RuDesktop

Документация

Кейсы

RuDesktop

Версия 3.1 • сформировано 21.11.2026

Оглавление

1 Двухфакторная авторизация **4**
1.1 Настройка двухфакторной авторизации через SMS 4
1.2 Настройка двухфакторной авторизации через Email 6
1.3 Настройка двухфакторной авторизации через Telegram 7
1.4 Настройка двухфакторной авторизации через MAX 10
1.5 Настройка двухфакторной авторизации через собственный сервер OTP 13
1.6 Настройка двухфакторной авторизации через TOTP 17
1.7 Настройка двухфакторной авторизации через FIDO2 19
1.8 Настройка двухфакторной авторизации через PKI Рутокен . . . 21

2 MDM **26**
2.1 Настройка Android через QR-код 26
2.2 Настройка Android через adb 40
2.3 Предустановка приложений через QR-код 43
2.4 Установка адреса сервера через QR-код 45
2.5 Устранение проблемы с автозапуском службы на Android . . . 53
2.6 Перевод Android-устройства в режим «Киоск» 54
2.7 Удалённый сброс Android-устройства до заводских настроек . 56
2.8 Включение отслеживания геолокации на Android 57
2.9 Блокировка камеры на Android 59
2.10 Подготовка корпоративного Android-устройства 60
2.11 Регистрация устройств 64
2.12 Управление устройствами 64

3 Настройка прав и доступов **66**
3.1 Настройка типовых ролей через группы 66
3.2 Подключение к устройствам без подтверждения 69
3.3 Подключение по мастер-паролю 71
3.4 Доступы через динамические группы 73
3.5 Общая адресная книга для подразделения 76

3.6 Временная группа устройств без изменения групп отделов . . 80

4 Установка ПО 84
4.1 Kaspersky Endpoint Security 84
4.2 Yandex Telemost 87
4.3 eXpress 87
4.4 PIX Task 88
4.5 1C 89
4.6 Публикация приложения в магазине приложений 90
4.7 Подключение сетевой папки с установщиками 97
4.8 Подготовка файлов на устройствах по прямой ссылке 100

5 Запись видеосессий и логи передачи файлов 104
5.1 Что вы получите 104
5.2 Шаг 1. Настройка хранения видеозаписей 105
5.3 Шаг 2. Включение записи и логов для группы 105
5.4 Шаг 3. Просмотр записей и логов 105
5.5 Что дальше 106

6 Развёртывание клиентов 107
6.1 Клонирование клиентов из единого образа 107
6.2 Использование hostname в качестве ID устройства 110
6.3 Развёртывание клиента в подсети 115

7 Мобильный клиент 119
7.1 Первое подключение к удалённому ПК с Android 119
7.2 Передача файлов с телефона на ПК и обратно 121
7.3 Раздача собственного экрана Android оператору 124
7.4 Запись сессий на мобильном клиенте 127
7.5 Прокси и альтернативные серверы на мобильном клиенте . . . 129
7.6 Подключение через корпоративный SOCKS5/HTTP-прокси . . . 131
7.7 Голосовой вызов оператор↔пользователь во время сессии . . . 134
7.8 Преднастройки подключения 137

8 Пригласительные ссылки 141
8.1 Управление пригласительными ссылками в веб-интерфейсе . . 141
8.2 Создание пригласительной ссылки в десктопном клиенте . . . 144
8.3 Создание пригласительной ссылки в мобильном клиенте Android 147
8.4 Что вы получите 153

9 Миграция Windows → Linux 154
9.1 1. Подготовка 154
9.2 2. Создание сценария миграции 157
9.3 3. Запуск и контроль миграции 161
9.4 4. После миграции 166
9.5 Шаги 169
9.6 Кратко: что делает миграция 169
9.7 См. также 170

10 Печать документа с удалённого устройства на своём принтере 171
10.1 Что вы получите 171
10.2 Подготовка 172

10.3 Шаг 1. Проверить виртуальный принтер на удалённом устройстве . . . 172
10.4 Шаг 2. Включить приём заданий печати у оператора . . . 173
10.5 Шаг 3. Отправить документ на печать . . . 173
10.6 Шаг 4. Подтвердить печать на своём устройстве . . . 174
10.7 Если печать не работает . . . 175
10.8 Что дальше . . . 175

11 Обновление ОС **176**
11.1 Обновление Windows в закрытой сети . . . 176

12 Поиск установленного ПО по категориям **180**
12.1 Что подготовить . . . 180
12.2 Собрать сведения об установленном ПО . . . 181
12.3 Найти программы нужной категории . . . 181
12.4 Проверить программы без категории . . . 182
12.5 Назначить подходящую запись вручную . . . 182
12.6 Если подходящего пакета нет . . . 183
12.7 Как понимать итог . . . 183

13 На каких устройствах включено расширение браузера **184**

14 Контроль количества лицензий на ПО **185**
14.1 Что подготовить . . . 185
14.2 Собрать данные и добавить лицензию . . . 186
14.3 Разобрать превышение . . . 186
14.4 Проверить назначения устройств . . . 187
14.5 Настроить уведомления и проверить результат . . . 187

ГЛАВА 1

Двухфакторная авторизация

1.1 Настройка двухфакторной авторизации через SMS

При выборе этого способа после ввода логина и пароля пользователю отправляется одноразовый код в SMS на номер телефона из его профиля

Важно

На стороне сервера поддерживается только SMS-шлюз `sms.ru`. Для других провайдеров отправка SMS работать не будет

1.1.1 Предварительные действия

Регистрация в sms.ru

1. Зарегистрируйте аккаунт на https://sms.ru/
2. Получите `api_id` в личном кабинете
3. При необходимости зарегистрируйте имя отправителя

1.1.2 Настройка на сервере

SMS-шлюз

1. Перейти в **Администрирование → Настройки → SMS шлюз**:
   - В поле SMS шлюз выбрать `sms.ru`

- В поле Отправитель указать имя отправителя, зарегистрированное в личном кабинете `sms.ru`
- В поле Ключ API указать `api_id` из личного кабинета `sms.ru`

2. Сохранить настройки, нажав Сохранить

Настройка пользователя

1. Открыть профиль пользователя в **Организация → Пользователи**
2. В поле Номер телефона указать номер в международном формате (например, `79001234567`)
3. Сохранить профиль, нажав Сохранить

Включение двухфакторной авторизации

Способ 1. Только для конкретных пользователей

Глобально 2FA на сервере включать **не нужно**. Достаточно зарегистрировать ключ телефона в профиле нужного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. Перейти на вкладку Безопасность аккаунта
3. Добавить ключ типа **Телефон**

После этого при входе **только у этого пользователя** будет запрошен второй фактор по SMS. Остальные пользователи войдут без 2FA

Способ 2. Для всех пользователей сервера

1. Перейти в **Администрирование → Настройки → Аутентификация**
2. В поле Двухфакторная авторизация выбрать **Телефон (OTP)**
3. Сохранить настройки, нажав Сохранить

После этого 2FA по SMS станет обязательной для **всех** пользователей сервера

> **Важно**
>
> Если у пользователя не указан номер телефона, он не сможет пройти двухфакторную авторизацию — код некуда будет отправить

1.1.3 Аварийное отключение

Если возникают проблемы и пройти двухфакторную авторизацию невозможно, выполните на сервере команду:

```
rude constance set TWO_FACTOR "off"
```

После внесения всех изменений при попытке авторизоваться одноразовые коды будут отправляться по SMS

1.2 Настройка двухфакторной авторизации через Email

При выборе этого способа после ввода логина и пароля пользователю отправляется одноразовый код на адрес электронной почты из его профиля

1.2.1 Предварительные действия

Подготовьте параметры SMTP-сервера, через который сервер **RuDesktop** будет отправлять письма:

- Адрес SMTP-сервера и порт (например, `smtp.yandex.ru` / `465`)
- Имя пользователя и пароль (для большинства провайдеров используется пароль приложения, а не основной пароль)
- Адрес отправителя
- Признак использования TLS

1.2.2 Настройка на сервере

SMTP

1. Перейти в **Администрирование → Настройки → Настройки SMTP**:
   - SMTP сервер — адрес SMTP-сервера
   - SMTP порт — порт SMTP-сервера. Стандартные значения: 25 (без шифрования), 465 (SSL), 587 (STARTTLS)
   - SMTP имя пользователя — имя пользователя для авторизации
   - SMTP пароль — пароль для авторизации (или пароль приложения)
   - SMTP использовать TLS — активировать, если провайдер требует TLS/STARTTLS
   - Отправитель по умолчанию — адрес, от имени которого будут отправляться письма
   - Получатель по умолчанию — адрес для общих уведомлений
2. Сохранить настройки, нажав Сохранить
3. Проверить отправку тестового сообщения, нажав Отправить

Настройка пользователя

1. Открыть профиль пользователя в **Организация → Пользователи**
2. В поле Электронная почта указать действующий e-mail пользователя
3. Сохранить профиль, нажав Сохранить

Подсказка

При синхронизации с Active Directory e-mail обычно подтягивается из домена автоматически

Включение двухфакторной авторизации

Способ 1. Только для конкретных пользователей

Глобально 2FA на сервере включать **не нужно**. Достаточно зарегистрировать Email-ключ в профиле нужного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. Перейти на вкладку Безопасность аккаунта
3. Добавить ключ типа **Email**

После этого при входе **только у этого пользователя** будет запрошен второй фактор на e-mail. Остальные пользователи войдут без 2FA

Способ 2. Для всех пользователей сервера

1. Перейти в **Администрирование → Настройки → Аутентификация**
2. В поле Двухфакторная авторизация выбрать **Email (OTP)**
3. Сохранить настройки, нажав Сохранить

После этого 2FA через e-mail станет обязательной для **всех** пользователей сервера

Важно

Если у пользователя не указан e-mail, он не сможет пройти двухфакторную авторизацию — код некуда будет отправить

1.2.3 Аварийное отключение

Если возникают проблемы и пройти двухфакторную авторизацию невозможно, выполните на сервере команду:

```
rude constance set TWO_FACTOR "off"
```

После внесения всех изменений при попытке авторизоваться одноразовые коды будут отправляться на электронную почту пользователя

1.3 Настройка двухфакторной авторизации через Telegram

При выборе этого способа после ввода логина и пароля пользователю отправляется одноразовый код в Telegram-бот

1.3.1 Предварительные действия

Создание Telegram-бота

1. Перейти к `@BotFather` (https://t.me/BotFather) в Telegram
2. Отправить команду `/newbot` и следовать инструкциям для создания нового бота

Подсказка

Скопируйте и сохраните полученный токен — он понадобится для настройки на сервере или в профиле пользователя

Получение ID чата

Бот может отправлять одноразовый код в личные сообщения пользователю или в общий чат

1. Активировать отображение ID в Telegram:
    1. Откройте Telegram и перейдите в **Настройки**
    2. Выберите **Продвинутые настройки**
    3. Перейдите в **Экспериментальные настройки**
    4. Активируйте чек-бокс `Show Peer IDs in Profile`
2. Получить ID:
    - **Личный ID профиля** — перейдите в **Мой профиль** и скопируйте значение **ID**
    - **ID группы** — откройте группу, ID будет показан рядом с её названием

Важно

Чтобы бот мог отправлять сообщения в личные сообщения пользователя, пользователь должен сам отправить боту команду `/start`. Без этого Telegram запрещает боту первым писать пользователю

1.3.2 Настройка на сервере

Подключение бота

1. Перейти в **Администрирование → Настройки → Настройки телеграм бота**:
    - В поле Токен для телеграм бота указать полученный у `@BotFather` токен
    - В поле ID чата телеграм бота указать ID личного профиля или группы для общих уведомлений

2. Сохранить настройки, нажав Сохранить
3. Проверить отправку тестового сообщения, нажав Отправить

> **Подсказка**
>
> Если бот заблокирован, разблокируйте его. При ошибке авторизации проверьте токен бота

Настройка пользователя

Чтобы код приходил в личные сообщения конкретного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. На вкладке Профиль указать:
   - Телеграм (токен) — токен бота, который пишет именно этому пользователю
   - Телеграм (ID чата) — ID личного чата пользователя с этим ботом

> **Важно**
>
> Если поле Телеграм (токен) оставить пустым, будет использован токен из настроек сервера — но только при включённой опции Использовать токен бота Telegram из настроек при отправке OTP для всех пользователей (см. ниже)

3. Сохранить профиль, нажав Сохранить

Включение двухфакторной авторизации

Способ 1. Только для конкретных пользователей

Глобально 2FA на сервере включать **не нужно**. Достаточно зарегистрировать Telegram-ключ в профиле нужного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. Перейти на вкладку Безопасность аккаунта
3. Добавить ключ типа **Telegram**

После этого при входе **только у этого пользователя** будет запрошен второй фактор через Telegram. Остальные пользователи войдут без 2FA

Способ 2. Для всех пользователей сервера

1. Перейти в **Администрирование → Настройки → Аутентификация**
2. В поле Двухфакторная авторизация выбрать **Telegram (OTP)**

Подсказка

Чтобы не указывать токен в профиле каждого пользователя, активируйте чек-бокс Использовать токен бота Telegram из настроек при отправке OTP для всех пользователей — тогда сервер будет использовать общий токен из настроек, а в профиле пользователя достаточно указать только Телеграм (ID чата)

3. Сохранить настройки, нажав Сохранить

После этого 2FA через Telegram станет обязательной для **всех** пользователей сервера

Важно

Если у пользователя не указан Телеграм (ID чата), он не сможет пройти двухфакторную авторизацию — код некуда будет отправить

1.3.3 Аварийное отключение

Если возникают проблемы и пройти двухфакторную авторизацию невозможно, выполните на сервере команду:

```
rude constance set TWO_FACTOR "off"
```

После внесения всех изменений при попытке авторизоваться одноразовые коды будут отправляться в указанные чаты

1.4 Настройка двухфакторной авторизации через MAX

При выборе этого способа после ввода логина и пароля пользователю отправляется одноразовый код в бота мессенджера **MAX**

1.4.1 Предварительные действия

Создание MAX-бота

1. Откройте мессенджер **MAX** и перейдите к `@MasterBot` (https://max.ru/MasterBot)
2. Следуйте инструкции для создания нового бота

Подсказка

Скопируйте и сохраните полученный токен — он понадобится для настройки на сервере или в профиле пользователя

Подробнее про API ботов **MAX**: https://dev.max.ru/docs/chatbots/bots-create

Получение ID чата

Бот может отправлять одноразовый код в личные сообщения пользователю или в общий чат

- **Личный чат** — пользователь должен сам открыть бота и отправить ему первое сообщение (обычно команду `/start`). После этого ID чата можно получить через API мессенджера
- **Групповой чат** — добавьте бота в группу и получите ID этой группы

> **Важно**
>
> Без первого сообщения от пользователя бот не сможет писать ему первым

1.4.2 Настройка на сервере

Подключение бота

1. Перейти в **Администрирование → Настройки → Настройки MAX бота**:
   - В поле Токен для MAX бота указать полученный токен
   - В поле ID чата MAX бота указать ID общего чата для уведомлений
2. Сохранить настройки, нажав Сохранить
3. Проверить отправку тестового сообщения, нажав Отправить

> **Подсказка**
>
> Если чат не найден, проверьте его ID и убедитесь, что бот добавлен в чат

Настройка пользователя

Чтобы код приходил в личные сообщения конкретного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. На вкладке Профиль указать:
   - MAX (токен) — токен бота, который пишет именно этому пользователю
   - MAX (ID чата) — ID личного чата пользователя с этим ботом

> **Важно**
>
> Если поле MAX (токен) оставить пустым, будет использован токен из настроек сервера — но только при включённой опции Использовать токен бота MAX из настроек при отправке OTP для всех пользователей (см. ниже)

3. Сохранить профиль, нажав Сохранить

Включение двухфакторной авторизации

Способ 1. Только для конкретных пользователей

Глобально 2FA на сервере включать **не нужно**. Достаточно зарегистрировать MAX-ключ в профиле нужного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. Перейти на вкладку Безопасность аккаунта
3. Добавить ключ типа **MAX**

После этого при входе **только у этого пользователя** будет запрошен второй фактор через MAX. Остальные пользователи войдут без 2FA

Способ 2. Для всех пользователей сервера

1. Перейти в **Администрирование → Настройки → Аутентификация**
2. В поле Двухфакторная авторизация выбрать **MAX (OTP)**

> **Подсказка**
>
> Чтобы не указывать токен в профиле каждого пользователя, активируйте чек-бокс Использовать токен бота MAX из настроек при отправке OTP для всех пользователей — тогда сервер будет использовать общий токен из настроек, а в профиле пользователя достаточно указать только MAX (ID чата)

3. Сохранить настройки, нажав Сохранить

После этого 2FA через MAX станет обязательной для **всех** пользователей сервера

> **Важно**
>
> Если у пользователя не указан MAX (ID чата), он не сможет пройти двухфакторную авторизацию — код некуда будет отправить

1.4.3 Аварийное отключение

Если возникают проблемы и пройти двухфакторную авторизацию невозможно, выполните на сервере команду:

```
rude constance set TWO_FACTOR "off"
```

После внесения всех изменений при попытке авторизоваться одноразовые коды будут отправляться в указанные чаты MAX

1.5 Настройка двухфакторной авторизации через собственный сервер OTP

При выборе этого способа сервер **RuDesktop** не генерирует одноразовый пароль сам, а обращается по HTTP к стороннему сервису: просит его отправить код пользователю, а затем — проверить введённый код

Способ подходит, когда одноразовые пароли уже выдаёт внешняя система (корпоративное решение 2FA, собственный шлюз рассылки, внутренний сервис аутентификации) и требуется использовать её вместо встроенных каналов **RuDesktop**

Важно

Способ доступен только на локальном сервере **RuDesktop**. В облачной версии он не отображается ни в настройках, ни в списке методов пользователя

1.5.1 Как это работает

Сервер **RuDesktop** выполняет `POST`-запрос на указанный URL с телом в формате JSON и ожидает ответ `2xx` с телом `{"ok": true}`

Запрос отправляется дважды за одну авторизацию:

1. **Отправка кода** — когда пользователь запрашивает одноразовый пароль. Сторонний сервис должен сгенерировать код и доставить его пользователю выбранным им способом
2. **Проверка кода** — когда пользователь ввёл код. Сторонний сервис должен сверить его и ответить, верен ли код

Важно

Одноразовый пароль целиком на стороне внешнего сервиса: **RuDesktop** его не генерирует, не хранит и не проверяет. Срок жизни кода, его длину и способ доставки определяет сам сервис

Формат запроса

Тело запроса — JSON со следующими полями:

Поле	Описание
`action`	`send` — отправить код пользователю, `verify` — проверить введённый код
`username`	Логин пользователя в **RuDesktop**
`full_name`	Полное имя пользователя из профиля
`email`	E-Mail из профиля
`phone`	Номер телефона из профиля
`telegram_chat_id`	ID чата Telegram из профиля
`max_chat_id`	ID чата MAX из профиля
`otp`	Введённый пользователем код. Передаётся только при `action: verify`
`manager_username`	Логин администратора, инициировавшего отправку. Передаётся только при регистрации ключа из веб-интерфейса

Подсказка

Контактные поля передаются, чтобы внешний сервис сам выбрал канал доставки кода. Пустые значения передаются как пустые строки

Формат ответа

Запрос считается успешным, если одновременно выполнены оба условия:

- HTTP-код ответа — успешный (2xx)
- тело ответа — корректный JSON, в котором поле `ok` равно `true`

Во всех остальных случаях (ошибка сети, код ответа 4xx/5xx, нечитаемый JSON, `ok` не равно `true`) операция завершается ошибкой: при отправке пользователь увидит сообщение о невозможности запроса, при проверке — отказ во входе

Важно

Таймаут запроса — **5 секунд**. Если внешний сервис не ответил за это время, запрос считается неуспешным

Ограничение частоты отправки

Запросить отправку кода можно не более **3 раз за 5 минут** для одного пользователя. При превышении лимита выводится сообщение с указанием, через сколько минут можно повторить попытку

1.5.2 Настройка на сервере

Общий URL для всех пользователей

1. Перейти в **Администрирование → Настройки → Настройки собственного сервера OTP**:
   - В поле URL собственного сервера OTP указать адрес сервиса, например `https://otp.example.com/rudesktop`
2. Перейти в **Администрирование → Настройки → Аутентификация**:
   - Активировать чек-бокс Использовать URL собственного сервера OTP из настроек при отправке OTP для всех пользователей
3. Сохранить настройки, нажав Сохранить

Подсказка

При включённой опции URL из профиля пользователя не используется — все запросы уходят на общий адрес из настроек. При регистрации ключа поле ввода URL заменяется подписью **«Будет использован общий URL собственного сервера OTP»**

Важно

Принимаются только адреса со схемой `http` или `https`. Некорректный адрес не будет сохранён

Включение двухфакторной авторизации

Способ 1. Только для конкретных пользователей

Глобально 2FA на сервере включать **не нужно**. Достаточно зарегистрировать ключ в профиле нужного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. Перейти на вкладку Безопасность аккаунта
3. Добавить ключ типа **Собственный сервер OTP**
4. Указать URL собственного сервера OTP — адрес сервиса, обслуживающего этого пользователя

Подсказка

Поле не отображается, если включена опция использования общего URL из настроек сервера

5. Нажать кнопку запроса одноразового пароля — сервер обратится к внешнему сервису с `action: send`
6. Ввести полученный код и подтвердить — сервер проверит его запросом с `action: verify` и сохранит ключ

После этого при входе **только у этого пользователя** будет запрошен второй фактор через внешний сервис. Остальные пользователи войдут без 2FA

Способ 2. Для всех пользователей сервера

1. Перейти в **Администрирование → Настройки → Аутентификация**
2. В поле Двухфакторная авторизация выбрать **Собственный сервер OTP**
3. Сохранить настройки, нажав Сохранить

После этого 2FA через внешний сервис станет обязательной для **всех** пользователей сервера. Пользователи, у которых ключ ещё не зарегистрирован, при первом входе будут проведены через мастер регистрации

Подсказка

Чтобы не указывать адрес в профиле каждого пользователя, заранее включите опцию Использовать URL собственного сервера OTP из настроек при отправке OTP для всех пользователей

1.5.3 Аварийное отключение

Если возникают проблемы и пройти двухфакторную авторизацию невозможно, выполните на сервере команду:

```
rude constance set TWO_FACTOR "off"
```

1.5.4 Диагностика

Ошибки обращения к внешнему сервису записываются в лог сервера. Наиболее частые причины отказа:

- **«URL собственного сервера OTP не задан»** — адрес не указан ни в профиле пользователя, ни в настройках сервера при включённой опции общего URL
- **«Введите корректный URL собственного сервера OTP»** — адрес указан не по схеме `http`/`https` либо синтаксически неверен

- **«Не удалось выполнить запрос к собственному серверу OTP»** — сервис недоступен, не ответил за 5 секунд или вернул ошибочный HTTP-код
- **«Собственный сервер OTP вернул некорректный ответ»** — тело ответа не является корректным JSON
- **«Собственный сервер OTP отклонил запрос»** — сервис ответил, но поле `ok` в ответе не равно `true`. При проверке кода это означает, что код неверен
- **«Собственный сервер OTP не настроен»** — у пользователя нет включённого ключа этого типа

1.6 Настройка двухфакторной авторизации через TOTP

При выборе этого способа после ввода логина и пароля пользователю требуется ввести одноразовый код, сгенерированный приложением-аутентификатором на его устройстве

В отличие от **Email/SMS/Telegram/MAX**, этот способ **не требует SMTP, SMS-шлюза и мессенджеров** — код вычисляется локально на устройстве пользователя по секретному ключу и текущему времени

1.6.1 Предварительные действия

На устройстве пользователя установить любое приложение-аутентификатор, например:

- **Google Authenticator**
- **Яндекс Ключ**
- **Kaspersky Password Manager**
- **Рутокен OTP**

1.6.2 Настройка на сервере

Включение двухфакторной авторизации

Способ 1. Только для конкретных пользователей

Глобально 2FA на сервере включать **не нужно**. Достаточно зарегистрировать TOTP-ключ в профиле нужного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. Перейти на вкладку Безопасность аккаунта
3. Нажать кнопку добавления **TOTP**
4. Отсканировать QR-код приложением-аутентификатором и ввести шестизначный код

После этого при входе **только у этого пользователя** будет запрошен код TOTP. Остальные пользователи войдут без 2FA

Способ 2. Для всех пользователей сервера

1. Перейти в **Администрирование → Настройки → Аутентификация**
2. В поле Двухфакторная авторизация выбрать **Аутентификатор (TOTP)**
3. Сохранить настройки, нажав Сохранить

После этого TOTP станет обязательной для **всех** пользователей сервера. Пользователи, у которых ещё нет ключа, при первом входе будут автоматически направлены на регистрацию:

1. Пользователь вводит логин и пароль на странице авторизации
2. Открывается экран **«Добавление нового TOTP»** с QR-кодом
3. В приложении-аутентификаторе выбрать **«Сканировать QR-код»** и отсканировать его

> **Подсказка**
>
> Если QR-код отсканировать не получается, нажмите на ссылку **«этот текст»** под QR-кодом и введите выданный секрет в приложение вручную

4. Ввести шестизначный код, выданный приложением, в поле Введите код
5. Нажать Сохранить

После сохранения пользователь будет авторизован, а ключ TOTP — сохранён в его профиле

> **Важно**
>
> Срок действия зарегистрированных ключей задаётся настройкой Срок действия ключей для входа (в **Администрирование → Настройки → Аутентификация**). По истечении срока пользователю придётся перерегистрировать ключ

1.6.3 Использование

При следующем входе пользователь:

1. Вводит логин и пароль
2. Открывает приложение-аутентификатор и копирует текущий шестизначный код
3. Вводит код в поле Введите код и нажимает Подтвердить

1.6.4 Аварийное отключение

Если возникают проблемы и пройти двухфакторную авторизацию невозможно, выполните на сервере команду:

```
rude constance set TWO_FACTOR "off"
```

1.7 Настройка двухфакторной авторизации через FIDO2

При выборе этого способа после ввода логина и пароля пользователь подтверждает вход аппаратным USB-ключом безопасности (стандарт FIDO2/WebAuthn)

В отличие от OTP-методов, при FIDO2 ничего вводить не нужно: пользователь подключает токен и нажимает на нём кнопку

1.7.1 Предварительные действия

Подготовьте на стороне пользователя:

- USB-ключ с поддержкой FIDO2 (например, `YubiKey`, `Рутокен MFA`, `Esmart Token`)
- Браузер с поддержкой WebAuthn — все современные браузеры (Chrome, Firefox, Edge, Safari, Yandex)

Важно

FIDO2 работает только при подключении к серверу по **HTTPS**. По обычному HTTP браузеры не позволяют использовать WebAuthn

1.7.2 Настройка на сервере

Включение двухфакторной авторизации

Способ 1. Только для конкретных пользователей

Глобально 2FA на сервере включать **не нужно**. Достаточно зарегистрировать FIDO2-ключ в профиле нужного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. Перейти на вкладку Безопасность аккаунта
3. Нажать кнопку добавления **FIDO2**
4. Подключить FIDO2-ключ к USB и подтвердить регистрацию (касанием сенсора, при необходимости — вводом PIN)

После этого при входе **только у этого пользователя** будет запрошен FIDO2-ключ. Остальные пользователи войдут без 2FA

Подсказка

К одному пользователю можно зарегистрировать **несколько ключей** — например, основной и резервный. Это полезно на случай потери одного из них

Способ 2. Для всех пользователей сервера

1. Перейти в **Администрирование → Настройки → Аутентификация**
2. В поле Двухфакторная авторизация выбрать **Электронный ключ (FIDO2)**
3. Сохранить настройки, нажав Сохранить

После этого FIDO2 станет обязательной для **всех** пользователей сервера. Пользователи, у которых ещё нет зарегистрированного ключа, при первом входе будут автоматически направлены на регистрацию:

1. Пользователь вводит логин и пароль
2. Открывается экран **«Добавить новый ключ FIDO2»** с сообщением **«Ваш браузер должен запросить подтверждение вашей личности»**
3. Браузер запросит подключить ключ безопасности
4. Подключить FIDO2-ключ к USB и нажать на нём кнопку (касание сенсора)
5. При первом использовании может быть запрошен PIN-код ключа

После подтверждения ключ будет зарегистрирован в профиле пользователя, и пользователь будет авторизован

Важно

Срок действия зарегистрированных ключей задаётся настройкой Срок действия ключей для входа (в **Администрирование → Настройки → Аутентификация**). По истечении срока пользователю придётся перерегистрировать ключ

1.7.3 Использование

При следующем входе пользователь:

1. Вводит логин и пароль
2. На экране **FIDO2** подключает свой ключ к USB
3. Касается сенсора на ключе (или вводит PIN, если он установлен)

1.7.4 Аварийное отключение

Если возникают проблемы и пройти двухфакторную авторизацию невозможно, выполните на сервере команду:

```
rude constance set TWO_FACTOR "off"
```

1.8 Настройка двухфакторной авторизации через PKI Рутокен

При выборе этого способа после ввода логина и пароля пользователь подтверждает вход электронной подписью на токене **Рутокен**

В отличие от других методов, **PKI** использует криптографию ГОСТ. Сервер **RuDesktop** держит собственный удостоверяющий центр и сам выпускает сертификат на токен пользователя при регистрации

1.8.1 Предварительные действия

На стороне пользователя

- Подключить Рутокен к USB
- Установить **Рутокен Плагин** для браузера (https://www.rutoken.ru/products/all/rutoken-plugin/)
- Установить драйверы Рутокен для операционной системы

Важно

PKI работает только при подключении к серверу по **HTTPS**

На стороне сервера

Удостоверяющий центр (УЦ) ГОСТ создаётся автоматически при первом запуске сервера **RuDesktop** при наличии установленного движка `rtengine`. Файлы УЦ располагаются в:

```
/var/lib/rudesktop/ca/gostCA/
```

Если этой папки нет, движок не установлен — обратитесь к администратору сервера

Важно

Если на сервере был выполнен переход с **OpenSSL 1** на **OpenSSL 3** и при этом используются ключи **PKI**, необходимо обновить путь к движку `rtengine` в конфигурации УЦ. Откройте файл:

```
/var/lib/rudesktop/ca/gostCA/config.cfg
```

и замените строку:

```
dynamic_path = /
↪usr/share/rudesktop/auth_mfa/bin/librtengine.so.1.6.2
```

на:

```
dynamic_path = /
↪usr/share/rudesktop/auth_mfa/bin/librtengine.so.3.3.3
```

1.8.2 Настройка на сервере

Включение двухфакторной авторизации

Способ 1. Только для конкретных пользователей

Глобально 2FA на сервере включать **не нужно**. Достаточно зарегистрировать PKI-ключ в профиле нужного пользователя:

1. Открыть профиль пользователя в **Организация → Пользователи**
2. Перейти на вкладку Безопасность аккаунта
3. Нажать кнопку добавления **PKI**
4. Подключить Рутокен, ввести PIN. На токене будет создан ключ, сервер выпустит сертификат и сохранит его в профиле пользователя

После этого при входе **только у этого пользователя** будет запрошен Рутокен. Остальные пользователи войдут без 2FA

Подсказка

К одному пользователю можно зарегистрировать **несколько токенов** — например, основной и резервный

Способ 2. Для всех пользователей сервера

1. Перейти в **Администрирование → Настройки → Аутентификация**
2. В поле Двухфакторная авторизация выбрать **ЭЦП Рутокен (PKI)**
3. Сохранить настройки, нажав Сохранить

После этого PKI станет обязательной для **всех** пользователей сервера. Пользователи, у которых ещё нет зарегистрированного ключа, при первом входе будут автоматически направлены на регистрацию:

1. Подключить Рутокен к USB
2. Пользователь вводит логин и пароль на странице авторизации
3. Открывается экран «**Добавление нового ключа PKI**»
4. **Рутокен Плагин** запросит PIN-код от токена
5. После ввода PIN на токене будет создан ключ, сервер выпустит сертификат и сохранит его в профиле пользователя

Важно

Срок действия зарегистрированных ключей задаётся настройкой Срок действия ключей для входа (в **Администрирование → Настройки → Аутентификация**). По истечении срока пользователю придётся перерегистрировать ключ

1.8.3 Использование

При следующем входе пользователь:

1. Подключает Рутокен к USB
2. Вводит логин и пароль
3. На экране **PKI Рутокен Плагин** запрашивает PIN-код от токена
4. После ввода PIN сервер проверяет подпись и пускает пользователя

1.8.4 Аварийное отключение

Если возникают проблемы и пройти двухфакторную авторизацию невозможно, выполните на сервере команду:

```
rude constance set TWO_FACTOR "off"
```

В сервере **RuDesktop** поддерживаются следующие способы двухфакторной авторизации:

- **Телефон (OTP)** — одноразовый код по SMS
- **Email (OTP)** — одноразовый код на электронную почту
- **Telegram (OTP)** — одноразовый код в Telegram-бот
- **MAX (OTP)** — одноразовый код в бот мессенджера MAX
- **Собственный сервер OTP** — одноразовый код выдаёт и проверяет сторонний сервис по HTTP. Только для локального сервера
- **Аутентификатор (TOTP)** — одноразовый код из приложения-аутентификатора
- **Электронный ключ (FIDO2)** — аппаратный USB-токен (FIDO2/WebAuthn)
- **ЭЦП Рутокен (PKI)** — электронная подпись на токене **Рутокен**

Двухфакторную авторизацию можно включить двумя способами:

- **Для конкретных пользователей** — администратор регистрирует ключ 2FA в профиле нужного пользователя на вкладке Безопасность аккаунта. У этого пользователя при входе будет запрошен второй фактор; остальные пользователи входят без 2FA. У одного пользователя можно зарегистрировать ключи нескольких методов
- **Для всех пользователей сервера** — в настройках Двухфакторная авторизация (**Администрирование → Настройки → Аутентификация**)

выбирается единый метод. Этот метод становится обязательным для всех пользователей сервера. Если у пользователя ещё нет зарегистрированного ключа выбранного метода, при первом входе он будет проведён через мастер регистрации

Подсказка

Эти два режима можно сочетать: например, глобально включить **TOTP** для всех, но конкретному пользователю дополнительно зарегистрировать **FIDO2** в профиле — тогда при глобально выбранном методе сервер всё равно будет использовать форс TOTP

Важно

Если возникают проблемы при входе и потеряна возможность пройти 2FA, отключите её на сервере командой:

```
rude constance set TWO_FACTOR "off"
```

