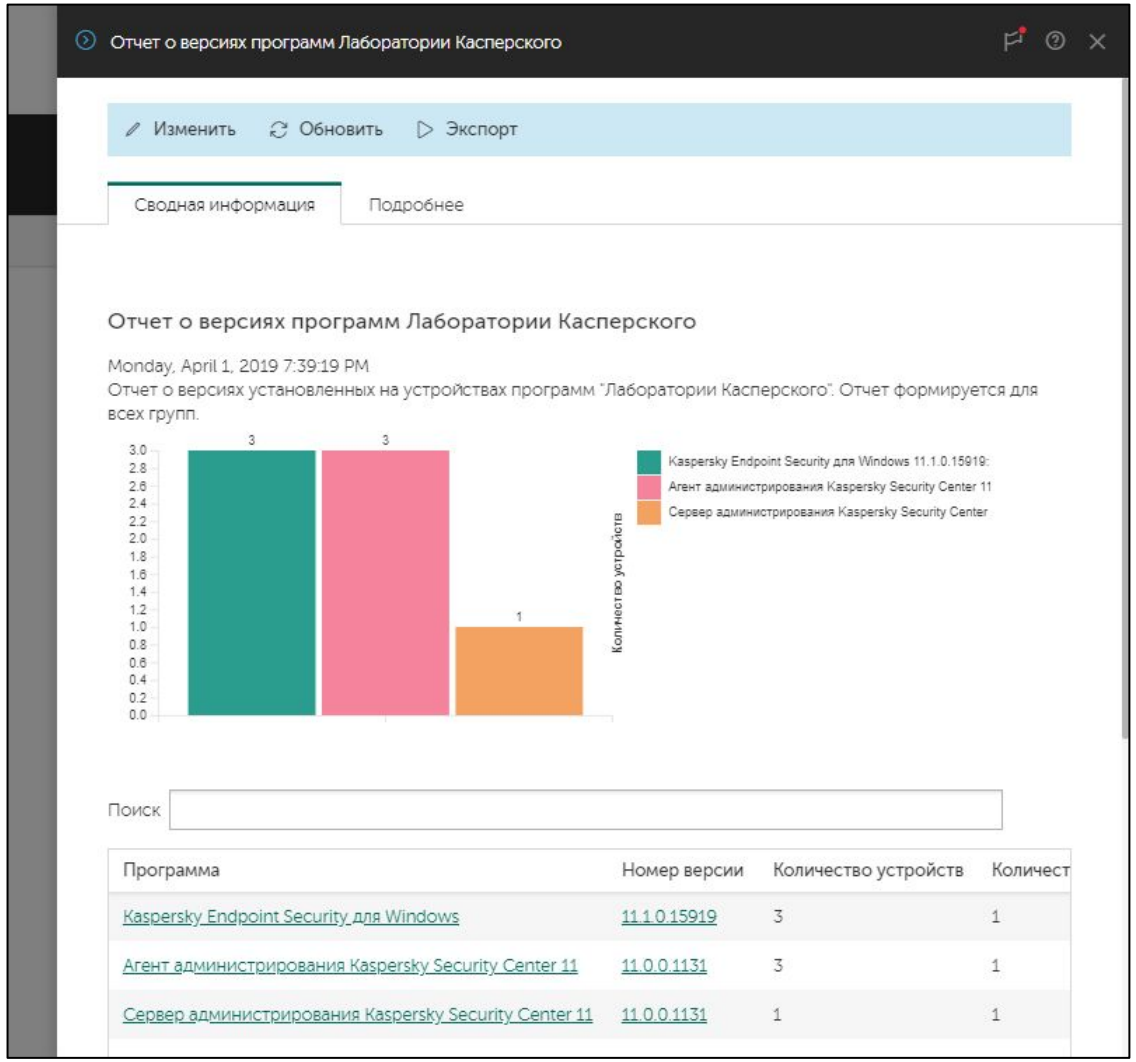
К сожалению, из главного окна непонятно какие управляемые компьютеры с защитой, а какие нет

Также нельзя сразу выйти на список неуправляемых компьютеров, неважно с Агентом или без

Единственное, если статус отличный от **ОК**, то можно по ссылке попасть на список устройств, которые не **ОК**

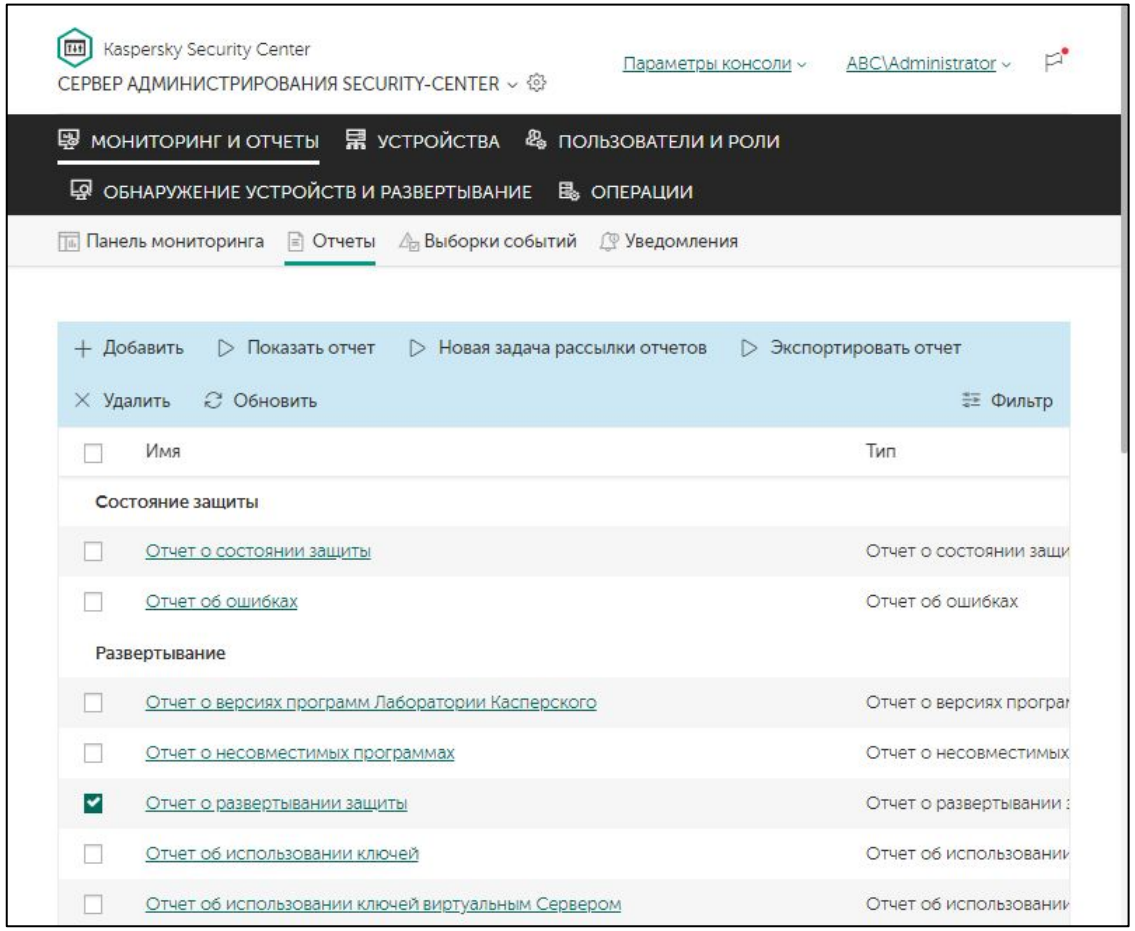
Отчет об установленных программах

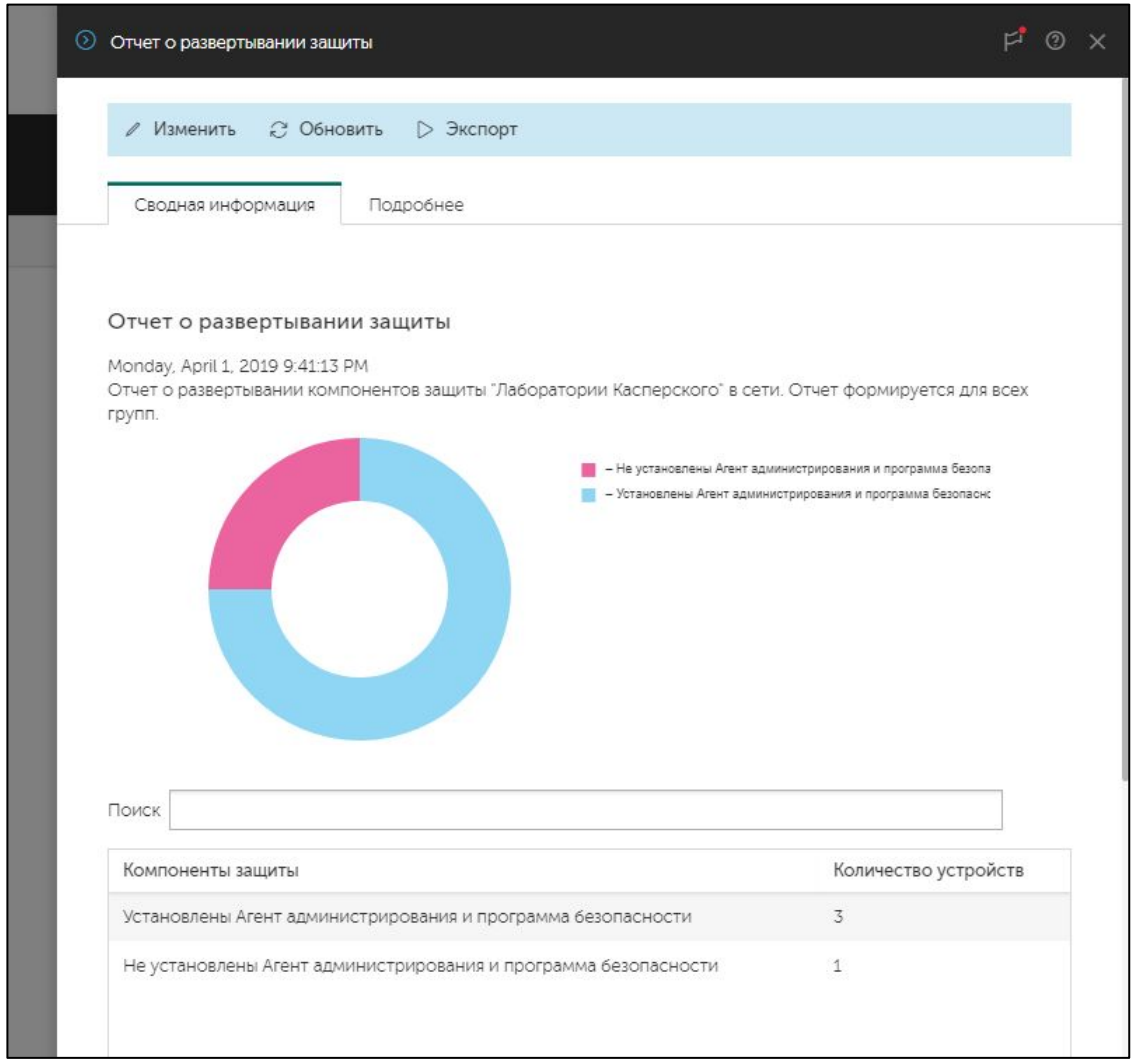




Удобный отчет при обновлении версий программ, показывает сколько установок разных версий есть в сети

Отчет о развертывании защиты





Показывает долю компьютеров без защиты и без Агента среди компьютеров, которые находятся в группах администрирования

Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Часть II. Управление защитой

Часть III. Контроль

Часть IV. Сопровождение

Как понять, что установка окончена

Как Сервер администрирования ищет компьютеры

Как создать или импортировать группы

Как автоматически распределить компьютеры по группам

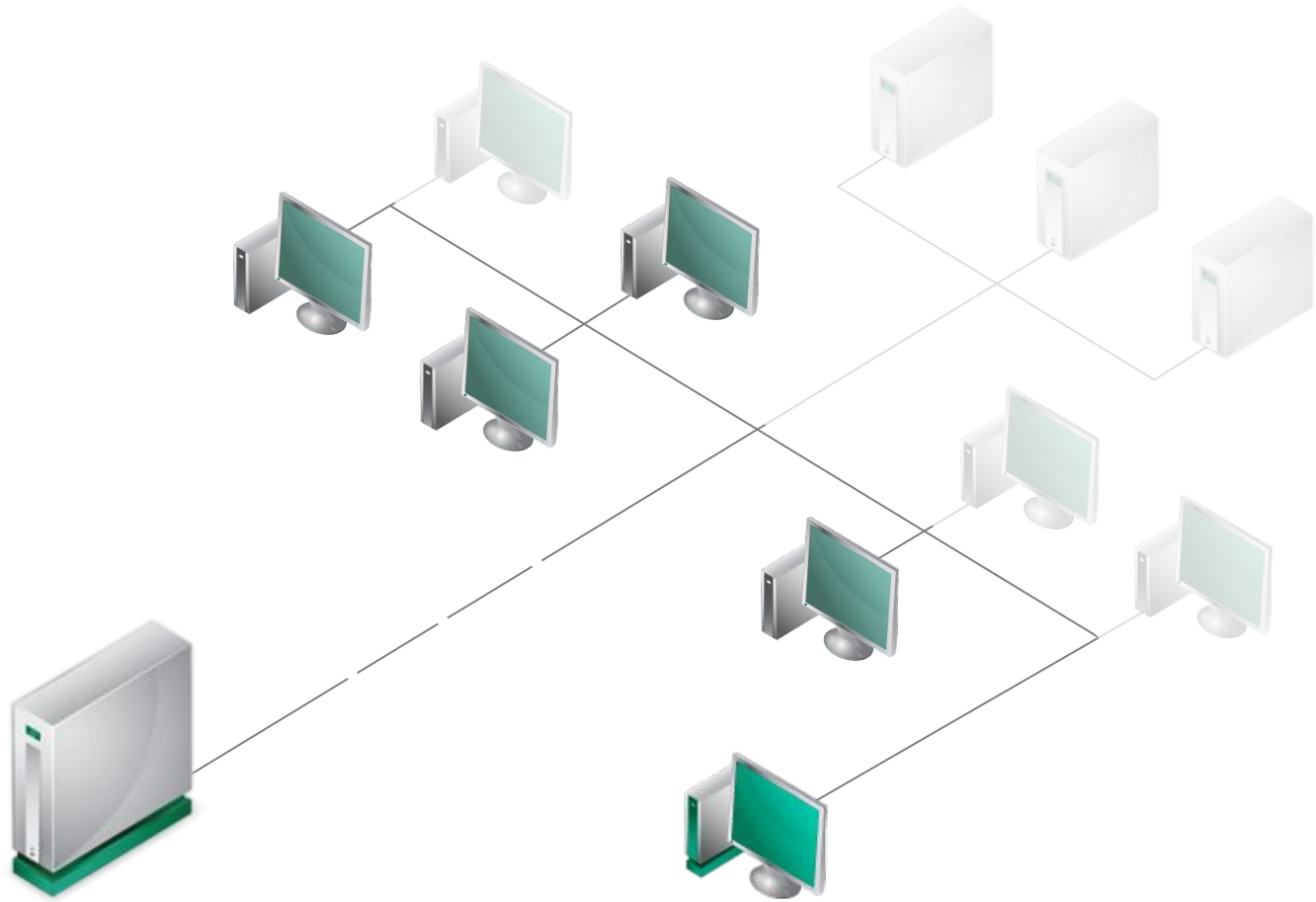
Как Kaspersky Security Center ищет компьютеры

Периодически (с разными периодами):

- Опрашивает сеть Microsoft
- Импортирует из Active Directory
- Сканирует IP-диапазоны (выключено по умолчанию)

Если Kaspersky Security Center не обнаруживает компьютер при опросе сети, установите на компьютер Агент администрирования:

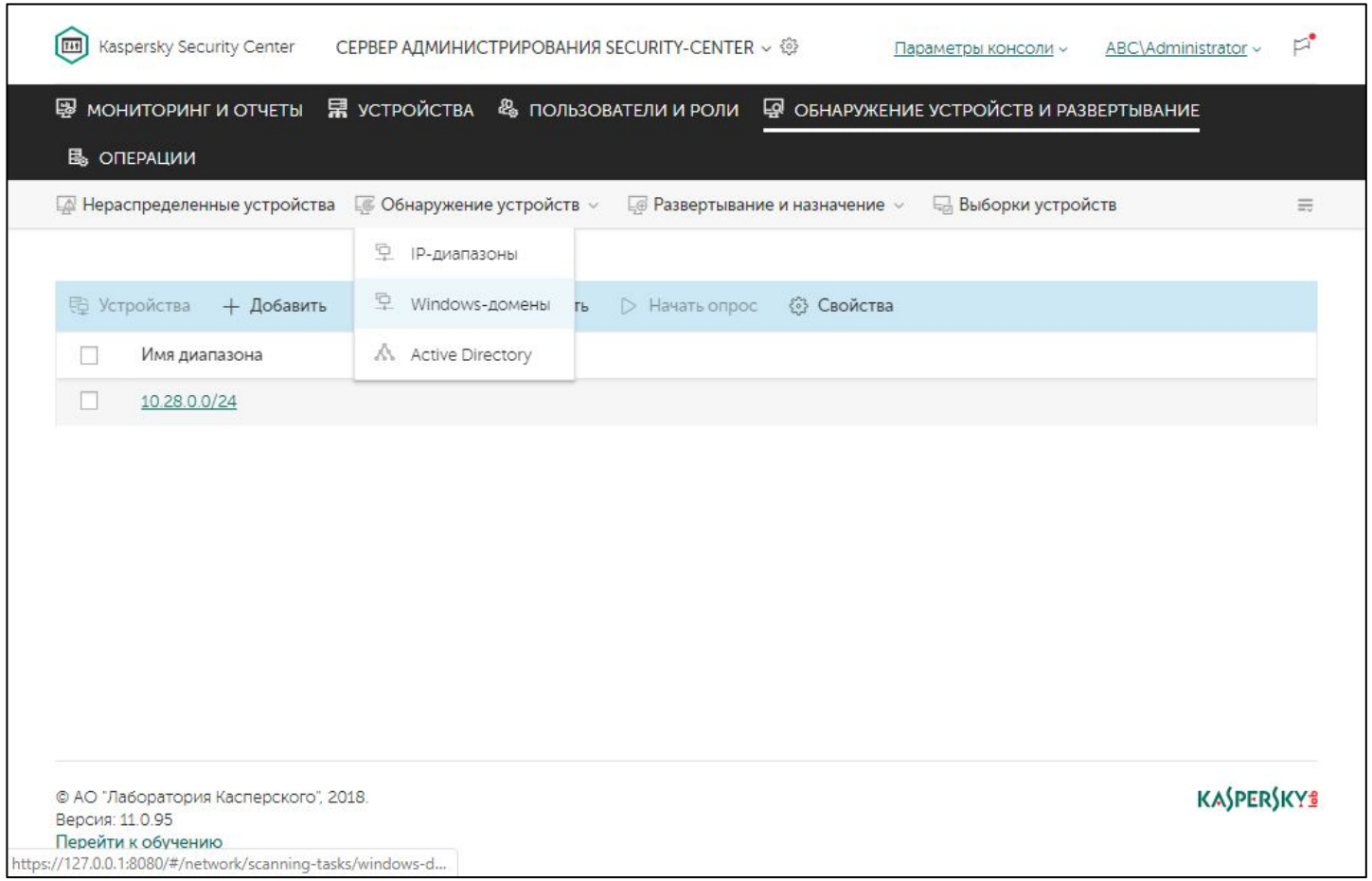
- Автономным пакетом
- Задачей (в задаче можно указать адреса не обнаруженных компьютеров)
- Любым другим способом



Сервер администрирования

Консоль администрирования

Опрос сети Windows



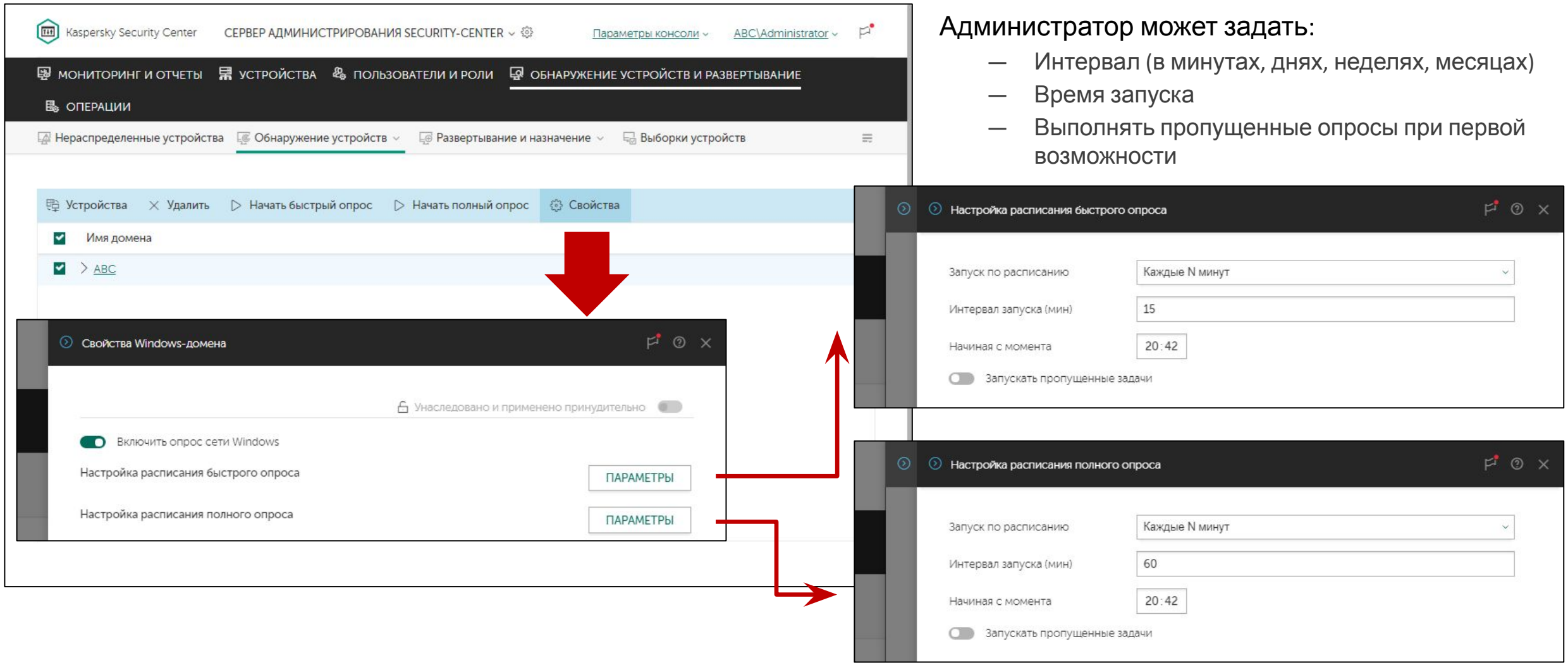
Быстрый опрос

- Работает через сетевое окружение в проводнике Windows (по умолчанию выключено в операционной системе)
- В результате получает список компьютеров в Windows-сети
- По умолчанию выполняется раз в 15 минут

Полный опрос

- Опрашивает компьютеры, обнаруженные во время быстрого опроса
- Пытается определить адреса, доменные имена и операционные системы компьютеров
- Генерирует трафик, пропорциональный количеству компьютеров
- По умолчанию выполняется раз в 60 минут

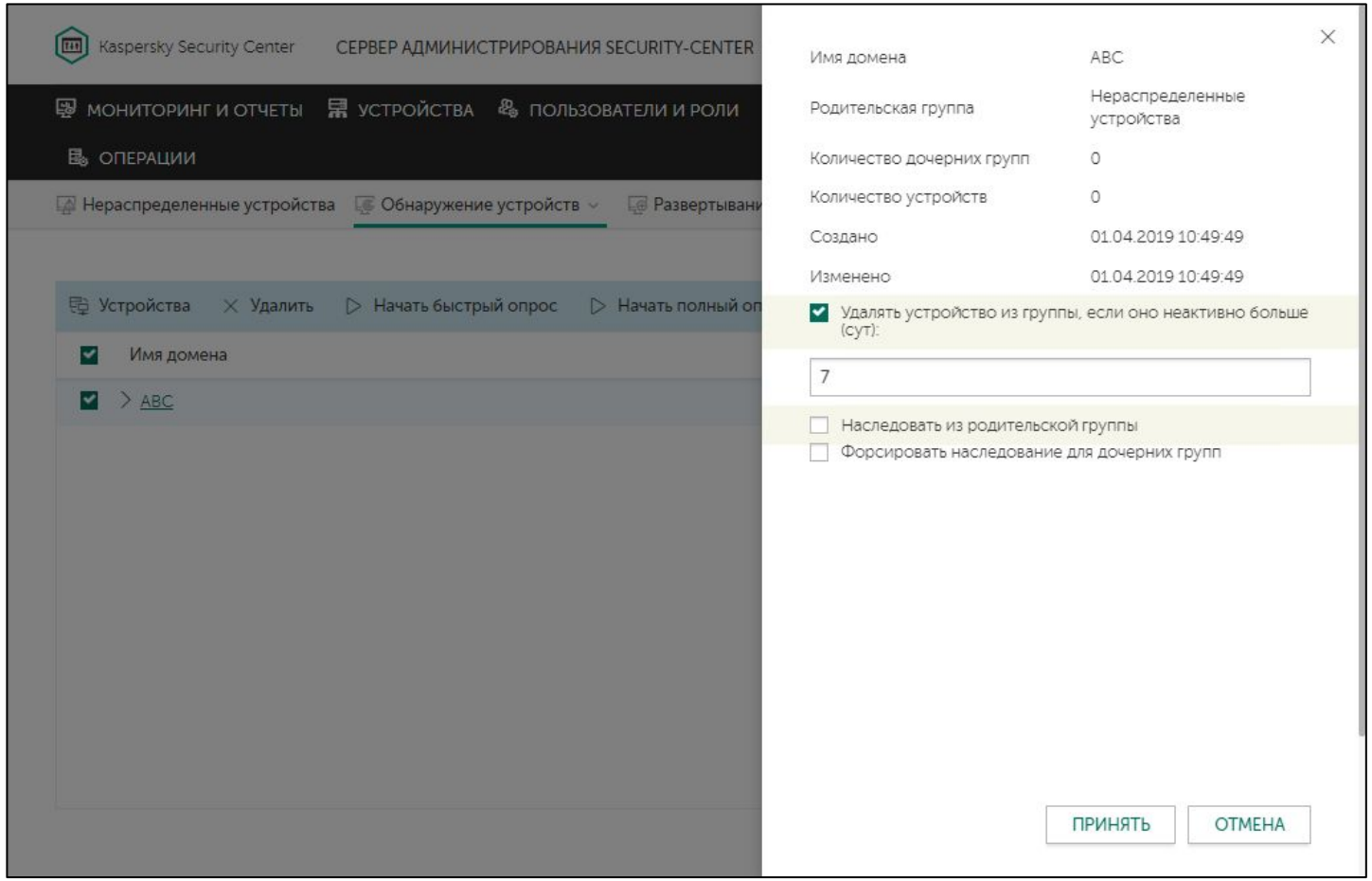
Параметры опроса сети Windows



Администратор может задать:

- Интервал (в минутах, днях, неделях, месяцах)
- Время запуска
- Выполнять пропущенные опросы при первой возможности

Время хранения информации о компьютерах

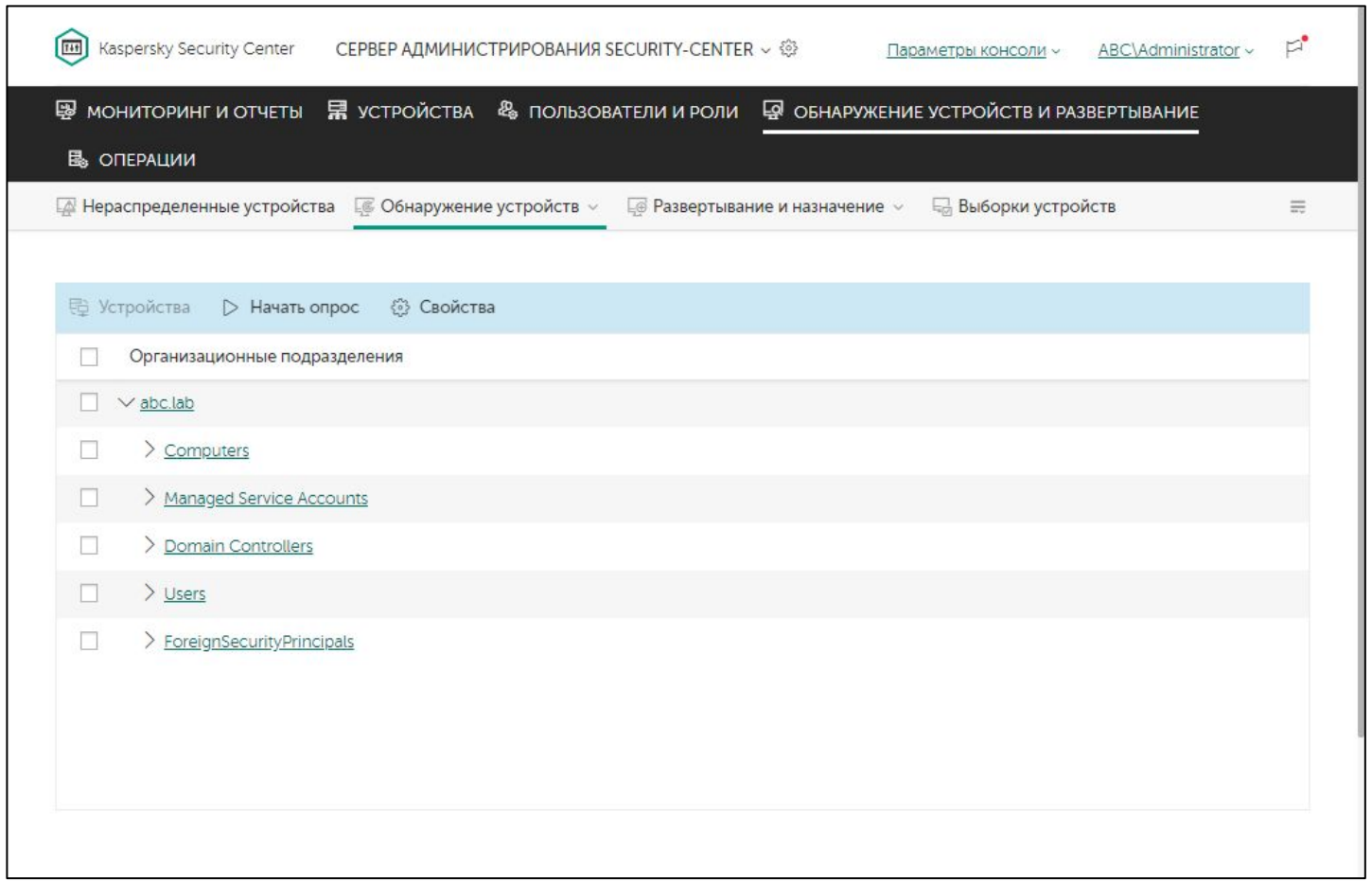


Компьютеры, которые давно не обнаруживались, автоматически удаляются из базы (по умолчанию, спустя 7 дней)

Домены и рабочие группы наследуют время хранения из настроек узла **Домены**

Администратор может указать разное время хранения для разных рабочих групп или доменов

Опрос Active Directory

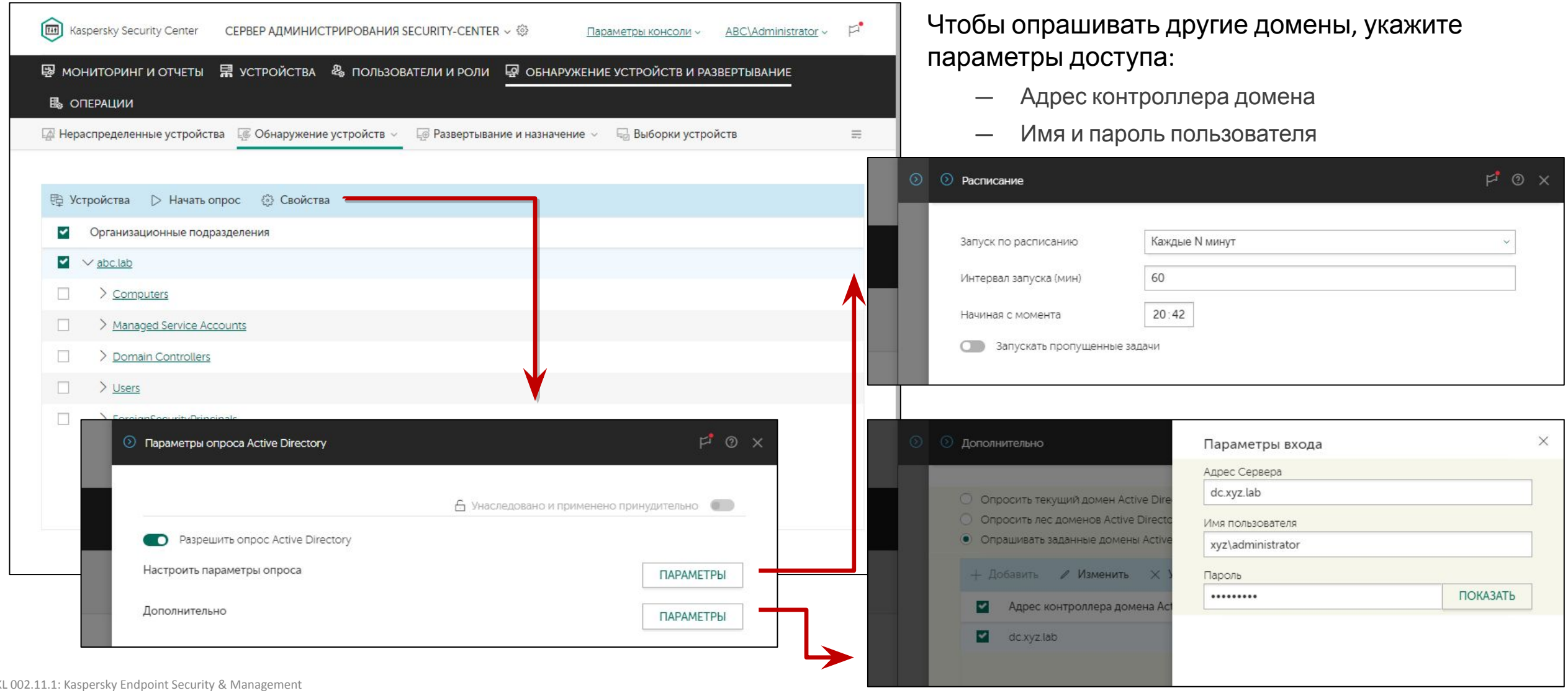


Запрашивает список компьютеров в Active Directory и отображает его в Консоли администрирования