Телефон (OTP)

Одноразовый код в SMS на номер из профиля пользователя. Требует SMS-шлюз `sms.ru`

Email (OTP)

Одноразовый код на адрес электронной почты из профиля. Требует настроенный SMTP-сервер

Telegram (OTP)

Одноразовый код в Telegram-бот. Требует создания и подключения собственного бота

MAX (OTP)

Одноразовый код в боте мессенджера **MAX**. Требует создания собственного бота

Собственный сервер OTP

Одноразовый код выдаёт и проверяет сторонний сервис по HTTP. Требует URL внешнего сервиса

Аутентификатор (TOTP)

Код, сгенерированный приложением-аутентификатором локально на устройстве. Не требует внешних сервисов

Электронный ключ (FIDO2)

Аппаратный USB-токен FIDO2/WebAuthn. Подтверждение входа нажатием на токене, без ввода кода

ЭЦП Рутокен (PKI)

Электронная подпись на токене **Рутокен** с криптографией ГОСТ. Сертификат выпускает встроенный УЦ сервера

ГЛАВА 2

MDM

2.1 Настройка Android через QR-код

2.1.1 Подготовка

1. Убедиться, что:
   - Устройство работает на Android 7.0+
   - Имеется доступ к разделу QR-коды MDM в панели администрирования сервера **Rudesktop**

     Подсказка

     Определяется наличием соответствующей лицензии и правами доступа

   - Устройство не привязано к аккаунту Google (FRP) – иначе потребуется авторизация
2. Создать QR-код в веб-интерфейсе сервера:
   1. В веб-интерфейсе сервера **Rudesktop** открыть страницу **Администрирование -> QR-коды MDM**
   2. Нажать на кнопку Добавить QR-код MDM
   3. Заполнить поля валидными данными
   4. Поля Ссылка на скачивание пакета и Адрес сервера заполняются автоматически
   5. Нажать на кнопку Сохранить

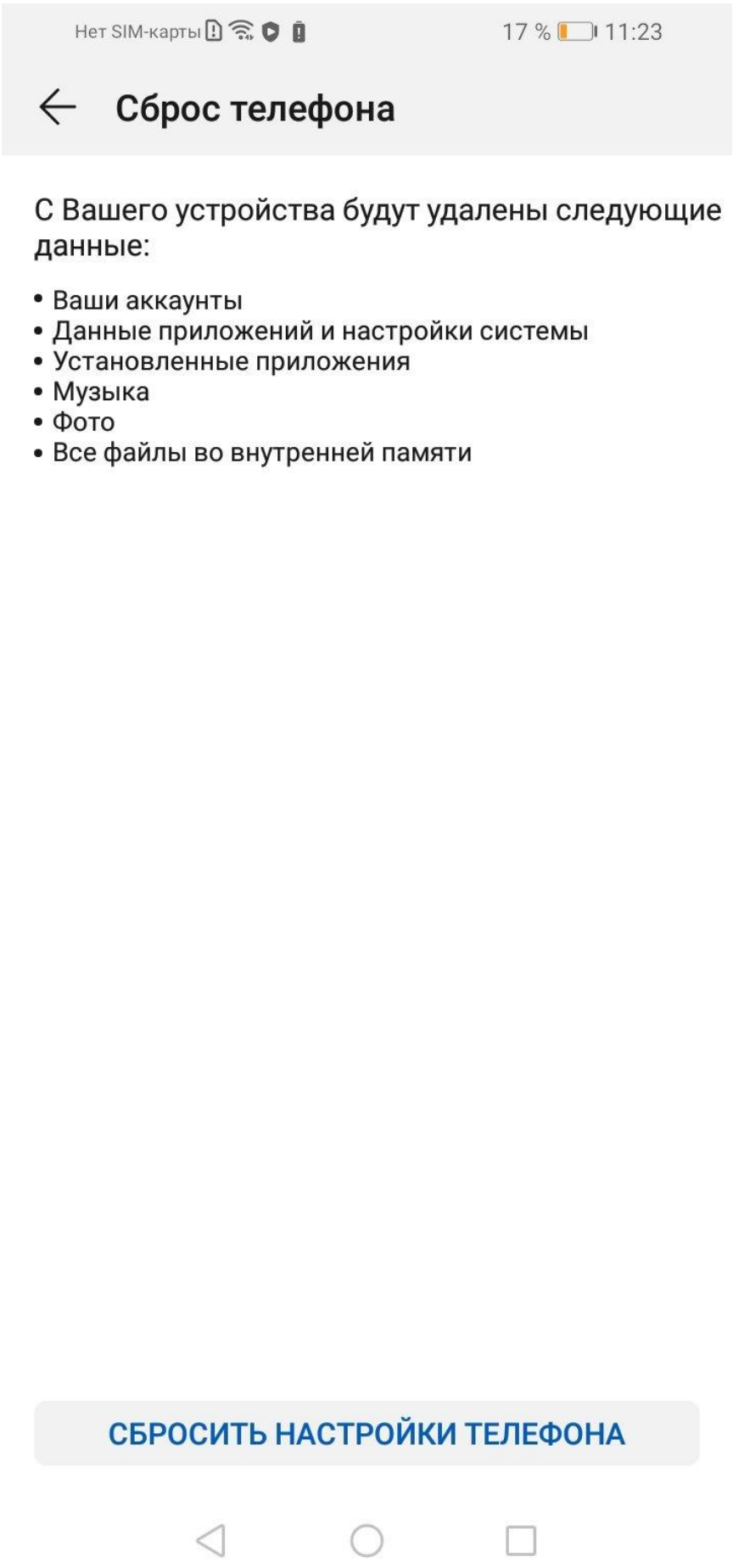
6. Нажать на ссылку Ссылка на QR код, откроется QR-код который потребуется далее

2.1.2 Настройка

1. Выполнить сброс до заводских настроек
    1. Открыть настройки → Система → Сброс

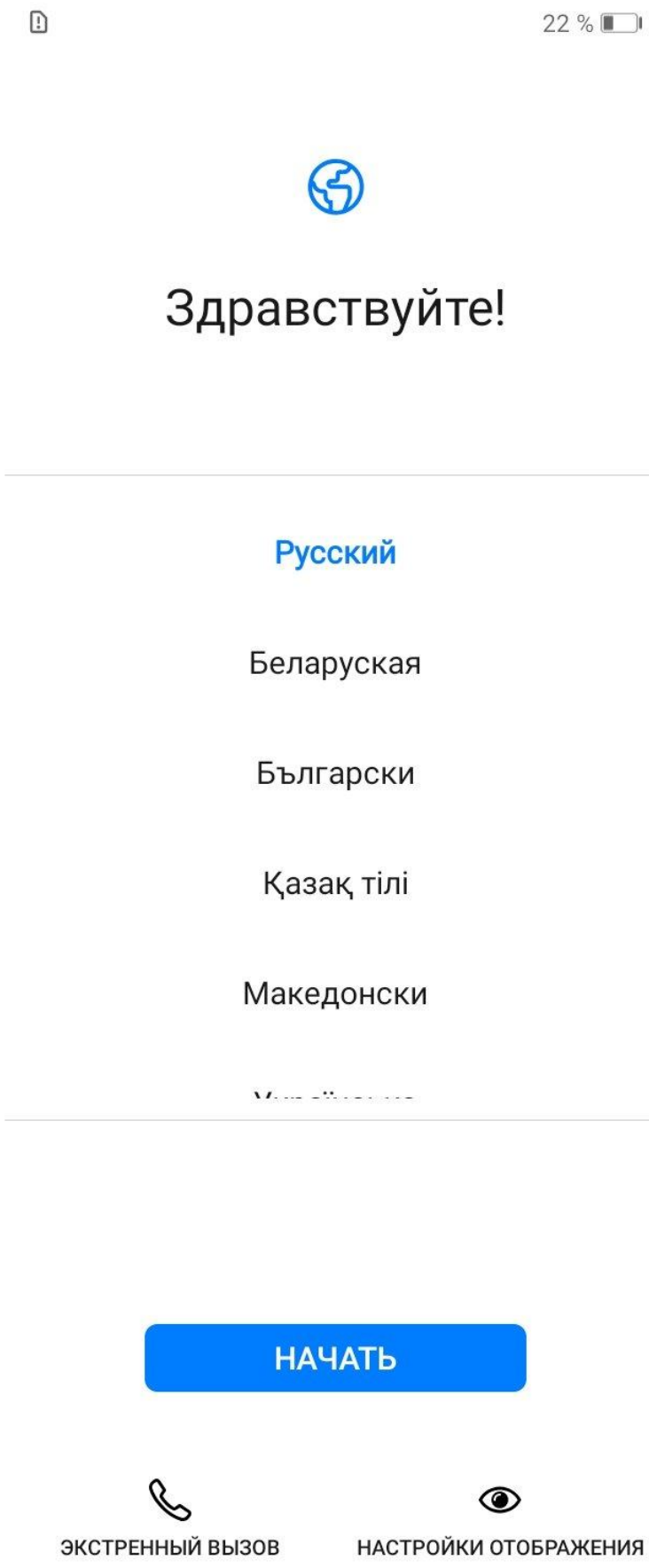

Нет SIM-карты
17 %
11:22
Сброс
Сброс всех настроек
Сброс настроек сети
Сброс телефона

2. Выбрать пункт в меню Сброс телефона

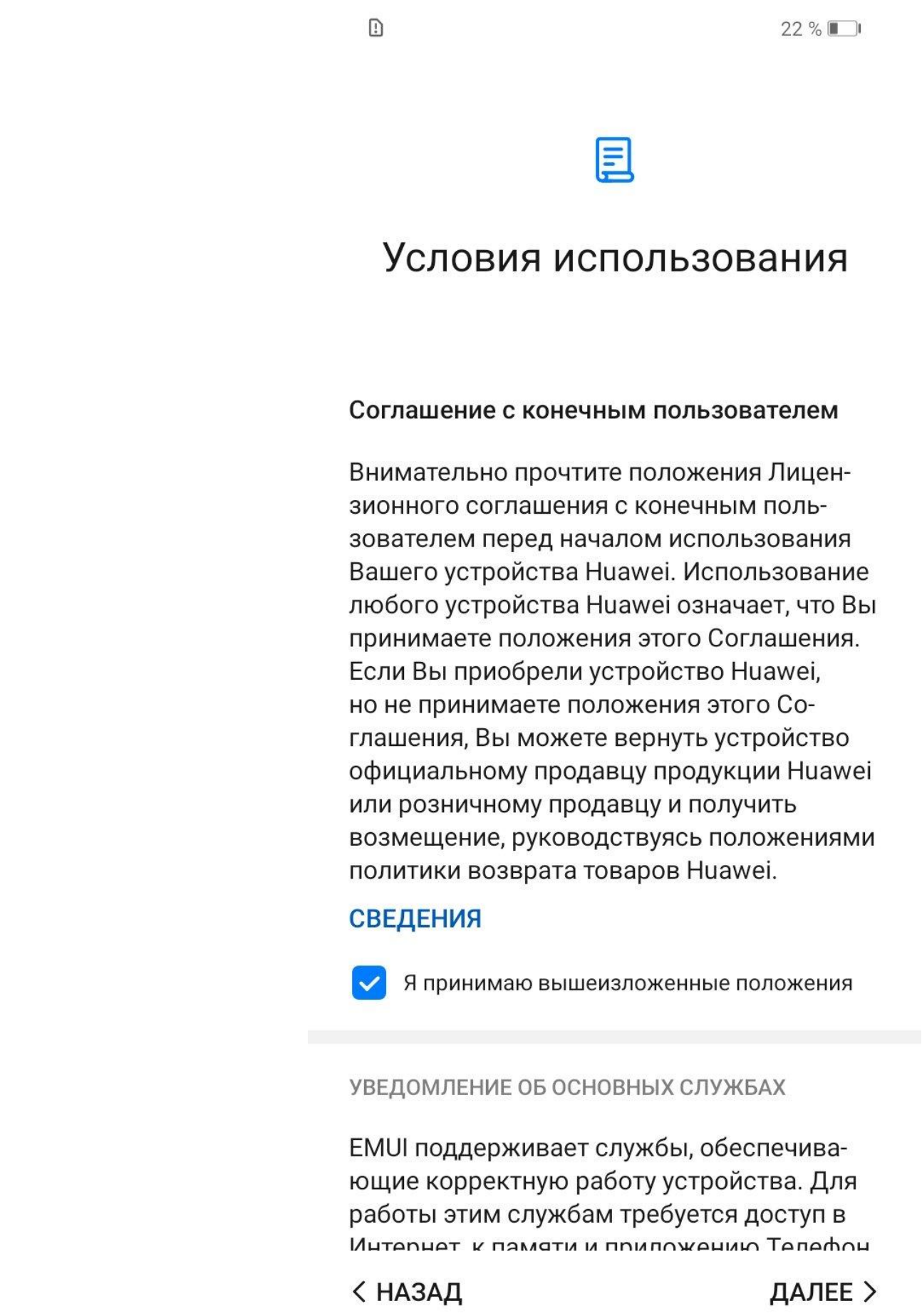

Нет SIM-карты
17 %
11:23
Сброс телефона
С Вашего устройства будут удалены следующие данные:
• Ваши аккаунты
• Данные приложений и настройки системы
• Установленные приложения
• Музыка
• Фото
• Все файлы во внутренней памяти
СБРОСИТЬ НАСТРОЙКИ ТЕЛЕФОНА

3. Подтвердить сброс и дождаться перезагрузки устройства

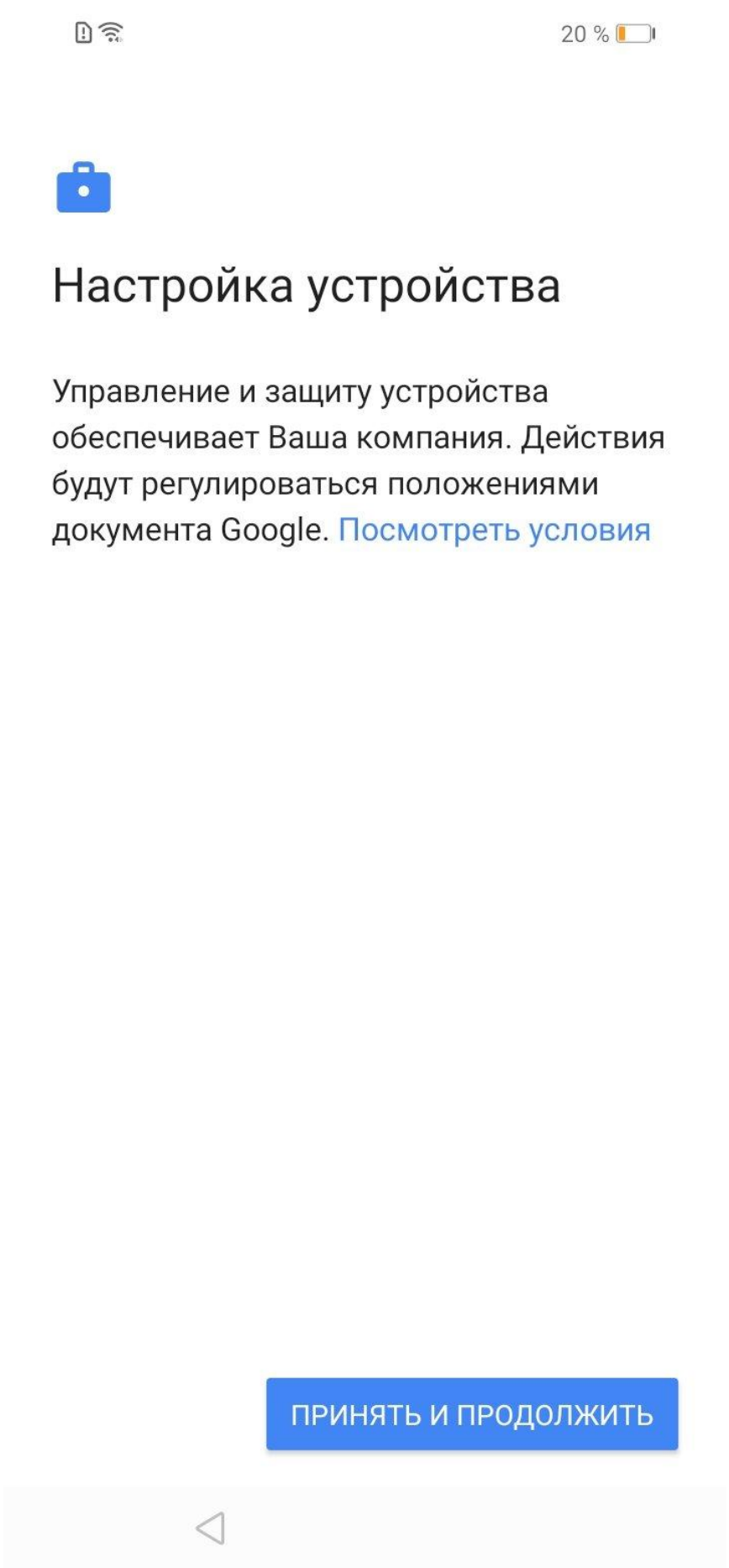
2. Начать настройку устройства
    1. После сброса откроется экран приветствия

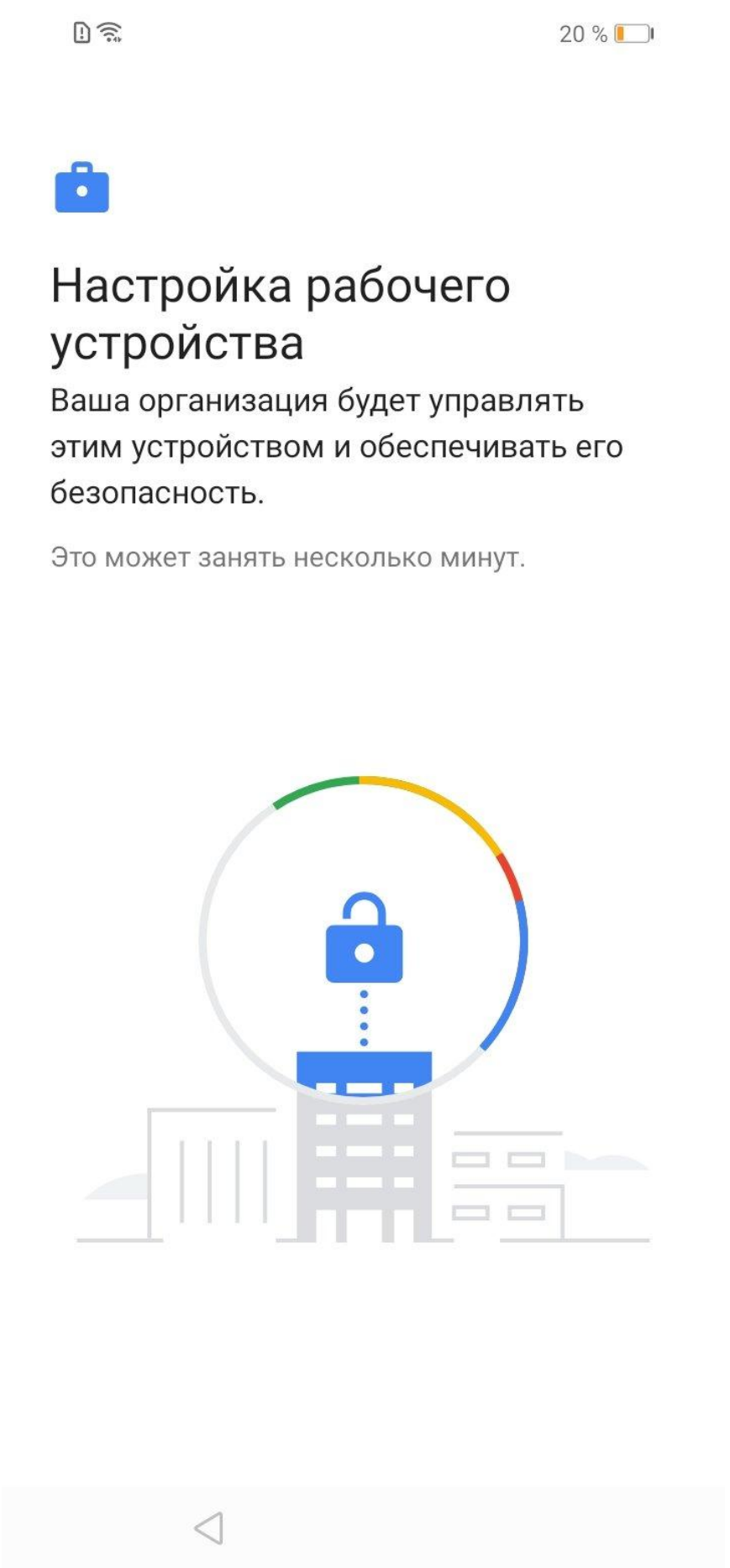

22 %
Здравствуйте!
Русский
Беларуская
Български
Қазақ тілі
Македонски
НАЧАТЬ
ЭКСТРЕННЫЙ ВЫЗОВ
НАСТРОЙКИ ОТОБРАЖЕНИЯ

2. На экране приветствия нажать 5–7 раз по пустому месту или выбрать **Настроить через QR-код**
3. Выбрать регион, принять пользовательское соглашение, установить или пропустить установку SIM-карты


22 %
Условия использования
Соглашение с конечным пользователем
Внимательно прочтите положения Лицензионного соглашения с конечным пользователем перед началом использования Вашего устройства Huawei. Использование любого устройства Huawei означает, что Вы принимаете положения этого Соглашения. Если Вы приобрели устройство Huawei, но не принимаете положения этого Соглашения, Вы можете вернуть устройство официальному продавцу продукции Huawei или розничному продавцу и получить возмещение, руководствуясь положениями политики возврата товаров Huawei.
СВЕДЕНИЯ
Я принимаю вышеизложенные положения
УВЕДОМЛЕНИЕ ОБ ОСНОВНЫХ СЛУЖБАХ
EMUI поддерживает службы, обеспечивающие корректную работу устройства. Для работы этим службам требуется доступ в
НАЗАД
ДАЛЕЕ

4. Отсканировать QR-код из веб-интерфейса
5. Подтвердить установку приложения **RuDesktop** в режиме Device Owner
6. Подтвердить настройку устройства

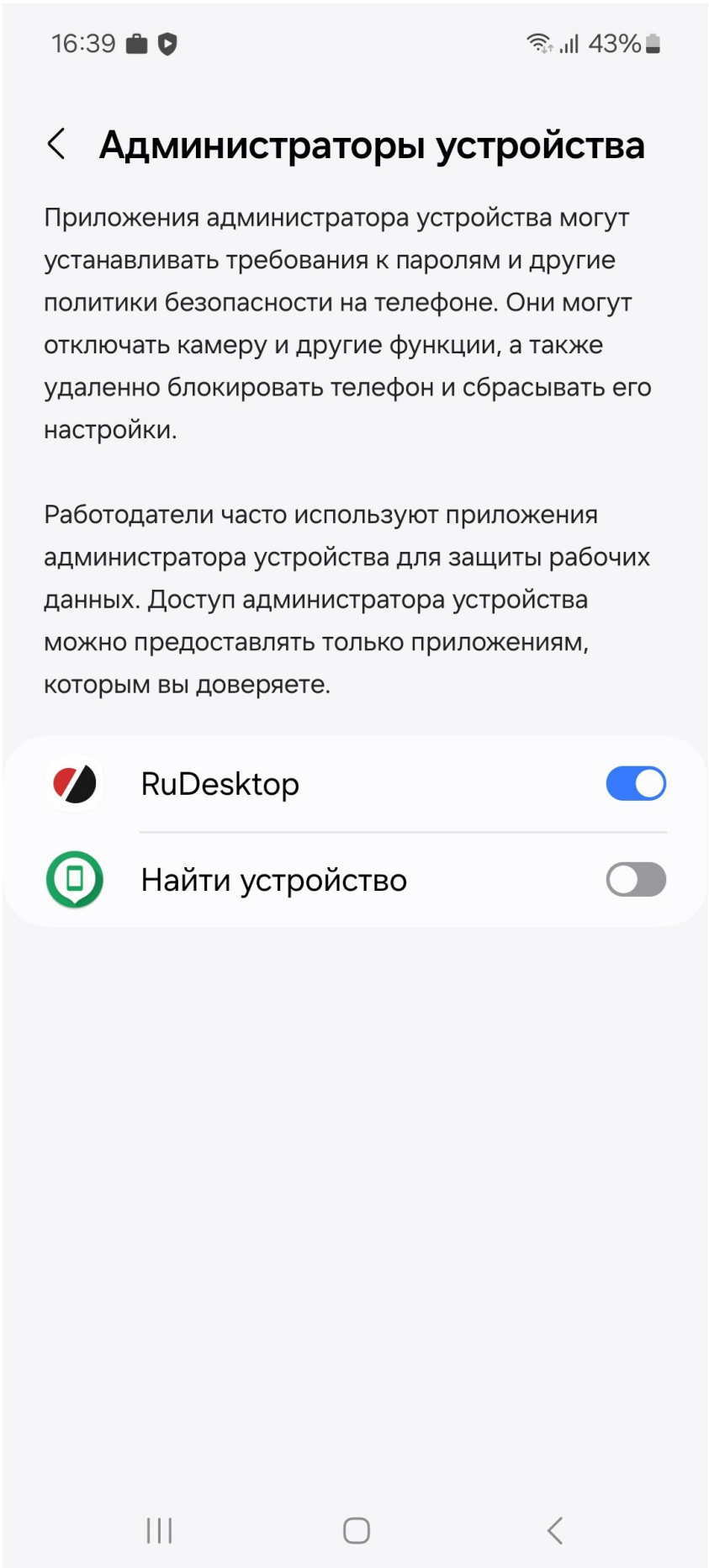

20 %
Настройка устройства
Управление и защиту устройства обеспечивает Ваша компания. Действия будут регулироваться положениями документа Google. Посмотреть условия
ПРИНЯТЬ И ПРОДОЛЖИТЬ


20 %
Настройка рабочего устройства
Ваша организация будет управлять этим устройством и обеспечивать его безопасность.
Это может занять несколько минут.

7. Выдать разрешения приложению **RuDesktop**
8. Устройство автоматически загрузит настройки и подключится к серверу

2.1.3 Проверка успешной регистрации

1. Убедиться, что приложение **RuDesktop** есть в списке и активировано:
    - Настройки → Безопасность → Расширенные настройки → Администраторы устройства


16:39
43%
Администраторы устройства
Приложения администратора устройства могут устанавливать требования к паролям и другие политики безопасности на телефоне. Они могут отключать камеру и другие функции, а также удаленно блокировать телефон и сбрасывать его настройки.
Работодатели часто используют приложения администратора устройства для защиты рабочих данных. Доступ администратора устройства можно предоставлять только приложениям, которым вы доверяете.
RuDesktop
Найти устройство

2. В веб-интерфейсе сервера **Rudesktop** проверить, что устройство появилось в списке устройств на странице Устройства

Важно

Шаги настройки и расположение конкретных настроек могут отличаться в зависимости от устройства и версии Android

После выполнения всех шагов вы можете перезагрузить телефон, чтобы убедиться, что служба **Rudesktop** запускается автоматически и устройство доступно для подключения, а также выполнять различные доступные политики для настройки устройства

2.2 Настройка Android через adb

2.2.1 Подготовка

1. Убедиться, что:
   - Устройство работает на Android 7.0+
   - Имеется доступ к разделу QR-коды MDM в панели администрирования сервера **Rudesktop**

     Подсказка

     Определяется наличием соответствующей лицензии и правами доступа

   - Устройство не привязано к аккаунту Google (FRP) – иначе потребуется авторизация
2. Создать QR-код в веб-интерфейсе сервера:
   1. В веб-интерфейсе сервера **Rudesktop** открыть страницу **Администрирование -> QR-коды MDM**
   2. Нажать на кнопку Добавить QR-код MDM
   3. Заполнить поля валидными данными
   4. Поля Ссылка на скачивание пакета и Адрес сервера заполняются автоматически
   5. Нажать на кнопку Сохранить
   6. В колонке Ссылка на скачивание нажать на URL, чтобы скачать **APK-файл для MDM**

      Важно

      Название APK-файла должно быть `rudesktop-mdm.apk`

2.2.2 Настройка

1. Активировать режим разработчика в настройках **Android** устройства
2. Открыть настройки разработчика и активировать опцию **Отладка по USB**
3. Подключить устройство через USB к ПК в режиме отладки
4. Выполнить команду для установки APK-файла:

```
adb install -r /path/to/rudesktop-mdm.apk
```

> **Важно**
>
> На ПК должен быть установлен пакет `adb` для выполнения команды
>
> Вместо `/path/to/rudesktop-mdm.apk` укажите путь до файла на ПК, который был загружен с веб-интерфейса сервера **RuDesktop** в блоке *Подготовка*

5. Выполнить команду для установки сервера для подключения:

```
adb shell am start -n ru.desktop.flutter_hbb/.
↪SplashScreenActivity --es rz_server АДРЕС_СЕРВЕРА
```

> **Важно**
>
> Вместо `АДРЕС_СЕРВЕРА` укажите ваш адрес сервера

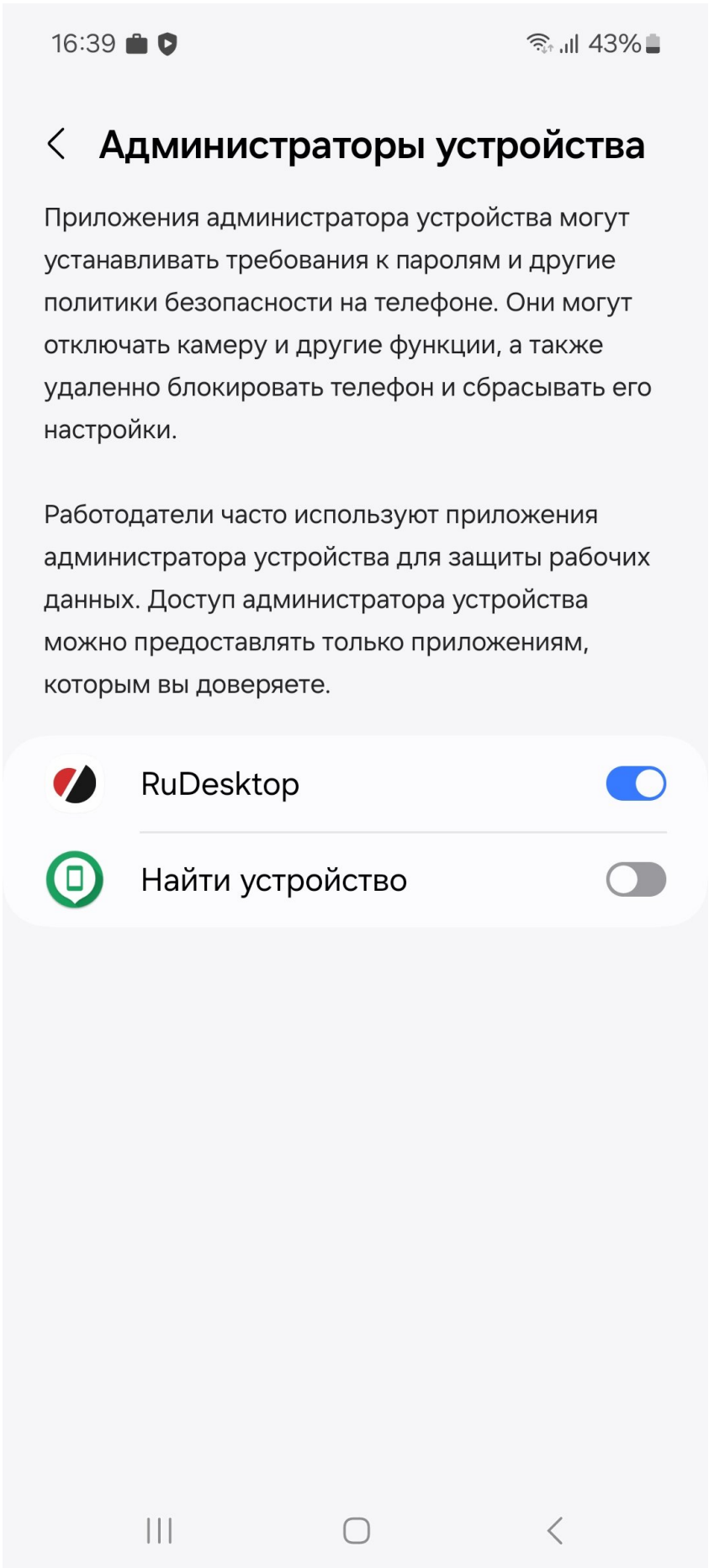
6. Выполнить команду для назначения приложения **Rudesktop** владельцем устройства:

```
adb shell dpm set-device-owner ru.desktop.flutter_hbb/.
↪AdminReceiver
```

7. Если это необходимо, то режим разработчика можно выключить

2.2.3 Проверка успешной регистрации

1. Убедиться, что приложение **RuDesktop** есть в списке и активировано:
   - Настройки → Безопасность → Расширенные настройки → Администраторы устройства


16:39
43%
Администраторы устройства
Приложения администратора устройства могут устанавливать требования к паролям и другие политики безопасности на телефоне. Они могут отключать камеру и другие функции, а также удаленно блокировать телефон и сбрасывать его настройки.
Работодатели часто используют приложения администратора устройства для защиты рабочих данных. Доступ администратора устройства можно предоставлять только приложениям, которым вы доверяете.
RuDesktop
Найти устройство

2. В веб-интерфейсе сервера **Rudesktop** проверить, что устройство появилось в списке устройств на странице Устройства

Важно

Шаги настройки и расположение конкретных настроек могут отличаться в зависимости от устройства и версии Android

После выполнения всех шагов вы можете перезагрузить телефон, чтобы убедиться, что служба **Rudesktop** запускается автоматически и устройство доступно для подключения, а также выполнять различные доступные политики для настройки устройства

2.3 Предустановка приложений через QR-код

2.3.1 Настройка

1. Убедиться, что:
   - Устройство работает на Android 7.0+
   - Имеется доступ к разделу QR-коды MDM в панели администрирования сервера **Rudesktop**

     Подсказка

     Определяется наличием соответствующей лицензии и правами доступа

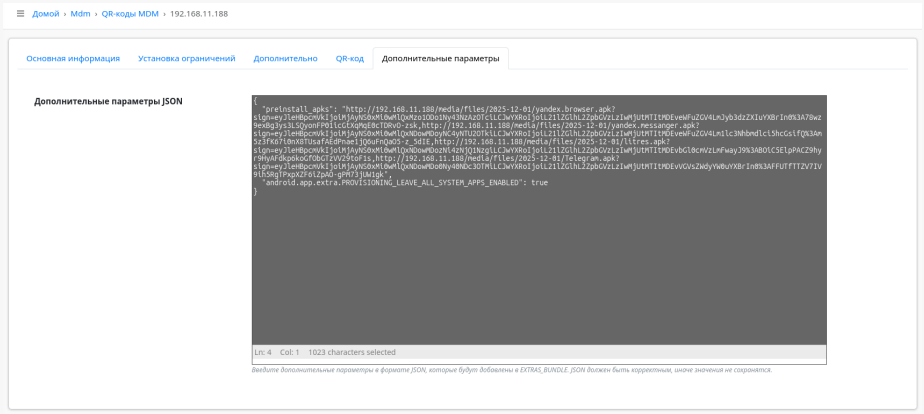
   - Устройство не привязано к аккаунту Google (FRP) – иначе потребуется авторизация
2. Создать QR-код в веб-интерфейсе сервера:
   1. В веб-интерфейсе сервера **Rudesktop** открыть страницу **Администрирование -> QR-коды MDM**
   2. Нажать на кнопку Добавить QR-код MDM
   3. Заполнить поля валидными данными
   4. Поля Ссылка на скачивание пакета и Адрес сервера заполняются автоматически
   5. Перейти на вкладку Дополнительные параметры
   6. В параметре `preinstall_apks` перечислить ссылки на пакеты через запятую. Для приложения из нескольких APK указать одну ссылку на архив целиком, например `.apks`

Подсказка

Вы можете загрузить apk на сервер **RuDesktop** на странице Файлы и использовать их URL-адреса для дальнейшего использования

Пример:

```
{
    "preinstall_apks": "http://192.168.11.188/file1.
↪apk,http://192.168.11.188/file2.apk"
}
```



Важно

- Если вы используете самоподписанные сертификаты, используйте протокол HTTP в URL-адресе
- При использовании HTTPS убедитесь, что у вас валидные сертификаты

7. Нажать на кнопку Сохранить
8. Нажать на ссылку Ссылка на QR код, откроется QR-код, который потребуется далее
9. Произвести *настройку Android через QR-код*

2.3.2 Описание

Во время настройки **Android** через QR-код на экране отобразится шаг **Прогресс установки**, если в QR-коде указаны ссылки на пакеты приложений

Важно

- Если при создании QR-кода не были указаны URL-адреса, экран **Прогресс установки** не будет отображаться во время настройки

- Для составного пакета клиент устанавливает базовый APK и подходящие части вместе
- Статус загрузки для каждого файла отображается в процентах
- Отображаются кнопки Повторить и Продолжить для повтора загрузки и установки в случае ошибки
- После завершения настройки убедитесь, что нужные приложения появились на устройстве и открываются

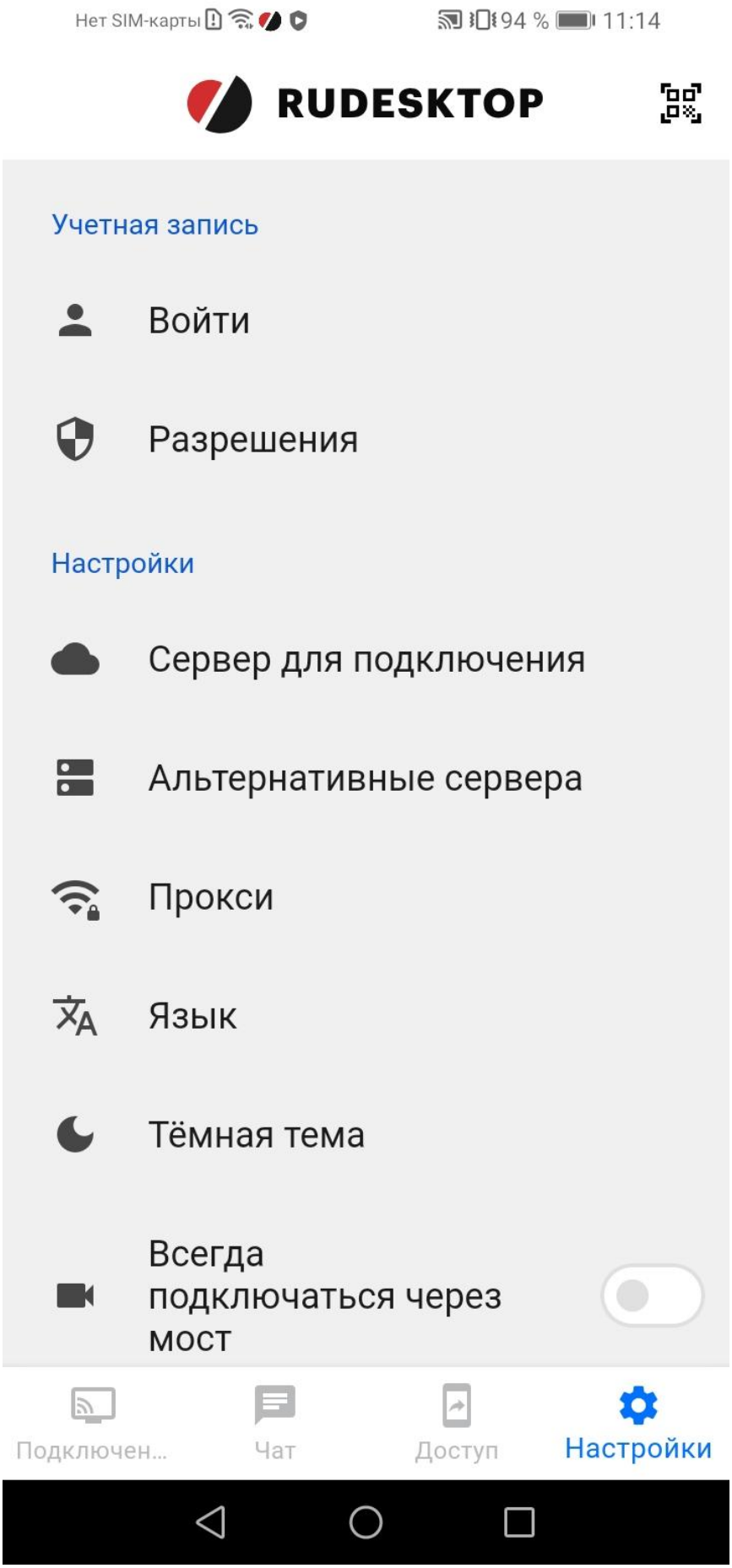
2.4 Установка адреса сервера через QR-код

На устройствах с Android 9 при настройке MDM через QR-код на стартовом экране (например, после сброса телефона) адрес сервера может не примениться автоматически в клиенте **RuDesktop**

В этом случае выполните повторное сканирование того же QR-кода уже внутри приложения

2.4.1 Порядок действий

1. Завершите *настройку Android через QR-код* и откройте установленное приложение **RuDesktop**
2. Перейдите на вкладку **«Настройки»**
3. В правом верхнем углу нажмите кнопку **«Сканер QR-кода»**

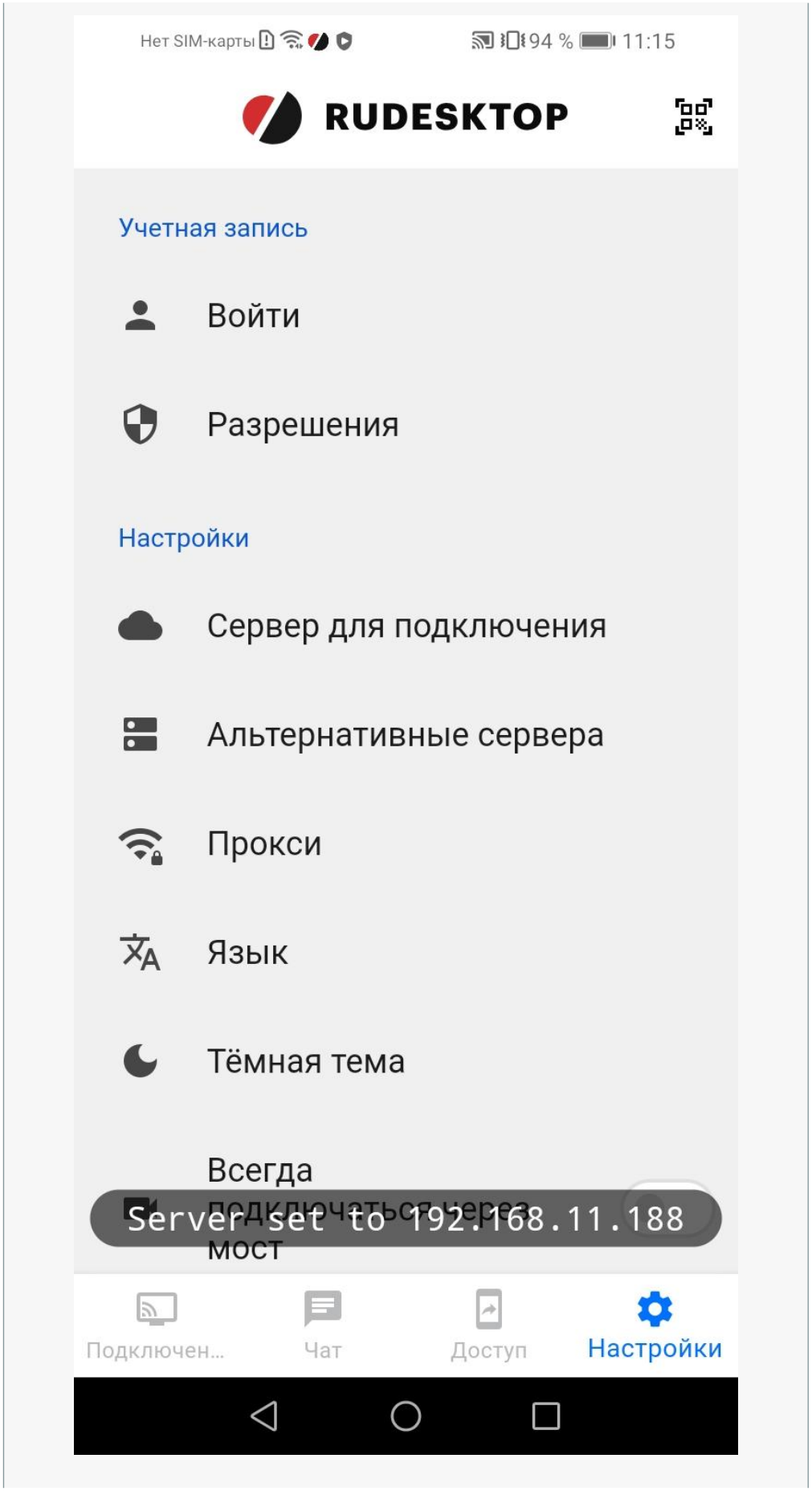

Нет SIM-карты
94 %
11:14
RUDESKTOP
Учетная запись
Войти
Разрешения
Настройки
Сервер для подключения
Альтернативные сервера
Прокси
Язык
Тёмная тема
Всегда подключаться через мост
Подключен...
Чат
Доступ
Настройки

4. Отсканируйте тот же QR-код, который использовали при настройке


Нет SIM-карты
94 %
11:15
Scan QR

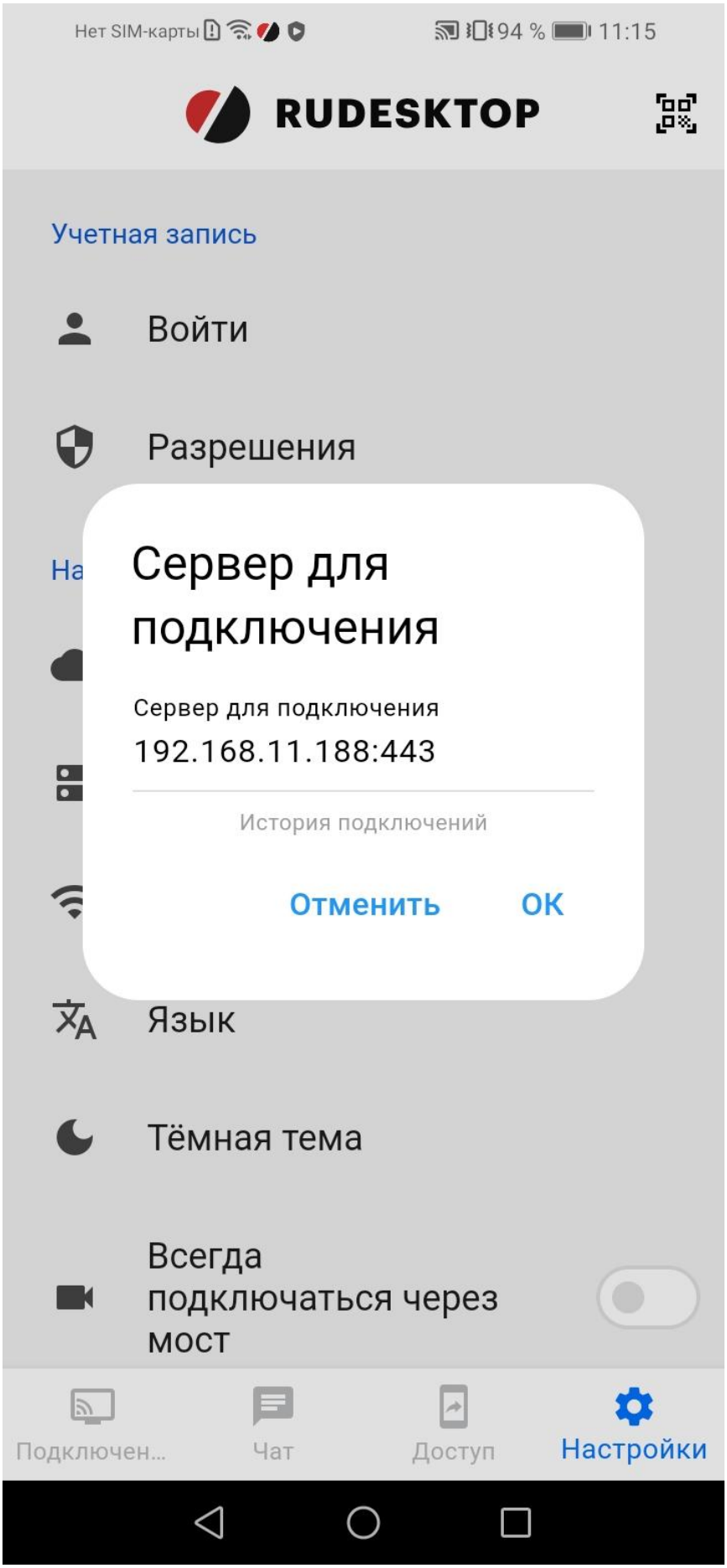
Важно

После сканирования должно появиться сообщение **«Server set to <адрес_сервера>»**


Нет SIM-карты
94 %
11:15
RUDESKTOP
Учетная запись
Войти
Разрешения
Настройки
Сервер для подключения
Альтернативные сервера
Прокси
Язык
Тёмная тема
Всегда подключаться через мост
Server set to 192.168.11.188
Подключен...
Чат
Доступ
Настройки

> Устройство отобразится на сервере **RuDesktop** в разделе Устройства

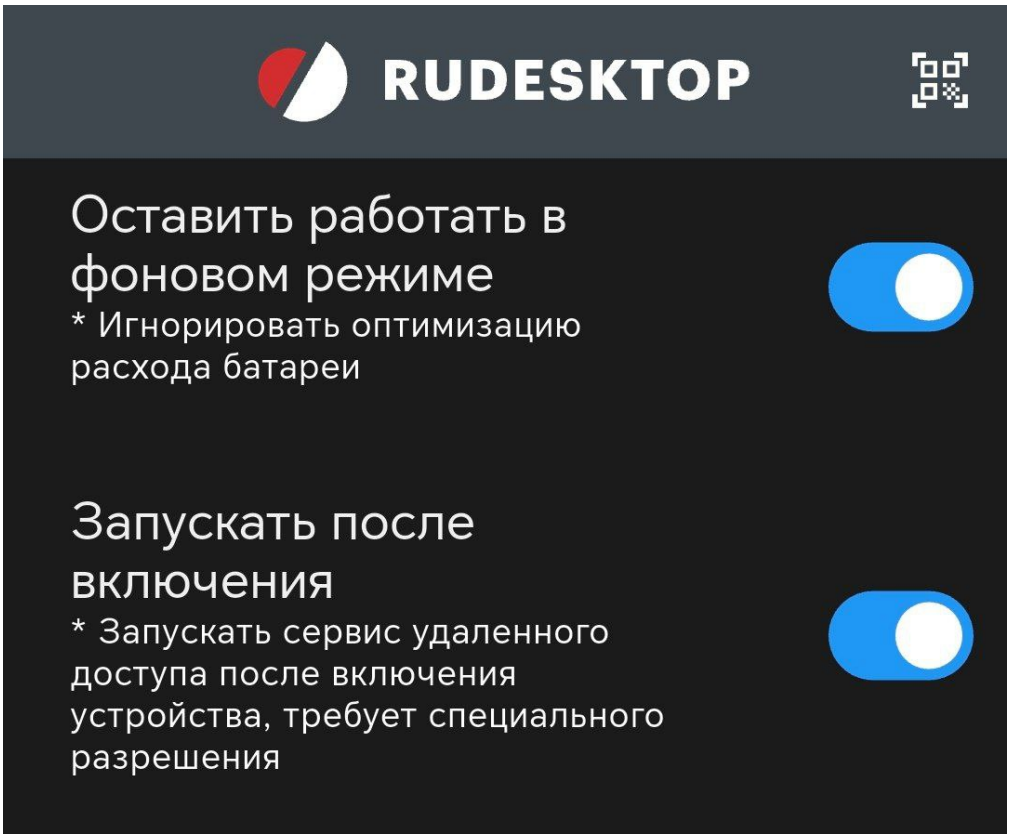
5. Адрес сервера применён и приложение готово к работе


Нет SIM-карты
94 %
11:15
RUDESKTOP
Учетная запись
Войти
Разрешения
Сервер для подключения
Сервер для подключения
192.168.11.188:443
История подключений
Отменить
OK
Язык
Тёмная тема
Всегда подключаться через мост
Подключен...
Чат
Доступ
Настройки

2.5 Устранение проблемы с автозапуском службы на Android

Чтобы активировать автозапуск службы в клиенте **RuDesktop** после перезагрузки устройства, которая находится во вкладке **Доступ**, выполните следующие шаги:

1. Открыть клиент **RuDesktop**
2. Перейти на вкладку **Настройки** и активировать следующие чекбоксы:
    - Оставить работать в фоновом режиме — игнорировать оптимизацию расхода батареи
    - Запускать после включения — запускать сервис удаленного доступа после включения устройства, требует специального разрешения



3. Активировать режим разработчика в настройках **Android** устройства
4. Открыть настройки разработчика и активировать опцию **Отладка по USB**
5. Подключить устройство через USB к ПК в режиме отладки
6. Выполнить команду:

```
adb shell appops set ru.desktop.flutter_hbb␣
↪PROJECT_MEDIA allow
```

Важно

На ПК должен быть установлен пакет `adb`

7. При необходимости режим разработчика можно выключить
8. Перезагрузить устройство

После перезагрузки устройства служба **RuDesktop** будет запущена автоматически, и к устройству можно будет подключиться без необходимости ручного подтверждения запуска

2.6 Перевод Android-устройства в режим «Киоск»

Доступна только в MDM версии

Кейс описывает, как централизованно перевести Android-устройство в режим **«Киоск»** — режим, в котором пользователь видит и может работать только с одним заданным приложением. Подходит для информационных терминалов, киосков самообслуживания, демонстрационных стендов

2.6.1 Подготовка

1. Узнайте имя пакета приложения, которое нужно запускать в режиме киоска

Подсказка

Имя пакета — это идентификатор Android-приложения, например `com.companyname.appname`. Узнать имя пакета можно в самом устройстве (**Настройки → Приложения → Сведения о приложении**) или у разработчика приложения

2. Убедитесь, что устройство:
   - Работает на **Android 9** или новее
   - Зарегистрировано на сервере как MDM-устройство (см. *Настройка Android через QR-код* или *Настройка Android через adb*)
   - Указанное приложение установлено и стабильно работает в полноэкранном режиме

2.6.2 Создание политики

1. В веб-интерфейсе сервера **RuDesktop** открыть страницу **UEM → Политики**
2. Нажать кнопку Добавить политику в правом верхнем углу
3. Выбрать шаблон **«Включение режима «Киоск» на Android»**

Полное описание полей политики — на странице Включение режима «Киоск» на Android

4. Заполнить поля:
   - Название — например, `Инфокиоск (приложение презентации)`
   - Выбор действия — **Включить**
   - Имя пакета — например, `com.company.presentation`
   - Функции системного пользовательского интерфейса — оставить только нужные элементы интерфейса (по умолчанию рекомендуется отключить всё)
   - Опции для выхода из режима киоск:
     - Активировать установку пароля выхода
     - Указать пароль (он понадобится для административного выхода из режима)
     - Указать таймаут возврата в режим (по умолчанию 30 минут)
     - Указать положение скрытой кнопки для вызова формы ввода пароля
5. Нажать кнопку Сохранить

2.6.3 Запуск на устройствах

1. Открыть страницу **UEM → Задачи**, нажать Добавить задачу
2. В поле Политики выбрать только что созданную политику
3. На вкладке Устройства и группы указать целевые устройства или группу
4. Запустить задачу

После применения:

- На выбранных устройствах будет активирован режим киоска и запущено указанное приложение в полноэкранном режиме
- Пользователь не сможет выйти в систему обычными средствами
- Для административного выхода: 5 нажатий за 2 секунды в скрытую область экрана (или 10 нажатий на кнопку уменьшения громкости) → ввод пароля выхода

Важно

Перед массовой раскаткой проверьте политику на одном устройстве через `Тестовый запуск`. Несовместимое приложение или неправильно подобранный набор элементов интерфейса могут сделать устройство непригодным для работы

2.6.4 Отключение режима

Чтобы вернуть устройства в обычный режим:

1. Создать ещё одну политику по тому же шаблону, выбрав Выбор действия → **Выключить**
2. Запустить её через задачу на тех же устройствах

После применения устройства вернутся в стандартный режим Android

2.7 Удалённый сброс Android-устройства до заводских настроек

Доступна только в MDM версии

Кейс описывает, как удалённо отправить команду полного сброса Android-устройства. Применяется при утере устройства, передаче устройства другому сотруднику или необходимости полной очистки корпоративных данных

Предупреждение

После выполнения политики **все** данные пользователя и локальные настройки на устройстве будут безвозвратно удалены. Действие необратимо

2.7.1 Подготовка

Убедитесь, что:

- Устройство зарегистрировано на сервере как MDM-устройство (см. *Настройка Android через QR-код*)
- На сервере выбрано именно нужное устройство — после запуска отменить операцию нельзя

2.7.2 Создание политики

1. В веб-интерфейсе сервера **RuDesktop** открыть страницу **UEM → Политики**
2. Нажать кнопку Добавить политику
3. Выбрать шаблон **«Сброс Android устройства до заводских настроек»**

   Полное описание полей политики — на странице Сброс Android устройства до заводских настроек
4. Заполнить поле Название — например, `Сброс утерянного устройства`
5. Нажать кнопку Сохранить

2.7.3 Запуск на устройстве

1. Открыть страницу **UEM → Задачи**, нажать Добавить задачу
2. В поле Политики выбрать только что созданную политику
3. На вкладке Устройства и группы указать **только** целевое устройство

> **Важно**
>
> Не применяйте политику к группе устройств без полной уверенности — все устройства в группе будут сброшены

4. Запустить задачу

После применения:

- На устройство уйдёт MDM-команда полного сброса
- Локальные данные, приложения и настройки будут удалены
- При следующем включении устройство потребует первоначальной настройки
- Для повторной регистрации в **RuDesktop** потребуется снова провести настройку через QR-код или adb

> **Подсказка**
>
> Если устройство утеряно и нужно гарантированно стереть данные, как только оно появится в сети — оставьте задачу запущенной. Сервер отправит команду, как только устройство выйдет на связь

2.8 Включение отслеживания геолокации на Android

Доступна только в MDM версии

Кейс описывает, как централизованно включить отправку геолокации Android-устройств на сервер **RuDesktop** для дальнейшего просмотра на карте. Подходит для контроля курьеров, выездных сотрудников, поиска утерянных устройств

Важно

Отслеживание геолокации связано с конфиденциальностью пользователей — убедитесь, что у вас есть правовые основания для этого, и сотрудники проинформированы

2.8.1 Подготовка

Убедитесь, что:

- Устройство зарегистрировано на сервере как MDM-устройство
- На устройстве разрешён доступ к местоположению (службы геолокации включены)
- У устройства есть постоянное подключение к интернету для отправки данных

2.8.2 Создание политики

1. В веб-интерфейсе сервера **RuDesktop** открыть страницу **UEM → Политики**
2. Нажать кнопку Добавить политику
3. Выбрать шаблон **«Управление отслеживанием геолокации Android»**

   Полное описание полей политики — на странице Управление отслеживанием геолокации Android
4. Заполнить поля:
   - Название — например, `Геолокация курьеров`
   - Выбор действия — **Включить**
   - Интервал обновления геолокации — частота отправки координат в минутах

   Подсказка

   Минимальное значение — 1 минута. Чем чаще обновление, тем точнее отслеживание, но выше расход батареи. Для большинства задач 5–15 минут достаточно
5. Нажать кнопку Сохранить

2.8.3 Запуск на устройствах

1. Открыть страницу **UEM → Задачи**, нажать Добавить задачу
2. В поле Политики выбрать только что созданную политику
3. На вкладке Устройства и группы указать целевые устройства или группу
4. Запустить задачу

После применения:

- На устройствах будет включена отправка геолокации с заданным интервалом
- Координаты устройств станут доступны на странице **Отчёты → Карта**

2.8.4 Отключение отслеживания

1. Создать ещё одну политику по тому же шаблону, выбрав Выбор действия → **Выключить**
2. Запустить её через задачу на тех же устройствах

После применения сбор и отправка координат будут прекращены

Предупреждение

Отслеживание геолокации значительно увеличивает расход батареи. Если устройство долго не подключено к зарядке, его автономная работа сократится

2.9 Блокировка камеры на Android

Доступна только в MDM версии

Кейс описывает, как централизованно запретить использование камеры на Android-устройстве. Подходит для устройств, работающих в зонах с ограничением фото- и видеосъёмки, в режимных помещениях, на терминалах самообслуживания

2.9.1 Подготовка

Убедитесь, что устройство зарегистрировано на сервере как MDM-устройство (см. *Настройка Android через QR-код*)

2.9.2 Создание политики

1. В веб-интерфейсе сервера **RuDesktop** открыть страницу **UEM → Политики**
2. Нажать кнопку Добавить политику
3. Выбрать шаблон **«Управление запретом использования камеры на Android»**

   Полное описание полей политики — на странице Управление запретом использования камеры на Android
4. Заполнить поля:
   - Название — например, `Запрет камеры в режимной зоне`
   - Выбор действия — **Запретить**
5. Нажать кнопку Сохранить

2.9.3 Запуск на устройствах

1. Открыть страницу **UEM → Задачи**, нажать Добавить задачу
2. В поле Политики выбрать только что созданную политику
3. На вкладке Устройства и группы указать целевые устройства или группу
4. Запустить задачу

После применения камера на выбранных устройствах будет заблокирована на уровне системы — её не смогут использовать ни встроенное приложение **Камера**, ни сторонние приложения

2.9.4 Снятие блокировки

1. Создать ещё одну политику по тому же шаблону, выбрав Выбор действия → **Разрешить**
2. Запустить её через задачу на тех же устройствах

После применения камера снова станет доступна

Важно

Блокировка камеры может повлиять на работу приложений, которым нужна фото- или видеосъёмка (например, сканеры QR-кодов, видеоконференции). Перед массовой раскаткой проверьте совместимость с используемыми приложениями

2.10 Подготовка корпоративного Android-устройства

Задача - настроить рабочее устройство так, чтобы сотрудник мог пользоваться нужными приложениями, а параметры связи и ограничения оставались под управлением администратора

2.10.1 Что подготовить

1. Зарегистрировать устройство по *инструкции MDM*
2. Проверить доступность устройства серверу и успешное выполнение простой политики
3. Узнать версию Android, чтобы выбрать поддерживаемые ограничения
4. Подготовить рабочую сеть Wi-Fi и резервный канал связи, если будут меняться параметры сети
5. Проверить, что пользователь знает PIN-код или пароль экрана, до ограничения биометрического входа

Примечание

Сначала выполнять каждую политику через **«Тестовый запуск»** на одном устройстве

Этот запуск действительно меняет настройки устройства

Следующую политику применять после проверки предыдущей

2.10.2 Настроить связь

1. Подключить устройство к рабочей сети Wi-Fi и убедиться, что сервер его видит
2. Для Android 13 и новее выбрать минимальный уровень безопасности Wi-Fi, которому соответствует рабочая сеть
3. Выполнить политику и снова проверить доступность устройства
4. Если сотрудник не должен выключать Wi-Fi, применить запрет переключения Wi-Fi

Важно

Политика минимальной защиты не передаёт пароль сети и не настраивает корпоративные сертификаты. Если устройство потеряло связь, сначала подключить его к разрешённой сети либо восстановить мобильный доступ. Новая разрешающая политика не сможет прийти на отключённое от сети устройство

2.10.3 Задать внешний вид

1. Создать политику установки обоев
2. Выбрать изображение JPG или PNG и нужный экран
3. Выполнить политику и проверить изображение на устройстве
4. После успешной установки применить запрет изменения обоев

Раздельные обои рабочего стола и экрана блокировки, а также запрет их изменения доступны с Android 7

2.10.4 Выбрать ограничения

Необязательно включать все ограничения сразу. Выбирать только те, которые нужны для работы сотрудников:

- Учётные записи - запретить добавление и удаление аккаунтов Android
- USB и накопители - закрыть передачу файлов и подключение внешних носителей
- NFC и Android Beam — на Android 15 и новее можно запретить NFC, на Android 5.1–9 — отправку файлов через Android Beam

- Микрофон - запретить использование микрофона, если рабочим приложениям не нужна запись звука
- Экран блокировки - скрыть уведомления, закрыть камеру на заблокированном экране или ограничить биометрию
- Режим полёта - ограничить его переключение пользователем на Android 9 и новее

2.10.5 Проверить результат и распространить настройки

1. Проверить статус каждого задания на сервере
2. На устройстве проверить рабочие приложения, сеть, разблокировку и доступность запрещённых действий
3. Убедиться, что устройство остаётся доступным серверу после применения всего набора
4. Назначить проверенные политики нужной группе устройств

Примечание

На устройствах разных моделей и версий Android проверку проводить отдельно. Например, запрет ярлыков экрана блокировки поддерживается с Android 14, а на более ранних версиях пропускается

2.10.6 Что проверить на самом устройстве

Проверить не только успешный статус задания, но и нужное действие:

- После запрета изменения аккаунтов попытаться открыть добавление учётной записи в настройках Android
- После ограничения USB проверить передачу файлов с компьютера и подключение внешнего накопителя
- После запрета микрофона проверить запись звука в приложении, которому выдано разрешение на микрофон
- После изменения экрана блокировки заблокировать устройство и проверить выбранные функции, затем войти по PIN-коду или паролю
- После настройки Wi-Fi убедиться, что устройство остаётся доступным серверу и переключатель ведёт себя согласно выбранной политике

Подсказка

Если действие осталось доступным, проверить результат именно этого задания, версию Android и поддержку ограничения на устройстве

Не назначать непроверенный набор ограничений сразу всей группе

2.10.7 Как отменить ограничения

Выполнить соответствующие политики с действием **«Разрешить»**. Для экрана блокировки выбрать **«Разрешить всё»**, а для снятия минимального уровня защиты Wi-Fi - **«Открытые (без шифрования)»**

Важно

Отключение расписания или удаление политики на сервере не отправляет устройству обратную команду и само по себе не снимает ранее установленный запрет. Если другая активная политика снова устанавливает тот же запрет, согласовать её параметры и расписание перед разрешающим запуском

MDM (*Mobile Device Management*) - это режим централизованного управления Android-устройствами, при котором клиент **RuDesktop** получает права владельца устройства (*Device Owner*) и выполняет административные действия по командам сервера. В этом режиме сервер может:

- Регистрировать устройство при первом включении или после сброса (через QR-код или `adb`)
- Удалённо устанавливать и удалять приложения, в том числе без участия пользователя
- Блокировать использование камеры, режима разработчика, изменения SIM-карты
- Переводить устройство в режим **«Киоск»** - работа только с одним приложением
- Отслеживать геолокацию устройства
- Удалённо блокировать или сбрасывать устройство до заводских настроек

Важно

Функции MDM доступны только в **MDM-версии** сервера **RuDesktop** и работают только на Android 7.0 и новее

Для перевода устройства в управляемый режим устройство должно быть сброшено до заводских настроек

Кейсы ниже разделены на две группы: **регистрация устройств** на сервере и **управление** уже зарегистрированными устройствами через политики

2.11 Регистрация устройств

Настройка Android через QR-код

Регистрация устройства как Device Owner на стартовом экране после сброса через сканирование QR-кода

Настройка Android через adb

Регистрация устройства как Device Owner через `adb`-подключение с компьютера администратора

Предустановка приложений через QR-код

Автоматическая установка набора `.apk`-приложений сразу при первичной регистрации устройства через QR-код

Установка адреса сервера через QR-код

Решение для Android 9, когда адрес сервера не применяется после сканирования QR-кода на стартовом экране

Устранение проблемы с автозапуском службы на Android

Настройка автозапуска службы клиента **RuDesktop** после перезагрузки и игнорирование оптимизации батареи

2.12 Управление устройствами

Перевод устройства в режим «Киоск»

Запуск устройства в режиме одного приложения для информационных терминалов и киосков самообслуживания

Удалённый сброс устройства до заводских настроек

Полная очистка устройства при утере или передаче другому сотруднику
Действие необратимо

Включение отслеживания геолокации

Отправка координат устройства на сервер для просмотра на карте - для контроля курьеров и поиска утерянных устройств

Блокировка камеры

Централизованный запрет использования камеры для устройств в режимных помещениях и зонах ограничения съёмки

Подготовка корпоративного Android-устройства

Настройка связи, обоев и ограничений с проверкой результата и порядком отмены

ГЛАВА 3

Настройка прав и доступов

3.1 Настройка типовых ролей через группы

Кейс описывает, как организовать разделение полномочий в **RuDesktop** через стандартные группы. Сервер из коробки содержит несколько предустановленных групп, которые покрывают типовые роли в организации:

- Администратор — полный доступ
- Руководитель подразделения — расширенный доступ к устройствам своего подразделения
- Сотрудник поддержки — подключение к устройствам пользователей для оказания помощи
- Гость — минимальные права (для новых пользователей и устройств по умолчанию)
- Без доступа — полная блокировка

Подсказка

Предустановленные группы нельзя удалить, но можно редактировать. При желании можно создать собственные группы под свои роли

3.1.1 Подготовка

Решите, какие роли нужны в вашей организации. Минимальный набор — три:

- **Администратор** — настраивает сервер, управляет пользователями и политиками

- **Сотрудник поддержки** — подключается к устройствам пользователей по заявкам
- **Сотрудник** — обычный пользователь рабочего устройства

3.1.2 Распределение по предустановленным группам

Администратор

1. Открыть страницу **Организация → Группы**
2. Открыть группу Администратор
3. Перейти на вкладку Пользователи и добавить учётные записи системных администраторов

> **Подсказка**
>
> В этой группе по умолчанию активированы все права. Подробное описание полей — на странице Права групп

Сотрудник поддержки

1. Открыть группу Сотрудник поддержки
2. На вкладке Пользователи добавить учётные записи сотрудников техподдержки
3. На вкладке Права оставить минимально необходимый набор. Рекомендуется:
   - Может авторизоваться в клиенте
   - Может видеть вкладку «Адресная книга» в приложении
   - Может видеть вкладку «Найдено» в приложении
   - Может использовать клавиатуры и мышь
   - Может использовать буфер обмена
   - Может видеть свой пароль
   - Может запускать политики — если сотрудник поддержки должен запускать политики на устройствах

Гость (новые пользователи и устройства)

1. Открыть группу Гость
2. На вкладке Права оставить только базовые:
   - Может подключаться к серверу — иначе клиент даже не зарегистрируется
3. Перейти в **Администрирование → Настройки → Безопасность** и в поле Группа по умолчанию для новых пользователей и Группа по умолчанию для новых устройств выбрать **Гость**

После этого все новые подключившиеся клиенты и зарегистрированные пользователи будут попадать в **Гость** с минимальными правами

3.1.3 Создание собственной роли

Если стандартных групп недостаточно, можно создать свою:

1. На странице **Организация → Группы** нажать Добавить Группу
2. Заполнить Название группы (например, `Бухгалтерия`)
3. На вкладке Права выбрать нужный набор полномочий
4. На вкладке Пользователи добавить учётные записи участников этой роли
5. На вкладке Устройства добавить рабочие устройства этих пользователей

> **Подсказка**
>
> В одной группе могут быть и пользователи, и устройства. Пользователи получают права через группу; устройства попадают в область действия этих прав

6. Сохранить группу

3.1.4 Настройка взаимных доступов

Группы определяют, **что разрешено** делать пользователю или устройству, но не **кто к кому может подключаться**. Для этого нужны **Доступы**:

1. Перейти на страницу **Удалённый доступ → Доступы**
2. Нажать Добавить Доступ
3. Создать минимально необходимый набор правил, например:

Доступ	Подключаемые устройства	Устройства для подключения
Администраторы → все	`Администратор`	Все устройства
Поддержка → пользовательские устройства	`Сотрудник поддержки`	Группа `Пользовательские устройства`
Бухгалтерия → между собой	`Бухгалтерия`	`Бухгалтерия`

4. На вкладке Права подключения выбрать нужные права (мастер-пароль, без подтверждения и т.д.)
5. На вкладке Разрешения выбрать типы подключений (Удалённый доступ, Передача файлов, Терминал и т.д.)