Может опрашивать разные домены

По умолчанию выполняется раз в 60 минут

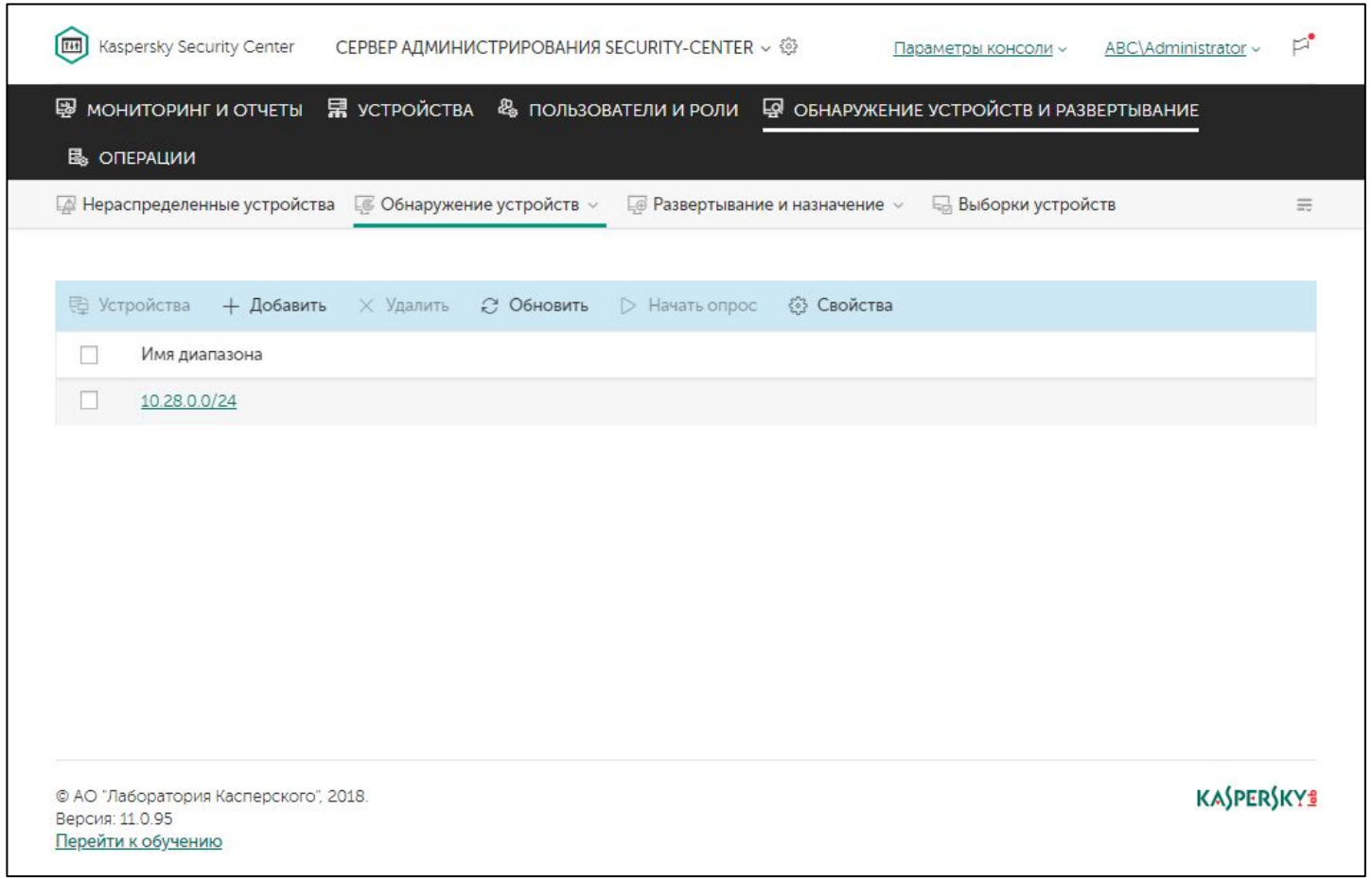
Параметры опроса Active Directory



Чтобы опрашивать другие домены, укажите параметры доступа:

- Адрес контроллера домена
- Имя и пароль пользователя

Опрос IP-диапазонов



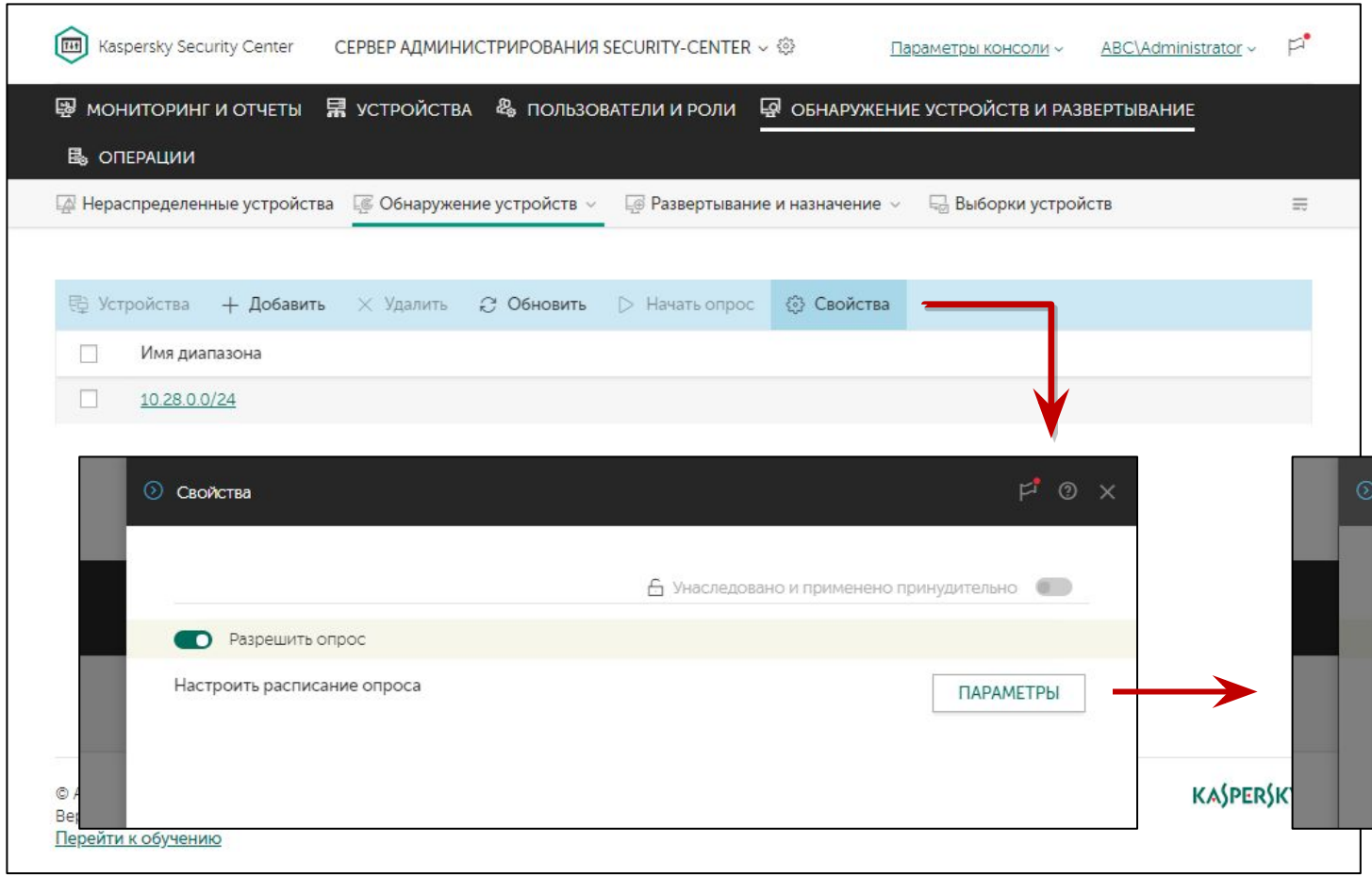
По умолчанию отключен

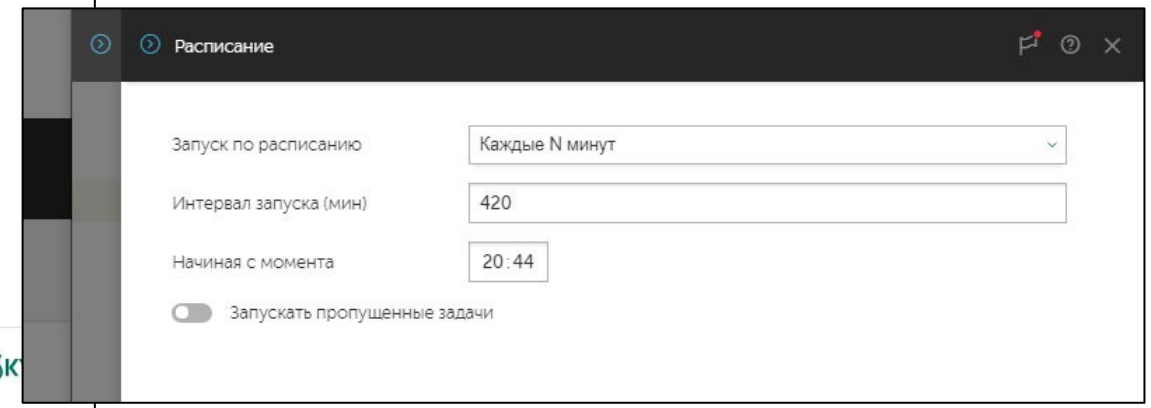
Использует ICMP (echo request), чтобы найти активные устройства

Игнорирует устройства, адреса которых не может разрешить в имена, чтобы не добавлять в результаты обнаружения маршрутизаторы, принтеры, камеры и пр.

Формирует список устройств, для которых удалось разрешить имя, сгруппированный по заданным IP-диапазонам

Опрос IP-диапазонов

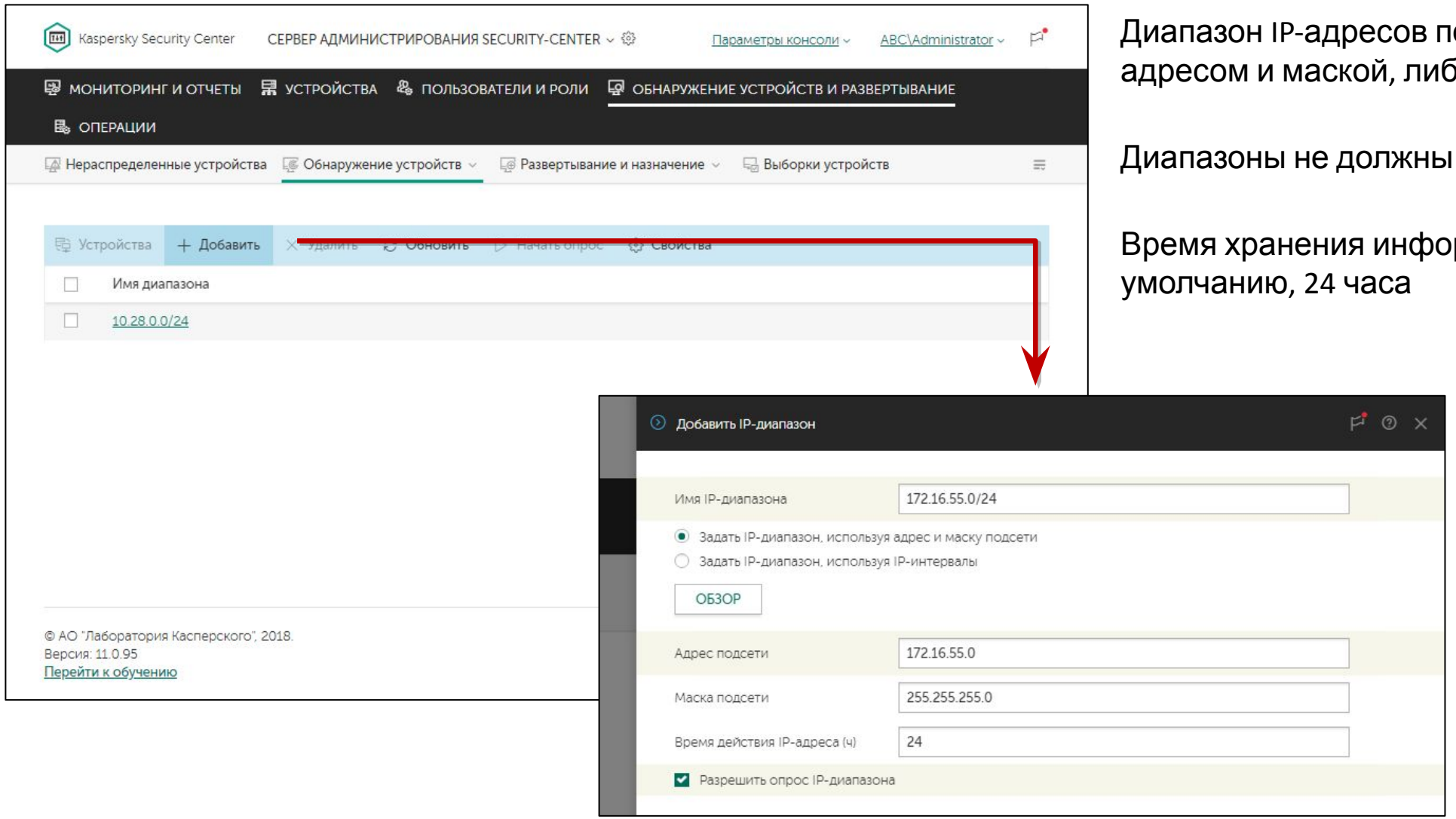




Период опроса IP-диапазонов по умолчанию равен 420 минутам (7 часам)