6. Сохранить

Подсказка

Подробнее о доступах — на странице Доступы

3.1.5 Проверка

1. Авторизуйтесь в клиенте под пользователем-сотрудником поддержки
2. Попробуйте подключиться к устройству, **разрешённому** правилом доступа — подключение должно пройти с правами и разрешениями, которые заданы в **Доступах**
3. Попробуйте подключиться к устройству, для которого правило доступа **не настроено** — подключение должно быть запрещено

Важно

Суперпользователь обходит все ограничения. Для тестирования прав используйте обычную учётную запись

3.2 Подключение к устройствам без подтверждения

Кейс описывает, как настроить подключение таким образом, чтобы сотрудники службы технической поддержки могли подключаться к устройствам пользователей без необходимости подтверждения с их стороны

Подходит для оперативного оказания помощи пользователям, когда ждать подтверждения нецелесообразно (например, удалённая инвентаризация, разовое вмешательство, поддержка вне рабочего времени)

Важно

Подключение без подтверждения — мощное право. Не выдавайте его всем подряд: оно убирает у пользователя возможность отказаться от сессии. Для целевых сотрудников рекомендуется использовать выделенную группу

3.2.1 Подготовка

Решите, **кому** разрешить подключение без подтверждения — обычно это сотрудники техподдержки. Для удобства такие операторы выносятся в отдельную группу

3.2.2 Создание группы операторов

1. Перейти на страницу **Организация → Группы**
2. Нажать Добавить Группу
3. Заполнить Название группы — например, `Техподдержка`
4. На вкладке Пользователи добавить учётные записи сотрудников службы технической поддержки
5. Сохранить группу

> **Подсказка**
>
> Подробное описание полей и доступных прав группы — на странице Права групп

3.2.3 Создание группы устройств пользователей

1. На странице **Организация → Группы** нажать Добавить Группу
2. Заполнить Название группы — например, `Пользовательские устройства`
3. На вкладке Устройства добавить устройства пользователей, к которым будет разрешено подключаться
4. На вкладке Права убедиться, что активны минимально необходимые права:
   - Может подключаться к серверу — иначе клиент не сможет зарегистрироваться
   - Может запускать политики — если на устройства должны применяться политики
5. Сохранить группу

3.2.4 Создание доступа без подтверждения

1. Перейти на страницу **Удалённый доступ → Доступы**
2. Нажать Добавить Доступ
3. На вкладке Основная информация:
   - Название — например, `Техподдержка пользователей`
   - Активировать чек-бокс Включено
4. На вкладке Подключаемые устройства в блоке Группы выбрать `Техподдержка`
5. На вкладке Устройства для подключения в блоке Группы выбрать `Пользовательские устройства`
6. На вкладке Права подключения активировать:

- Может подключаться без подтверждения со стороны пользователя — основное право, позволяющее инициировать сессию без запроса разрешения у пользователя устройства

Подсказка

Чтобы оператор мог подключаться **без знания пароля устройства** и/или скрытно (без появления окна подключения у пользователя), дополнительно активируйте Доступ к устройствам по мастер паролю и Скрывать окно подключения при использовании мастер пароля. Подробнее — на странице *Подключение по мастер-паролю*

7. На вкладке Разрешения выбрать нужные типы подключения (например, **Удалённый доступ**, **Передача файлов**, **Терминал**)
8. Нажать Сохранить

3.2.5 Использование на стороне оператора

1. Открыть клиент **RuDesktop**, авторизоваться под пользователем, входящим в группу `Техподдержка`
2. Инициировать подключение к целевому устройству (ввести ID устройства в поле подключения или выбрать его из любого доступного источника)
3. Подключение начнётся без появления окна подтверждения у пользователя устройства

3.2.6 Проверка

1. Авторизоваться в клиенте под пользователем-сотрудником поддержки
2. Попробовать подключиться к устройству, **попадающему** в группу `Пользовательские устройства` — подключение должно начаться без запроса подтверждения у пользователя устройства
3. Попробовать подключиться к устройству, **не попадающему** в группу — подключение должно быть запрещено или потребовать подтверждения (если для него действуют другие правила доступа)

Важно

Суперпользователь обходит все ограничения. Для тестирования прав используйте обычную учётную запись

3.3 Подключение по мастер-паролю

Кейс описывает, как настроить подключение к устройствам по **мастер-паролю** — без необходимости вводить временный или постоянный пароль удалённого устройства

Подходит, например, для администраторов, которые подключаются к большому количеству устройств, или для сотрудников техподдержки, чтобы ускорить начало сессии

3.3.1 Подготовка

Решите, **кому** разрешить подключение по мастер-паролю — обычно это группы Администратор и Сотрудник поддержки

Важно

Подключение по мастер-паролю — мощное право. Не выдавайте его всем подряд: оно даёт вход в любое устройство, попадающее под доступ, без знания пароля этого устройства

3.3.2 Создание доступа с мастер-паролем

1. Перейти на страницу **Удалённый доступ → Доступы**
2. Нажать Добавить Доступ
3. На вкладке Основная информация:
   - Название — например, `Техподдержка по мастер-паролю`
   - Активировать чек-бокс Включено
4. На вкладке Подключаемые устройства выбрать **группу** или **пользователей**, которым разрешено подключаться по мастер-паролю (например, `Сотрудник поддержки`)
5. На вкладке Устройства для подключения указать целевые устройства или группу (например, `Пользовательские устройства`)
6. На вкладке Права подключения активировать:
   - Доступ к устройствам по мастер паролю — основное право, которое и включает подключение по мастер-паролю
   - Может подключаться без подтверждения со стороны пользователя — иначе на удалённом устройстве всё равно появится окно «Разрешить подключение?»

     Подсказка

     Если это право не активно, но активно Доступ к устройствам по мастер паролю, то для подключения всё равно потребуется подтверждение со стороны пользователя

   - Скрывать окно подключения при использовании мастер пароля — если нужно «незаметное» подключение, чтобы окно подтверждения не появлялось у пользователя вообще

Важно

Это право работает **только** в связке с Доступ к устройствам по мастер паролю

7. На вкладке Разрешения выбрать нужные типы подключения (например, **Удалённый доступ**, **Передача файлов**, **Терминал**)
8. Нажать Сохранить

3.3.3 Использование на стороне оператора

1. Открыть клиент **RuDesktop**, авторизоваться под пользователем, входящим в группу с правом мастер-пароля
2. Инициировать подключение к целевому устройству (ввести ID устройства в поле подключения или выбрать его из любого доступного источника)
3. Подключение пройдёт без запроса пароля удалённого устройства

   Если активно право Скрывать окно подключения при использовании мастер пароля — пользователь удалённого устройства не увидит уведомления о подключении

3.3.4 Отличие от обычного подключения «без подтверждения»

- Может подключаться без подтверждения со стороны пользователя — позволяет начать сессию без запроса разрешения у пользователя устройства, **но** оператор всё равно должен знать временный или постоянный пароль устройства
- Доступ к устройствам по мастер паролю — оператор подключается **вообще без знания пароля устройства**, используя мастер-пароль

Эти права независимы и комбинируются: если активны оба, оператор подключается мгновенно, без пароля и без подтверждения

3.4 Доступы через динамические группы

Кейс описывает, как настроить доступы не на статические группы устройств, а на **динамические группы**, которые автоматически пересчитываются по правилу — например, «все устройства Linux», «устройства подсети 192.168.10.0/24», «устройства, попавшие в кастомный фильтр»

Подходит, когда состав устройств часто меняется и поддерживать списки вручную невозможно

Подсказка

Динамические группы доступны только в локальной версии сервера **Управление конфигурациями (UEM)**

3.4.1 Подготовка

Чётко сформулируйте критерий, по которому устройства должны попадать в группу. Поддерживаются три типа выражений:

- **Маска** — Ansible-выражение по фактам устройства (ОС, подсеть, hostname и т.д.)
- **SQL запрос** — произвольный SQL-запрос к базе сервера
- **Группа из фильтра** — фиксированный набор условий, заданный фильтром на странице **Удалённый доступ → Устройства**

Подробное описание — на странице Динамические группы

3.4.2 Создание динамической группы

Пример: «Все устройства на Linux»

1. Перейти на страницу **Организация → Динамические группы**
2. Нажать Добавить Динамическую группу
3. Заполнить:
   - Название группы — например, `По типу ОС`
   - Тип группы — **Маска**
   - Выражение для создания динамической группы:

     ```
     {{ ansible_facts.system | default('') }}
     ```

     В результате на каждый встретившийся вариант ОС (Linux, Windows, Darwin) будет создана отдельная **загруженная** дочерняя группа
4. Нажать Проверить и загрузить динамические группы и дождаться завершения
5. Сохранить группу

После этого на вкладке Загруженные динамические группы появятся дочерние группы — например, `Linux`, `Win32NT`, `Darwin`

Пример: «Все устройства из подсети 192.168.10.0/24»

1. На странице **Удалённый доступ → Устройства** настроить фильтр по подсети
2. В меню **Действия** выбрать **Создать динамическую группу на основе фильтра**. Для этого требуется право **Динамические группы → Создание**
3. Указать имя — например, `Бухгалтерия (подсеть 10)`

Тип группы будет автоматически проставлен как **Группа из фильтра**

3.4.3 Создание доступа на динамическую группу

1. Перейти на страницу **Удалённый доступ → Доступы**
2. Нажать Добавить Доступ
3. На вкладке Основная информация указать название (например, `Поддержка → все Linux`) и активировать Включено
4. На вкладке Подключаемые устройства:
    - В блоке Группы выбрать группу с операторами (например, `Сотрудник поддержки`)
5. На вкладке Устройства для подключения:
    - В блоке Дин.Группы выбрать нужную **загруженную** дочернюю группу (например, `Linux`)

> **Важно**
>
> В правиле доступа выбирается именно **загруженная** группа (дочерняя), а не родительская динамическая группа

6. На вкладке Права подключения выбрать нужные права (мастер-пароль, без подтверждения, скрытое подключение и т.д.)
7. На вкладке Разрешения выбрать типы подключения (Удалённый доступ, Терминал, Передача файлов и т.д.)
8. Нажать Сохранить

3.4.4 Поддержание группы в актуальном состоянии

Состав динамической группы пересчитывается:

- **Вручную** — при нажатии Проверить и загрузить динамические группы в свойствах группы
- **Автоматически** — при выполнении политики Инвентаризация на устройствах. В рамках этой политики сервер собирает факты Ansible с устройств и пересчитывает все динамические группы по их выражениям

Чтобы пересчёт происходил регулярно, настройте инвентаризацию по расписанию:

1. Перейти на страницу **UEM → Задачи**
2. Открыть существующую задачу Инвентаризация (создаётся автоматически после установки сервера) или создать новую с политикой **Инвентаризация**
3. Настроить расписание (например, ежедневно ночью) и активировать чекбокс Активно

Подсказка

Без выполненной инвентаризации динамические группы по типу **Маска** не получат свежих фактов устройств и могут не учесть их в дочерней группе

3.4.5 Проверка

1. Открыть свойства динамической группы в **Организация → Динамические группы**, перейти на вкладку Загруженные динамические группы и убедиться, что нужные устройства попали в дочернюю группу
2. Авторизоваться в клиенте под пользователем-оператором
3. Попробовать подключиться к устройству, которое **попадает** в динамическую группу — подключение должно пройти с правами и разрешениями, заданными в правиле доступа
4. Попробовать подключиться к устройству, которое **не попадает** в группу — подключение должно быть запрещено (если для него нет других подходящих доступов)
5. Если состав группы устарел — запустить задачу инвентаризации или нажать Проверить и загрузить динамические группы вручную

Подсказка

Динамические группы можно использовать не только в доступах, но и при назначении политик через задачи. Это удобно, чтобы политика автоматически применялась ко всем устройствам, попадающим под условие

3.5 Общая адресная книга для подразделения

Кейс описывает, как организовать **общую адресную книгу** — единый набор адресов устройств, доступный сразу нескольким сотрудникам

Подходит, например, для отдела техподдержки, которому нужен общий список обслуживаемых устройств, или для команды, работающей с одним пулом серверов. Вместо того чтобы каждый сотрудник вручную заводил одни и те же адреса в своей личной книге, администратор один раз наполняет общую книгу и выдаёт к ней доступ

Подсказка

Доступ к общей книге выдаётся на одном из трёх уровней:

- Просмотр — видеть адреса и теги книги и подключаться к устройствам
- Изменение — дополнительно добавлять, редактировать и удалять адреса и теги

- Управление — дополнительно редактировать саму книгу, управлять доступом, включать/выключать и удалять её

3.5.1 Подготовка

Определите:

- **какой книгой пользоваться** — у каждого подразделения при его создании уже появляется автоматически созданная книга **«Общая книга — название_подразделения»**, которой управляет руководитель подразделения. Часто отдельную книгу создавать не нужно
- **кому и на каком уровне** выдать доступ — отдельным пользователям или целым группам

Важно

Чтобы сотрудник видел страницы адресной книги в веб-интерфейсе, у него должно быть право **Адресная книга → Просмотр** (см. Права групп). Уровень доступа к конкретной книге (Просмотр/Изменение/Управление) и это право работают **совместно**

3.5.2 Шаг 1. Взять готовую или создать книгу

Вариант А — книга подразделения

1. Перейти на страницу **Удалённый доступ → Адресные книги**
2. Найти книгу **«Общая книга — название_подразделения»** (тип **Общая**)
3. Открыть её через Редактировать

Дальнейшие шаги по наполнению и выдаче доступа одинаковы для любой общей книги

Вариант Б — создать отдельную книгу

1. На странице **Адресные книги** нажать Добавить адресную книгу

Примечание

Кнопка доступна при наличии права **Адресная книга → Создание**

2. Заполнить поля:
   - Название — например, `Обслуживаемые серверы`
   - Описание — назначение книги (необязательно)

- Подразделение — при необходимости привязать книгу к подразделению (поле доступно при наличии права **Подразделения → Просмотр**)

3. Нажать Сохранить

Созданная книга является **общей**, и вы автоматически получаете к ней уровень доступа **Управление** (как её владелец, а при привязке к подразделению — как его руководитель)

Подсказка

Если нужный набор адресов уже есть в вашей книге, общую книгу можно создать сразу из них — массовым действием Создать новую книгу из выбранных адресов на странице Адреса (действие доступно суперпользователю и пользователю с правом **«Руководитель подразделения»**)

3.5.3 Шаг 2. Наполнить книгу адресами

Любым из способов:

- **По одному** — в свойствах книги на вкладке Адреса нажать Добавить адрес (книга уже будет выбрана)
- **Массово из существующих адресов** — на странице Адреса отметить нужные адреса, выбрать действие Скопировать в адресную книгу, указать книгу-получатель и нажать Скопировать
- **Из файла** — импортировать адреса в личную книгу (Импорт адресов), а затем скопировать их в общую книгу тем же действием Скопировать в адресную книгу

Примечание

Адреса, устройства которых уже есть в книге-получателе, повторно не копируются

3.5.4 Шаг 3. Выдать доступ к книге

1. Открыть свойства книги (Редактировать) и перейти на вкладку Доступ к адресной книге
2. Нажать Добавить ещё доступ
3. Заполнить строку:
   - Пользователь **или** Группа — кому выдаётся доступ
   - Право — уровень доступа: **Просмотр**, **Изменение** или **Управление**
4. При необходимости добавить ещё строки для других пользователей или групп
5. Нажать Сохранить

Важно

- В одной строке заполняется **либо** Пользователь, **либо** Группа, но не оба сразу
- Одному и тому же пользователю или группе нельзя выдать доступ дважды в пределах одной книги
- При выдаче доступа группе его получают все участники группы
- В облачной версии доступ выдаётся только пользователям — поле Группа недоступно

Подсказка

Для отдела техподдержки удобно выдать доступ **группе** (например, `Сотрудник поддержки`) на уровне Просмотр — тогда новые сотрудники получают общий список автоматически при добавлении в группу. Тем, кто ведёт список, выдайте уровень Изменение

3.5.5 Что увидят участники

- **В веб-интерфейсе** — на странице Адреса появятся адреса общей книги; по ним можно подключаться и (при уровне **Изменение**) редактировать их
- **В клиенте RuDesktop** — общая книга появится в **переключателе книг** на вкладке Адресная книга. Участник выбирает её в списке и работает с её адресами и тегами отдельно от личной книги

Примечание

Редактировать содержимое общей книги **в клиенте** можно, только если у участника есть доступ уровня **Изменение** или **Управление** — тогда добавление, переименование и удаление адресов и тегов выполняются прямо в выбранной общей книге. На уровне **Просмотр** книга открывается в режиме чтения: подключаться к устройствам можно, а редактировать её содержимое — нет. Массово наполнять книгу по-прежнему удобнее в веб-интерфейсе сервера

3.5.6 Что важно учесть

- **Право и уровень доступа работают в связке.** Чтобы участник мог не только видеть, но и **добавлять или изменять** адреса и теги общей книги через веб-интерфейс, ему нужны одновременно модельное право (**Адресная книга → Создание** и/или **Изменение**) и уровень доступа к книге **Изменение** или **Управление**. Одного из двух недостаточно
- **Удаление книги.** Удалить общую книгу может только пользователь с уровнем доступа **Управление**. Личную книгу удалить нельзя — это доступно только суперпользователю

3.5.7 Временная приостановка доступа

Если доступ к книге нужно приостановить, не удаляя её содержимое, переведите книгу в состояние **Выключена** — переключателем Включена в свойствах книги или массовым действием Включить / выключить адресные книги на странице **Адресные книги**

У выключенной книги содержимое (адреса и теги) скрывается от пользователей, но сама книга остаётся видимой владельцу, чтобы её можно было включить обратно

3.6 Временная группа устройств без изменения групп отделов

Нужно собрать компьютеры нескольких отделов в одну обычную группу, например для выбора устройств в задаче обновления. При этом каждый компьютер должен сохранить свои прежние группы. Для такого сценария использовать массовое действие **«Изменить группы»** в режиме **«Добавить»**, а после завершения работ - в режиме **«Удалить»**

3.6.1 Подготовка

1. Создать обычную группу, например **«Обновление - пилот»**, в разделе **«Организация → Группы»**
2. Проверить, какие права назначены этой группе и в каких правилах доступа она используется
3. Открыть **«Удалённый доступ → Устройства»** и отобрать нужные компьютеры
4. Проверить их текущие группы и записать состав тестового устройства для сравнения после операции

Для отображения списка групп нужно право **«Группы → Просмотр»**. Не использовать этот сценарий для ручного наполнения динамической группы - её состав вычисляется по правилам. Для доменных устройств учитывать, что следующая синхронизация может заново сформировать членство по данным каталога

3.6.2 Добавить временную группу

1. Сначала отметить одно тестовое устройство
2. Выбрать действие **«Изменить группы»** и нажать **«Выполнить»**
3. Проверить устройство и столбец **«Текущие группы»** в форме
4. Оставить режим **«Добавить»**
5. Найти и отметить **«Обновление - пилот»**
6. Нажать **«Изменить группы»**
7. Вернуться к устройству и проверить, что новая группа добавилась, а прежние сохранились

8. Повторить операцию для остальных подготовленных компьютеров

Например, компьютер состоял в группе **«Бухгалтерия»**. После добавления он должен состоять и в **«Бухгалтерия»**, и в **«Обновление - пилот»**

Важно

Режим **«Назначить»** в этом примере не подходит - он заменит весь набор групп выбранной временной группой. После изменения членства проверить доступ к тестовому устройству под учётной записью сотрудника, для которого он должен сохраняться

Само добавление в группу не запускает политику обновления. Отдельно выбрать группу в нужной задаче и проверить её параметры и расписание

3.6.3 Убрать временную группу

1. После завершения работ открыть список устройств
2. Отфильтровать устройства по группе **«Обновление - пилот»** и проверить выборку
3. Отметить нужные устройства и открыть **«Изменить группы»**
4. Выбрать режим **«Удалить»**
5. Отметить только **«Обновление - пилот»** и применить действие
6. Проверить карточку тестового устройства - группа отдела должна остаться, а временная группа исчезнуть

Если после операции устройство исчезло из отфильтрованного списка, снять фильтр временной группы и найти его по ID. Это ожидаемый результат удаления членства, а не удаление устройства. Сама группа тоже сохраняется - это действие убирает её только у устройств

3.6.4 Если результат отличается от ожидаемого

- Список групп пуст - проверить право просмотра групп
- Нужная группа не видна - использовать поиск по имени
- Отметились не все группы - кнопка выбора всех действует только на загруженную часть списка
- Форма сообщает **«Не выбраны группы»** - отметить хотя бы одну группу
- Прежние группы исчезли - проверить, не был ли выбран режим **«Назначить»** Восстановить нужное членство по заранее сохранённым сведениям
- После синхронизации AD состав снова изменился - проверить членство устройства в домене и использовать его как источник настройки

Описание всех режимов находится на странице Устройства

В **RuDesktop** разграничение полномочий строится на трёх независимых уровнях, которые работают **совместно**:

- **Группы и права** (**Организация → Группы**) - определяют, **что** разрешено делать конкретному пользователю или устройству: какие страницы веб-интерфейса видеть, какие политики запускать, какие функции в клиенте использовать
- **Доступы** (**Удалённый доступ → Доступы**) - определяют, **кто к кому** может подключаться: задают пары «оператор → клиент» и набор прав в рамках сессии (без подтверждения, мастер-пароль, скрытое подключение)
- **Разрешения** (вкладка в **Доступах**) - определяют, **по какому типу подключения** работает доступ: Удалённый доступ, Передача файлов, Терминал, RDP, TCP-туннелирование, Проброс USB

При подключении сервер собирает итоговый набор прав по **всем** активным правилам, в которые попадает пара «оператор → клиент». Если подходящего правила нет - подключение запрещено

Подсказка

Группы можно делать как **статическими** (состав задаётся вручную), так и **динамическими** (состав пересчитывается по правилу - например, «все Linux»)

Динамические группы можно использовать в доступах вместо статических

Кейсы ниже покрывают типовые сценарии настройки

Настройка типовых ролей через группы

Разделение полномочий через предустановленные группы: Администратор, Руководитель, Сотрудник поддержки, Гость

Подключение к устройствам без подтверждения

Сценарий для службы техподдержки: подключение к устройствам пользователей без необходимости подтверждения с их стороны

Подключение по мастер-паролю

Подключение к устройствам по единому мастер-паролю - без ввода временного или постоянного пароля устройства

Доступы через динамические группы

Настройка доступов через группы с автоматическим составом по правилу (например, «все Linux», подсеть, кастомный фильтр)

Общая адресная книга для подразделения

Создание общей адресной книги, наполнение адресами и выдача доступа пользователям и группам

Временная группа устройств

Добавление группы для выбранных компьютеров с сохранением групп отделов и удаление временного членства после работ

ГЛАВА 4

Установка ПО

4.1 Kaspersky Endpoint Security

Особенности работы после установки описаны в разделе Совместимость с Kaspersky Endpoint Security

Чтобы установить **Kaspersky Endpoint Security** для Windows с помощью политики Установка пакета из архива, необходимо:

1. Подготовить установочный файл

> **Важно**
>
> Установочный файл **Kaspersky Endpoint Security** для Windows `keswin.exe` является самораспаковывающимся архивом (self-extracting archive)

    1. Запустите его, чтобы распаковать содержимое
    2. Все извлеченные файлы упакуйте в новый архив с расширением `.zip`
2. Открыть Панель управления сервера в браузере
3. Перейти на страницу Политики
4. Добавить новую политику, нажав на кнопку Добавить Политику в верхнем правом углу экрана
5. Выбрать шаблон политики Установка пакета из архива из списка предложенных шаблонов
6. Ввести название для политики в поле Название

7. Выбрать файл `.zip` архива
8. В поле Пакет указать:

```
setup_kes.exe
```

9. В поле Параметры установки указать:

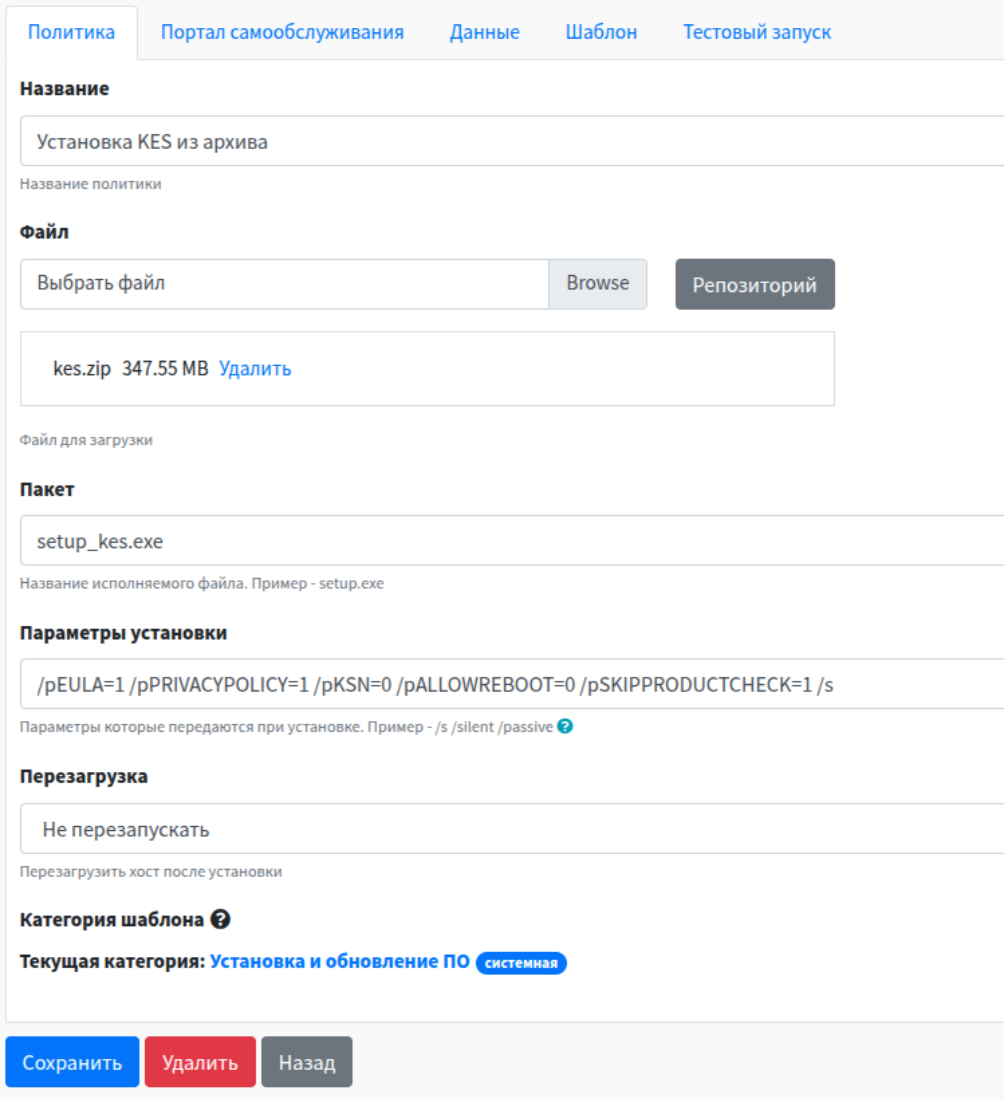
```
/pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pALLOWREBOOT=0 /
↪pSKIPPRODUCTCHECK=1 /s
```

Подсказка

В этом примере представлены базовые параметры:

- `/pEULA` — согласие с положениями Лицензионного соглашения
- `/pPRIVACYPOLICY` — согласие с Политикой конфиденциальности
- `/pKSN` — согласие или отказ участвовать в Kaspersky Security Network (KSN)
- `/pALLOWREBOOT` — автоматическая перезагрузка компьютера после установки или обновления приложения, если требуется
- `/pSKIPPRODUCTCHECK` — отключение проверки установленного ПО
- `/s` — ключ тихой установки

Для получения полной информации и дополнительных настроек, пожалуйста, посетите официальную страницу https://support.kaspersky.ru/kes-for-windows/12.10/123468?page=help



10. Сохранить политику
11. Создать задачу, выбрав созданную политику в поле Политики
12. Во вкладке Устройства и группы добавить необходимые устройства или группы, на которые планируется установить **Kaspersky Endpoint Security**
13. Запустить задачу и дождаться выполнения задачи

Важно

Задача может завершиться по таймауту, так как установка **Kaspersky Endpoint Security** может занять продолжительное время

Необходимо увеличить таймаут выполнения задач в настройках сервера, например до 3600

После успешного выполнения задачи, **Kaspersky Endpoint Security** будет установлен на выбранных устройствах или группе устройств

4.2 Yandex Telemost

Чтобы установить **Yandex Telemost** на Windows с помощью политики Установка пакета, необходимо:

1. Открыть Панель управления сервера в браузере
2. Перейти на страницу Политики
3. Добавить новую политику, нажав на кнопку Добавить Политику в верхнем правом углу экрана
4. Выбрать шаблон политики Установка пакета из списка предложенных шаблонов
5. Ввести название для политики в поле Название

   Например: Установка пакета Yandex Telemost
6. Выбрать файл `.exe`
7. В поле Параметры установки указать:

   ```
   /silent
   ```
8. Поле Пакет оставить пустым
9. Активировать чекбокс Установка от имени пользователя

   Важно

   Yandex Telemost размещается в профиле пользователя, поэтому установка выполняется через **«Планировщик задач»** Windows
10. В поле Перезагрузка выбрать значение, например Не перезапускать
11. Сохранить политику
12. Создать задачу, выбрав созданную политику в поле Политики
13. Во вкладке Устройства и группы добавить необходимые устройства или группы, на которые планируется установить **Yandex Telemost**
14. Запустить задачу и дождаться выполнения задачи

После успешного выполнения задачи, **Yandex Telemost** будет установлен на выбранных устройствах или группе устройств

4.3 eXpress

Чтобы установить **eXpress** на Windows с помощью политики Установка пакета, необходимо:

1. Открыть Панель управления сервера в браузере
2. Перейти на страницу Политики

3. Добавить новую политику, нажав на кнопку Добавить Политику в верхнем правом углу экрана
4. Выбрать шаблон политики Установка пакета из списка предложенных шаблонов
5. Ввести название для политики в поле Название

   Например: Установка пакета eXpress
6. Выбрать файл `.exe`
7. В поле Параметры установки указать:

```
/S
```

8. Поле Пакет оставить пустым
9. Активировать чекбокс Установка от имени пользователя

> **Важно**
>
> **eXpress** размещается в профиле пользователя, поэтому установка выполняется через **«Планировщик задач»** Windows

10. В поле Перезагрузка выбрать значение, например Не перезапускать
11. Сохранить политику
12. Создать задачу, выбрав созданную политику в поле Политики
13. Во вкладке Устройства и группы добавить необходимые устройства или группы, на которые планируется установить **eXpress**
14. Запустить задачу и дождаться выполнения задачи

После успешного выполнения задачи, **eXpress** будет установлен на выбранных устройствах или группе устройств

4.4 PIX Task

Чтобы установить **PIX Task** на Windows с помощью политики Установка пакета, необходимо:

1. Открыть Панель управления сервера в браузере
2. Перейти на страницу Политики
3. Добавить новую политику, нажав на кнопку Добавить Политику в верхнем правом углу экрана
4. Выбрать шаблон политики Установка пакета из списка предложенных шаблонов
5. Ввести название для политики в поле Название

   Например: Установка пакета PIX Task
6. Выбрать файл `.msi`

7. В поле Параметры установки указать:

```
/quiet PSURL=https://pixps.ru:555 STARTUP_MODE=all␣
↪INSTALLDESKTOPSHORTCUT=0
```

Подсказка

- `quiet` — установка в тихом режиме
- `PSURL` — URL студии, к которому рекордер будет подключен
- `STARTUP_MODE` — отвечает за добавление рекордера в автозагрузку. Доступные значения — **current** и **all**
- `INSTALLDESKTOPSHORTCUT` — отвечает за создание ярлыка на рабочем столе. Доступные значения — **0** (ярлык не будет создан) и **1** (ярлык будет создан)

8. Поле Пакет заполнится автоматически после выбора файла
9. Активировать чекбокс Установка от имени пользователя
10. В поле Перезагрузка выбрать значение, например Не перезапускать
11. Сохранить политику
12. Создать задачу, выбрав созданную политику в поле Политики
13. Во вкладке Устройства и группы добавить необходимые устройства или группы, на которые планируется установить **PIX Task**
14. Запустить задачу и дождаться выполнения задачи

После успешного выполнения задачи, **PIX Task** будет установлен на выбранных устройствах или группе устройств

4.5 1C

Чтобы установить **1C** из `.zip` архива на Windows с помощью политики Установка пакета из архива, необходимо:

1. Подготовить `.zip` архив с установочными файлами

Важно

Архив должен быть собран правильно — файл `setup.exe` должен находиться в корневой директории архива `1c.zip\setup.exe`, а не быть вложенным в дополнительные папки, например `1c.zip\1c\setup.exe`

2. Открыть Панель управления сервера в браузере
3. Перейти на страницу Политики

4. Добавить новую политику, нажав на кнопку Добавить Политику в верхнем правом углу экрана
5. Выбрать шаблон политики Установка пакета из архива из списка предложенных шаблонов
6. Ввести название для политики в поле Название

   Например: Установка пакета 1С
7. Выбрать `.zip` архив
8. В поле Установщик в архиве указать:

   ```
   setup.exe
   ```
9. В поле Параметры установки указать:

   ```
   /S
   ```

   Подсказка

   `/S` — ключ тихой установки
10. В поле Перезагрузка выбрать значение Не перезапускать

    Подсказка

    Для установки данного пакета перезагрузка не обязательна
11. Сохранить политику
12. Создать задачу, выбрав созданную политику в поле Политики
13. Во вкладке Устройства и группы добавить необходимые устройства или группы, на которые планируется установить **1С**
14. Запустить задачу и дождаться выполнения задачи

После успешного выполнения задачи, **1С** будет установлен на выбранных устройствах или группе устройств

4.6 Публикация приложения в магазине приложений

Кейс описывает, как опубликовать политику установки ПО в магазине приложений, чтобы конечный пользователь мог самостоятельно установить приложение через портал самообслуживания, без участия администратора

Подходит для типовых установок (офисные пакеты, корпоративные клиенты, утилиты), когда не требуется массовое развёртывание задачей, но пользователь должен иметь возможность поставить приложение по запросу

Подсказка

Сам магазин приложений доступен и в редакции **Удалённый доступ**, и в **Управление конфигурациями (UEM)**, но шаблоны установки стороннего ПО (Установка пакета, Установка пакета из архива, Установка/удаление пакета из репозитория) требуют **UEM** - без него на их основе нельзя создать политику

В редакции **Удалённый доступ** в магазин можно опубликовать только встроенные RD-шаблоны (например, Автоматическое обновление клиента RuDesktop)

4.6.1 Условия доступа к магазину

1. Открыть магазин из клиента **RuDesktop** на том устройстве, куда нужно установить приложение
2. Если запрошена авторизация, войти в учётную запись в браузере

После входа учитываются права пользователя и группы устройства совместно:

- Может видеть магазин приложений в портале самообслуживания — просмотр каталога и запрос установки приложений без автоматического запуска
- Может использовать магазин приложений — дополнительно разрешает самостоятельную установку приложений с автоматическим запуском

Право использования достаточно предоставить пользователю либо группе устройства.

Примечание

Для доступа без авторизации должны выполняться все условия:

- На сервере разрешён доступ к магазину без авторизации
- У группы устройства есть право использования магазина
- IP-адрес запроса совпадает с сетевым адресом устройства

Подробнее — в разделе *Доступ к магазину без авторизации пользователя*

4.6.2 Подготовка

1. Подготовьте политику установки приложения

   Подойдёт любой из шаблонов раздела Обновление и установка ПО, например:

   - Установка пакета - для `.msi` / `.exe` / `.deb` / `.rpm`
   - Установка пакета из архива - для самораспаковывающихся архивов (см. кейс *Kaspersky Endpoint Security*)

- Установка/удаление пакета из репозитория - для пакетов из менеджеров пакетов: Chocolatey (Windows), apt/yum/apt-rpm (Linux), Homebrew (macOS)

2. Подготовьте иконку приложения

> **Подсказка**
>
> Рекомендуется использовать формат `.svg` - иконка масштабируется без потери качества

4.6.3 Выдача прав

Для работы магазина приложений настраиваются права в двух группах: устройства и пользователя

Права группы устройства

Права **группы устройства** определяют доступность кнопок портала и магазина в клиенте **RuDesktop**

1. Перейти на страницу **Организация → Группы**
2. Открыть группу, в которой состоит устройство клиента (например, Сотрудник поддержки - группа устройств по умолчанию)
3. На вкладке Права активировать:
   - Может использовать портал самообслуживания - отображает в клиенте кнопку **Поддержка и портал самообслуживания**
   - Может использовать магазин приложений - отображает в клиенте кнопку **Магазин приложений** и разрешает серверу открывать страницу магазина для устройства
4. Сохранить группу

> **Важно**
>
> - Без авторизации право Может использовать магазин приложений обязательно у группы устройства
> - После входа в браузере доступ может быть предоставлен и за счёт прав пользователя

Права группы пользователя

1. Открыть группу пользователя (например, Гость - группа пользователей по умолчанию - или собственную группу) на странице **Организация → Группы**
2. На вкладке Права активировать:

- Может видеть магазин приложений в портале самообслуживания — просмотр каталога и запрос установки приложений без автоматического запуска
- Может использовать магазин приложений — самостоятельная установка приложений с автоматическим запуском, если это право не предоставлено группой устройства

3. Сохранить группу

Примечание

При неавторизованном доступе по IP (см. ниже) права группы пользователя не задействованы - сервер опознаёт клиента по устройству, поэтому достаточно прав, выданных группе устройства

4.6.4 Публикация политики

1. Открыть Панель управления сервера в браузере
2. Перейти на страницу Политики
3. Открыть существующую политику установки или добавить новую кнопкой Добавить Политику
4. На вкладке Политика заполнить параметры установки в зависимости от выбранного шаблона
5. Перейти на вкладку Портал самообслуживания и в блоке Магазин приложений активировать:
    - Показывать в магазине приложений

    Подсказка

    При активации этого чекбокса автоматически активируется чекбокс Показывать в разделе: «Портал самообслуживания» в блоке Общие настройки

6. Заполнить карточку приложения для магазина:
    - Название приложения - отображается в карточке магазина
    - Описание приложения - краткое описание для пользователя (назначение, версия, особенности)
    - Иконка приложения - графический значок карточки
7. Сохранить политику

Примечание

Сервер разрешает запуск из магазина только для политики с обоими флагами: **Показывать в магазине приложений** и **Показывать в разделе: «Портал самообслуживания»**. После снятия одного из них политика недоступна для нового запроса установки, даже если пользователь сохранил ранее открытый адрес карточки

Важно

Флаг Автоматический запуск в блоке Общие настройки определяет, как сервер обработает нажатие кнопки в карточке приложения:

- **активен** - кнопка отображается как Установить, и сервер сразу создаёт задачу на выполнение политики и запускает её на устройстве
- **не активен** - кнопка отображается как Запросить установку, и сервер вместо запуска создаёт обращение типа **Запрос на выполнение политик**, которое ожидает обработки администратором

Для установки без участия администратора нужны:

- Активный чекбокс Автоматический запуск
- Право Может использовать магазин приложений

4.6.5 Порядок категорий магазина

Категория выбирается в поле **«Категория приложения»** политики

Для изменения порядка категорий:

1. Открыть соответствующую запись **«Категории приложений»**
2. Задать **«Порядок»** — чем меньше число, тем раньше категория отображается в магазине
3. Сохранить запись и проверить последовательность в магазине

Примечание

Для редактирования нужно право изменения категорий приложений

При одинаковом значении категории сортируются по названию

Например, задать браузерам порядок `10`, офисным программам - `20`, утилитам - `30`. После сохранения обновить страницу магазина и проверить последовательность

Примечание

Порядок задаётся для категории целиком, а не для отдельной карточки приложения. Он не меняет права доступа к приложениям и параметры их установки

4.6.6 Проверка

1. Открыть клиент **RuDesktop** на устройстве, для которого опубликовано приложение
2. В разделе **Магазин приложений** нажать Открыть - в браузере откроется страница магазина

   Подсказка

   Магазин также можно открыть из раздела **Поддержка и портал самообслуживания** - в портале появится пункт **Магазин приложений** в боковом меню

3. Если браузер запрашивает вход, авторизоваться под учётной записью с нужными правами
4. Должна появиться карточка с указанными названием, описанием и иконкой
5. Нажать Установить (либо Запросить установку, если флаг Автоматический запуск не активен)
6. Дождаться завершения установки на устройстве
7. Обновить страницу магазина - рядом с приложением появится кнопка История установок

   По кнопке доступны дата и статус каждой попытки установки

Примечание

Если карточка приложения не появилась в магазине, проверьте:

- магазин открыт для нужного устройства из клиента RuDesktop
- после входа есть право просмотра или использования магазина у пользователя либо группы устройства
- в политике активен чекбокс Показывать в магазине приложений
- устройство пользователя удовлетворяет условиям политики (ОС, архитектура и т.д.)

Подсказка

- Если каталог доступен, но кнопка **Установить** недоступна, проверить право **Может использовать магазин приложений**
- Право просмотра позволяет запросить установку только тех приложений, для которых отключён **Автоматический запуск**

4.6.7 Доступ к магазину без авторизации пользователя

Сценарий применяется, когда нужно дать клиентам доступ к магазину приложений без ввода логина и пароля - переход в браузер из клиента **RuDesktop** должен сразу открывать магазин и позволять выполнять политики установки или обновления ПО. Идентификация в этом случае выполняется по устройству, а не по пользователю: сервер сравнивает IP-адрес запроса с сетевым адресом устройства в его карточке

1. Перейти на страницу Администрирование → Настройки и в блоке Безопасность активировать:
    - Неавторизованный пользователь может видеть магазин приложений (IP адрес должен совпадать)

Важно

Условие совпадения IP означает, что значение поля Сетевой адрес в свойствах устройства в веб-интерфейсе должно совпадать с IP, с которого устройство фактически выполняет запрос к серверу

Если в сети используется обратный proxy, его необходимо настроить на передачу заголовка `X-Real-IP` с реальным IP клиента - иначе сервер увидит адрес proxy и проверка не пройдёт. Proxy должен перезаписывать этот заголовок, а не передавать значение от клиента. `X-Forwarded-For` для этой проверки не используется

Подсказка

Если несколько устройств выходят в сеть через один внешний IP (например, через NAT), сервер не сможет однозначно опознать конкретное устройство только по IP-адресу

В этом случае открывать магазин следует кнопкой в клиенте **RuDesktop** на нужном устройстве — клиент передаст серверу данные устройства

IP-адрес используется лишь как резервный способ опознать устройство

2. Убедиться, что у **группы устройства** активно право Может использо-

вать магазин приложений (см. раздел *Права группы устройства*)

Без этого права сервер откажет в доступе к магазину независимо от настройки и наличия авторизации

После применения настроек кнопка магазина приложений в клиенте **RuDesktop** будет открывать браузер с разделом магазина без запроса учётных данных. Пользователю будут доступны установка и обновление ПО через политики, опубликованные в магазине

Примечание

Настройка не отменяет обычную авторизацию: пользователи, которые входят в портал самообслуживания со своими учётными данными, продолжают видеть магазин по правилам из раздела *Выдача прав*

Чекбокс лишь добавляет дополнительный путь - открыть магазин по совпадению IP-адреса без логина

4.7 Подключение сетевой папки с установщиками

В организации установщики уже лежат в общей папке файлового сервера. Нужно выбирать их в RuDesktop без ручной загрузки каждого файла через браузер. Для этого подключить папку как **диск репозитория**. В примере используется Samba-ресурс `//files.example.org/software/installers`. Это пример адреса - заменить его адресом своей папки

Для SFTP и WebDAV последовательность аналогична, форматы путей приведены в справке Диски репозиториев

4.7.1 Что получится

В разделе **«Файлы»** появятся записи установщиков из сетевой папки. Их можно будет выбирать из репозитория в политиках

Примечание

Файлы останутся на файловом сервере, поэтому его доступность нужна и после первой синхронизации. Подключение папки само по себе не запускает установку программ на устройствах

4.7.2 Подготовить папку и доступ

1. На файловом сервере создать отдельную папку для установщиков
2. Положить туда один пробный файл, например `tool-1.0.msi`

   Использовать настоящий установщик, предназначенный для тестового устройства
3. Подготовить учётную запись с правом чтения папки, вложенных папок и файлов

4. Убедиться, что ресурс доступен с сервера RuDesktop

   Доступ к папке с рабочего компьютера администратора этого не подтверждает

5. В RuDesktop подготовить права на добавление, просмотр и изменение дисков, создание репозитория и просмотр файлов

4.7.3 Подключить папку

1. Открыть **«Хранилище → Репозитории»** и создать пользовательский репозиторий, например **«Сетевые установщики»**

   Оставить его пустым - загружать пробный файл через браузер не нужно

2. Открыть **«Хранилище → Диски репозиториев»** и добавить диск
3. Указать название, например **«Установщики с файлового сервера»**, и выбрать репозиторий **«Сетевые установщики»**
4. Выбрать тип **«Samba»**, ввести сетевой путь и учётные данные

   При необходимости указать пользователя в формате `DOMAIN\user`

5. На вкладке **«Синхронизация»** оставить расписание каждые 30 минут или задать подходящее расписание
6. Сохранить диск, затем выполнить **«Подключить»**
7. Обновить страницу после выполнения операции

   На вкладке **«Состояние»** проверить состояние **«Подключён»**, статус синхронизации **«Успешно»** и счётчики результата

Подсказка

Первая синхронизация выполняется при подключении автоматически. Если запись только сохранена, а действие **«Подключить»** не выполнено, файлы ещё не появятся

4.7.4 Проверить результат

1. Открыть **«Хранилище → Файлы»** и выбрать репозиторий **«Сетевые установщики»** в фильтре
2. Найти `tool-1.0.msi` и проверить размер
3. Выполнить **«Скачать»** для проверки доступности содержимого

   Наличие строки в таблице само по себе не подтверждает, что файл сейчас читается

4. При использовании UEM создать тестовую политику Установка пакета

   В поле **«Файл»** нажать **«Репозиторий»** и выбрать этот установщик

5. Настроить параметры установки по инструкции изготовителя приложения и выполнить тестовый запуск на одном подходящем устройстве

6. Проверить результат выполнения политики и наличие приложения

   Только после проверки использовать политику для остальных устройств

4.7.5 Обновить установщик

1. Положить новую версию рядом со старой на файловом сервере, например `tool-1.1.msi`
2. В карточке диска выполнить **«Синхронизировать»** или дождаться расписания
3. Дождаться завершения, найти новый файл в репозитории и проверить скачивание
4. В нужной политике выбрать новый файл и проверить параметры пакета и версии
5. Повторить тестовый запуск
6. Удалять старый файл на файловом сервере только после проверки, что он больше не нужен использующим его политикам и другим объектам

Важно

Новое имя не переключает существующие политики на новый файл. Переименование старого файла тоже не переносит ссылки на него. Если исходник удалён, а его запись сохранена из-за ссылок других объектов, это не означает, что файл по-прежнему можно скачать

4.7.6 Если что-то не получилось

- **Репозиторий не принимается при сохранении** - проверить, что он пользовательский, пустой и к нему ещё не привязан другой диск
- **Подключение завершилось ошибкой** - прочитать **«Последнюю ошибку»**, проверить адрес, учётные данные и доступность ресурса с сервера RuDesktop
- **Один файл не появился, остальные есть** - проверить счётчик пропущенных файлов, имя и длину пути по справке дисков репозиториев
- **В списке есть файл, но он не скачивается** - проверить, что диск подключён, исходник существует и доступен учётной записи подключения

  Выполнить синхронизацию и прочитать её результат
- **Нельзя поменять пароль** - сначала отключить диск и дождаться состояния **«Отключён»**, затем ввести новый пароль, сохранить и подключить снова
- **Диск занят другой операцией** - дождаться её завершения, обновить страницу и повторить нужное действие

Для временной остановки выполнить **«Отключить»**. Записи файлов сохранятся, но чтение через диск и синхронизация по расписанию прекратятся до повторного подключения

4.8 Подготовка файлов на устройствах по прямой ссылке

Нужно заранее доставить установщик или архив на несколько компьютеров, чтобы затем использовать его в отдельной операции установки. В этом примере файл сохраняется на Windows-устройствах в `C:\Company\Packages`. Для Linux и macOS используется тот же порядок действий с абсолютным путём своей ОС, например `/opt/company/packages`

4.8.1 Подготовить источник

1. Получить прямой URL файла, а не ссылку на страницу с кнопкой скачивания
2. Проверить доступ к URL с целевого устройства
3. Получить ожидаемую контрольную сумму файла у поставщика или вычислить её для заранее проверенного файла
4. Выбрать постоянную папку и имя, по которым файл будет использоваться дальше

Важно

Файл скачивает само устройство. Доступность адреса из браузера администратора или с сервера RuDesktop не означает, что адрес доступен всем клиентам

4.8.2 Создать политику скачивания

1. Открыть **«Политики»** и создать политику по шаблону Скачивание файла по URL
2. Указать **«Название»**, например **«Подготовить пакет приложения»**
3. В **«URL файла»** вставить фактический адрес установщика
4. В **«Имя файла»** задать имя с расширением, например `application-setup.msi`
5. В **«Свой путь к папке»** указать `C:\Company\Packages`
6. Заполнить обязательное поле **«Стандартная папка»**, например **«Временная папка»**
7. В **«Контрольная сумма файла»** указать `sha256:` и полную ожидаемую сумму из 64 шестнадцатеричных символов
8. Если источник требует имя пользователя и пароль, заполнить поля доступа к файлу
9. Сохранить политику

При заполненном собственном пути стандартная папка не используется. Недостающие каталоги будут созданы автоматически. Отдельная политика

создания директории нужна только тогда, когда каталог требуется подготовить до скачивания для других действий

4.8.3 Проверить на одном устройстве

1. Выполнить **«Тестовый запуск»** на одном Windows-устройстве
2. Проверить итоговый статус и журнал задания
3. Убедиться, что итоговый путь - `C:\Company\Packages\application-setup.msi`
4. Проверить размер и успешную проверку контрольной суммы
5. После проверки назначить политику остальным нужным устройствам

Примечание

Политика только скачивает файл, установка приложения автоматически не начинается. Следующее действие настройки или установки выполнять отдельно и только после успешной загрузки

4.8.4 Если файл не появился

1. Открыть журнал задания и проверить, на каком этапе возникла ошибка
2. При ошибке доступа к URL проверить адрес и учётные данные с самого целевого устройства
3. При ошибке записи проверить доступ к выбранной папке и свободное место на диске
4. При несовпадении контрольной суммы проверить, не был ли файл у источника заменён другой версией
5. Исправить причину и повторить запуск на одном устройстве

Примечание

Не убирать контрольную сумму только для того, чтобы задание завершилось успешно

Сначала проверить, что источник отдаёт нужный файл, а не страницу входа или сообщение об ошибке

4.8.5 Обновление и очистка

Предупреждение

Повторный запуск с тем же именем может заменить файл по тому же пути. Для хранения нескольких версий указывать разные имена или папки. При замене файла у источника обновить и ожидаемую контрольную сумму. Если сумма не совпадёт, скачанный файл будет удалён, а задание завершится ошибкой

Для удаления старых пакетов можно использовать отдельный каталог и политику удаления директории. Перед удалением проверить, что каталог не содержит нужных данных и больше не используется заданиями

На этой странице представлены инструкции по установке различного программного обеспечения с использованием политик **RuDesktop**. Инструкции предназначены как для системных администраторов, так и для DevOps-инженеров, которые стремятся упростить и ускорить развертывание ПО в своих инфраструктурах

Kaspersky Endpoint Security

Установка антивируса на Windows из самораспаковывающегося `.zip` архива через политику **Установка пакета из архива**

Yandex Telemost

Установка `.exe` пакета от имени пользователя через политику **Установка пакета** - для приложений в профиле пользователя

eXpress

Установка корпоративного мессенджера из `.exe` от имени пользователя через политику **Установка пакета**

PIX Task

Установка рекордера `.msi` с параметрами подключения к студии через политику **Установка пакета**

1C

Установка `1C` из `.zip` архива на Windows через политику **Установка пакета из архива**

Публикация приложения в магазине приложений

Публикация политики установки в магазине приложений - пользователь сам ставит ПО через портал самообслуживания

Подключение сетевой папки с установщиками

Подключение Samba-ресурса к репозиторию и обновление установщиков для политик

Подготовка файлов на устройствах по прямой ссылке

Скачивание пакета в заданную папку, проверка контрольной суммы и повторные запуски

ГЛАВА 5

Запись видеосессий и логи передачи файлов

Кейс — пошаговая настройка администратором двух функций аудита удалённых сессий: автоматическая видеозапись подключений и подробные логи передачи файлов

Подсказка

Обе функции доступны только при использовании локального сервера **Управление конфигурациями (UEM)**

5.1 Что вы получите

После настройки в системе будет:

- Автоматически записываться видео всех удалённых сессий выбранных пользователей или групп
- Сохраняться подробный журнал по каждой передаче файлов (имя файла, размер, направление, время, инициатор)
- Запись и логи будут доступны для просмотра в свойствах сессии на странице **Удалённый доступ → Сессии**

5.2 Шаг 1. Настройка хранения видеозаписей

Перед включением записи задайте параметры хранения и качества видео в **Администрирование → Настройки → Видеозаписи**:

- Путь хранения видеозаписей — каталог на сервере, где будут сохраняться файлы. По умолчанию `/var/lib/rudesktop/media/sessions/`
- Качество записи — компромисс между размером файла и детализацией изображения

После изменения настроек нажмите Сохранить внизу страницы

Важно

Видеозаписи могут занимать значительный объём — при массовой записи планируйте свободное место и регулярную ротацию старых записей. Подробности о расположении и составе медиа-каталога: Резервное копирование

5.3 Шаг 2. Включение записи и логов для группы

И запись видеосессий, и подробные логи передачи файлов настраиваются в одном месте — на вкладке Мониторинг в свойствах группы

1. Перейдите на страницу **Организация → Группы**
2. Откройте свойства нужной группы (например, **Сотрудники поддержки**)
3. Перейдите на вкладку Мониторинг
4. Включите нужные опции:
   - **Запись видеосессий** — все удалённые сессии участников группы будут автоматически записываться
   - **Логи передачи файлов** — для каждой передачи файла в сессии будет сохраняться подробная запись (имя файла, размер, направление, время, инициатор)
5. Сохраните изменения кнопкой Сохранить

После сохранения новые сессии участников группы будут записываться и логироваться. Уже завершённые сессии не затрагиваются — повторно их записать невозможно

Подробнее о свойствах группы: Группы

5.4 Шаг 3. Просмотр записей и логов

После того как пользователи группы выполнят удалённые сессии:

1. Перейдите на страницу **Удалённый доступ → Сессии**
2. Откройте свойства нужной сессии (двойной клик по записи в таблице)

3. На вкладке свойств доступны:
    - Видеозапись — встроенный плеер с записью сессии (если запись была включена)
    - Логи передачи файлов — детальный журнал по каждой операции (если включены подробные логи у группы)

Подробнее о сессиях и доступных вкладках: Сессии

Важно

Записи и логи привязаны к свойствам сессии. Если сессия удалена из журнала, связанные с ней файлы видеозаписи и логи передачи также будут удалены

5.5 Что дальше

- Настройте регулярное резервное копирование каталога `/var/lib/rudesktop/media/` — там хранятся видеозаписи
- Настройте дублирование событий аудита в Syslog — события подключений и завершения сессий будут уходить во внешний SIEM

ГЛАВА 6

Развёртывание клиентов

6.1 Клонирование клиентов из единого образа

Кейс описывает, как корректно развернуть клиент **RuDesktop** на множестве машин, созданных из общего образа (VDI, шаблон ВМ, golden-image для PXE, контейнер) — так, чтобы каждая клонированная машина получила уникальную идентификацию на сервере и не конфликтовала с другими клонами

Важно

Кейс применим только при работе с **локальным сервером RuDesktop**. Используемые команды клиента use-random-uuid и reset-state доступны только в локальной версии клиента — в облачной версии они отключены

6.1.1 В чём проблема

Внутренний UUID клиента по умолчанию формируется из `machine_uid` операционной системы — стабильного идентификатора, привязанного к параметрам железа. Это удобно для физических машин, но в виртуальных средах `machine_uid` часто **совпадает у всех клонов**: все они унаследовали одинаковые параметры от исходного образа

Если клиент уже зарегистрирован на сервере **в момент снятия образа** или просто запущен с одинаковым UUID на разных клонах:

- сервер видит клонов как **одно и то же устройство**, переписывая запись при каждой регистрации
- параллельные сессии с разных клонов «смешиваются» под один ID
- инвентаризация и логи действий «прыгают» между машинами

- в списке устройств часть клонов вообще не появляется

6.1.2 Как решить

Связка двух команд клиента:

- use-random-uuid — переключает клиент в режим случайного UUID (отвязывает его от `machine_uid`)
- reset-state — обнуляет `id`, сертификат и мастер-пароль и инициирует перегенерацию UUID

После их выполнения каждый клон получает:

- уникальный случайный UUID
- пустой публичный `id` — будет выдан сервером при первой регистрации
- свежий сертификат, выпускаемый сервером заново
- новый мастер-пароль, который клиент тут же отправит на сервер

6.1.3 Подготовка базового образа

Вариант, при котором клиент в образе **ещё не зарегистрирован на сервере**. Это самый чистый сценарий — на сервере не появляется лишних «фантомных» записей

1. Установить клиент **RuDesktop** обычным способом, дождаться завершения установки
2. **Не запускать клиент**, либо сразу после первого запуска выполнить:

   ```
   rudesktop services stop
   ```

3. Включить режим случайного UUID, чтобы последующая перегенерация UUID сразу выдала случайный, не привязанный к `machine_uid`:

   ```
   rudesktop --use-random-uuid true
   ```

4. Удалить состояние, которое клиент мог сохранить за время установки и тестирования, и перегенерировать UUID в случайный:

   ```
   rudesktop --reset-state
   ```

5. Снять образ системы (sysprep на Windows, очистка `machine-id` на Linux при необходимости — отдельный шаг ОС, не относящийся к **RuDesktop**)

Подсказка

Если клиент во время подготовки образа всё-таки успел зарегистрироваться на сервере — после снятия образа удалите эту «эталонную» запись на странице Устройства, чтобы её ID не «занимал место»

6.1.4 Применение на клонированной машине

После того как клон загружен и получил уникальные сетевые параметры (имя хоста, MAC, IP), на нём нужно один раз выполнить связку команд:

```
rudesktop --use-random-uuid true
rudesktop --reset-state
```

Что произойдёт:

- `--use-random-uuid true` сразу выдаст случайный UUID, не зависящий от `machine_uid` ОС
- `--reset-state` обнулит `id`, сертификат и мастер-пароль, после чего клиент при следующем подключении к серверу пройдёт **новую регистрацию** и получит собственный `id`

Дальше клиент работает как обычно — на сервере появляется свежая запись, не пересекающаяся с другими клонами

Важно

Порядок важен. Сначала `--use-random-uuid true` (включает режим), затем `--reset-state` (использует включённый режим при перегенерации UUID). При обратном порядке `--reset-state` сгенерирует UUID из `machine_uid` — то есть тот же самый, что и у других клонов

Важно

Флаги нельзя передать в одной команде (`rudesktop --use-random-uuid true --reset-state`) — клиент обработает только первый флаг и завершит работу, второй будет проигнорирован. Связка должна выполняться **двумя отдельными вызовами** `rudesktop` в указанном порядке

6.1.5 Автоматизация запуска связки

Команды нужно выполнять только один раз — при первой загрузке клона. Удобные способы это автоматизировать:

- **Linux** — добавить связку в cloud-init[1] (`runcmd`), в скрипт `rc.local` с однократным маркером, или в `systemd`-юнит типа `oneshot` с условием существования файла-флага
- **Windows** — выполнить связку из `setupcomplete.cmd` после `sysprep` или из задания планировщика, отключающего себя после выполнения
- **VDI** — встроить связку в скрипт первой загрузки сессии (например, в шаблоне Citrix/VMware Horizon)
- **Контейнеры** — выполнить связку в ENTRYPOINT перед запуском основной службы клиента

[1] https://cloud-init.io

Также для разовой ручной раскатки на уже стоящих клонах годится политика Выполнить команду — её можно запустить на группе устройств, но **только если клиенты до этого уже корректно зарегистрировались на сервере под разными** `id` (иначе политика не сможет их различить)

6.1.6 Проверка

1. Запустить на каждой клонированной машине:

   ```
   rudesktop --get-uuid
   ```

   Полученные значения должны **отличаться** между всеми клонами

2. Открыть в веб-интерфейсе сервера страницу Устройства и убедиться, что:
   - каждая клонированная машина присутствует отдельной записью
   - `id` всех записей различаются
   - в свойствах устройства поле UUID уникально для каждой записи
3. Подключиться к одному из клонов по ID — сессия должна установиться именно к нему, без «прыжка» на другую машину

Примечание

Если на сервере всё равно остаются дубликаты, проверьте:

1) что `--use-random-uuid true` отработал ДО `--reset-state`;
2) что в исходном образе клиент не успел зарегистрироваться под общим `id` (если успел — удалите эталонную запись на сервере и повторите связку на клонах)

См. также

Если в инфраструктуре имена хостов уникальны (например, доменные устройства), альтернативой может быть назначение устройствам `hostname` в качестве идентификатора — см. кейс *Использование hostname в качестве ID устройства*

6.2 Использование hostname в качестве ID устройства

Кейс описывает, как настроить сервер **RuDesktop** так, чтобы устройствам в качестве идентификатора присваивался их сетевой `hostname`, а не числовой ID. Это удобно для парка машин с управляемыми уникальными именами хостов - например, доменных устройств, VDI и развёртываний из общего образа

6.2.1 В чём проблема

По умолчанию сервер выдаёт каждому устройству числовой `id`. У такого подхода есть неудобства при управлении крупным парком:

- числовой ID не несёт смысла - по нему сложно понять, что это за машина
- при клонировании из образа или переустановке ОС устройство может зарегистрироваться как новое и «потерять» прежний ID
- администратору приходится сопоставлять числовые ID с именами хостов вручную

Если в инфраструктуре имена хостов и так уникальны (типичный случай - устройства, заведённые в домен), удобнее использовать сам `hostname` как идентификатор устройства. Для выбора поведения ID доступны две взаимоисключающие настройки сервера в блоке Настройки клиента на странице Администрирование → Настройки

6.2.2 Как это работает

Использовать hostname в качестве ID устройства - при подключении сервер требует, чтобы ID устройства совпадал с его `hostname`:

- если у устройства ID не равен имени хоста - сервер присваивает ему `hostname` в качестве ID
- если настройку выключить - устройствам, у которых ID равен имени хоста, выдаётся **новый числовой ID**

Выдавать новый ID устройства при смене имени его хоста - сервер отслеживает изменение `hostname` у уже известного устройства. При изменении имени хоста устройство регистрируется как **новое** и получает новый идентификатор

Важно

Настройки взаимоисключающие - одновременно включить их нельзя. Когда одна включена, переключатель второй заблокирован. Чтобы сменить режим, сначала выключить текущую настройку, затем включить нужную и сохранить настройки

Использовать hostname как ID	Выдавать новый ID при смене имени	Результат
Выключено	Выключено	Поведение по умолчанию: числовой ID, при смене имени хоста идентификатор сохраняется
Включено	Выключено	ID всегда равен текущему `hostname` При переименовании хоста устройство получит новый ID, равный новому имени
Выключено	**Включено**	ID остаётся числовым, но при переименовании хоста устройство регистрируется как новое и получает новый числовой ID
Включено	**Включено**	Недопустимое сочетание - форма не позволяет сохранить обе настройки включёнными

Примечание

Поведение в таблице описано для **Windows** и **Linux**

На **Android** настройка hostname как ID не применяется, а у **macOS** есть особенность для настройки Выдавать новый ID устройства при смене имени его хоста - подробнее в разделе «Подводные камни и их решение»

6.2.3 Что проверить до включения

Настройка действует на сервер, а не только на выбранную группу устройств

1. Проверить уникальность имён хостов среди устройств этого сервера
2. Зафиксировать текущие ID и записи адресных книг для важных устройств
3. Согласовать время смены ID и способ сообщить новые ID операторам
4. Проверить версию клиента - сервер применяет механизм hostname как ID к клиентам новее `2.6.1216`