Чтобы опрашивать IP-диапазоны, включите этот тип опроса

Параметры опроса IP-диапазонов

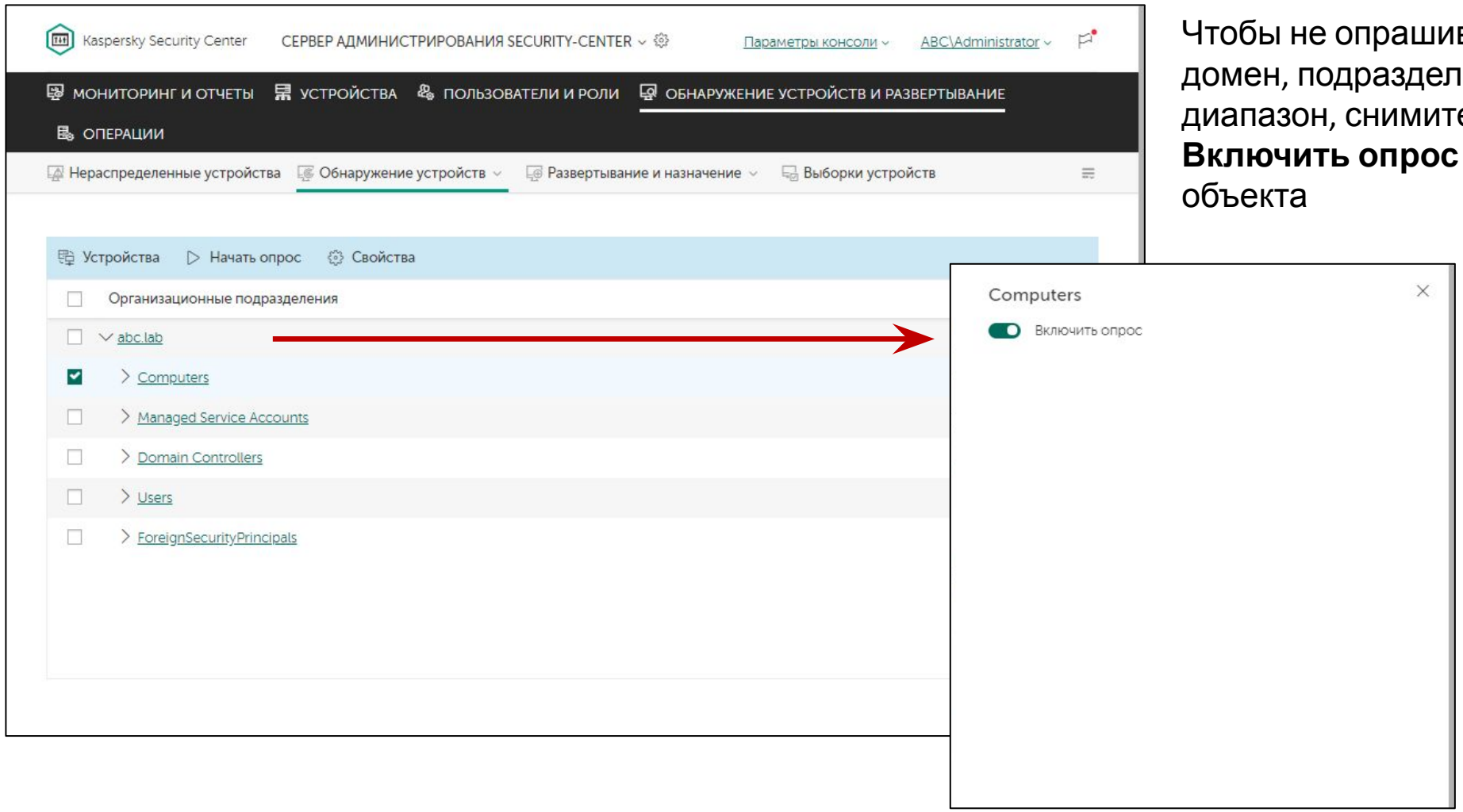


Диапазон IP-адресов подсети можно задавать адресом и маской, либо интервалом

Диапазоны не должны пересекаться

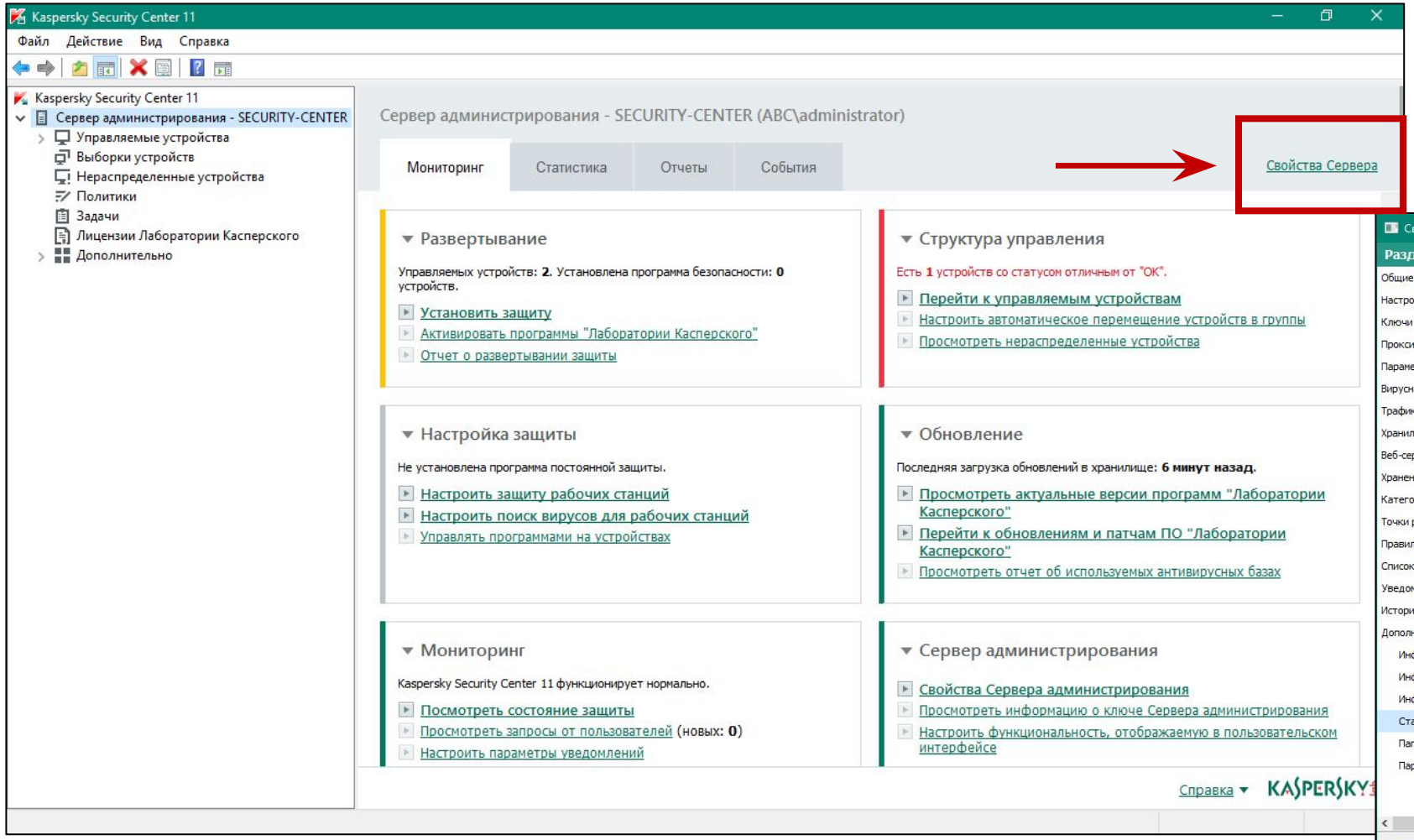
Время хранения информации об IP-адресах, по умолчанию, 24 часа

Опрос отдельных доменов, подразделений или диапазонов

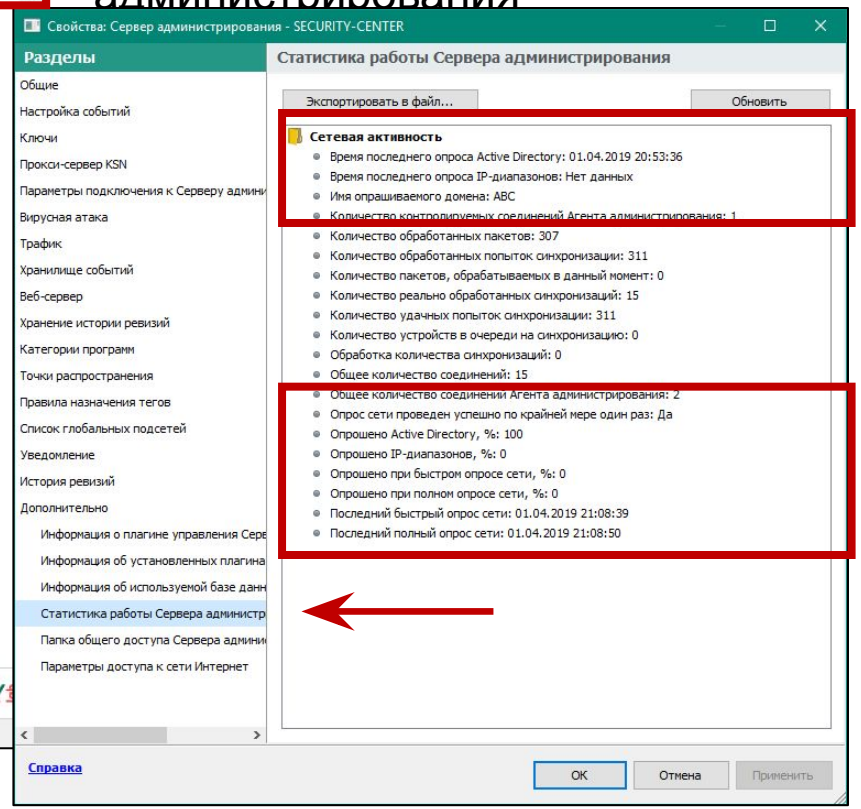


Чтобы не опрашивать отдельную рабочую группу, домен, подразделение Active Directory или IP-диапазон, снимите отметку с параметра **Включить опрос** в свойствах соответствующего объекта

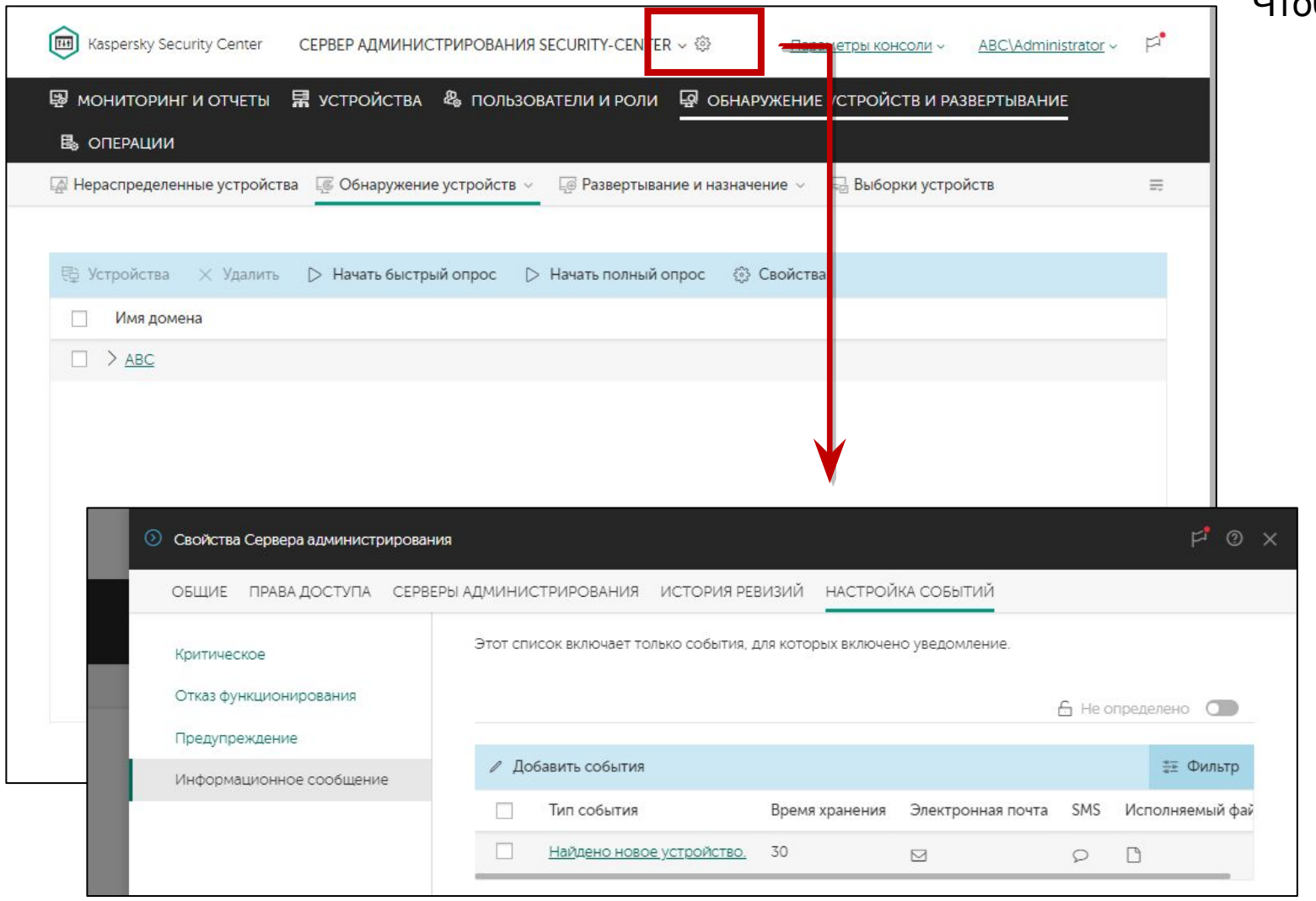
Информация о выполнении опроса сети



Время последнего опроса и прогресс текущего опроса можно найти только в MMC консоли в статистике работы Сервера администрирования

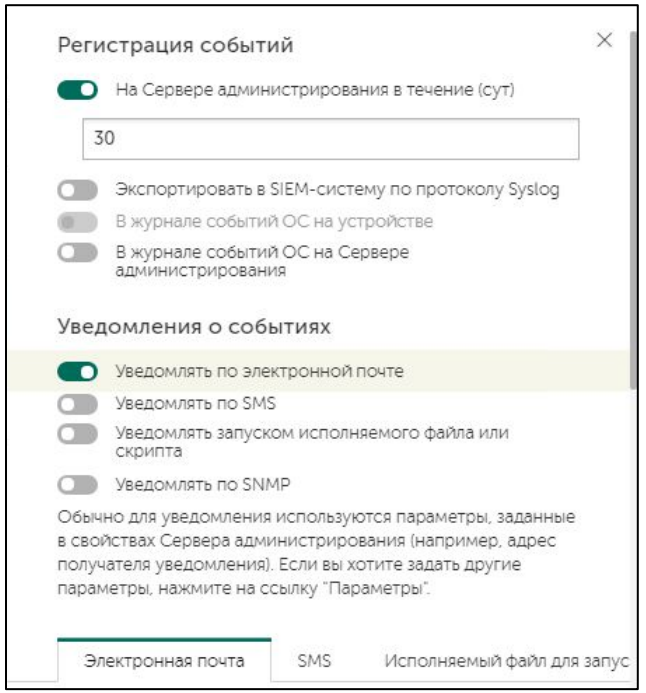


Уведомления о новых компьютерах



Чтобы узнавать о новых компьютерах в сети

- Используйте стандартную выборку устройств **Новые устройства в сети**
- Создайте выборку событий для события **Найдено новое устройство**
- Настройте уведомления для события **Найдено новое устройство**



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Как понять, что установка окончена

Как Сервер администрирования ищет компьютеры

Как создать или импортировать группы

Как автоматически распределить компьютеры по группам

Часть II. Управление защитой

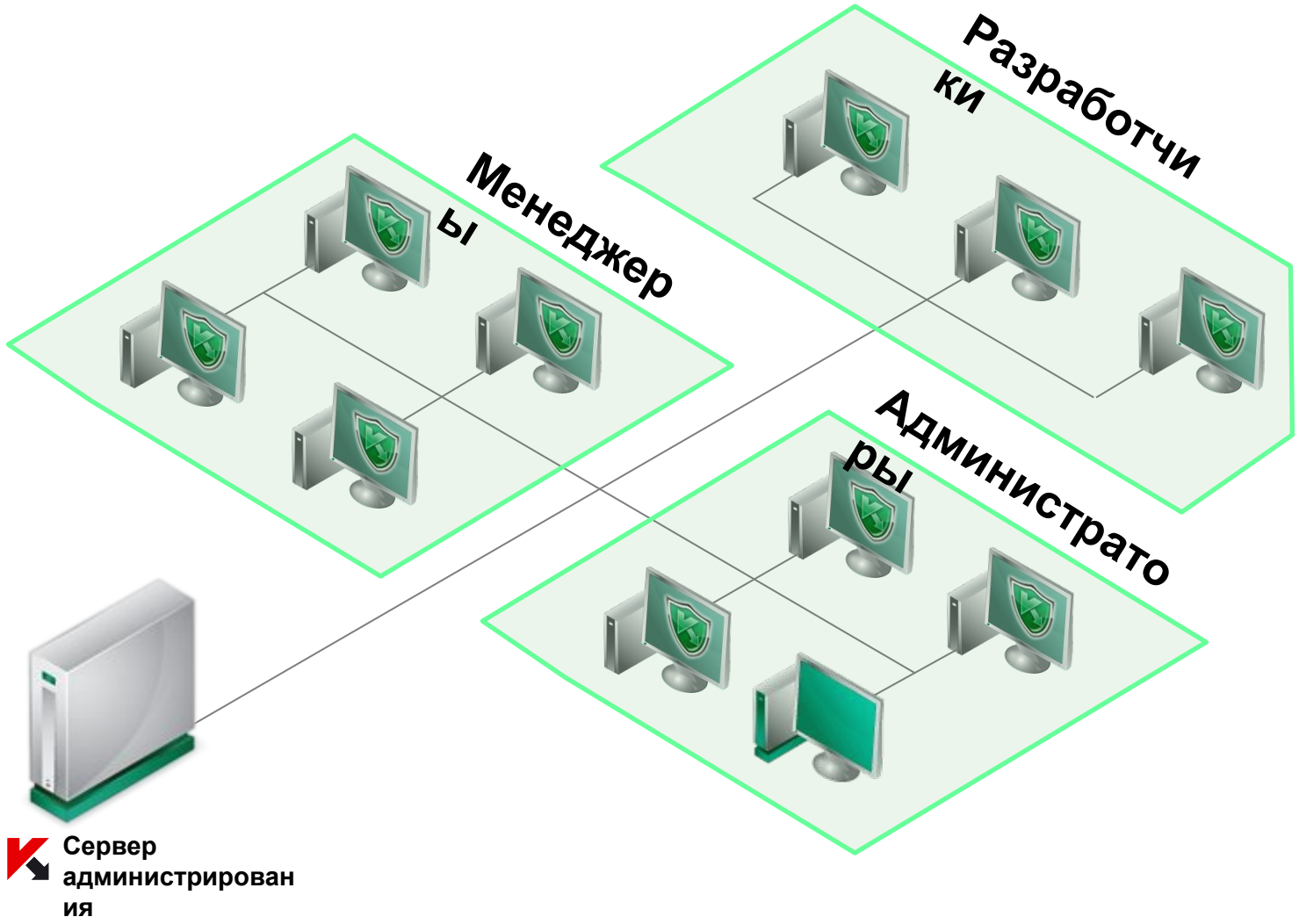
Часть III. Контроль

Часть IV. Сопровождение

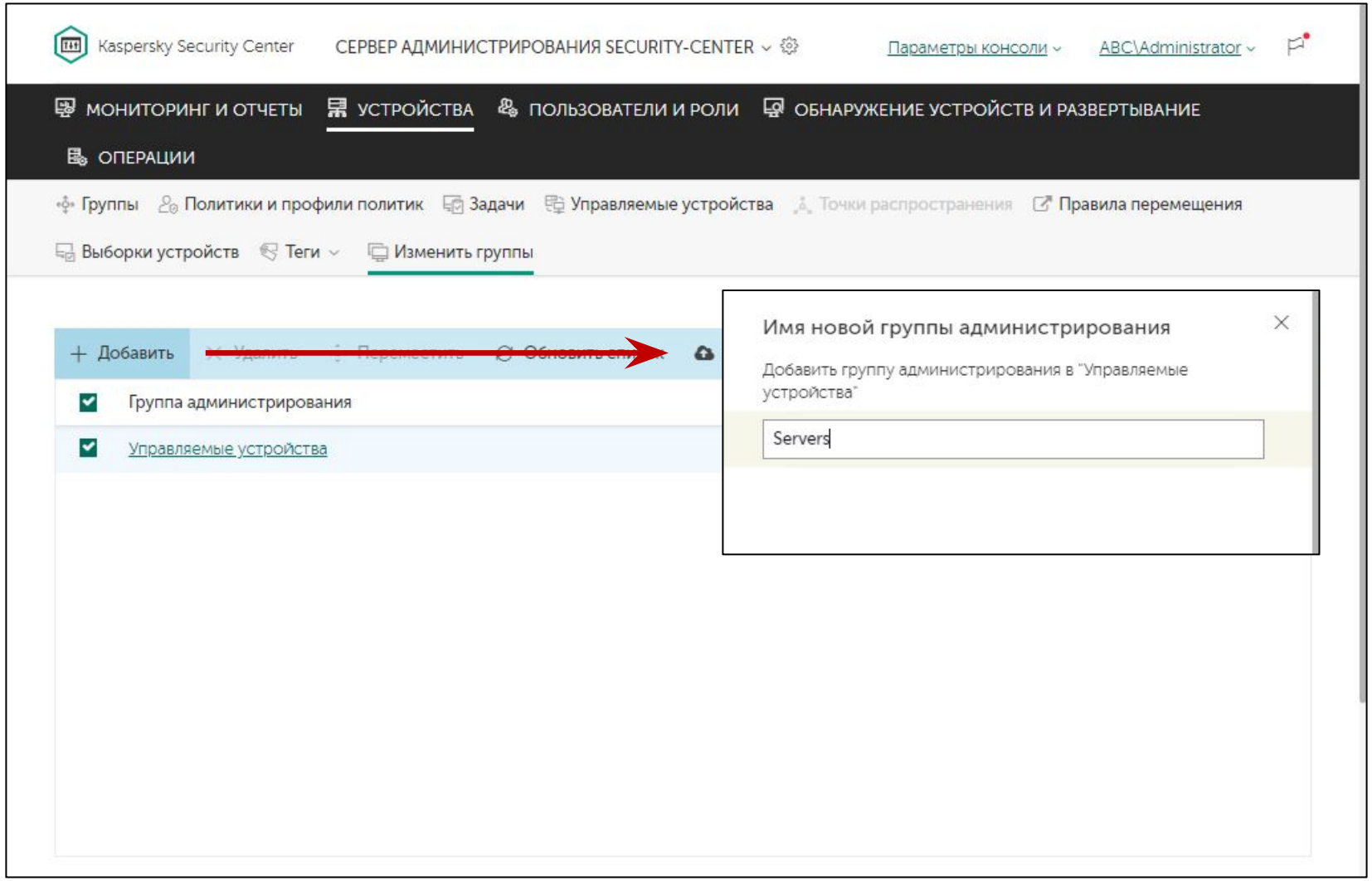
Мотивация для создания групп

Различия в настройках

- Компоненты
- Исключения
- Параметры контроля
- Расписание задач
- И другое



Создание групп

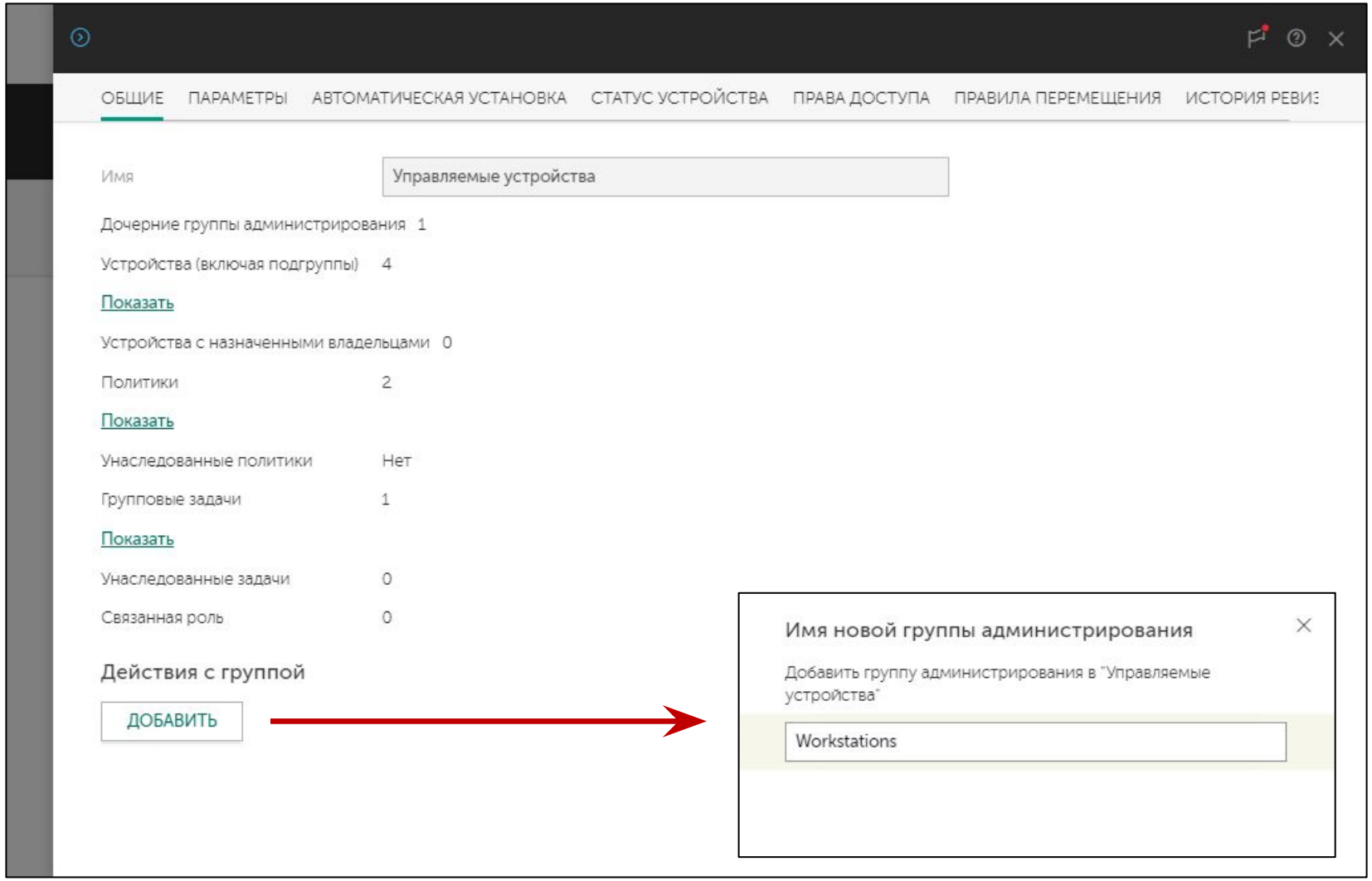


Создавайте группы в разделе **Устройства | Изменить группы**

Выберите на каком уровне создать подгруппу и нажмите **Добавить**

Ограничений на глубину вложенности нет

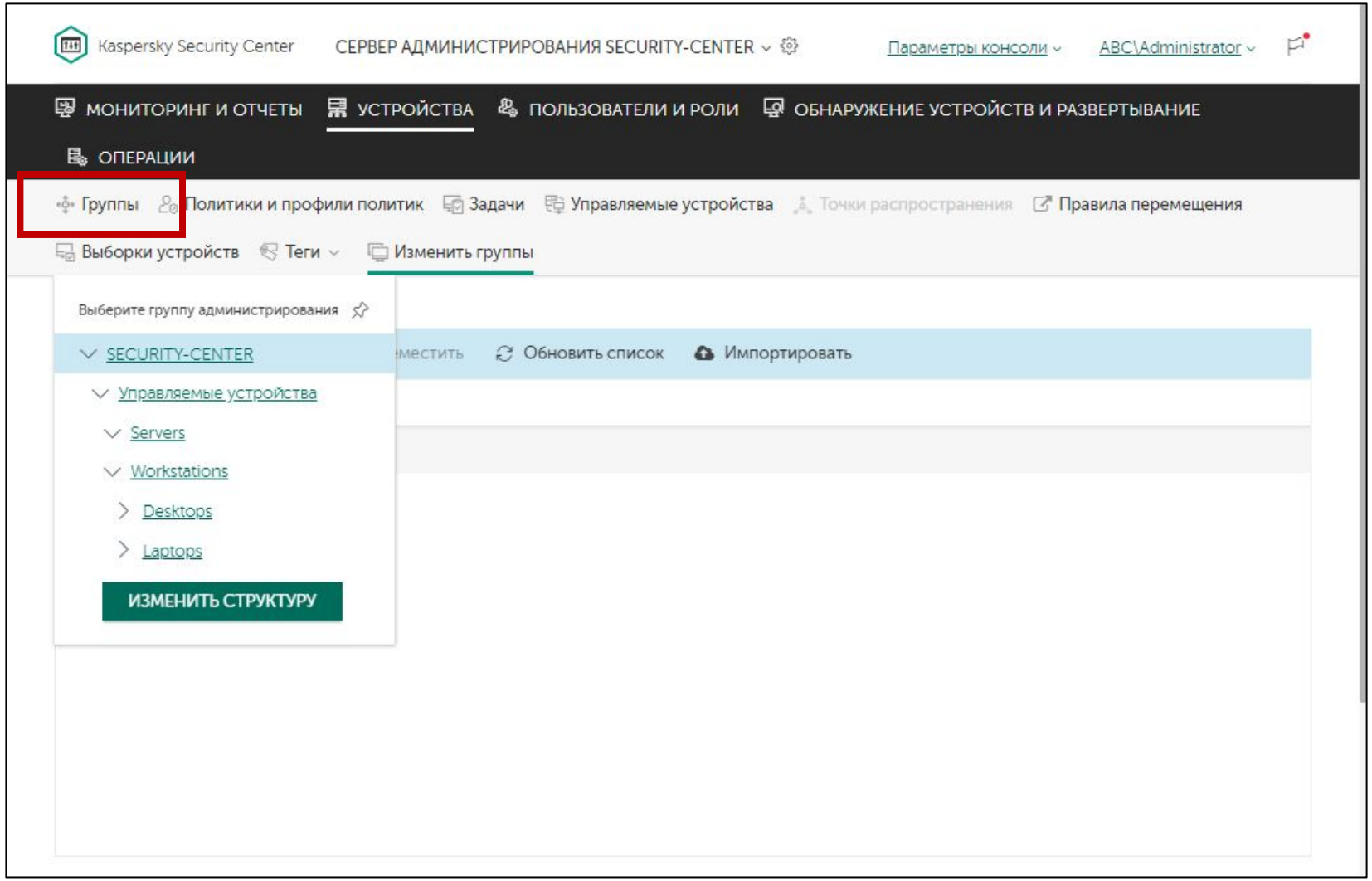
Создание групп



Также подгруппы можно создавать в свойствах группы

Откройте свойства и нажмите **Добавить**

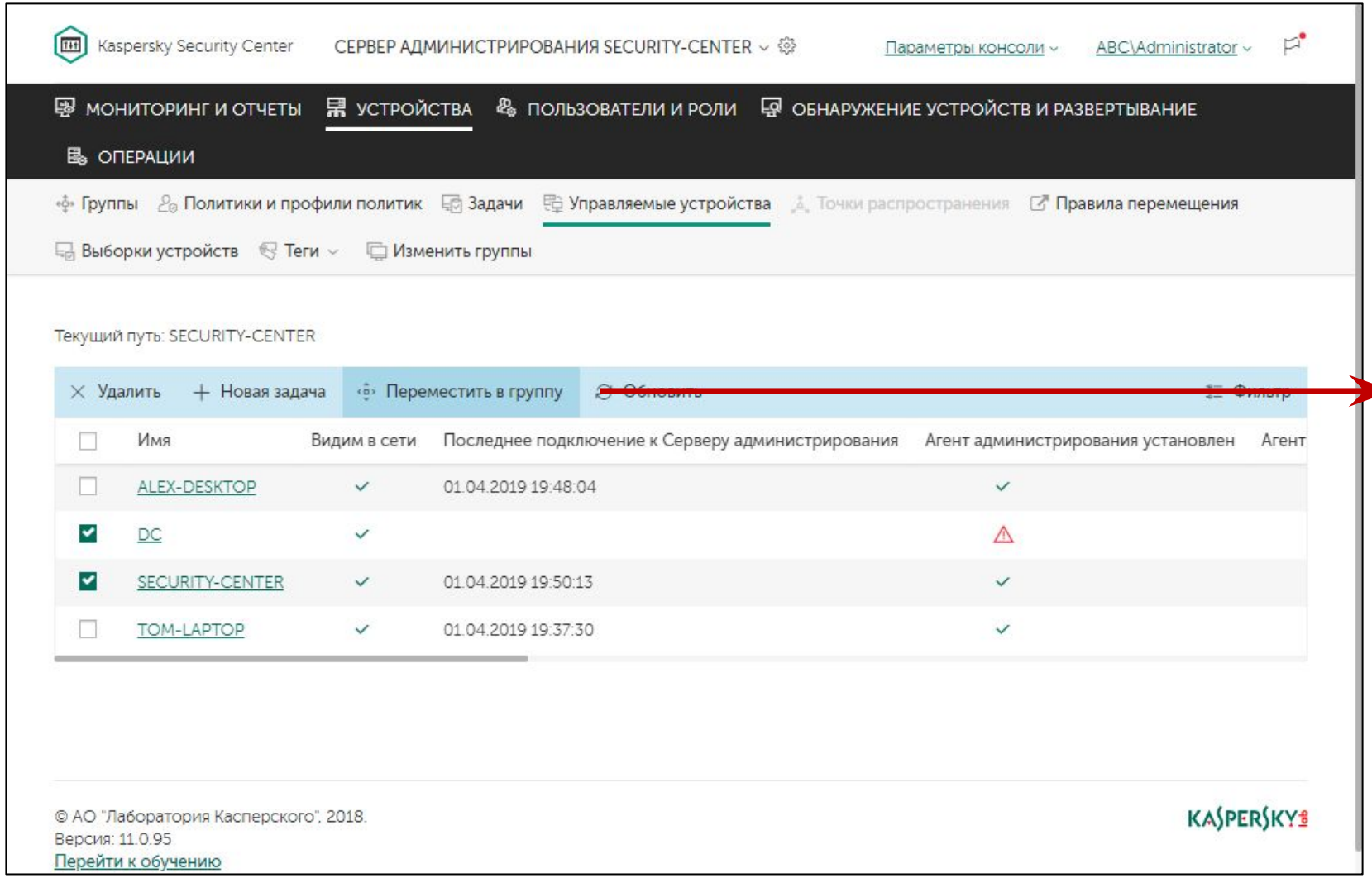
Навигация по структуре групп



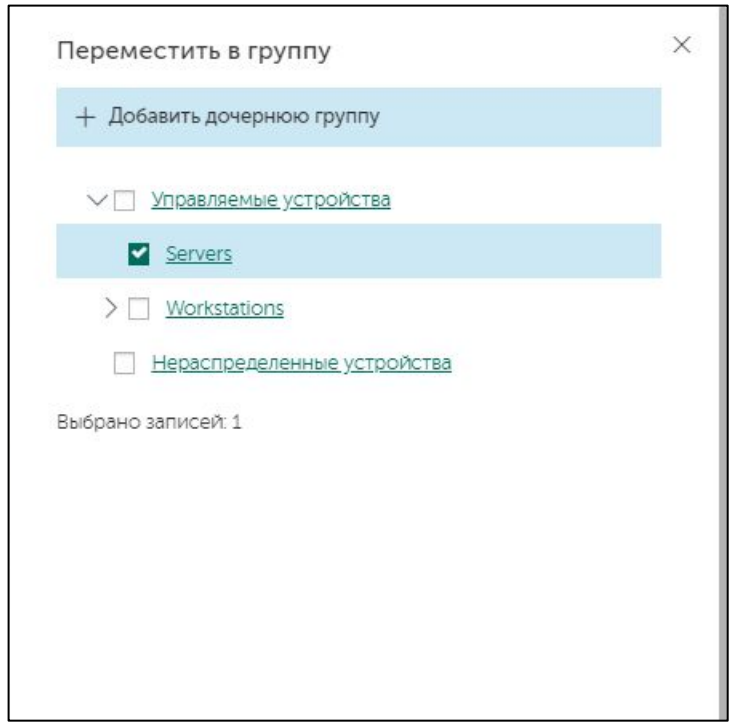
Для просмотра политик, задач, устройств используйте навигацию по группам –**Устройства | Группы**