Для предварительной проверки использовать отдельный тестовый сервер

6.2.4 Включение настройки

1. Перейти на страницу Администрирование → Настройки
2. Открыть блок Настройки клиента
3. Если включена настройка Выдавать новый ID устройства при смене имени его хоста, сначала выключить её
4. Активировать настройку Использовать hostname в качестве ID устройства
5. Убедиться, что настройка Выдавать новый ID устройства при смене имени его хоста выключена
6. Сохранить изменения

Изменения применяются при следующем подключении устройства к серверу: устройство получает требуемый ID и **переподключается** уже под ним

6.2.5 Что происходит при смене ID

Важно

Любая смена ID (включение или выключение настройки, переименование хоста) приводит к тому, что:

- **меняется сам ID** - сохранённые подключения, записи в адресной книге и доступы, привязанные к старому ID, перестанут работать
- на устройстве **сбрасывается мастер-пароль** (используемый для подключения по мастер-паролю)
- на сервере **остаётся старая запись** устройства со старым ID, а новая создаётся под новым ID

Постоянный пароль устройства при этом не сбрасывается

6.2.6 Подводные камни и их решение

Проблема	Решение
Неуникальные имена хостов Если у двух устройств совпадает `hostname`, они претендуют на один ID и могут не пройти регистрацию из-за конфликта идентификаторов	Перед включением настройки обеспечить уникальность имён хостов во всей инфраструктуре Для клонов из общего образа имя хоста часто наследуется - задайте уникальные имена до подключения
Дубликаты записей на сервере После смены ID старая запись устройства не удаляется автоматически	Периодически удалять устаревшие записи на странице Устройства Учитывать дубли при инвентаризации и отчётах
Смена ID рвёт привязки к старому ID (сохранённые подключения, адресная книга, доступы), а мастер-пароль сбрасывается	Планировать включение/выключение настройки в окно обслуживания После смены ID сообщить операторам новый ID и при необходимости перенастроить доступы и записи адресной книги
Выключение настройки не возвращает прежние числовые ID Устройствам, у которых ID равен имени хоста, выдаётся новый числовой ID	Не рассчитывать на восстановление старых ID После выключения раздать операторам актуальные ID
Hostname как ID не применяется к Android	Для Android использовать текущие ID устройств, не ожидать их замены на hostname
macOS и настройка «Выдавать новый ID при смене имени хоста» На macOS при изменении только `hostname` новый ID по этой настройке не выдаётся (в отличие от Windows и Linux)	Для парка macOS не полагаться на настройку Выдавать новый ID устройства при смене имени его хоста для отслеживания переименований Настройка Использовать hostname в качестве ID устройства на macOS при этом работает

6.2.7 Проверка

1. Открыть в веб-интерфейсе сервера страницу Устройства и убедиться, что в качестве ID устройств отображаются их имена хостов
2. Подключиться к устройству по его `hostname` - сессия должна установиться именно к этой машине
3. При необходимости удалить устаревшие записи со старыми ID

См. также

Если требуется обеспечить уникальную идентификацию именно для **клонов из общего образа** (VDI, шаблон ВМ, контейнер), где совпадает внутренний UUID, используйте кейс *Клонирование клиентов из единого образа* - это альтернативный подход на стороне клиента

6.3 Развёртывание клиента в подсети

Сценарий: обнаружить Linux-устройства в подсети `192.168.10.0/24`, установить клиент RuDesktop на одно тестовое устройство, затем настроить установку на остальные подготовленные устройства этой подсети. Адреса в примере заменить адресами своей сети

6.3.1 Что подготовить

- Доступ к разделу **«Сканирование сети»** с правами создания и изменения профилей, учётных данных и правил, а также изменения обнаруженных устройств
- Сервер или уже подключённое устройство RuDesktop, которому доступна подсеть

  Это устройство можно выбрать агентом-исполнителем
- На целевых Linux-устройствах - доступный SSH и учётную запись с правами установки клиента, включая повышение прав при необходимости
- Доступ целевых устройств к установочным файлам сервера RuDesktop и источникам необходимых зависимостей

  Обнаружение по IP само по себе не подтверждает возможность загрузки и установки клиента

6.3.2 Шаг 1. Найти устройства

1. Открыть **«Сканирование сети → Профили обнаружения»** и добавить профиль
2. Назвать его, например, `Linux - офис` и выбрать тип **«IP-диапазон»**
3. В **«Маске подсети для сканирования»** указать `192.168.10.0/24`
4. В **«Портах для проверки»** указать 22; если SSH настроен на другом порту, указать его

   Остальные параметры можно оставить исходными
5. Если поиск должен идти из другой сети, выбрать находящийся в ней **«Агент-исполнитель»**

   Если подсеть доступна серверу, оставить поле пустым
6. Сохранить профиль и выполнить **«Запустить сканирование»**

7. Проверить **«Лог сканирования»**, затем открыть **«Обнаруженные устройства»** и найти тестовый компьютер по IP-адресу

Примечание

Проверить открытые порты в карточке. Устройство, обнаруженное только по ICMP или таблице соседей, тоже может попасть в список, даже если SSH недоступен. Для него сначала потребуется обеспечить доступ по SSH

6.3.3 Шаг 2. Подготовить подключение

1. Открыть **«Учётные данные обнаружения»** и добавить набор, например `Linux - установка клиента`
2. Выбрать транспорт **«SSH»**, метод **«Пароль»**, указать пользователя и пароль
3. Если учётной записи нужно повышение прав, включить **«Повышение прав»**, указать метод, например `sudo`, пользователя `root` и пароль повышения прав, если он требуется
4. Для нестандартного SSH-порта заполнить **«Порт»**

   Для порта 22 поле можно оставить пустым
5. Сохранить набор

Подсказка

Вместо пароля SSH можно использовать ключ или другой поддерживаемый метод - см. Учётные данные обнаружения

6.3.4 Шаг 3. Установить клиент на тестовое устройство

1. В **«Обнаруженных устройствах»** найти тестовый компьютер и выполнить **«Запустить установку»**
2. В окне **«Установка агента»** выбрать созданные учётные данные и **«Полный клиент»**
3. Выбрать **«Агент-исполнитель»**

   Для воспроизводимой проверки указать конкретного агента или **«Напрямую с сервера»**, откуда доступен SSH устройства
4. Запустить установку и открыть **«Лог установки»** в карточке устройства
5. После завершения проверить **«Попытки установки»** и ссылку **«Управляемое устройство»**

   Перейти по ней и проверить подключение клиента

Важно

Если установка завершилась ошибкой, сначала проверить журнал, транспорт, порт и права учётной записи. Расширять развёртывание после успешной проверки на тестовом устройстве

6.3.5 Шаг 4. Настроить правило для подсети

1. Открыть **«Правила авто-установки»** и добавить правило
2. Снять **«Включено»** на время проверки, чтобы не запускать установку по расписанию до настройки условий
3. Указать профиль `Linux - офис`, тип **«Полный клиент»** и созданный набор учётных данных
4. Для первой проверки задать условие **«IP-адрес» = IP тестового устройства**

   Проверить число совпадений в форме
5. Выполнить **«Запустить установку»** и проверить журнал

   Если на тестовом устройстве клиент уже установлен, включённое **«Применять однократно»** исключит его из установки

   Для проверки самой установки через правило выбрать ещё одно подготовленное тестовое устройство без клиента
6. После проверки заменить условие на **«IP-адрес» → «в подсети» → ``192.168.10.0/24``**, только если все подходящие устройства этой подсети подготовлены к развёртыванию

   Иначе оставить более узкие условия
7. Оставить **«Применять однократно»** включённым

   При необходимости явно выбрать исполнителя и уменьшить **«Параллельных установок»**
8. Для автоматической работы включить профиль и правило, затем настроить их расписания отдельно: сначала поиск, после его завершения - установка

Важно

В текущей beta3.1 флаг **«Только сопоставление (dry-run)»** не гарантирует отсутствие установки

Для просмотра количества совпадений использовать счётчик в форме без запуска правила; для пробной установки - ограниченный набор тестовых устройств

6.3.6 Что получится

Новые устройства обнаруживаются по расписанию профиля. Правило при своём запуске выбирает подходящие записи и выполняет установку. Успешно установленные клиенты пропускаются при включённом **«Применять однократно»**, а неудачные попытки могут повторяться при следующих запусках

Подсказка

Устройства, на которые не нужно устанавливать клиент, отметить состоянием **«Игнорируется»**. Это исключает их из автоматического отбора

Подробное описание полей и способов поиска: Сканирование сети

На этой странице собраны кейсы по развёртыванию клиента **RuDesktop**: обнаружение устройств и установка по сети, клонирование из общего образа и назначение hostname в качестве ID

Клонирование клиентов из единого образа

Развёртывание клиента **RuDesktop** на машинах из общего образа (VDI, шаблон ВМ, golden-image, контейнер) с уникальной идентификацией каждого клона

Использование hostname в качестве ID устройства

Назначение устройствам имени хоста вместо числового ID - наглядная и стабильная идентификация парка машин с управляемыми hostname

Развёртывание клиента в подсети

Поиск Linux-устройств, проверка установки по SSH и настройка автоустановки

ГЛАВА 7

Мобильный клиент

7.1 Первое подключение к удалённому ПК с Android

Кейс — пошаговое подключение к удалённому компьютеру с мобильного клиента **RuDesktop** для **Android** с публичного или корпоративного сервера. Подходит для пользователя, который только что установил клиент и впервые открывает приложение

7.1.1 Что вы получите

- Установленный и подключённый к нужному серверу клиент **RuDesktop** на Android
- Активную сессию с удалённым рабочим столом
- Возможность переключить режим управления курсором (Сенсорный режим / Режим мыши)

7.1.2 Подготовка

- Установлен мобильный клиент **RuDesktop** для Android (из `Google Play`, `RuStore` или с сайта rudesktop.ru/downloads[2])
- На стороне удалённого устройства запущен клиент **RuDesktop**, доступен ID и пароль
- Пользователь оператора имеет право Авторизовываться в приложении (для корпоративного сервера)

[2] https://rudesktop.ru/downloads

7.1.3 Шаг 1. Указать сервер для подключения

По умолчанию мобильный клиент подключается к публичному серверу **RuDesktop**. Для корпоративного сервера нужно изменить адрес

1. Откройте вкладку Настройки
2. Откройте пункт Сервер для подключения
3. Введите адрес сервера (например, `rz.example.com`) и нажмите OK

Подсказка

Адрес сервера также можно применить через QR-код. Нажмите Сканер QR-кода в правом верхнем углу шапки и считайте QR-код, выданный администратором. Подробнее: Сканер QR-кодов

7.1.4 Шаг 2. Авторизоваться (для корпоративного сервера)

Если используется корпоративный сервер с ограничениями по доступам:

1. В шапке приложения нажмите или откройте Настройки → пункт **Войти**
2. Введите логин и пароль учётной записи
3. После авторизации во вкладке Соединение появятся доступные адресные вкладки (Последние сеансы, Избранное, Адресная книга, Организация, Пригласительные ссылки) в зависимости от прав

Примечание

На публичном сервере авторизация не обязательна — можно подключаться по ID и паролю без входа в учётную запись

7.1.5 Шаг 3. Подключиться к удалённому устройству

1. Откройте вкладку Соединение
2. В поле `Удаленный идентификатор` введите ID удалённого устройства

Подсказка

При вводе под полем отображается выпадающий список совпадений из последних подключений, обнаруженных по локальной сети устройств и адресной книги

3. Нажмите кнопку справа от поля
4. Если на удалённом устройстве установлен временный или постоянный пароль — приложение запросит его. Введите пароль и нажмите OK
5. На стороне удалённого устройства, в зависимости от настроек, может потребоваться подтверждение подключения

После принятия запроса откроется окно подключения с трансляцией удалённого рабочего стола

7.1.6 Шаг 4. Выбрать режим управления курсором

В нижней панели окна подключения нажмите кнопку / для переключения режима:

- **Сенсорный режим** — координаты курсора совпадают с точкой касания. Удобно для коротких операций (нажать кнопку, открыть программу)
- **Режим мыши** — курсор двигается относительными жестами, как с тачпадом. Удобно для точных операций (выделение текста, графические редакторы)

Подробнее о жестах: Жесты управления

Примечание

При подключении к удалённому **Android**-устройству переключение режима недоступно

7.1.7 Шаг 5. Сохранить устройство для быстрого доступа

Чтобы не вводить ID каждый раз:

- В контекстном меню устройства во вкладке Последние сеансы выберите **Добавить в избранное** или **Добавить в Адресную книгу**
- В адресной книге устройство можно пометить тегами и фильтровать по ним

Подробнее: Адресная книга

7.1.8 Что дальше

- Включите запись исходящих сессий — *Запись сессий на мобильном*
- Настройте Преднастройки подключения, чтобы все будущие сессии открывались с нужным качеством и режимом
- Если устройство в локальной сети — попробуйте подключение через Wake On Lan, чтобы будить выключенный ПК

7.2 Передача файлов с телефона на ПК и обратно

Кейс — пошаговая передача файлов между мобильным устройством на **Android** и удалённым компьютером с использованием встроенного режима передачи файлов мобильного клиента **RuDesktop**

7.2.1 Что вы получите

- Открытое подключение в режиме передачи файлов
- Возможность копировать файлы и папки между мобильным устройством и удалённым ПК в обе стороны
- Возможность создавать папки, удалять файлы и работать со скрытыми файлами

7.2.2 Подготовка

- На мобильном устройстве установлен и настроен клиент **RuDesktop** для Android
- На стороне удалённого ПК запущен клиент **RuDesktop** и доступны ID и пароль
- У оператора есть право подключения в режиме Передача файлов к этому устройству

7.2.3 Шаг 1. Запустить подключение в режиме передачи файлов

Подключение в режиме передачи файлов можно открыть несколькими способами:

- Во вкладке Соединение ввести ID удалённого устройства, нажать справа от поля и выбрать **Передача файлов**
- В контекстном меню записи во вкладке Последние сеансы, Избранное или Адресная книга выбрать **Передача файлов**
- По пригласительной ссылке с типом Передача файлов

После подключения откроется окно передачи файлов с переключателем сторон в шапке: Локальный (файлы мобильного) / Удалённый (файлы ПК)

7.2.4 Шаг 2. Перейти в нужный каталог

1. Переключитесь на нужную сторону кнопкой Локальный / Удалённый в шапке
2. Используйте навигационные элементы:
    - **Хлебные крошки** › … — нажатие на сегмент пути открывает соответствующий каталог
    - **Вверх** — родительский каталог
    - **Назад** — предыдущий каталог по истории
    - **Сортировка** — изменить порядок отображения файлов
3. Чтобы открыть папку — короткое нажатие на её строке

Подсказка

Если нужно увидеть скрытые файлы (имя начинается с точки или с системным атрибутом) — откройте в шапке и активируйте **Показать скрытые файлы**

7.2.5 Шаг 3. Выделить файлы и папки для передачи

1. Включите режим множественного выбора одним из способов:
   - в шапке → **Многоэлементный выбор**
   - **Долгое нажатие** на любую запись — режим включится и запись будет выделена
   - в строке записи → **Многоэлементный выбор**
2. Отметьте флажками нужные файлы и папки

В нижней части появится панель с заголовком **Выбрано**, количеством элементов и стороной (например, `5 элементов [Локальный]`)

7.2.6 Шаг 4. Скопировать выделенные файлы на другую сторону

1. На нижней панели **Выбрано** нажмите кнопку — приложение переключится на противоположную сторону, при этом выделение сохраняется
2. Перейдите в каталог-назначения на новой стороне обычной навигацией
3. Нижняя панель сменит заголовок на **Вставить сюда?**
4. Нажмите кнопку — начнётся копирование

Во время передачи на нижней панели отображается индикатор прогресса, заголовок **Ожидание** и текущая скорость передачи. После завершения панель показывает **Успешно!** или **Ошибка!**

7.2.7 Шаг 5. Удалить файлы (опционально)

- Удалить выделенные элементы можно из панели **Выбрано** кнопкой
- Удалить одну запись без режима выделения — в строке записи → **Удалить**

Важно

Удаление выполняется без перемещения в корзину. Восстановить файл штатными средствами клиента невозможно

7.2.8 Шаг 6. Создать папку (опционально)

1. Перейдите в каталог, где нужна новая папка
2. Откройте в шапке → **Создать папку**
3. Введите имя папки в диалоге и нажмите OK

7.2.9 Что дальше

- При больших объёмах включите запись логов передачи файлов на сервере — *Запись видеосессий и логи передачи файлов*
- Завершить передачу можно прерыванием задачи на нижней панели кнопкой или закрытием подключения кнопкой в шапке
- Полное описание режима передачи файлов: Передача файлов

7.3 Раздача собственного экрана Android оператору

Кейс — настройка мобильного клиента **RuDesktop** для **Android** так, чтобы оператор технической поддержки или коллега смог подключиться к этому Android-устройству и видеть его экран. Подходит для удалённой помощи пользователю с проблемами на телефоне или планшете

7.3.1 Что вы получите

- Запущенную службу удалённого доступа на Android-устройстве
- Постоянный или одноразовый пароль для подключения
- Все нужные системные разрешения, чтобы оператор мог видеть экран, передавать файлы и при необходимости управлять устройством

7.3.2 Подготовка

- На устройстве установлен мобильный клиент **RuDesktop** для Android
- Известен сервер, через который оператор будет подключаться (публичный или корпоративный)
- Устройство работает на **Android 7.0** и выше (для голосовых вызовов и аудио — **Android 11** и выше)

7.3.3 Шаг 1. Запустить службу удалённого доступа

1. Откройте вкладку Доступ
2. Нажмите Запустить службу
3. Подтвердите системный диалог Android **Начать запись или трансляцию с устройства?**

После запуска службы появится ваш ID и блок **Одноразовый пароль**

7.3.4 Шаг 2. Выдать необходимые разрешения

В блоке **Разрешения** активируйте нужные разрешения:

- **Захват экрана** — обязательно. Включается автоматически при старте службы
- **Захват ввода** — если нужно, чтобы оператор мог управлять устройством, а не только смотреть. Это разрешение использует системные **Специальные возможности** Android — подробности в Активация захвата ввода
- **Захват системных звуков** — если нужно передавать звук с устройства (Android 11+)
- **Передача файлов** — если оператор должен иметь возможность копировать файлы на устройство и обратно
- **Отправлять уведомления** — для отображения системных уведомлений во время сессии
- **Отображать поверх других приложений** — для отображения плавающих элементов клиента (например, окна чата)
- **Разрешение записи звука** — для голосовых вызовов и трансляции системного аудио (Android 11+)

Важно

Разрешения **Захват ввода**, **Передача файлов**, **Отображать поверх других приложений** требуют ручного выдачи через системные настройки Android — приложение само открывает нужный экран настроек

7.3.5 Шаг 3. Выбрать способ аутентификации

В блоке **Одноразовый пароль** нажмите для меню паролей

Выберите способ:

- **Использовать временный пароль** — оператору нужно будет ввести одноразовый пароль, действительный только до следующего нажатия или перезапуска службы. Длину пароля можно задать (6, 8 или 10 символов) пунктом **Длина временного пароля**
- **Использовать постоянный пароль** — задайте постоянный пароль через **Установить постоянный пароль** (минимум 6 символов). Постоянный пароль не отображается в интерфейсе после ввода

- **Использовать оба пароля** — оператор сможет подключиться по любому из паролей

Подсказка

Для разовой помощи проще использовать **Временный пароль** — после завершения сеанса достаточно нажать для обновления пароля или остановить службу

7.3.6 Шаг 4. Передать ID и пароль оператору

- Нажмите рядом с ID — идентификатор скопируется в буфер обмена
- Нажмите рядом с одноразовым паролем — пароль скопируется в буфер обмена
- Передайте ID и пароль оператору любым удобным способом (мессенджер, телефон, SMS)

Примечание

Если в **Меню паролей** выбран пункт **Скрыть временный пароль**, пароль отображается точками. Снимите эту настройку, чтобы видеть пароль перед отправкой

7.3.7 Шаг 5. Подтвердить входящее подключение

Когда оператор отправит запрос на подключение, в блоке Активные подключения появится карточка с информацией:

- **Удалённое подключение** — для удалённого управления
- **Файловое соединение** — для работы с файлами

Нажмите Принять, чтобы разрешить подключение, или Отклонить

После принятия в карточке станут доступны:

- Кнопка **Чат** — переключает на вкладку Чат для переписки с оператором (отображается только для **Удалённого подключения**, не для **Файлового соединения**)
- Кнопка Отключить — принудительно завершить сессию

7.3.8 Шаг 6. Завершить раздачу экрана

- Закройте сессию из карточки активного подключения кнопкой Отключить
- Полностью остановите службу — Остановить службу в блоке **Разрешения**. После этого подключение к устройству невозможно до повторного запуска службы

7.3.9 Что дальше

- Если служба должна запускаться автоматически после перезагрузки устройства — Автозапуск службы
- Чтобы запись входящих сессий сохранялась автоматически — *Запись сессий на мобильном*
- Если оператор предпочитает разовую ссылку вместо ID/пароля — *Создание пригласительной ссылки в мобильном клиенте Android*

7.4 Запись сессий на мобильном клиенте

Кейс — настройка автоматической записи входящих и исходящих сессий мобильного клиента **RuDesktop** для **Android**, а также запуск записи отдельной сессии вручную из окна подключения

7.4.1 Что вы получите

- Автоматическую запись всех входящих подключений к этому устройству (когда оператор подключается к вам)
- Автоматическую запись всех исходящих подключений с этого устройства (когда вы подключаетесь к удалённому ПК)
- Возможность включать или выключать запись прямо во время сессии

7.4.2 Подготовка

- Установлен и настроен мобильный клиент **RuDesktop** для Android
- На устройстве достаточно свободного места — видеозаписи занимают значительный объём

7.4.3 Шаг 1. Открыть параметры записи

Откройте вкладку Настройки — параметры записи разнесены по двум блокам:

- Блок **Запись экрана** — настройки автоматической записи
- Блок **Доступ** — общий выключатель функции записи

7.4.4 Шаг 2. Включить функцию записи сессий

В блоке **Доступ** активируйте переключатель **Включить запись сессии**. Без этого переключателя кнопка ручного запуска записи в меню сессии будет недоступна

7.4.5 Шаг 3. Настроить автоматическую запись

В блоке **Запись экрана**:

- **Автоматически записывать входящие подключения** — все сессии, в которых **оператор подключается к вашему устройству**, будут записываться автоматически с момента принятия подключения

- **Автоматически записывать исходящие подключения** — все сессии, в которых **вы подключаетесь к удалённому ПК**, будут записываться автоматически с момента установки сессии

Под каждым переключателем указан каталог, куда сохраняются видеофайлы

Подсказка

Если нужно записывать только отдельные сессии — оставьте оба переключателя выключенными и запускайте запись вручную в каждой сессии (см. шаг 4)

7.4.6 Шаг 4. Запустить запись вручную в активной сессии

1. Подключитесь к удалённому ПК
2. В нижней панели окна подключения нажмите
3. Выберите пункт **Начать запись сессии**

При активной записи пункт меняется на **Остановить запись сессии**

7.4.7 Шаг 5. Добавить примечание к записи (опционально)

Во время активной записи в меню появляется дополнительный пункт **Примечание** . Примечание сохраняется локально на устройстве оператора и привязывается к идентификатору удалённого устройства — при следующем подключении к тому же устройству ранее введённый текст автоматически подставляется в диалог

7.4.8 Шаг 6. Найти сохранённые записи

- На устройстве — каталог, указанный под пунктами **Автоматически записывать ...** в настройках
- На сервере — свойства сессии на странице **Удалённый доступ → Сессии**, вкладка Видеозапись. Запись отображается, если на серверной стороне в свойствах группы оператора активирован пункт *Запись видеосессий*

7.4.9 Что дальше

- Если место на устройстве заполняется — отключите автозапись и запускайте запись вручную только при необходимости
- Полное описание раздела: Окно клиента → Настройки → Запись экрана
- Серверная политика записи: *Запись видеосессий и логи передачи файлов*

7.5 Прокси и альтернативные серверы на мобильном клиенте

Кейс — настройка работы мобильного клиента **RuDesktop** для **Android** через **SOCKS5** или **HTTP**-прокси и список **альтернативных серверов**. Подходит для сценариев, когда основной сервер периодически недоступен из сети устройства, или когда подключение должно идти только через корпоративный прокси

7.5.1 Что вы получите

- Подключение к серверу **RuDesktop** через прокси (SOCKS5 или HTTP) с авторизацией или без
- Список резервных адресов сервера, которые автоматически будут использованы при недоступности основного

7.5.2 Подготовка

- Установлен и настроен мобильный клиент **RuDesktop** для Android
- Известны:
  - Тип прокси (SOCKS5 или HTTP), адрес прокси-сервера, имя пользователя и пароль (если требуется)
  - Адреса альтернативных серверов **RuDesktop** (выдаёт администратор)
- Учётная запись имеет право Изменять сервер подключения, либо используется публичный сервер

Примечание

Пункты Сервер для подключения, Альтернативные сервера и Прокси-сервер отображаются в настройках только при наличии указанного права или при использовании публичного сервера

7.5.3 Настройка прокси

Шаг 1. Открыть диалог настройки прокси

1. Откройте вкладку Настройки
2. В блоке Настройки (сетевые) откройте пункт Прокси-сервер

Шаг 2. Заполнить параметры

В диалоге Прокси-сервер заполните поля:

- **Тип прокси** — выпадающий список с вариантами **SOCKS5** (по умолчанию) или **HTTP**

- **Адрес** — адрес прокси-сервера, при необходимости с портом (например, `proxy.example.com:1080`)
- **Имя пользователя** — если прокси требует аутентификации
- **Пароль** — если прокси требует аутентификации

Нажмите OK для сохранения

После сохранения иконка пункта Прокси-сервер в настройках подсвечивается цветом — это сигнал, что прокси активен

Подсказка

Чтобы отключить прокси — откройте тот же диалог, очистите поле **Адрес** и нажмите OK

7.5.4 Настройка альтернативных серверов

Шаг 1. Открыть список

1. Откройте вкладку Настройки
2. В блоке Настройки (сетевые) откройте пункт Альтернативные сервера

Откроется диалог Альтернативные сервера со списком уже добавленных адресов

Шаг 2. Добавить адрес

1. Введите адрес сервера в поле **Добавить адрес** (например, `rz-backup.example.com`)
2. Нажмите кнопку справа от поля или подтвердите ввод клавишей **Готово** на клавиатуре

Адрес появится в списке. Можно повторять для добавления нескольких адресов

Важно

Лимит — до **7** альтернативных адресов. После достижения лимита поле ввода становится неактивным, а его подпись меняется с **Добавить адрес** на **Max addresses**

Шаг 3. Удалить адрес (опционально)

В строке адреса нажмите кнопку удаления — запись скрывается с анимацией и список синхронизируется с сервером

Шаг 4. Закрыть диалог

Нажмите Закрыть. Изменения применяются автоматически по мере добавления и удаления адресов

7.5.5 Поведение при подключении

- При запуске приложение пытается подключиться к **основному серверу** (Сервер для подключения)
- Если основной сервер недоступен — клиент перебирает альтернативные адреса в том порядке, в котором они указаны в списке
- При активной настройке прокси все обращения к серверам проходят через указанный SOCKS5-прокси

7.5.6 Что дальше

- Если адрес сервера выдаётся через QR-код — Сканер QR-кодов
- Полное описание раздела: Окно клиента → Настройки → блок «Настройки»

7.6 Подключение через корпоративный SOCKS5/HTTP-прокси

Кейс — настройка мобильного клиента **RuDesktop** для **Android** на работу через корпоративный прокси-сервер с авторизацией. Подходит для пользователей, у которых выход в интернет с устройства разрешён только через корпоративный прокси (например, в локальной сети организации с фильтрацией трафика)

7.6.1 Что вы получите

- Подключение к серверу **RuDesktop** через **SOCKS5** или **HTTP**-прокси
- Поддержку прокси с авторизацией по логину и паролю
- Корректную работу клиента в сетях с обязательной маршрутизацией через корпоративный прокси

Примечание

Если основная задача — резервирование адресов сервера на случай его недоступности, а не корпоративная фильтрация трафика — см. *Прокси и альтернативные серверы на мобильном клиенте*

7.6.2 Подготовка

- Установлен мобильный клиент **RuDesktop** для Android
- От сетевого администратора получены параметры прокси:

  - Тип прокси: **SOCKS5** или **HTTP**
  - Адрес и порт прокси (например, `proxy.corp.example.com:1080`)
  - Логин и пароль (если прокси требует аутентификации)
- Учётная запись имеет право Изменять сервер подключения, либо клиент использует публичный сервер **RuDesktop**

Примечание

Пункт Прокси-сервер отображается в настройках только при наличии указанного права или при использовании публичного сервера

7.6.3 Когда какой тип прокси использовать

- **SOCKS5** — универсальный прокси на транспортном уровне, передаёт TCP-трафик любого протокола. Подходит для большинства корпоративных инфраструктур. **Тип по умолчанию** в мобильном клиенте
- **HTTP** — прокси на уровне HTTP CONNECT. Используется реже, обычно когда корпоративный шлюз поддерживает только HTTP-туннелирование

Подсказка

Если администратор не уточнил тип — начните с **SOCKS5**: это значение по умолчанию и в большинстве случаев работает с корпоративными прокси

7.6.4 Шаг 1. Открыть диалог настройки прокси

1. Откройте вкладку Настройки
2. В блоке **Настройки** нажмите пункт Прокси-сервер

Откроется диалог Прокси-сервер с полями параметров

7.6.5 Шаг 2. Выбрать тип прокси

Сверху диалога расположен выпадающий список с двумя вариантами:

- **SOCKS5** — выбор по умолчанию
- **HTTP**

Выберите тот тип, который указал администратор

7.6.6 Шаг 3. Заполнить адрес и порт

В поле **Адрес** введите адрес прокси-сервера. Формат:

- `host` — если прокси использует стандартный порт (1080 для SOCKS5)
- `host:port` — если порт нестандартный (например, `proxy.corp.example.com:3128`)

Важно

Адрес проверяется на валидность при сохранении. Если адрес некорректен, под полем появится сообщение об ошибке, и сохранение не выполнится

7.6.7 Шаг 4. Указать учётные данные (если требуются)

Если корпоративный прокси требует аутентификации, заполните поля:

- **Имя пользователя** — логин для прокси
- **Пароль** — пароль для прокси (с кнопкой переключения видимости)

Если прокси работает без авторизации, оставьте поля пустыми

Важно

Учётные данные прокси хранятся локально на устройстве и не передаются на сервер **RuDesktop**

7.6.8 Шаг 5. Сохранить параметры

Нажмите OK для сохранения

После сохранения:

- Иконка пункта Прокси-сервер в настройках подсвечивается цветом — это сигнал, что прокси активен
- Все обращения клиента к серверам **RuDesktop** (включая сервер-ретранслятор) проходят через указанный прокси

7.6.9 Шаг 6. Проверить подключение

1. Перейдите на вкладку Подключение
2. Введите ID известного удалённого устройства и нажмите
3. Если подключение установилось — прокси настроен корректно

Подсказка

Если подключение не устанавливается:

- Перепроверьте адрес и порт прокси
- Уточните у администратора, разрешён ли исходящий трафик до сервера **RuDesktop** через этот прокси
- Проверьте логин и пароль на чувствительность к регистру

7.6.10 Отключение прокси

Чтобы отключить прокси и вернуться к прямому подключению:

1. Откройте Настройки → Прокси-сервер
2. Очистите поле **Адрес** (логин и пароль также можно очистить)
3. Нажмите OK

Иконка пункта Прокси-сервер перестанет подсвечиваться — прокси неактивен, обращения к серверу идут напрямую

7.6.11 Особенности

- Прокси применяется ко **всем сетевым операциям клиента**: к серверу **RuDesktop**, серверу-ретранслятору, скачиванию обновлений
- Настройка прокси **локальна для устройства** и не синхронизируется через учётную запись
- При смене сервера через QR-код настройки прокси сохраняются — QR-код задаёт только адрес сервера
- Прокси и список альтернативных серверов работают независимо: при включённом прокси все альтернативные адреса также пробиваются через прокси

7.6.12 Что дальше

- Дополнительно настроить альтернативные сервера на случай недоступности основного — *Прокси и альтернативные серверы на мобильном клиенте*
- Полное описание раздела: Окно клиента → Настройки → блок «Настройки»

7.6.13 Связанные кейсы

- *Прокси и альтернативные серверы на мобильном клиенте*
- *Первое подключение к удалённому ПК с Android*

7.7 Голосовой вызов оператор↔пользователь во время сессии

Кейс — установление голосовой связи между оператором, подключившимся с мобильного клиента **RuDesktop** для **Android**, и пользователем удалённого устройства во время активной сессии. Голосовая связь идёт поверх существующего подключения и не разрывает сессию

7.7.1 Что вы получите

- Голосовое общение во время демонстрации экрана без необходимости использовать сторонние мессенджеры
- Возможность инициировать вызов с любой стороны: оператор → пользователь или пользователь → оператор
- Управление микрофоном (mute) и завершением вызова без разрыва основной сессии

7.7.2 Подготовка

- На мобильном клиенте **RuDesktop** для Android, который инициирует или принимает вызов, требуется **Android 11 (API 30)** или выше
- Разрешение **Разрешение записи звука** (*RECORD_AUDIO*):
  - На мобильном клиенте оператора — приложение запросит разрешение при первом нажатии на кнопку вызова
  - На принимающей стороне — выдаётся через Окно клиента → Доступ → Разрешения
- Между устройствами установлено активное подключение (рабочий стол)

Важно

Без разрешения **Разрешение записи звука** вызов не установится — на инициирующей стороне появится уведомление о неудаче

7.7.3 Сценарий 1. Исходящий вызов с мобильного клиента

Шаг 1. Подключиться к удалённому устройству

Установите обычное подключение к рабочему столу с мобильного клиента — см. *Первое подключение к удалённому ПК с Android*

Шаг 2. Запустить вызов

В нижней панели окна подключения нажмите кнопку ☎

Откроется окно подтверждения с заголовком **Голосовой вызов** и текстом **Позвонить удалённому устройству?**

- OK — отправляет запрос на удалённое устройство
- Отклонить — закрывает окно без вызова

Подсказка

При первом запуске вызова приложение запросит у системы разрешение **Разрешение записи звука**. Согласитесь — без него вызов не установится

Шаг 3. Дождаться ответа

После отправки запроса в окне отображается сообщение **Запрос отправлен. Ожидание ответа…**