Кнопка **Изменить структуру** перенаправляет на закладку **Изменить группы**

Добавление компьютеров в группу

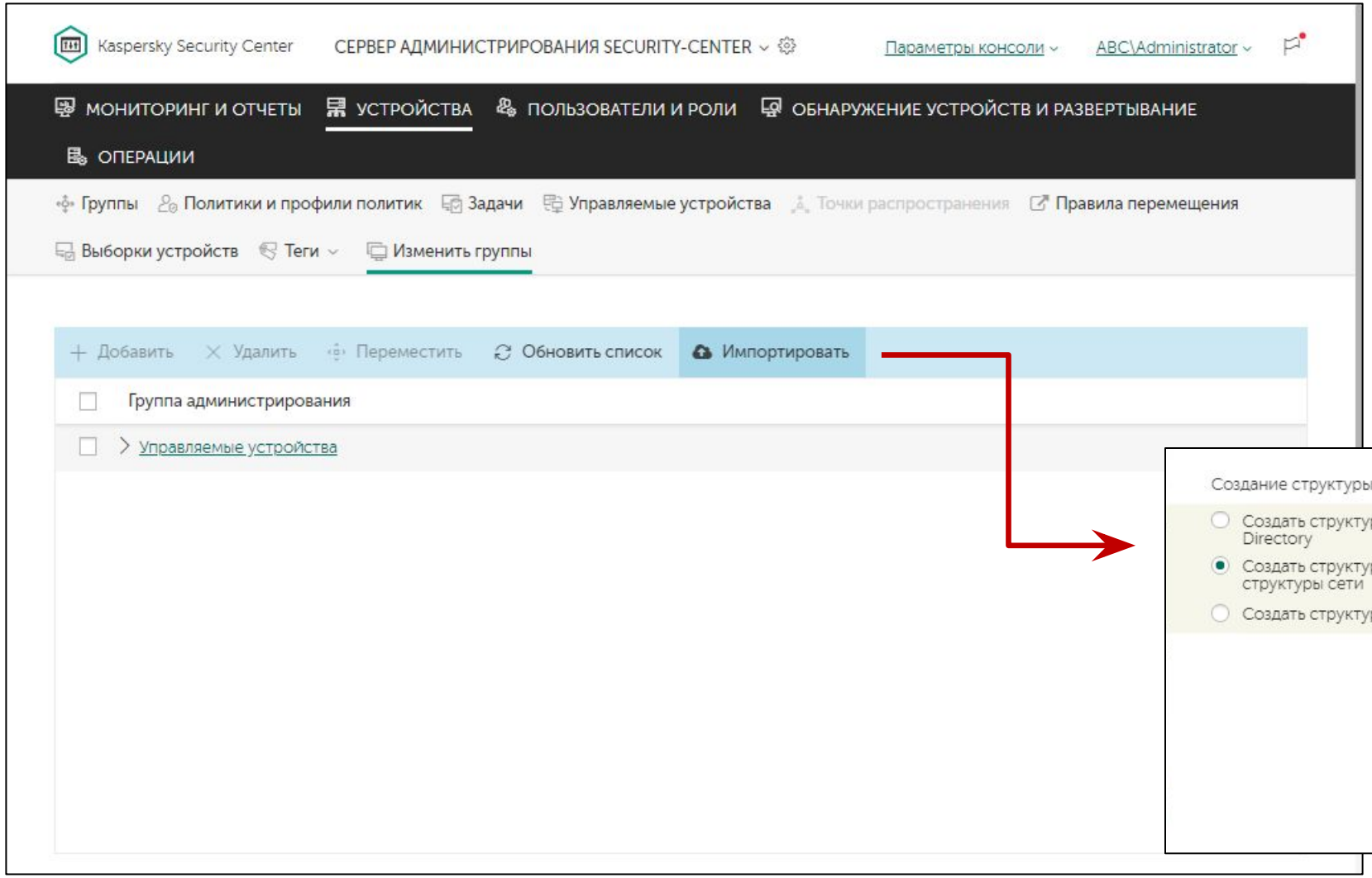


Выделите один или несколько компьютеров и используйте команду **Переместить в группу**



KASPERSKY

Импорт структуры групп

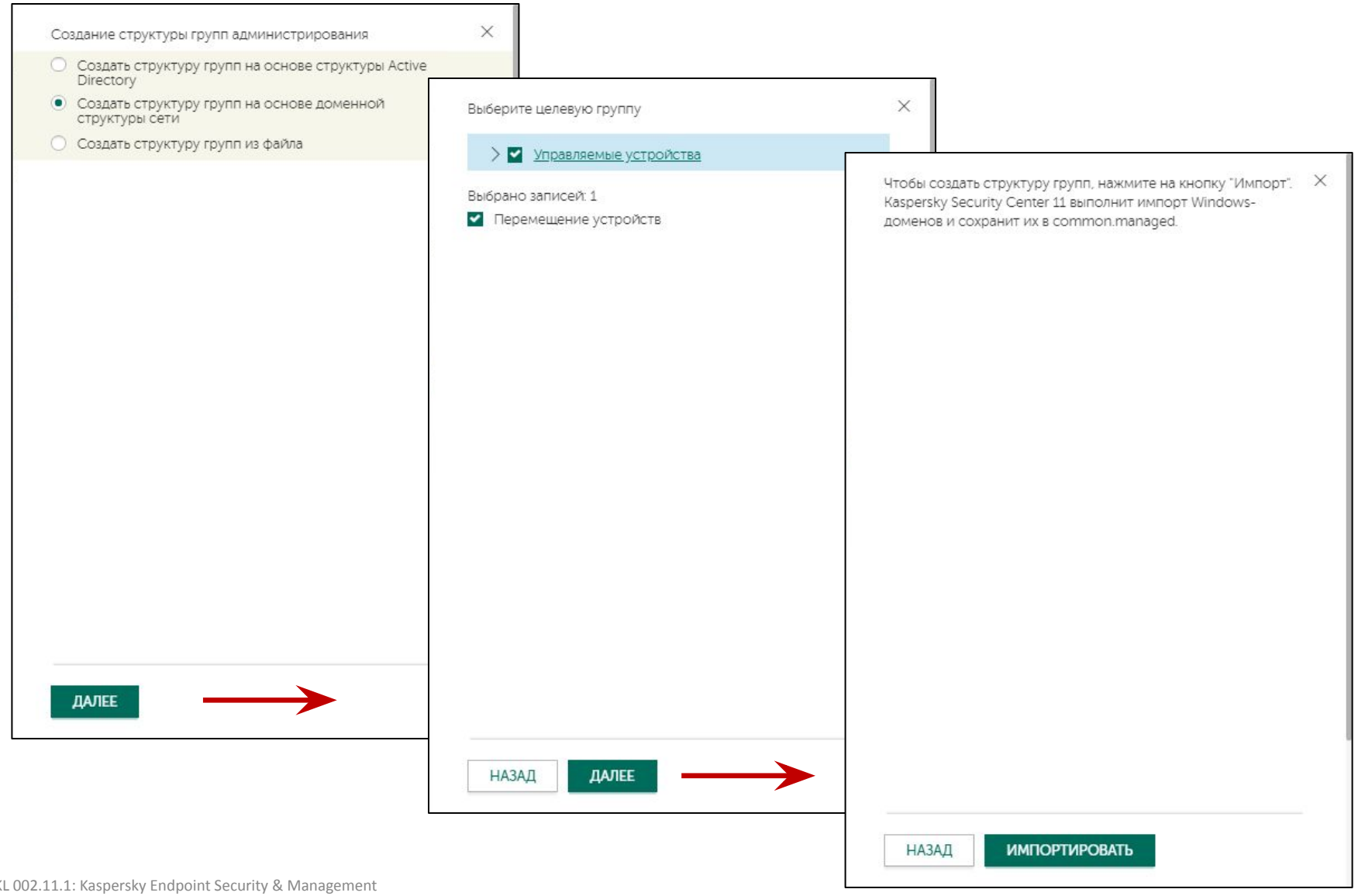


Вызовите мастер в разделе **Устройства | Изменить группы | Импортировать**

Мастер может импортировать группы и компьютеры из:

- Опрошенных доменов Active Directory
- Обнаруженных доменов и рабочих групп
- ла (только группы)

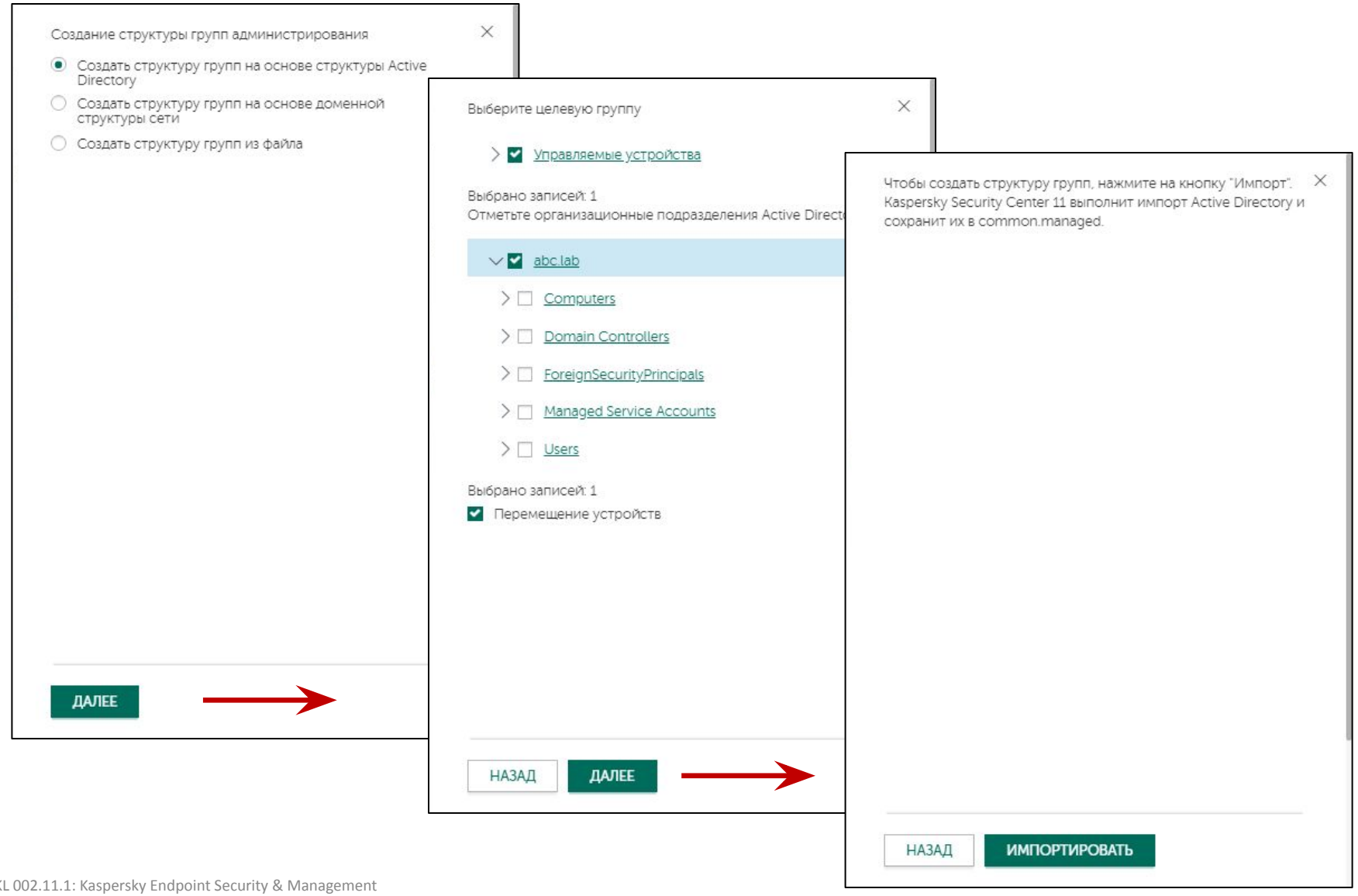
Импорт структуры Windows-сети



Группа назначения — можно импортировать в любую группу

Перемещать компьютеры — затрагивает только нераспределенные компьютеры

Импорт структуры Active Directory



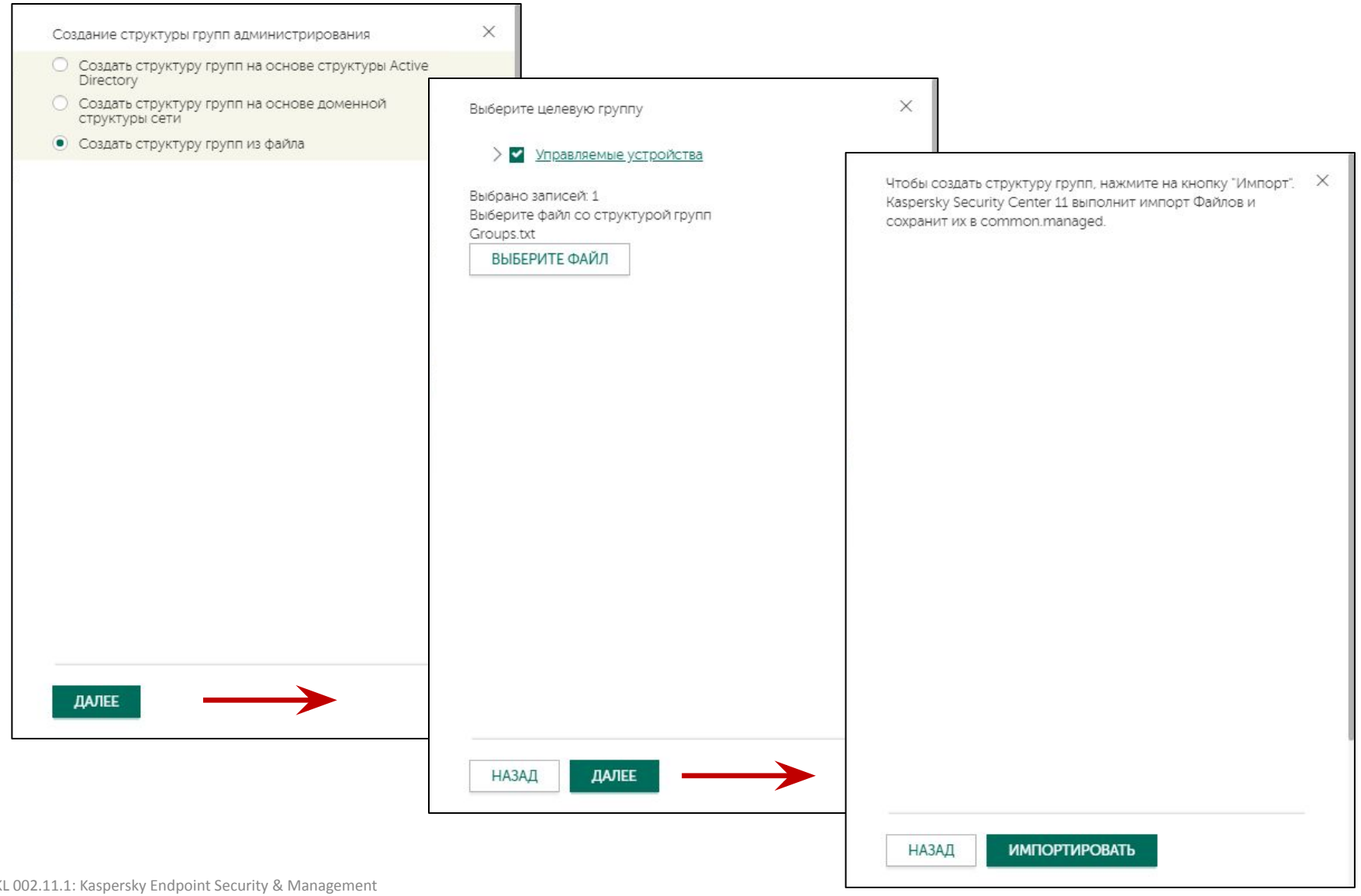
Группа назначения — можно импортировать в любую группу

Выберите подразделения, которые хотите импортировать из Active Directory

Мастер предназначен для одноразового импорта структуры Active Directory

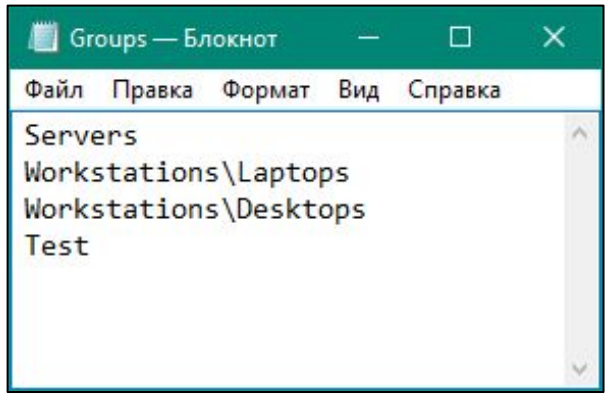
Чтобы постоянно поддерживать синхронизацию групп со структурой Active Directory, настройте правила перемещения компьютеров

Импорт структуры групп из файла



Файл должен содержать все группы и подгруппы, одна подгруппа в строке

Подгруппы должны быть разделены символом «\»