- Окно ожидания можно закрыть кнопкой OK — вызов продолжит ожидание ответа в фоне
- Принудительно отменить вызов до ответа можно кнопкой Отклонить

На удалённое устройство приходит уведомление с возможностью принять или отклонить вызов

Шаг 4. Управлять активным вызовом

После принятия иконка телефона ☎ в нижней панели сменяется на иконку завершения вызова . Нажатие на неё открывает меню:

- **Завершить голосовой вызов** — прекращает аудиосвязь, не разрывая основное подключение
- **Заглушить микрофон** — переключает состояние микрофона. Иконка микрофона справа от пункта отражает текущее состояние

7.7.4 Сценарий 2. Входящий вызов на мобильный клиент

Голосовой вызов также может быть инициирован удалённым оператором, подключённым к вашему устройству

Шаг 1. Запустить службу удалённого доступа

На вкладке Доступ запустите службу — см. *Раздача собственного экрана Android оператору*

Шаг 2. Принять подключение оператора

Когда оператор подключается, в карточке активного подключения появляется кнопка Принять. После её нажатия начинается активная сессия

Шаг 3. Принять входящий вызов

Когда оператор инициирует голосовой вызов:

- Если приложение открыто — в карточке активного подключения на вкладке Доступ появляется блок **Входящий голосовой вызов** с кнопками Принять и Отменить
- Если приложение свёрнуто — отображается системное уведомление Android, принять или отклонить вызов можно прямо из уведомления

Шаг 4. Управлять активным вызовом

После принятия в карточке активного подключения отображается блок **Голосовой вызов** с кнопкой Завершить вызов. Нажатие на неё прекращает аудиосвязь, не разрывая основное подключение

Примечание

Управление микрофоном (mute) для входящего вызова из приложения не предусмотрено — пункт **Заглушить микрофон** доступен только инициирующей стороне (оператору)

7.7.5 Особенности

- Голосовая связь работает поверх основного соединения и **не разрывает** сессию демонстрации экрана
- Завершение голосового вызова не закрывает само подключение к удалённому рабочему столу
- При обрыве сетевого соединения активный голосовой вызов автоматически завершается
- На устройствах с **Android 10 (API 29)** и ниже функция голосового вызова **недоступна** — приложение покажет уведомление о требуемой версии

7.7.6 Что дальше

- Описание всех элементов окна голосового вызова: Голосовой вызов
- Управление разрешениями приложения: Окно клиента → Доступ → Разрешения

7.7.7 Связанные кейсы

- *Раздача собственного экрана Android оператору*
- *Первое подключение к удалённому ПК с Android*

7.8 Преднастройки подключения

Нужно подключаться с Android-телефона к рабочим компьютерам с удобными параметрами изображения и управления, не меняя их заново при каждом подключении. В этом примере для большинства компьютеров используется режим мыши, а для одного устройства сохраняется сенсорный режим

7.8.1 Подготовка

1. Подключить мобильный клиент RuDesktop к нужному серверу
2. Убедиться, что есть доступ к тестовому компьютеру
3. Определить, какие параметры должны быть общими, а какие нужны только для отдельного устройства

7.8.2 Задать общие параметры

1. Открыть вкладку **«Настройки»** мобильного клиента
2. В блоке **«Дополнения»** открыть **«Преднастройки»**
3. В блоке **«Режим управления»** выбрать **«Режим мыши»**
4. Выбрать сбалансированное качество изображения и размер **«Уменьшить»**
5. При необходимости включить показ удалённого курсора или отключить звук
6. Закрыть настройки и подключиться к тестовому компьютеру

Примечание

Изменения сохраняются автоматически, отдельной кнопки сохранения нет

Подсказка

Для медленной сети можно выбрать **«Быстрое время реакции»** и проверить, достаточно ли чётким остаётся изображение

Для наблюдения без ввода с телефона включить **«Режим просмотра»**

Описание всех параметров находится на странице Преднастройки подключения

7.8.3 Выбрать другой режим для одного компьютера

1. Открыть меню нужного устройства в списке мобильного клиента
2. Выбрать **«Настройки подключения»**
3. В блоке **«Режим управления»** выбрать **«Сенсорный режим»**
4. Подключиться к этому компьютеру и проверить управление касаниями
5. Завершить подключение и открыть его снова

Для этого компьютера должен сохраниться сенсорный режим. Другие устройства без собственного выбора продолжают использовать общий режим мыши

Примечание

Переключение режима курсора в открытой сессии также запоминается для этого устройства

Последующее изменение общих преднастроек не заменяет его индивидуальный выбор

7.8.4 Вернуть общий режим

1. Снова открыть **«Настройки подключения»** нужного устройства
2. В блоке **«Режим управления»** выбрать **«По умолчанию»**
3. Подключиться к устройству и проверить, что используется режим из общих преднастроек

Примечание

При подключении к Android-устройству используется сенсорное управление, выбор режима для него не требуется

7.8.5 Если результат отличается от ожидаемого

- Режим меняется только на одном компьютере - проверить его индивидуальные настройки и при необходимости выбрать **«По умолчанию»**
- Указатель движется относительно движения пальца - включён режим мыши
- Нажатие передаётся в точку касания - включён сенсорный режим
- Изображение есть, но управление не работает - проверить режим просмотра и разрешение удалённой стороны на ввод

Описание жестов приведено на странице Режим курсора

В этом разделе собраны кейсы по типовым сценариям работы с **мобильным клиентом RuDesktop** для **Android**: подключение к удалённому ПК с телефона, передача файлов, раздача собственного экрана оператору, запись сессий, голосовой вызов, преднастройки, работа через прокси и альтернативные серверы

Подсказка

Подробное описание интерфейса мобильного клиента — Руководство пользователя → Мобильный клиент

Сценарии создания пригласительных ссылок (в том числе на Android) вынесены в отдельный раздел — *Пригласительные ссылки*

Первое подключение с Android

Установка клиента, подключение к серверу и открытие первой сессии с удалённым ПК с мобильного устройства

Передача файлов с телефона

Копирование файлов и папок между Android-устройством и удалённым ПК через встроенный режим передачи файлов

Раздача экрана Android оператору

Запуск службы удалённого доступа на телефоне, чтобы оператор мог подключиться и видеть экран Android-устройства

Запись сессий на мобильном

Автоматическая запись входящих и исходящих сессий мобильного клиента, а также ручной запуск записи во время сессии

Голосовой вызов во время сессии

Голосовая связь оператор ↔ пользователь поверх активной сессии без сторонних мессенджеров

Преднастройки подключения

Единые параметры качества и переключателей по умолчанию для всех будущих исходящих подключений

Прокси и альтернативные серверы

Подключение через **SOCKS5/HTTP**-прокси и список резервных адресов сервера на случай недоступности основного

Корпоративный SOCKS5/HTTP-прокси

Настройка работы через корпоративный прокси с авторизацией для сетей с обязательной маршрутизацией трафика

ГЛАВА 8

Пригласительные ссылки

8.1 Управление пригласительными ссылками в веб-интерфейсе

Кейс — создание и управление пригласительными ссылками в веб-интерфейсе сервера **RuDesktop**. В отличие от клиентов, веб-интерфейс предоставляет полный набор параметров: дата начала действия, тип ограничения, группа прав подключения и комментарий

8.1.1 Что вы получите

- Готовую пригласительную ссылку с произвольным временем начала и сроком действия
- Возможность ограничить, кто именно может подключиться по ссылке (любой / устройство / пользователь / группа)
- Опциональное переопределение прав подключения через выбранную группу
- Список всех созданных ссылок с возможностью копирования и удаления

8.1.2 Подготовка

- Учётная запись имеет права на доступ к странице **Пригласительные ссылки** и право Может управлять приглашениями для устройств
- Если требуется выбирать группу прав подключения — учётная запись имеет право **Может выбирать группу при создании ссылки для подключения**

- Если требуется видеть ссылки других пользователей — учётная запись имеет право **Может видеть все пригласительные ссылки** или является руководителем подразделения

8.1.3 Шаг 1. Открыть страницу пригласительных ссылок

В веб-интерфейсе сервера перейдите **Удалённый доступ → Пригласительные ссылки**

На странице отображается таблица ранее созданных ссылок и кнопка добавления новой ссылки. Подробное описание колонок и фильтров — Пригласительные ссылки

8.1.4 Шаг 2. Создать новую ссылку

1. Нажмите кнопку Добавить пригласительная ссылка
2. Заполните параметры на открывшейся странице добавления:
   - Запрашивать пароль при подключении — выбор: подключаться с вводом пароля устройства или без него

> **Примечание**
>
> Если у устройства отсутствует право **Может подключаться без подтверждения со стороны пользователя**, при подключении всё равно появится окно подтверждения на стороне устройства

> **Примечание**
>
> В облачной версии **RuDesktop** этот параметр скрыт: подключение по пригласительной ссылке всегда выполняется с запросом пароля

   - Устройство* — выбор устройства, для которого создаётся ссылка
   - Группа прав подключения — переопределяет права подключения, заданные в Доступах

> **Важно**
>
> Поле доступно только при наличии у учётной записи права **Может выбирать группу при создании ссылки для подключения**

   - Дата начала действия* — дата и время, с которой ссылка начинает работать. Можно задать в будущем, чтобы ссылка стала валидной только в нужное окно времени

- Время действия ссылки — продолжительность действия с момента, заданного в **Дата начала действия**
- Тип подключения — допустимый тип сессии: **Рабочий стол**, **Передача файлов**, **Терминал** и др.
- Максимальное количество использований* — лимит подключений по ссылке. После исчерпания ссылка перестаёт работать

> **Подсказка**
>
> Значение 1 делает ссылку одноразовой — после первого подключения повторное по этой же ссылке невозможно

- Тип ограничения — кто может воспользоваться ссылкой:
  - Без ограничений — любое устройство, у которого есть подходящие права доступа
  - Устройство — выбор конкретного устройства-инициатора
  - Пользователь — выбор конкретного пользователя
  - Группа — все устройства, добавленные в выбранную группу, смогут подключиться
- Комментарий — текстовая заметка для администратора (например, причина выдачи ссылки)

3. Нажмите Сохранить — ссылка создаётся и страница возвращается к списку. Кнопка Сохранить и продолжить оставляет форму открытой для ввода следующей ссылки

8.1.5 Шаг 3. Скопировать ссылку и передать оператору

В списке пригласительных ссылок:

- Скопируйте URL ссылки из колонки **Ссылка**
- Передайте URL оператору любым удобным способом (мессенджер, e-mail, SMS, корпоративный портал)

8.1.6 Шаг 4. Управление существующими ссылками

- **Просмотр и редактирование** — открывайте запись из таблицы для просмотра подробных параметров и при необходимости их изменения
- **Удаление** — выберите запись в таблице и используйте действие удаления. Удалённую ссылку нельзя восстановить, но активные сессии, открытые по ней до удаления, не разрываются

8.1.7 Шаг 5. Просмотр ссылок в свойствах устройства

Чтобы увидеть все ссылки, привязанные к конкретному устройству:

1. Перейдите на страницу **Удалённый доступ → Устройства**
2. Откройте свойства нужного устройства
3. Перейдите на вкладку Приглашения

Подсказка

Вкладка Приглашения отображается только при наличии у учётной записи права **Может видеть пригласительные ссылки в свойствах устройства**

8.1.8 Подключение к другому серверу по приглашению

Если оператор и устройство-цель находятся на разных серверах **RuDesktop**:

- На сервере, к которому подключён оператор, у учётной записи должно быть право Подключаться к другому серверу по приглашению
- На сервере, где находится устройство-цель, должна быть указана группа для подключения, для которой автоматически создаётся доступ на странице **Доступы**

8.1.9 Что дальше

- Подключение **с десктопного клиента**: *Создание пригласительной ссылки в десктопном клиенте*
- Подключение **с мобильного клиента**: *Создание пригласительной ссылки в мобильном клиенте Android*
- Подробное описание страницы веб-интерфейса: Пригласительные ссылки

8.2 Создание пригласительной ссылки в десктопном клиенте

Кейс — создание пригласительной ссылки на текущее устройство-инициатор из десктопного клиента **RuDesktop** (Windows / Linux / macOS) и её последующая выдача оператору. Подходит для сценариев разовой помощи, когда удобнее сгенерировать ссылку прямо с устройства, а не через веб-интерфейс

8.2.1 Что вы получите

- Пригласительную ссылку с заданным сроком действия и числом использований
- Возможность подключения по ссылке с любого клиента **RuDesktop** на этом или другом сервере

- Видимость созданной ссылки в свойствах устройства в веб-интерфейсе

8.2.2 Подготовка

- На устройстве установлен десктопный клиент **RuDesktop** и подключён к корпоративному серверу
- У пользователя или устройства активно право Может управлять приглашениями для устройств

Важно

В десктопном клиенте набор полей сокращён по сравнению с веб-интерфейсом: нельзя задать дату начала действия, тип ограничения и группу прав подключения. Ссылка автоматически создаётся для устройства, с которого выполняется создание

8.2.3 Шаг 1. Открыть диалог создания ссылки

В блоке Ваше устройство рядом с идентификатором устройства расположена иконка

1. Убедитесь, что в блоке Ваше устройство отображаются ID устройства и иконка рядом с шестерёнкой настроек
2. Нажмите на иконку — откроется диалог Пригласить

Примечание

Если кнопка не отображается — у учётной записи или устройства нет права Может управлять приглашениями для устройств. Обратитесь к администратору сервера

8.2.4 Шаг 2. Заполнить параметры ссылки

В диалоге Пригласить заполните поля:

- **Максимальное кол-во использований (от 1 до 99)** — максимальное число подключений по ссылке. Для разовой помощи укажите 1. По умолчанию 1
- **Срок действия** — выбор из списка:
  - **15 минут**
  - **1 час**
  - **2 часа**
  - **5 часов**
  - **1 день**
  - **1 неделя**

  - **1 месяц**

- **Сделать бессрочной** — переключатель. При активации поле срока действия становится неактивным, и ссылка не имеет даты окончания
- **Тип подключения** — допустимый тип сессии:
  - **Рабочий стол** — удалённое управление рабочим столом
  - **Передача файлов** — режим работы с файловой системой удалённого устройства
  - **RDP** — подключение по протоколу RDP к Windows-устройству
  - **Терминал** — терминальная сессия (SSH/PowerShell/cmd) к удалённому устройству
- **Запрашивать пароль при подключении** — переключатель. При активации, помимо принятия запроса на устройстве, оператор должен будет ввести временный или постоянный пароль

Нажмите OK для создания ссылки

8.2.5 Шаг 3. Скопировать и отправить ссылку оператору

Созданная ссылка появится во вкладке Приглашения в окне клиента

В таблице доступны:

- **Кнопка копирования** — копирует URL ссылки в буфер обмена. Под кнопкой отображается индикатор статуса:
  - — ссылка активна
  - — срок действия истёк
- **Тип подключения** — тип сессии, которую откроет оператор по ссылке
- **Количество использований** — текущее число использований и максимально разрешённое
- **Начало действия** и **Время истечения** — отображаются в всплывающей подсказке рядом с записью. Для ссылок без срока в поле истечения отображается **Бессрочная**

Передайте URL оператору любым удобным способом (мессенджер, e-mail, SMS)

Подсказка

Скопировать ссылку также можно через контекстное меню записи (нажмите справа от ссылки → **Копировать**)

8.2.6 Шаг 4. Принять подключение оператора

Когда оператор откроет ссылку:

- Клиент оператора автоматически инициирует сессию указанного типа к вашему устройству

- Если в диалоге создания ссылки была включена опция **Запрашивать пароль при подключении** — оператор увидит окно ввода пароля
- При отсутствии у учётной записи оператора права на подключение без подтверждения — на вашем устройстве появится окно подтверждения подключения. Подтвердите его кнопкой Принять

8.2.7 Шаг 5. Удаление и обновление ссылок

Во вкладке Приглашения:

- **Удалить ссылку** — нажмите справа от записи → **Удалить**. Удалённую ссылку нельзя восстановить
- **Загрузить ещё** — кнопка в конце списка подгружает следующую страницу
- **Обновить список** — кнопка в шапке таблицы

Примечание

Удаление ссылки в десктопном клиенте также удалит её из веб-интерфейса. Активные сессии, открытые по этой ссылке до её удаления, не разрываются

8.2.8 Где найти ссылку в веб-интерфейсе

Все ссылки, созданные в десктопном клиенте, отображаются:

- На общей странице **Удалённый доступ → Пригласительные ссылки**
- В свойствах устройства на вкладке Приглашения

8.2.9 Что дальше

- Полный набор параметров ссылки доступен в веб-интерфейсе: *Управление пригласительными ссылками в веб-интерфейсе*
- Аналогичный сценарий на Android: *Создание пригласительной ссылки в мобильном клиенте Android*
- Подробное описание функции: Пригласительные ссылки

8.3 Создание пригласительной ссылки в мобильном клиенте Android

Кейс - создание пригласительной ссылки на текущее Android-устройство из мобильного клиента **RuDesktop** и её последующая выдача оператору. Подходит для разовой помощи, когда удобнее сгенерировать ссылку прямо с телефона, не передавая ID и пароль

8.3.1 Что вы получите

- Пригласительную ссылку с заданным сроком действия и числом использований
- Подключение оператора по ссылке, в том числе с Android-клиента, настроенного на другой сервер
- Видимость созданной ссылки в свойствах устройства в веб-интерфейсе

8.3.2 Подготовка

- На устройстве установлен мобильный клиент **RuDesktop** для Android и подключён к корпоративному серверу
- У пользователя или устройства активно право Может управлять приглашениями для устройств

Важно

В мобильном клиенте набор полей сокращён по сравнению с веб-интерфейсом: нельзя задать дату начала действия, тип ограничения и группу прав подключения

Ссылка автоматически создаётся для устройства, с которого выполняется создание

8.3.3 Шаг 1 - Открыть диалог создания ссылки

Вкладка Приглашения расположена среди адресных вкладок во вкладке Подключение мобильного клиента

1. Откройте вкладку Подключение
2. Среди адресных вкладок выберите Приглашения
3. Откройте диалог создания ссылки:
    - Если список ссылок пуст - нажмите кнопку Приглашения в центре экрана
    - Если в списке уже есть ссылки - нажмите плавающую кнопку в правом нижнем углу

Примечание

Если вкладка Приглашения не отображается - у учётной записи или устройства нет права Может управлять приглашениями для устройств

Обратитесь к администратору сервера

8.3.4 Шаг 2 - Заполнить параметры ссылки

В диалоге Пригласить заполните поля:

- **Максимальное кол-во использований (от 1 до 99)** - максимальное число подключений по ссылке

  Для разовой помощи укажите 1

  По умолчанию 1

- **Срок действия** - выбор из списка:
  - **15 минут**
  - **1 час**
  - **2 часа**
  - **5 часов**
  - **1 день**
  - **1 неделя**
  - **1 месяц**
- **Сделать бессрочной** - переключатель

  При активации поле срока действия становится неактивным, и ссылка не имеет даты окончания

- **Тип подключения** - допустимый тип сессии:
  - **Рабочий стол** - удалённое управление рабочим столом
  - **Передача файлов** - передача файлов
- **Запрашивать пароль при подключении** - переключатель

  При включённой опции для подключения потребуется пароль удалённого устройства

  Подтверждение на самом устройстве зависит от прав подключения

Примечание

По умолчанию включены **«Сделать бессрочной»** и **«Запрашивать пароль при подключении»**

Для разовой помощи отключить **«Сделать бессрочной»**, выбрать нужный срок и оставить одно использование

Бессрочность отменяет только ограничение по времени, но не лимит использований

Нажмите OK для создания ссылки

8.3.5 Шаг 3 - Скопировать и отправить ссылку оператору

Созданная ссылка появится во вкладке Приглашения. В списке доступны:

- **Кнопка копирования** - копирует URL ссылки в буфер обмена

  На кнопке наложен цветной кружок-индикатор статуса:

  - - срок и лимит использований ещё не исчерпаны (зелёный)
  - - срок действия истёк или лимит использований исчерпан (красный)

- **Тип подключения** - тип сессии, которую откроет оператор по ссылке
- **Количество использований** - текущее число использований и максимально разрешённое
- **Информация о сроке** - при нажатии отображается всплывающая подсказка с двумя строками: **Начало действия** (дата создания ссылки) и **Время истечения** (либо «Бессрочная» для ссылок без срока)

Передайте URL оператору любым удобным способом (мессенджер, e-mail, SMS)

Подсказка

Скопировать ссылку также можно жестом смахивания строки влево или вправо

8.3.6 Шаг 4 - Принять подключение оператора

Когда оператор откроет ссылку:

- Клиент оператора автоматически инициирует сессию указанного типа к вашему устройству
- Если в диалоге создания ссылки была включена опция **Запрашивать пароль при подключении** - оператор увидит окно ввода пароля
- На вашем устройстве во вкладке Доступ в блоке Активные подключения появится карточка нового подключения
  - Если у оператора **нет** права на подключение без подтверждения - в карточке отображаются кнопки Принять и Отклонить

    После принятия запроса начинается сессия
  - Если у оператора **есть** это право - карточка сразу отображается как авторизованная (без кнопок Принять/Отклонить)

После начала сессии в карточке доступна кнопка Отключить для принудительного завершения подключения

8.3.7 Шаг 5 - Удаление и обновление ссылок

Во вкладке Приглашения:

- **Удалить ссылку** - нажмите в строке записи

  Подтвердите удаление кнопкой OK (окрашена в красный) в диалоге **Предупреждение** с текстом **Вы уверены, что хотите удалить эту ссылку?**

  Удалённую ссылку нельзя восстановить

- **Обновить список** - потяните список вниз и отпустите (жест `Pull to refresh`)

  Список синхронизируется с сервером

Примечание

Удаление ссылки в мобильном клиенте также удалит её из веб-интерфейса

Активные сессии, открытые по этой ссылке до её удаления, не разрываются

8.3.8 Где найти ссылку в веб-интерфейсе

Все ссылки, созданные в мобильном клиенте, отображаются:

- На общей странице **Удалённый доступ → Пригласительные ссылки**
- В свойствах устройства на вкладке Приглашения

8.3.9 Что дальше

- Полный набор параметров ссылки доступен в веб-интерфейсе: *Управление пригласительными ссылками в веб-интерфейсе*
- Аналогичный сценарий в десктопе: *Создание пригласительной ссылки в десктопном клиенте*
- Подробное описание интерфейса мобильного клиента: Пригласительные ссылки
- Чтобы оператор не увидел запрос подтверждения на устройстве - настройте в админке *подключение без подтверждения*

8.3.10 Открыть приглашение с другого сервера на Android

Оператор может открыть на Android приглашение к устройству другого сервера RuDesktop

1. Получить полную пригласительную ссылку от владельца устройства или администратора
2. Открыть ссылку на телефоне и подтвердить переход в приложение RuDesktop, если браузер запрашивает приложение
3. Для передачи файлов предоставить приложению запрошенный доступ к файлам

4. Дождаться подключения или подтверждения со стороны пользователя удалённого устройства

Подсказка

Использовать всю ссылку, а не только ID устройства: приглашение содержит данные для нужного подключения

Примечание

На Android поддерживаются приглашения для удалённого рабочего стола и передачи файлов

Для другого типа приглашения приложение покажет сообщение о неподдерживаемом типе подключения

Примечание

Если уже открыта сессия, новое подключение закрывает предыдущую

Повторное открытие той же ссылки при уже работающей сессии не создаёт ещё одно подключение

Если подключение не удалось, проверить доступность сервера из сети телефона, срок действия и лимит использований ссылки. Если срок или число использований исчерпаны, попросить владельца устройства создать новое приглашение. Если передача файлов не открывается после отказа в доступе к файлам, предоставить разрешение в настройках Android и открыть ссылку повторно

При ожидании подтверждения попросить пользователя удалённого устройства принять запрос

Примечание

Наличие ссылки не отменяет ограничения доступа, действующие на удалённой стороне

Пригласительные ссылки — одноразовые или ограниченные по времени URL-адреса, по которым третье лицо может подключиться к конкретному устройству без знания ID и пароля и без явного назначения прав в Доступах

Раздел собирает кейсы по работе с пригласительными ссылками в трёх точках:

- В **веб-интерфейсе** сервера — полный набор параметров ссылки (дата начала действия, тип ограничения, группа прав подключения)
- В **десктопном клиенте** — упрощённое создание ссылки на текущее устройство-инициатор

- В **мобильном клиенте Android** — упрощённое создание ссылки на текущее Android-устройство

Подсказка

Полное описание функции и страницы веб-интерфейса: Пригласительные ссылки

Важно

- Для отображения кнопки создания ссылки в десктопном или мобильном клиенте у пользователя или устройства должно быть активно право Может управлять приглашениями для устройств
- Ссылки, созданные в веб-интерфейсе, **не отображаются** в клиенте. Ссылки, созданные в клиенте, отображаются и в клиенте, и в веб-интерфейсе

8.4 Что вы получите

После настройки в системе будет:

- Один или несколько разовых или ограниченных по времени URL-адресов для подключения к выбранному устройству
- Возможность распространить ссылку через мессенджер, e-mail или SMS, не передавая ID и пароль
- Журнал использований ссылки в свойствах устройства на странице **Удалённый доступ → Устройства** (вкладка Приглашения)

Управление в веб-интерфейсе

Полный набор параметров: дата начала, тип ограничения (любой / устройство / пользователь / группа), переопределение прав подключения

Создание в десктопном клиенте

Упрощённое создание ссылки на текущее устройство-инициатор из десктопного клиента (Windows / Linux / macOS)

Создание в мобильном клиенте Android

Упрощённое создание ссылки на текущее Android-устройство прямо с телефона — без передачи ID и пароля

ГЛАВА 9

Миграция Windows → Linux

9.1 1. Подготовка

Перед запуском миграции нужно подготовить целевой образ **Linux**, включить поддержку **PXE** в прошивке устройств и заранее спланировать, какое ПО потребуется на **Linux**

9.1.1 Подготовить целевой образ Linux

1. Открыть раздел Установка OS → Образы OS
2. Если нужный образ ещё не добавлен — нажать Добавить Образ OS и заполнить поля. Пример для офисного сценария:
    - Название — `RedOS 8.0.2 — офис`
    - Тип OS — `RedOS 8 Linux`
    - ISO образ — ISO-файл из репозитория сервера или с компьютера
    - Язык — `Русский`
    - Часовой пояс — `Europe/Moscow`
    - Локальный администратор — `rdadmin`
    - Пароль локального администратора — задать пароль не короче 8 символов
    - Задачи после установки — для сценария миграции это поле можно не заполнять

Примечание

Поле Задачи после установки относится **только к чистой установке ОС** через PXE. При миграции эти задачи **не выполняются** — используется отдельное поле Задачи после миграции в *сценарии миграции*. Если этот же образ применяется и для чистых PXE-установок, поле Задачи после установки менять не нужно

3. Сохранить образ. Публиковать вручную **не нужно**: при запуске задачи миграции образ публикуется автоматически

Важно

Локальный администратор образа (`rdadmin`) — это пользователь, которого создаст установщик **Linux**. Он не связан с переносимыми с **Windows** учётными записями. Имя не должно совпадать с именами переносимых пользователей

9.1.2 Подготовить устройства Windows

1. На каждом устройстве, которое будет мигрироваться, в **BIOS**:
   - включить **Network Stack** и **IPv4 PXE Support** (вкладка `Network Stack Configuration` или аналогичная) — это нужно, чтобы в прошивке появилась загрузочная запись **UEFI: PXE IPv4**;
   - отключить **Fast Boot** (вкладка `Boot`).

Примечание

Делать **UEFI: PXE IPv4** первым вариантом загрузки **не требуется**. На этапе `Сброс загрузчика` сервер **RuDesktop** автоматически переключает устройство в PXE-загрузку:

- на UEFI — задаёт одноразовую загрузку с PXE через `bcdedit` (отрабатывает, если в прошивке зарегистрирована запись PXE/Network — см. шаги выше);
- на BIOS/Legacy — если предыдущий способ не сработал, ломает загрузку с диска, чтобы устройство ушло на следующий вариант (обычно PXE).

Описание стандартных предварительных настроек BIOS — Предварительные настройки устройства (раздел относится к чистой PXE-установке, но шаги по включению PXE в прошивке те же)

2. Убедиться, что устройство и сервер **RuDesktop** находятся в одной локальной сети, а **DHCP** и **PXE** в этой сети настроены: устройство при за-

грузке должно получить IP-адрес и загрузочные файлы с сервера

Важно

Встроенный **PXE-сервер RuDesktop** работает только в пределах одной локальной сети. Для устройств в удалённых сетях нужен отдельный экземпляр сервера или внешние средства

3. Убедиться, что **RuDesktop**-клиент на устройстве зарегистрирован на сервере и онлайн — иначе оркестратор миграции не сможет запустить плейбук сбора данных

Примечание

Если устройство временно недоступно во время миграции, оркестратор автоматически повторяет запуск плейбука до **10 раз** с интервалом **30 секунд**

9.1.3 Спланировать перенос данных

Миграция переносит **только пользовательские данные**. Заранее определить, что будет включено в перенос:

- стандартные папки пользователя (`Desktop` / `Documents` / `Downloads` / `Pictures` / `Videos` / `Music`);
- содержимое несистемных дисков (`D:\`, `E:\` и т.д.);
- дополнительные пути (например, `C:\Projects` с рабочими проектами или путь относительно домашней папки пользователя);
- профильные данные браузеров (только **AppData** выбранных Chrome/Edge/Firefox/Yandex Browser).

Важно

Установленные программы Windows, реестр Windows, системные настройки и драйверы при миграции **не переносятся**. Сразу спланируйте, какой софт нужен на **Linux** после миграции — он будет ставиться через задачи UEM, выбранные в *сценарии миграции*

Важно

Установка **Linux** через PXE затирает диск, выбранный установщиком. При нескольких физических дисках установщик может выбрать любой подходящий — содержимое диска будет потеряно. Убедитесь, что важные данные включены в сценарий миграции либо сохранены отдельно

9.1.4 Спланировать перенос пользователей

- **Локальные пользователи** переносятся с временным паролем, заданным в миграции. Пользователь обязан сменить пароль при первом входе. Локальные пароли **Windows** не переносятся
- **Доменные пользователи** переносятся с использованием доменных учётных данных (нужен логин/пароль администратора домена с правом ввода устройств в домен) и продолжают входить под своим доменным паролем

Важно

Для **ALT Linux** и **RED OS** имена локальных пользователей с кириллическими символами автоматически транслитерируются в латиницу (`Иванов` → `ivanov`). Логин в новой ОС будет другим. Доменные пользователи переносятся без изменения имени. Заранее предупредите пользователей и подготовьте список соответствий имён, если это критично

После выполнения подготовки можно перейти к *созданию сценария миграции*

9.2 2. Создание сценария миграции

Сценарий миграции описывает, **что и как** будет переноситься: целевой образ, какие пользователи, какие данные, какие задачи **UEM** запустить после восстановления. На один сценарий миграции в дальнейшем может ссылаться несколько *задач миграции*

9.2.1 Открыть форму создания

1. Перейти в Установка ОС → Миграции
2. Нажать кнопку Добавить Миграцию. Открывается форма с тремя вкладками: Основная информация, Пользователи, Выбор данных

9.2.2 Вкладка «Основная информация»

Заполнить поля. Пример для офисного сценария на **RedOS 8.0.2**:

1. Название — `Миграция офиса на RedOS 8.0.2`

   Примечание

   Название должно быть уникальным среди всех миграций

2. Целевой образ ОС — выбрать `RedOS 8.0.2 — офис` (образ, добавленный на шаге *Подготовка*)
3. Временный пароль локальных пользователей — задать пароль не короче 8 символов, например `Migrate2026!`

Примечание

Этот пароль будет установлен **всем** перенесённым локальным пользователям после миграции. Пользователь должен сменить его при первом входе. Если оставить поле пустым, пароль локальным пользователям задаваться не будет (войти можно будет только через root/sudo)

4. Логин администратора домена — имя доменной учётной записи с правом ввода устройств в домен. Заполняется, если на устройствах есть доменные пользователи. Указывается без префикса домена, например `domain_admin` или `Administrator`
5. Пароль администратора домена — пароль соответствующей доменной учётной записи

Важно

Если на устройстве есть доменные пользователи, а учётные данные администратора домена не заполнены, этап `Восстановление` завершится с ошибкой. После заполнения учётных данных миграцию можно *продолжить* — перезапустится только этап с ошибкой

6. Задачи после миграции — выбрать задачи UEM, которые будут выполнены на устройстве после восстановления. Для офисного сценария можно выбрать заранее подготовленные задачи, например:
    - `Установка LibreOffice` — установка офисного пакета
    - `Базовая настройка GNOME` — преднастройка рабочего стола

Примечание

- Выбираются задачи, не политики
- Порядок выполнения задаётся перетаскиванием
- Расписание выбранных задач игнорируется: они выполняются однократно, сразу после восстановления, только на мигрируемом устройстве
- Задачи из поля Задачи после установки образа OS при миграции **не выполняются**

9.2.3 Вкладка «Пользователи»

Определяет, чьи данные собирать с устройства

1. Перенос всех пользователей — оставить включённым, чтобы перенести всех найденных на устройстве пользователей (локальных и доменных).

В зависимости от значения флага в форме отображается одно из двух полей-списков:

- флаг включён — отображается Исключить пользователей
- флаг снят — отображается Перенести пользователей

2. Перенести пользователей — отображается, если флаг Перенос всех пользователей снят. Переносятся **только** перечисленные пользователи. Например:
   - `ivanov`
   - `corp\petrov`
   - `Сидоров` (имя профильной папки в `C:\Users\`)
3. Исключить пользователей — отображается, если флаг Перенос всех пользователей включён. Список логинов, которые **не** нужно переносить — переносятся все найденные пользователи, кроме указанных. Например, для исключения служебной учётной записи:
   - `svc-backup`

Примечание

В обоих списках имя сопоставляется с любым из вариантов:

- полное имя учётной записи в виде `DOMAIN\username`;
- короткое имя без домена (`username`);
- имя профильной папки в `C:\Users\`.