Введение

Часть I. Внедрение

Глава 1. Как установить Kaspersky Endpoint Security для бизнеса

Глава 2. Как установить Kaspersky Security Center

Глава 3. Как установить Kaspersky Endpoint Security на компьютеры

Глава 4. Как организовать компьютеры в группы

Часть II. Управление защитой

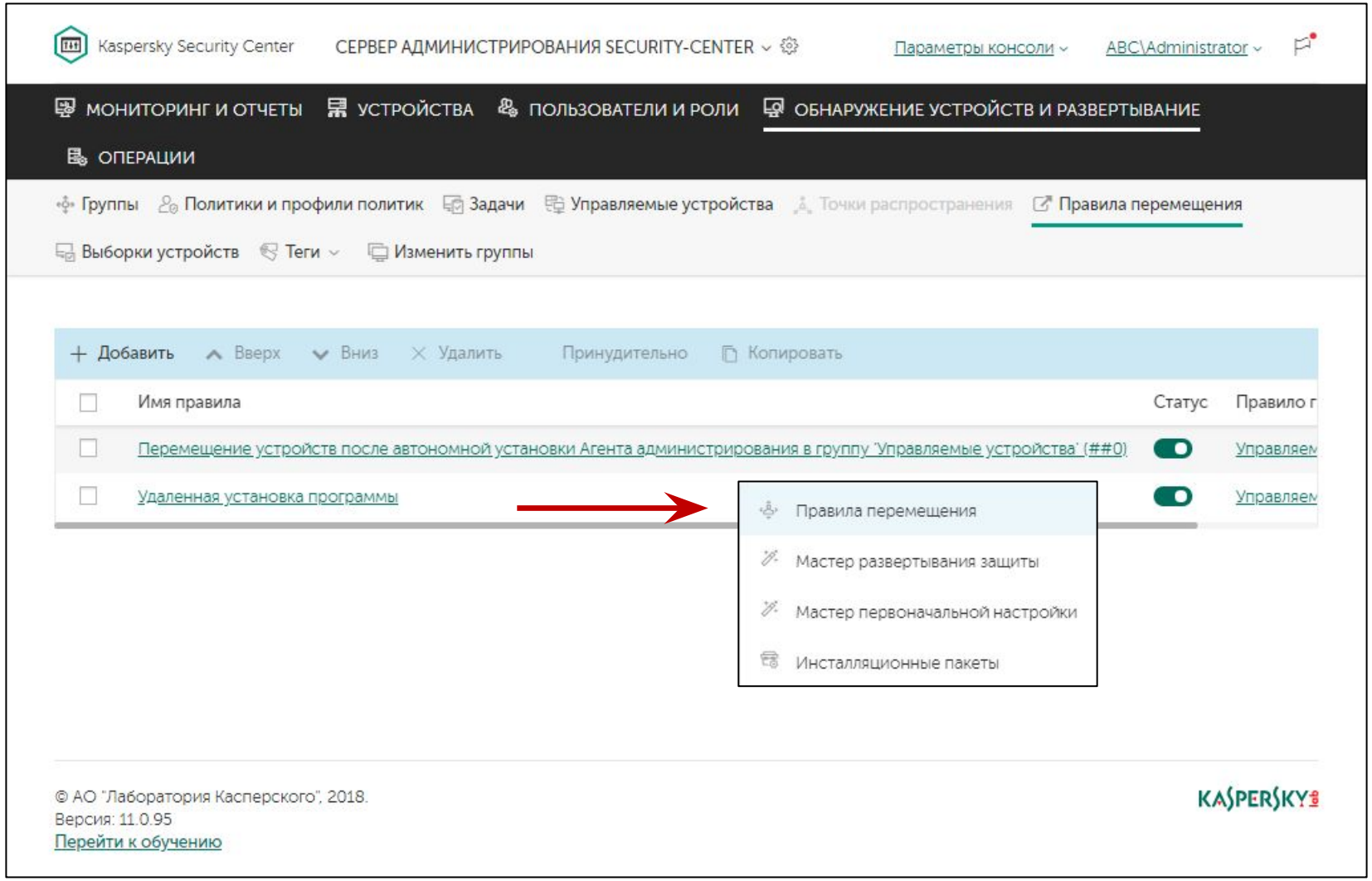
Часть III. Контроль

Часть IV. Сопровождение

Как понять, что установка окончена
Как Сервер администрирования ищет компьютеры
Как создать или импортировать группы

Как автоматически распределить компьютеры по группам

Правила перемещения компьютеров

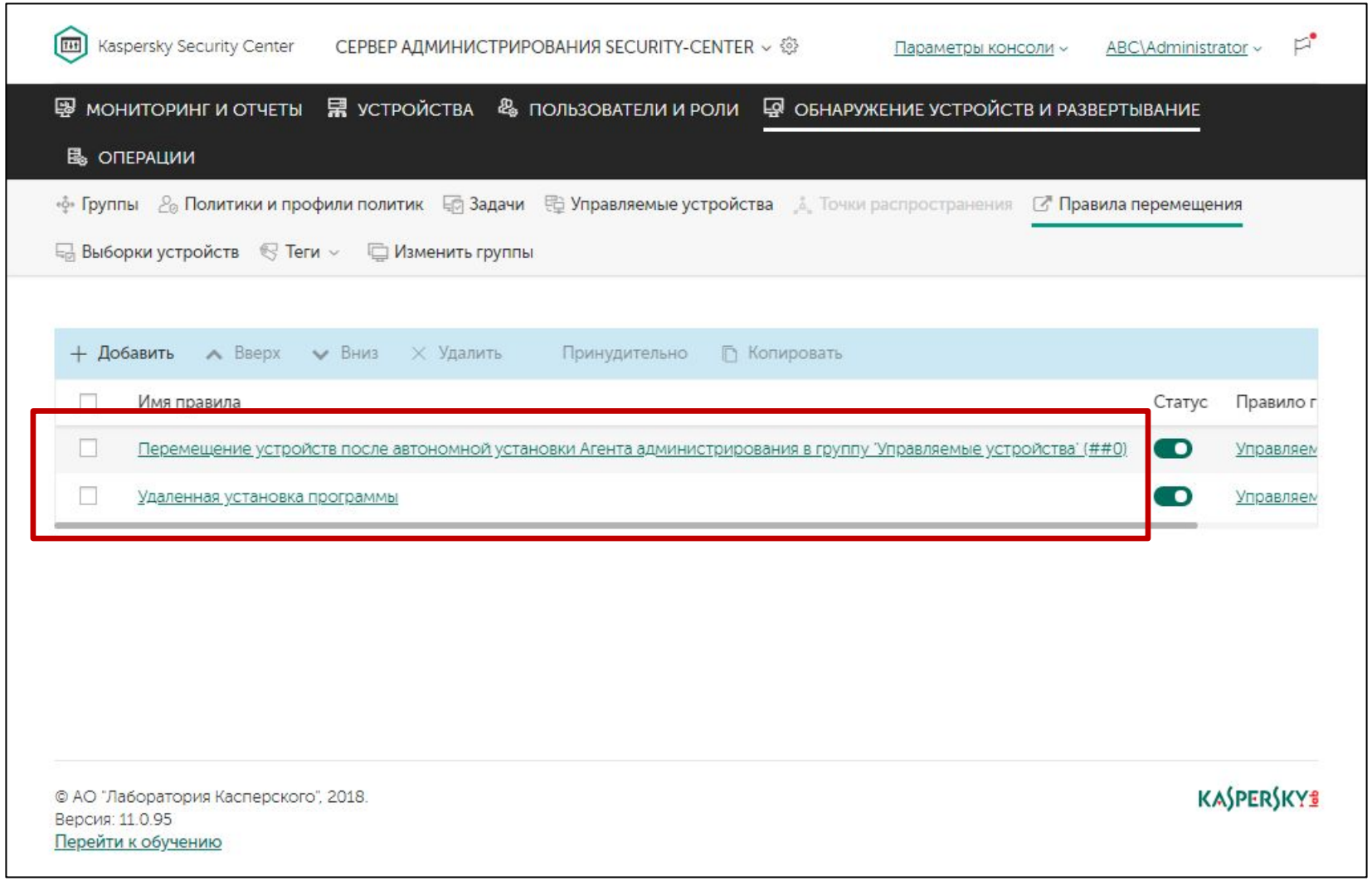


Автоматизируют помещение компьютеров в группы

Оперативно реагируют на изменения в расположении компьютеров

Позволяют организовать динамическое управление защитой компьютеров

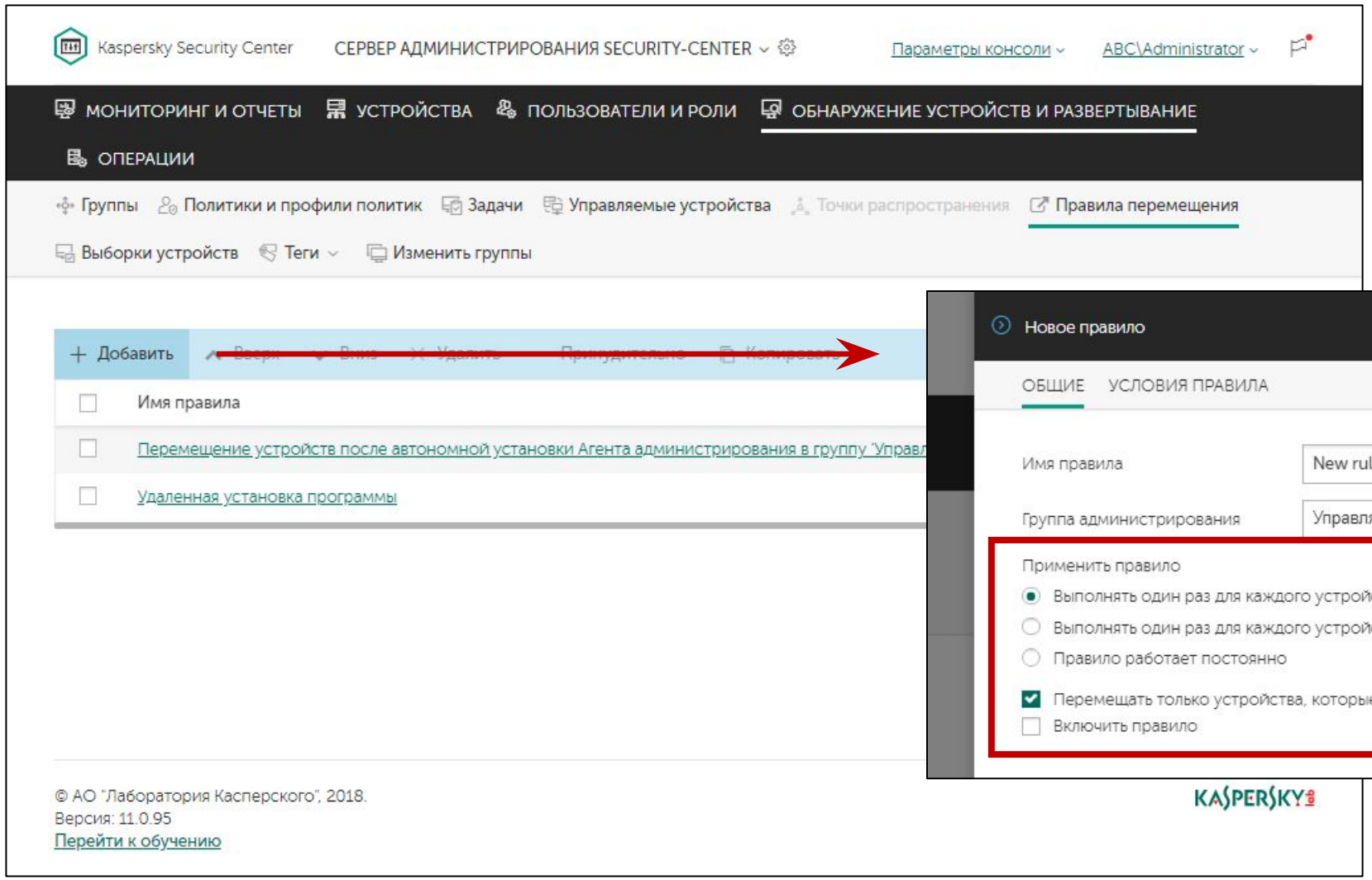
Правила перемещения компьютеров, созданные автоматически

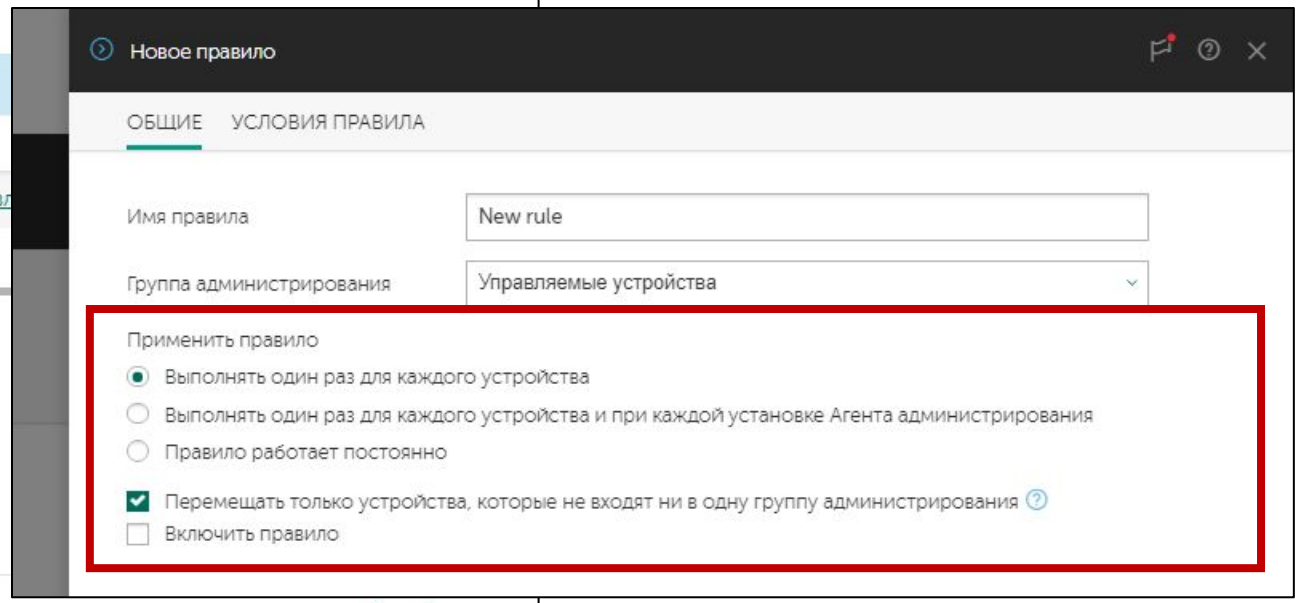


При настройке перемещения компьютеров в задаче установки или автономном пакете автоматически создаются правила перемещения

Их нельзя удалить, они пропадают при удалении создавшей их задачи или автономного пакета

Параметры правил перемещения

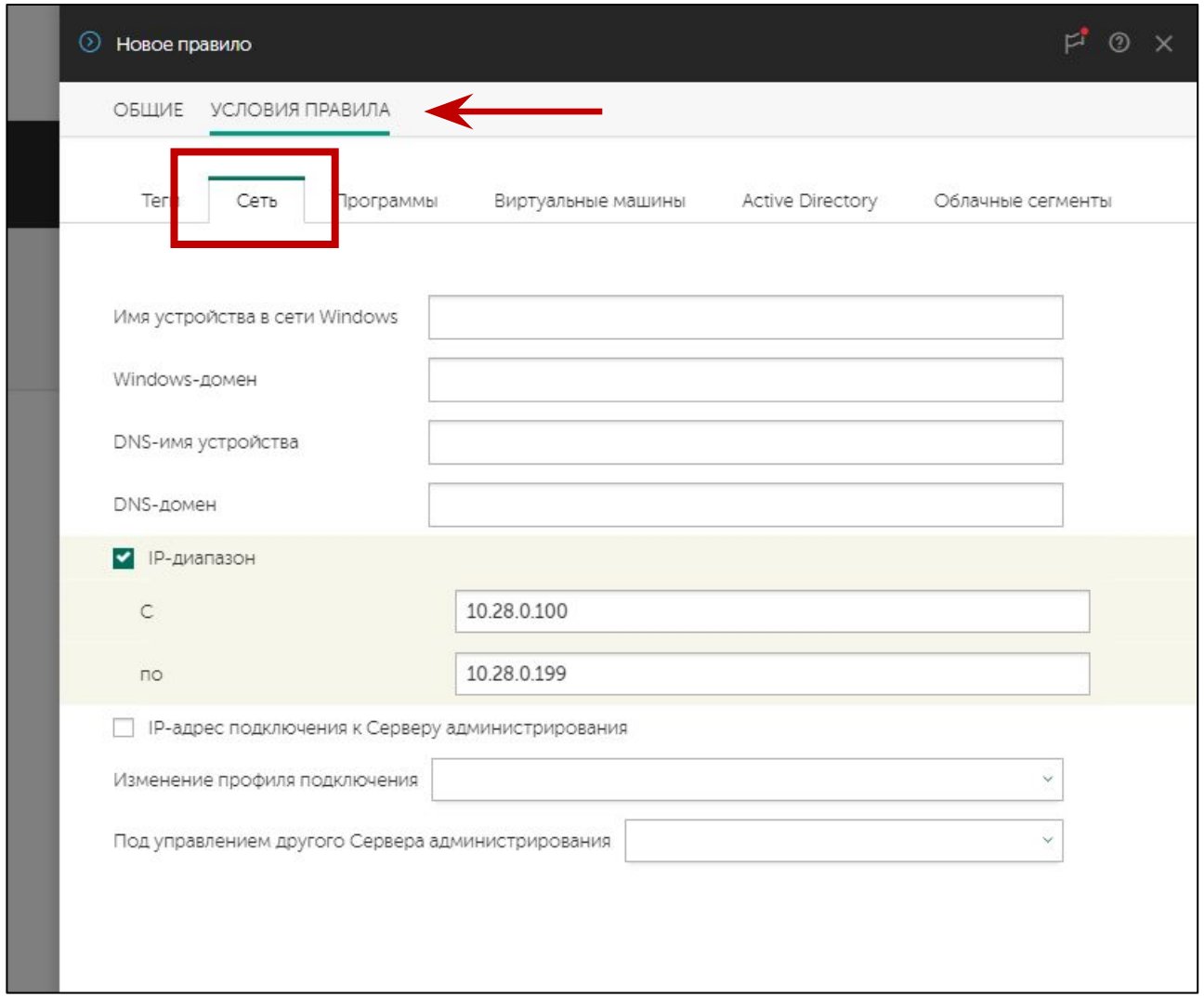




Параметры отвечают на три вопроса

- Что перемещать
- Куда перемещать
- Когда перемещать

Расположение в сети

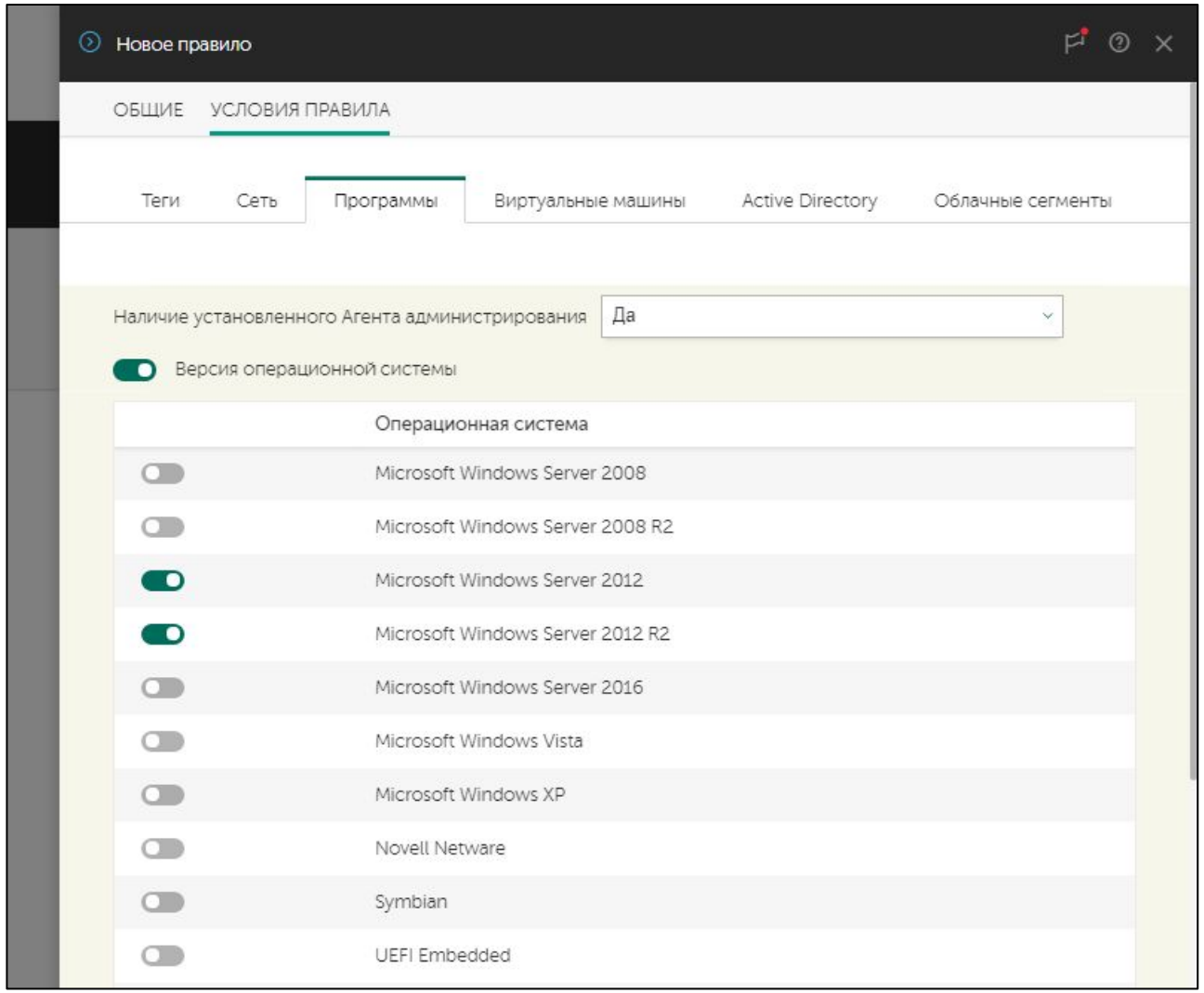


Используйте маски в имени компьютера, например, ***desktop**

В одном правиле можно указать только один IP-интервал (диапазон, домен и т. п.)

Чтобы переместить в одну группу компьютеры из нескольких подсетей, создайте несколько правил

Операционная система



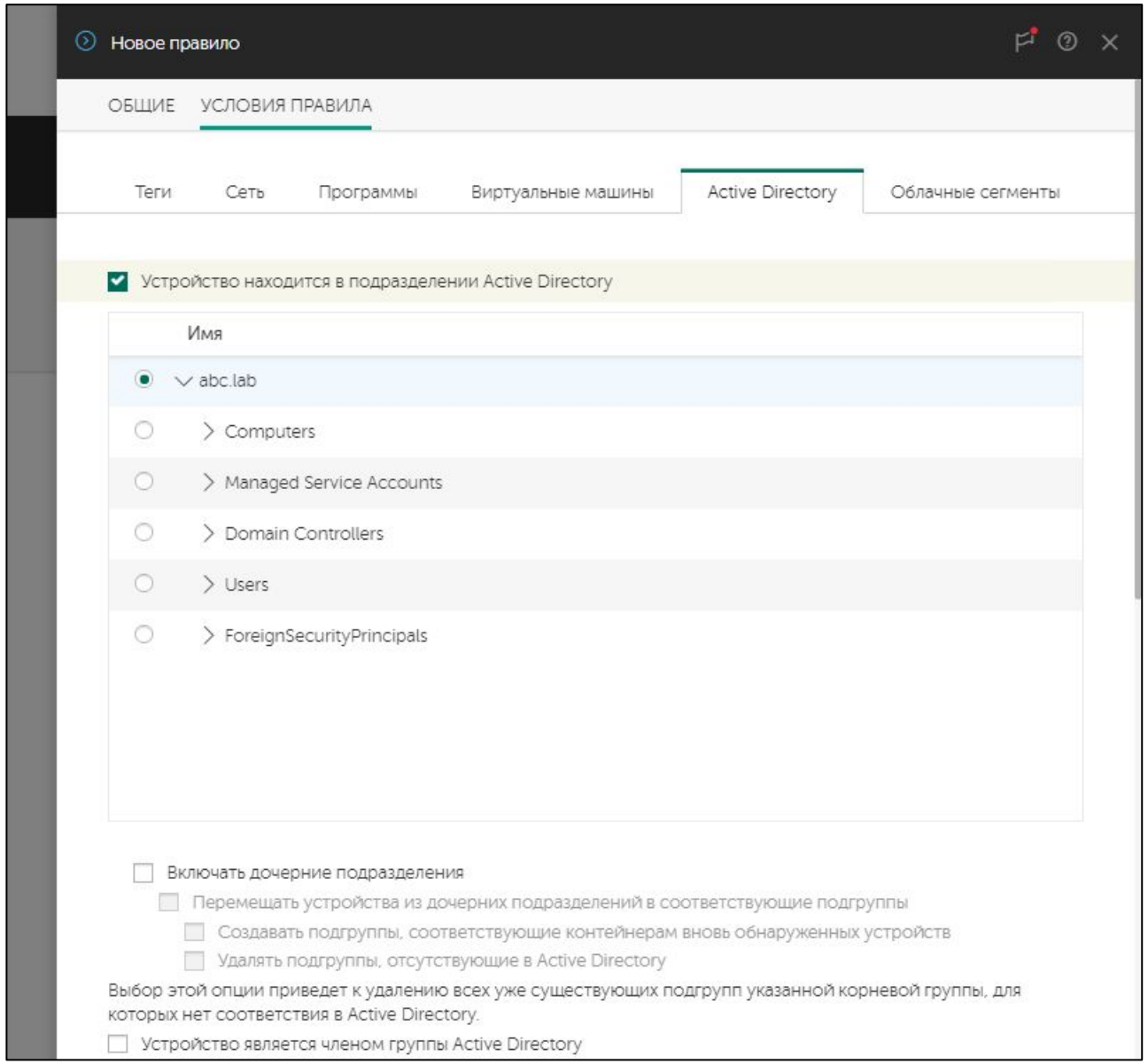
Наличие работающего Агента администрирования позволяет перемещать только компьютеры с установленным Агентом (или только компьютеры без Агента)

Версия операционной системы позволяет перемещать компьютеры с известной операционной системой (*Microsoft Windows Server 2012 R2*) или типом операционной системы (*<Microsoft Windows>*, *<Linux>* и т.п.)

- **Архитектура операционной системы** позволяет уточнить разрядность операционной системы (x86, AMD64, IA64, неизвестно)
- **Версия пакета обновления операционной системы** уточняет версию пакета исправлений операционной системы

Пользовательский сертификат позволяет перемещать устройства, на которых установлен сертификат для взаимной аутентификации с Сервером администрирования

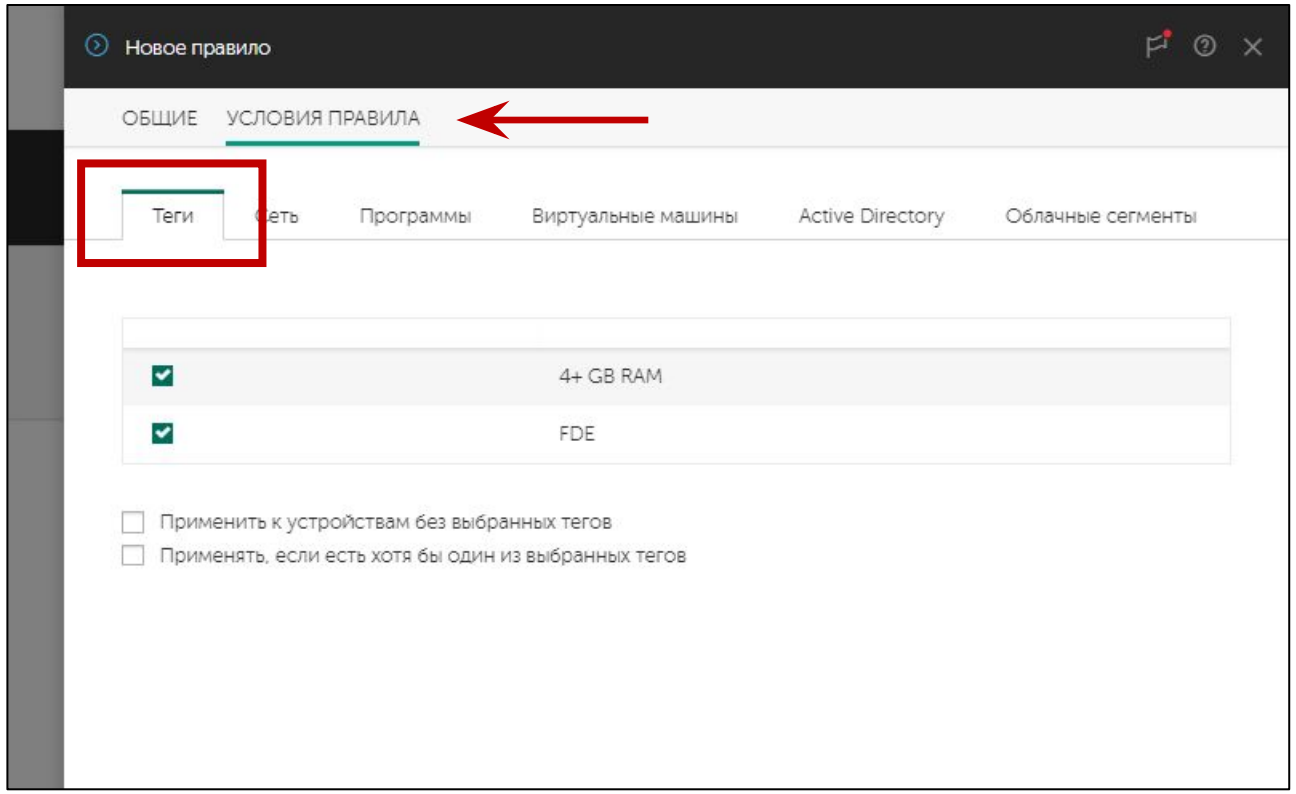
Расположение в Active Directory



Условия для Active Directory позволяют автоматически синхронизировать структуру управляемых компьютеров с Active Directory:

- Создавать новые группы для новых подразделений
- Удалять группы для тех подразделений, которых больше нет
- Перемещать компьютеры между группами, когда компьютеры меняют подразделение

Теги

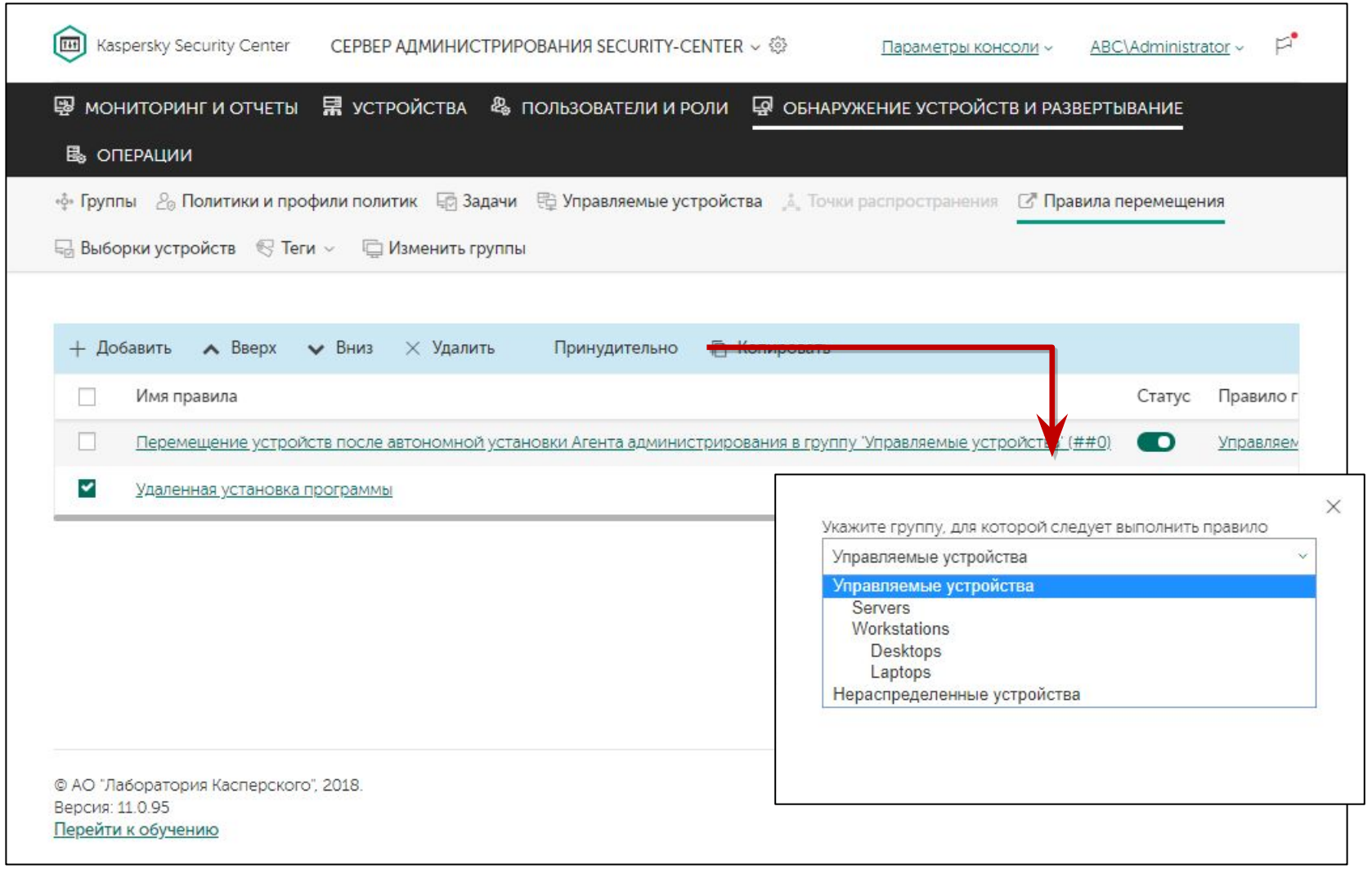


Если стандартных условий не хватает, отметьте компьютеры тегами и настройте правила перемещения на основе тегов

Назначайте теги:

- в свойствах компьютеров (выделите несколько компьютеров, чтобы назначить им одинаковый тег)
- при установке Агента администрирования (укажите тег в свойствах пакета Агента администрирования)
- правилами назначения тегов в свойствах Сервера администрирования

Порядок применения правил



При конфликте применяется верхнее правило в списке

Постоянные правила всегда имеют приоритет над одноразовыми

Кнопка **Принудительно** позволяет повторно применить правило к ранее перемещенным компьютерам:

- Имеет смысл только для правил, которые не применяются постоянно
- Применяет правило к компьютерам в выбранной группе
- Может повторно перемещать компьютеры, к которым это правило уже применялось

Лабораторная работа №3

Как создать структуру управляемых компьютеров

1. Создайте группы для рабочих станций, мобильных компьютеров и серверов
2. Распределите компьютеры по группам с помощью правил