Сравнение регистронезависимое. Системные учётные записи Windows (`Administrator`, `Guest`, `DefaultAccount`, `WDAGUtilityAccount` и встроенные сервисные SID) исключаются автоматически — добавлять их в Исключить пользователей не требуется

Важно

Для **ALT Linux** и **RED OS** имена локальных пользователей с кириллическими символами автоматически транслитерируются в латиницу (`Иванов` → `ivanov`). Логин в новой ОС будет другим — пользователю нужно входить под транслитерированным именем. Доменные пользователи переносятся без изменения имени

9.2.4 Вкладка «Выбор данных»

Определяет, **какие** данные собирать с **Windows**

1. Перенос стандартных директорий пользователя — оставить включённым: соберутся `Desktop` / `Documents` / `Downloads` / `Pictures` / `Videos` / `Music`

Примечание

На **Linux** эти папки восстанавливаются в домашние каталоги соответствующих пользователей (`/home/<user>/...`) с автоматическим сопоставлением русских и английских имён (`Documents` ↔ `Документы` и т.д.)

2. Перенос данных из не системных разделов — включить, если на устройствах используются `D:\`, `E:\` и т.д.

Примечание

Содержимое несистемных разделов восстанавливается в каталог `/opt/from_migration/` на **Linux**

3. Дополнительные директории/файлы — добавить пути, которые не входят в стандартные. Например для офисного сценария:
    - `C:\Projects` — общие рабочие проекты (абсолютный путь)
    - `AppData\Roaming\Notepad++` — настройки Notepad++ относительно домашней папки пользователя

Примечание

- Абсолютные пути восстанавливаются в `/opt/from_migration/` (к имени каталога добавляется короткий хеш, чтобы одноимённые исходные пути не смешивались)
- Относительные пути восстанавливаются в домашних каталогах пользователей
- Запрещены сегмент `..`, двойной слеш (кроме UNC-префикса), символы перевода строки и нулевой байт

4. Сбор данных браузеров — отметить нужные. Например `Chrome`

Важно

Перед сбором данных выбранные браузеры **принудительно закрываются** на исходном устройстве. Несохранённые вкладки и работа в браузерах будут потеряны — заранее предупредите пользователей

Важно

Собирается только **AppData** выбранных браузеров. Данные копируются как обычные пользовательские файлы и оказываются в каталоге `~/from_migration/` мигрируемого пользователя на **Linux**, **не** подставляются автоматически в профиль установленного на Linux браузера. Полнота переноса «рабочего» профиля не гарантируется

9.2.5 Сохранить сценарий

Нажать Сохранить и продолжить. Сценарий появится в списке на странице Миграции

После сохранения сценарий можно использовать в одной или нескольких *задачах миграции*

9.3 3. Запуск и контроль миграции

Сценарий миграции описывает, **как** переносить. Задача миграции запускает этот сценарий на конкретном наборе устройств и отслеживает их прохождение этапов

9.3.1 Создать задачу миграции

1. Перейти в Установка OS → Задачи миграции
2. Нажать Добавить Задачу миграции

   Заполнить вкладки

Вкладка «Основная информация»

- Название - например, `Миграция офиса - пилот`
- Миграция - выбрать ранее созданный сценарий `Миграция офиса на RedOS 8.0.2`

Вкладка «Устройства и группы»

Для пилотного запуска выберите подготовленные устройства или группы. Поля можно комбинировать:

- Устройства - конкретные хосты по одному

  Подсказка

  Удобно для пилота на 2-3 машинах

- Группы - группы устройств целиком (например, `Офис / Бухгалтерия`)

- Динамические группы - группы по фильтрам инвентаризации (например, «все Windows 10 в офисе»)

  После выбора нажать Загрузить динамические группы, чтобы зафиксировать состав

Чтобы запустить миграцию на всех Windows-устройствах, оставьте три списка пустыми и включите **Запускать на всех устройствах**. Если устройства или группы выбраны вручную, задача использует этот выбор

Важно

Устройство не может одновременно участвовать в двух выполняющихся задачах миграции

Если устройство уже задействовано в другой задаче в статусе Запущена, оно автоматически пропускается и в текущую задачу не включится - без явной ошибки в UI

Дождитесь завершения предыдущей задачи на этом устройстве

Примечание

Несколько задач миграции могут выполняться **параллельно** - ограничение действует только на уровне отдельного устройства

Можно одновременно мигрировать «Бухгалтерию» и «Отдел продаж» в разных задачах

9.3.2 (Опционально) Настроить уведомления

До запуска удобно подключить уведомления, чтобы получать оповещения о ходе миграции, не открывая страницу задачи

1. Перейти на страницу Уведомления
2. Нажать Добавить Уведомление

   Пример настройки для офисного сценария:

   На вкладке Основная информация:

   - Название - Миграция офиса - MAX
   - Пользователи - выбрать ответственного администратора (у которого в профиле заполнен **MAX**)
   - Тип уведомления - MAX
   - Уведомление в общий чат - снять, если уведомления нужны только администратору

   На вкладке Завершение задачи миграции:

   - Задачи миграции - выбрать созданную задачу Миграция офиса - пилот

- Уведомлять о завершении миграции на каждом устройстве - оставить включённым, чтобы видеть прогресс по каждому хосту (по умолчанию включено)
- Уведомлять в конце задачи миграции - включить, чтобы получить итоговое уведомление с прогрессом «X из N» (по умолчанию выключено)

3. Нажать Сохранить

Примечание

Уведомления отправляются только при заполненных контактных данных у выбранного пользователя (Telegram, Email, MAX, телефон) и/или в общем чате из настроек сервера

Подробное описание полей - на странице Уведомления

9.3.3 Запустить миграцию

1. Сохранить задачу - Сохранить и продолжить
2. Нажать Запустить/продолжить миграцию

При старте сервер:

- публикует целевой образ ОС, если он ещё не опубликован, и снимает с публикации остальные образы;
- запоминает, какой образ был фактически опубликован для этой задачи (поле Опубликованный образ);
- формирует состояния миграции для каждого устройства;
- переводит задачу в статус `Запущена` и ставит в очередь этапы миграции на каждом устройстве

Важно

Пока выполняется задача миграции с опубликованным образом, операции **«Опубликовать» / «Снять с публикации»** недоступны для **всех** образов до завершения этой задачи

Не пытайтесь публиковать другой образ во время активной миграции

9.3.4 Контроль выполнения

На странице задачи миграции после запуска становятся активны вкладки Статус, Лог исполнения и Состояния миграции устройств

1. Открыть вкладку Состояния миграции устройств

   Каждая строка - одно устройство со столбцами:

   - `Стадия` - этап, на котором сейчас устройство: `Сбор данных` → `Сброс загрузчика` → `Установка ОС` → `Восстановление` → `Готово`

- `Статус` - статус текущего этапа: `Ожидает` / `Выполняется` / `Успешно` / `Ошибка`
- `Устройство после миграции` - запись устройства, на которой выполняется `Восстановление`

> **Примечание**
>
> В штатном сценарии указывает на ту же запись, что и `Устройство`

- `Ошибка` - текст последней ошибки этапа

> **Примечание**
>
> После миграции запись устройства на странице Устройства не дублируется - сохраняется та же запись, у которой меняется платформа с **Windows** на **Linux**

2. Открыть вкладку Лог исполнения - онлайн-лог задачи

> **Подсказка**
>
> В шапке логов каждого устройства есть ссылка Открыть лог устройства для подробного журнала плейбуков

> **Примечание**
>
> После завершения этапа `Сбор данных` проверяются целостность и размер архивов с пользовательскими данными
>
> При несовпадении этап завершается с ошибкой

> **Важно**
>
> Готовность мигрированного устройства определяется только по статусу `Готово` соответствующего состояния миграции
>
> До этого момента не используйте устройство - на нём ещё могут выполняться этапы восстановления и задачи **UEM** после миграции

9.3.5 Если на устройстве возникла ошибка

Задачу пересоздавать не нужно - миграцию можно продолжить с того этапа, на котором она прервалась

1. Найти устройство в статусе `Ошибка` на вкладке Состояния миграции устройств

2. Открыть детальный журнал по ссылке Открыть лог устройства и найти причину
3. Устранить причину

   Типовые случаи:

   - **Не заполнены учётные данные администратора домена**, а на устройстве есть доменные пользователи. → Открыть *сценарий миграции* и заполнить Логин администратора домена и Пароль администратора домена
   - **Устройство офлайн в момент сбора данных** - сервер повторяет запуск **10 раз** с интервалом **30 секунд**

     Проверить сеть и доступность хоста в веб-интерфейсе
   - **Не настроен PXE/DHCP** - устройство не получило загрузочный образ

     Проверить настройки PXE-сервера и BIOS устройства
4. Вернуться в задачу миграции и нажать Запустить/продолжить миграцию

> **Примечание**
>
> Сервер заново выполнит **только** этап с ошибкой на затронутых устройствах
>
> Этапы, успешно завершённые ранее (`Успешно`), повторно не запускаются
>
> Устройства в статусе `Готово` пропускаются

9.3.6 Когда нужен «сброс»

Сбросить миграцию - отдельное действие, **не** для штатного восстановления после ошибки

Оно удаляет состояния всех устройств в статусах `Ошибка` и `Выполняется` и переводит задачу в статус `Ошибка`. После сброса последующий Запустить/продолжить миграцию начнёт миграцию для этих устройств **заново с этапа ``Сбор данных``**

> **Важно**
>
> После сброса задачи и последующего запуска повторный сбор данных удаляет ранее собранную резервную копию данных устройства
>
> Если эти данные нужны вне задачи миграции, сохраните их отдельно **до** выполнения сброса

Подсказка

Сброс полезен, например, если изменилась структура данных на исходном устройстве после неудачного сбора и нужно собрать заново. В большинстве случаев достаточно Запустить/продолжить миграцию - сценарий продолжится с места ошибки

9.3.7 Завершение задачи

Когда **все** устройства завершают миграцию, задача переходит в статус:

- `Выполнено` - все устройства успешно достигли этапа `Готово`
- `Ошибка` - хотя бы одно устройство завершилось с ошибкой

Если в задаче подключены уведомления, сервер отправит:

- уведомление о завершении задачи миграции с итоговым статусом и прогрессом (количество успешно мигрированных устройств от общего числа);
- уведомление о завершении миграции на каждом устройстве с указанием стадии и статуса (включается отдельным флагом)

После статуса `Готово` у устройств можно перейти к шагу *После миграции*

9.3.8 Если установка долго не переходит к следующему этапу

1. Проверить, что нужный образ опубликован и его тип соответствует установщику внутри ISO
2. Посмотреть экран устройства: идёт ли загрузка файлов, работает ли установщик или уже загружена новая ОС
3. При сообщениях о повторной загрузке проверить доступность узла публикации и DHCP
4. Если ОС уже установлена, проверить её сеть и подключение клиента RuDesktop к серверу
5. Затем проверить состояние задачи миграции и заданий после установки

Повторные попытки загрузки при медленной сети описаны на странице Образы OS. Не начинать новую установку для устранения сетевой задержки: установка снова может удалить данные на диске. Прежде чем повторять миграцию, определить этап сбоя и проверить сохранность резервной копии пользовательских данных

9.4 4. После миграции

Когда устройство переходит в статус `Готово`, миграция считается выполненной — пользователи могут начинать работу. Этот шаг описывает, как проверить результат и установить оставшийся софт на **Linux**

9.4.1 Проверить пользователей

1. На странице Устройства открыть карточку мигрированного устройства. Платформа должна стать **Linux**, поле инвентаризации обновится автоматически после первого сбора фактов
2. Под доменной учётной записью пользователь входит со своим **доменным паролем** — без изменений
3. Под локальной учётной записью пользователь входит:
   - с **временным паролем**, заданным в *сценарии миграции* на вкладке Основная информация;
   - на **ALT Linux** и **RED OS** — под транслитерированным именем (например, `Иванов` → `ivanov`);
   - при первом входе **обязан** сменить временный пароль на постоянный

Примечание

Для отдельных дистрибутивов **Linux** возможны особенности дисплейного менеджера при первом входе доменного пользователя — например, имя пользователя может потребоваться ввести вручную. Это не зависит от **RuDesktop** и определяется поведением выбранного дистрибутива

9.4.2 Проверить перенесённые данные

1. **Стандартные пользовательские папки** (`Documents` / `Desktop` / `Downloads` / `Pictures` / `Videos` / `Music`) — должны быть в домашнем каталоге пользователя `/home/<user>/...`. Имена сопоставляются автоматически между русскими и английскими (`Documents` ↔ `Документы` и т.д.)
2. **Содержимое несистемных дисков** Windows и **абсолютные пути** из Дополнительные директории/файлы — в каталоге `/opt/from_migration/` (общий для устройства, не привязан к пользователю)
3. **Относительные пути** из Дополнительные директории/файлы — в домашних каталогах пользователей
4. **AppData браузеров** — в каталоге `~/from_migration/` мигрируемого пользователя как обычные файлы

Важно

Перенос «рабочего» профиля браузера на **Linux** не гарантируется и зависит от версии браузера и совместимости форматов. Если профиль не подхватился автоматически, выполните импорт вручную средствами самого браузера, используя данные из `~/from_migration/`

9.4.3 Установить ПО на Linux

Программы Windows и реестр Windows при миграции **не переносятся** — необходимый софт ставится на **Linux** через задачи UEM

Если задачи установки ПО уже были выбраны в *сценарии миграции* в поле Задачи после миграции (например, `Установка LibreOffice`), они выполнились автоматически сразу после восстановления — отдельных действий не требуется. Проверить результат можно в статистике выполнения или в логах задач

Если ПО нужно доустановить **после** миграции, например по итогам обратной связи от пользователей:

1. Перейти в Политики, добавить политику установки нужного пакета (см. шаблоны политик Установка пакета, Установка пакета из архива и т.д.)
2. Создать задачу, добавив политику и выбрав мигрированные устройства/-группы
3. Запустить задачу

Готовые примеры установки конкретных пакетов — в *Кейсе «Установка ПО»*

9.4.4 Чек-лист после миграции

- Платформа устройства переключилась на **Linux** в Устройствах
- Доменные пользователи входят со своим доменным паролем
- Локальные пользователи входят с временным паролем (с учётом транслитерации на ALT/RED) и сменили его при первом входе
- Стандартные пользовательские папки восстановлены в `/home/<user>/`
- Несистемные разделы и абсолютные пути из миграции восстановлены в `/opt/from_migration/`
- Задачи **UEM** из поля Задачи после миграции выполнены успешно (см. Статистику выполнения)
- Установлено всё необходимое для пользователя ПО

После прохождения чек-листа устройство считается готовым к продуктивной работе на **Linux**

Кейс описывает полный путь администратора при переводе парка устройств с **Windows** на **Linux** с помощью раздела Установка ОС сервера **RuDesktop**: подготовка образа и устройств, создание сценария миграции, запуск, контроль выполнения и финальная настройка после переустановки

В качестве примера используется офисный сценарий: миграция группы рабочих станций с **Windows 10** на **RedOS 8.0.2** с переносом локальных и доменных пользователей, документов из стандартных папок, дополнительной директории `C:\Projects` и пользовательских настроек **Chrome**. После миграции на устройства устанавливается **LibreOffice** через задачу **UEM**

Подсказка

Раздел **«Установка OS»** и миграция доступны только при использовании локального сервера **Управление конфигурациями (UEM)**

Важно

Миграция поддерживается **только в направлении Windows → Linux**. Обратный сценарий и миграция между разными версиями одной и той же ОС не поддерживаются

9.5 Шаги

1. Подготовка

Образ ОС, BIOS/PXE на устройстве, проверка сети и того, что нужно перенести

2. Создание миграции

Запись миграции: целевой образ, пользователи, данные и задачи после миграции

3. Запуск и контроль

Создание задачи миграции, запуск, мониторинг этапов, восстановление после ошибок

4. После миграции

Проверка пользователей, установка ПО на **Linux** через задачи **UEM**

9.6 Кратко: что делает миграция

- собирает с **Windows** пользовательские данные (стандартные папки, выбранные дополнительные пути, **AppData** браузеров) и упаковывает их в **TAR**-архивы на сервере;
- через **PXE** устанавливает выбранный образ **Linux** поверх Windows;
- восстанавливает локальных и доменных пользователей и собранные данные на **Linux**;
- запускает выбранные администратором задачи **UEM** (например, установку ПО) после восстановления.

Важно

Миграция переносит **только пользовательские данные/файлы**. Установленные программы Windows, реестр Windows, системные настройки и драйверы не переносятся. Необходимое программное обеспечение для **Linux** ставится отдельно — через задачи UEM, выбранные в поле Задачи после миграции (см. шаг *После миграции*)

9.7 См. также

- Установка OS — справочник раздела
- Образы OS — справочник образов
- Миграции — справочник сценариев миграции
- Задачи миграции — справочник задач миграции
- Настройка PXE-сервера
- *Установка ПО* — кейсы установки ПО через политики

ГЛАВА 10

Печать документа с удалённого устройства на своём принтере

Кейс — настройка удалённой печати: оператор подключается к удалённому устройству, открывает там документ и печатает его на своём локальном принтере

Подсказка

Удалённая печать поддерживается только на **Windows**. На **Linux** и **macOS** категория Принтер в настройках клиента не отображается

10.1 Что вы получите

- На удалённом устройстве в диалоге печати любого приложения появится виртуальный принтер **RuDesktop Printer**
- Задания, отправленные на этот принтер, будут передаваться на устройство оператора и печататься на его физическом принтере
- Печать будет выполняться либо автоматически на заранее выбранном принтере, либо с подтверждением и выбором принтера в каждом задании

Важно

В одном сеансе печать работает в одну сторону: задания уходят с устройства, к которому подключились, на принтер оператора. Обратное направление — печать документа со своего устройства на принтере удалённого — не поддерживается

10.2 Подготовка

- На обоих устройствах — **Windows 7 SP1 / Windows Server 2008 R2 SP1** или новее
- На обоих устройствах при установке клиента **RuDesktop** не был исключён компонент Удаленная печать — см. Установка на Windows
- На устройстве оператора доступна библиотека XPS-печати `XpsPrint.dll` — поставляется вместе с **Windows**
- У оператора есть право Может настраивать доступ к удаленной печати — без него настройки удалённой печати доступны только для просмотра
- У оператора есть доступ к удалённому устройству в режиме управления рабочим столом

10.3 Шаг 1. Проверить виртуальный принтер на удалённом устройстве

Виртуальный принтер **RuDesktop Printer** должен быть установлен на том устройстве, **с которого** будут отправляться документы — то есть на удалённом

1. В клиенте на удалённом устройстве нажмите и перейдите в категорию Принтер
2. В блоке Исходящие задания печати проверьте статус:
   - `RuDesktop виртуальный принтер установлен и готов к работе` — всё готово, переходите к следующему шагу
   - `RuDesktop виртуальный принтер не установлен` — нажмите кнопку Установить RuDesktop виртуальный принтер

Важно

- Для установки виртуального принтера потребуется подтверждение прав администратора системы
- На время установки на кнопке отображается индикатор ожидания
- Если установка не удалась, под кнопкой отобразится сообщение `Ошибка установки` с описанием причины

Подсказка

В обычном случае виртуальный принтер добавляется в систему самим установщиком клиента вместе с компонентом Удаленная печать. Кнопка нужна, если автоматическая установка не прошла — например, в системе были отключены компоненты XPS-печати

10.4 Шаг 2. Включить приём заданий печати у оператора

Настройки выполняются на устройстве оператора — том, **на принтере которого** будут печататься документы

1. В клиенте нажмите и перейдите в категорию Принтер
2. В блоке Входящие задания печати включите опцию **Разрешить удаленную печать**
3. В поле Принтер выберите принтер, на который будут отправляться входящие задания

Подсказка

Первым в списке идёт системный принтер в формате `(По умолчанию) <название принтера>`. При его выборе задания печатаются на принтере, назначенном основным в операционной системе

4. При необходимости включите опцию **Автоматически выполнять входящие задания печати** — задания будут сразу уходить на выбранный принтер без подтверждения

Важно

- Поле Принтер и опция **Автоматически выполнять входящие задания печати** становятся доступны только после включения опции **Разрешить удаленную печать**
- Пока опция **Разрешить удаленную печать** выключена, виртуальный принтер на удалённом устройстве заданий не передаёт
- Если блок Входящие задания печати не отображается — устройство не соответствует требованиям из раздела **Подготовка**

10.5 Шаг 3. Отправить документ на печать

1. Подключитесь к удалённому устройству в режиме управления рабочим столом
2. На удалённом устройстве откройте нужный документ

3. Отправьте его на печать и в диалоге печати приложения выберите принтер **RuDesktop Printer**
4. Подтвердите печать — задание будет передано на устройство оператора

Важно

Удалённая печать работает только при подключении в режиме управления рабочим столом. При других типах подключений — передаче файлов, TCP-туннелировании, подключении к терминалу и прочих — она недоступна

10.6 Шаг 4. Подтвердить печать на своём устройстве

Дальнейшее поведение зависит от опции **Автоматически выполнять входящие задания печати**:

- **Опция включена** — документ сразу печатается на выбранном принтере, никаких действий не требуется
- **Опция выключена** — откроется окно Выбрать принтер:
  1. В поле Принтер выберите принтер для этого задания
  2. При необходимости отметьте флажки:
     - **Сохранить** — выбранный принтер запомнится в настройках и будет использоваться по умолчанию
     - **Не показывать снова** — включит опцию **Автоматически выполнять входящие задания печати**, следующие задания будут печататься без подтверждения
  3. Нажмите OK — начнётся печать. Кнопка Отменить отклонит задание

Подсказка

Флажки **Сохранить** и **Не показывать снова** отображаются только при наличии права Может настраивать доступ к удаленной печати. Без него в окне доступен только выбор принтера — и тот заблокирован, задание печатается на принтере из настроек

10.7 Если печать не работает

Признак	Что проверить
Категории Принтер нет в настройках клиента	Устройство работает не под **Windows**, либо виртуальный принтер не установлен **и** при установке клиента был исключён компонент Удаленная печать — в этом случае переустановите клиент с этим компонентом
Принтера **RuDesktop Printer** нет в диалоге печати на удалённом устройстве	На удалённом устройстве в блоке Исходящие задания печати установите виртуальный принтер кнопкой Установить RuDesktop виртуальный принтер
Блока Входящие задания печати нет у оператора	Проверьте, что установлена **Windows 7 SP1 / Windows Server 2008 R2 SP1** или новее, доступен компонент Удаленная печать и библиотека `XpsPrint.dll`. Для **Windows 7** и **Windows Server 2008 R2** пакет обновления **SP1** обязателен
Настройки печати отображаются, но недоступны для изменения	Пользователю не выдано право Может настраивать доступ к удаленной печати
Задание отправлено, но ничего не печатается	У оператора выключена опция **Разрешить удаленную печать**, либо подключение выполнено не в режиме управления рабочим столом
Выбранный принтер не найден при автоматической печати	Принтер удалён или недоступен в системе — откроется окно Выбрать принтер для выбора другого

10.8 Что дальше

- Выдайте право Может настраивать доступ к удаленной печати сразу группе пользователей, чтобы не настраивать каждого отдельно
- При массовой установке клиентов включайте компонент печати флагом `ADDLOCAL=FeatureCore,FeatureRemotePrint` — см. Установка в тихом режиме
- Полное описание настроек: Принтер

ГЛАВА 11

Обновление ОС

Практические сценарии поиска и установки обновлений на управляемых устройствах

11.1 Обновление Windows в закрытой сети

Доступно только в UEM версии

Сценарий: определить необходимые обновления Windows, перенести их пакеты в закрытую сеть и установить выбранные обновления на управляемые устройства. Сначала проверяется одно тестовое устройство, затем остальные

11.1.1 Что подготовить

- Лицензию UEM и права на каталог, задачи сканирования, пакеты и обновления устройств, включая создание задач установки
- Windows-устройства с работающим клиентом RuDesktop и доступом к файлам в инфраструктуре сервера
- Актуальный файл каталога `Wsusscn2.cab`, предварительно полученный и перенесённый в закрытую сеть
- Возможность получить файлы нужных обновлений вне закрытой сети и перенести их в хранилище RuDesktop

  Список нужных пакетов станет известен после сканирования

Примечание

Каталог используется для проверки применимости обновлений. Он не содержит вместо них готовый комплект установочных пакетов. Поэтому поиск и подготовка файлов - два отдельных шага

11.1.2 Шаг 1. Добавить каталог

1. Открыть **«Обновления ОС → Каталоги обновлений Windows»**
2. Добавить запись с понятным названием, например `Каталог для проверки октября`
3. В поле **«Wsusscn2.cab»** загрузить подготовленный файл или выбрать ранее загруженный файл из хранилища
4. Сохранить запись

11.1.3 Шаг 2. Проверить тестовое устройство

1. Открыть **«Задачи сканирования обновлений»** и добавить задачу
2. Указать название, выбрать созданный каталог и узел выполнения в поле **«Точка распространения»**

   Для этого примера выбрать **«Основной сервер»**
3. На вкладке **«Устройства»** выбрать только тестовый компьютер Windows

   Оставить **«Запускать по расписанию»** выключенным для первого ручного запуска
4. Сохранить задачу и выполнить **«Запустить задачу»**
5. Дождаться результата **«Успешно»** у устройства

   Посмотреть число найденных обновлений и **«Лог исполнения»**

При нулевом результате проверить каталог и журнал. При ошибке или недоступности сначала устранить причину: отсутствие результатов после неудачного запуска не означает, что устройство обновлено

11.1.4 Шаг 3. Подготовить файлы обновлений

1. Открыть **«Обновления устройств»**, выбрать каталог в фильтре и **«Требуется установка»**

   Найти тестовый компьютер по имени или ID
2. Перейти к нужным записям в **«Пакетах обновлений»**

   Сверить название, статьи KB, Update ID и ревизию, посмотреть **«Ссылки загрузки»**
3. Получить соответствующие файлы во внешней сети и перенести их в закрытую

Для обновления из нескольких файлов подготовить ZIP со всеми нужными файлами в корне архива, сохранив исходные имена

4. В карточке каждого обновления открыть **«Пакет»**, выбрать файл в поле **«Пакет обновления»** и сохранить
5. Проверить статус **«Готов»** у всех пакетов, которые будут выбраны для установки

Если узел, выполняющий скачивание, имеет доступ к внешним источникам, вместо ручного переноса можно использовать **«Скачать пакет»**. При отсутствии ссылок загрузки или ошибке автоматического скачивания файл требуется подготовить вручную

Примечание

Статус **«Готов»** означает, что к обновлению привязан файл

Совместимость и полнота содержимого проверяются при установке

Один файл с похожим номером KB не заменяет проверку соответствия выбранному обновлению

11.1.5 Шаг 4. Установить выбранные обновления

1. Вернуться в **«Обновления устройств»**, найти тестовый компьютер через поиск и проверить фильтры каталога и **«Требуется установка»**
2. Отметить только записи с подготовленными пакетами и выполнить **«Установить»**
3. Открыть созданную задачу в **«Задачах установки обновлений»**

   Действие сразу ставит её в очередь; отдельное подтверждение запуска не требуется
4. Проверить результат устройства, количество установленных обновлений, ошибки и **«Лог исполнения»**
5. Если отмечено **«Требуется перезагрузка»**, выполнить перезагрузку отдельно в подходящее время
6. Повторить задачу сканирования с тем же каталогом и проверить оставшиеся требуемые обновления

Важно

Выборочная установка создаёт задачу с автоматическим выбором узла. Выбор **«Основной сервер»** у задачи сканирования на неё не переносится. Если установка должна выполняться на конкретном узле, создать отдельную задачу установки и выбрать узел в ней. Такая задача установит все сохранённые требуемые обновления выбранных устройств, включая записи других каталогов

11.1.6 Шаг 5. Повторить для остальных устройств

1. Добавить подготовленные устройства или группы в задачу сканирования
2. Выполнить поиск по выбранному каталогу и подготовить дополнительные пакеты, если они обнаружены
3. Отфильтровать **«Обновления устройств»** по каталогу и выбрать нужные записи
4. Выполнить установку, проверить результаты и организовать необходимые перезагрузки

Для повторяющейся работы можно настроить расписания сканирования и установки. Установка использует уже сохранённые результаты поиска: убедиться, что сканирование завершилось и все нужные пакеты подготовлены до её запуска. В полностью закрытой сети новые файлы каталога и пакетов потребуется переносить отдельно

11.1.7 Если возникла ошибка

- **Не удалось подготовить пакеты** - проверить, всем ли выбранным обновлениям назначены файлы

  При автоматическом скачивании откройте карточку пакета и прочитайте поле **Ошибка скачивания**. Если превышен максимальный размер пакета, проверьте ограничение в настройках **Обновления ОС**. Если не хватает места, сравните требуемый и доступный объём в сообщении и освободите недостающее место в репозитории. При ошибке соединения проверьте доступ к источнику

- **В пакете отсутствует файл** - сверить имена и состав файлов, для ZIP проверить отсутствие лишней внешней папки в архиве
- **Недоступно** - проверить клиент RuDesktop, узел выполнения и доступ устройства к инфраструктуре сервера
- **0x80240016** - дождаться окончания другой установки или выполнить необходимую перезагрузку, после чего повторить попытку

Справочник полей и состояний: Обновления ОС

Обновление Windows в закрытой сети

Подготовка каталога и пакетов, проверка одного устройства и выборочная установка обновлений без доступа клиентских устройств к внешним источникам

ГЛАВА 12

Поиск установленного ПО по категориям

Администратору нужно понять, какие программы выбранного назначения установлены на устройствах, и проверить программы без классификации. Для этого использовать данные инвентаризации и **«Классификатор ПО»**. Например, можно выбрать категорию нужного офисного ПО и посмотреть, на каких устройствах обнаружены относящиеся к ней программы. Названия категорий выбирать из справочника своего сервера

12.1 Что подготовить

- Управляемые устройства с возможностью выполнения инвентаризации
- Права на просмотр наличия ресурсов и классификатора
- Для ручного исправления связи - право изменения наличия ресурсов
- Для добавления недостающих пакетов и продуктов - права на их добавление

Примечание

Результат показывает сведения, полученные при инвентаризации. Если пользователь только что установил или удалил программу, старые данные могут ещё не отражать изменение

12.2 Собрать сведения об установленном ПО

1. Создать или открыть политику Инвентаризация
2. В поле **«Выберите типы данных для сбора»** включить **«Установленные приложения»** для устройств, поддерживающих этот сбор
3. Сохранить политику и выполнить её на нужных устройствах
4. Проверить завершение выполнения и ошибки по устройствам

   Неудачный запуск не подтверждает отсутствие приложений
5. Открыть **«Инвентаризация → Наличие ресурсов»**
6. Выбрать нужное устройство или группу и присутствующие ресурсы в фильтре **«Наличие»**
7. Найти известную установленную программу по имени и проверить её версию

После обработки данных сервер автоматически пытается классифицировать присутствующее ПО, у которого ещё нет связи со справочником. Отдельно запускать политику классификации не требуется

12.3 Найти программы нужной категории

1. Оставить фильтр присутствующих ресурсов
2. Выбрать **«Категория ПО»**, при необходимости добавить **«Тип ПО»**, **«Значимость для безопасности»** или правообладателя
3. Применить фильтры и посмотреть строки результата
4. Для каждой нужной строки проверить ресурс, устройство и версию

Примечание

Одна программа может встречаться в нескольких строках на разных устройствах. Число строк не следует автоматически считать числом уникальных программ или устройств. Пустой результат означает, что нет строк, подходящих под все выбранные условия. Он не доказывает, что ни на одном устройстве нет программ такого назначения. Часть программ могла не пройти инвентаризацию или остаться без классификации

12.4 Проверить программы без категории

1. Снять фильтры категории, типа ПО, значимости и правообладателя

   Иначе они могут исключить неклассифицированные записи из результата

2. Оставить нужную группу или устройство и присутствующие ресурсы
3. В фильтре **«Классифицирован»** выбрать **«Нет»**
4. Отобрать программные ресурсы для проверки

   В общей таблице есть также оборудование и другие ресурсы, а службы автоматически не классифицируются

5. Для нужной программы запомнить имя, ОС устройства и идентификатор ресурса
6. Открыть **«Классификатор ПО»** и найти подходящий пакет

   Сверить семейство ОС, пакет и ProductCode, если он используется

Прочерк в категории означает отсутствие назначенной классификации. Он не является оценкой безопасности программы

12.5 Назначить подходящую запись вручную

1. Вернуться в **«Наличие ресурсов»** и найти строку нужной программы именно на нужном устройстве
2. В меню строки выбрать **«Редактировать»**

   Не переходить по названию ресурса - оно ведёт в каталог ресурсов

3. В поле **«Классификатор ПО»** найти пакет по имени, ProductCode, продукту или категории ПО

   Подсказка

   Запись в списке содержит категорию, имя пакета и семейство ОС. Например:

   ```
   Браузеры: firefox-esr (debian)
   ```

   Перед выбором сверить пакет и ОС с данными устройства

4. Выбрать проверенную запись и сохранить
5. Вернуться к списку и проверить категорию и значимость для безопасности
6. Повторно применить фильтр категории - исправленная строка должна попадать в результат при соответствии остальным условиям

Важно

Так изменяется только выбранная запись наличия ресурса. Это не команда изменить все устройства с такой программой. Последующая автоматическая классификация уже заполненную связь не заменяет. Если выбрана неправильная запись, исправить её вручную

12.6 Если подходящего пакета нет

Администратор с необходимыми правами может добавить пакет в классификатор и связать его с продуктом. Категория, тип ПО и значимость относятся к продукту и общие для связанных с ним пакетов - перед изменением продукта проверить, какие записи его используют. Категории, типы и значимости для безопасности выбираются из готовых справочников. Их создание и редактирование в интерфейсе недоступны

Не назначать похожую программу только ради заполнения пустой категории. После добавления подходящего пакета повторить инвентаризацию устройств и проверить результат либо назначить связь вручную нужной строке. Если автоматического совпадения нет, сверить поля по правилам Классификатора ПО

12.7 Как понимать итог

Полученный список помогает найти ПО по назначению и устройствам. Он не устанавливает и не удаляет программы. Значимость для безопасности описывает продукт в справочнике, а не результат сканирования устройства на уязвимости. Категории магазина приложений настраиваются отдельно и не меняют классификацию уже установленного ПО

ГЛАВА 13

На каких устройствах включено расширение браузера

Чтобы найти компьютеры с определённым расширением, соберите сведения о плагинах и отберите нужное расширение в списке ресурсов

1. Откройте политику Инвентаризация. В поле **Выберите типы данных для сбора** укажите **Пакет → Плагин браузера**
2. Выполните политику на нужных компьютерах с Windows, Linux или macOS. Убедитесь, что сбор завершился успешно на тех устройствах, которые хотите проверить
3. Откройте Инвентаризация → Наличие ресурсов. В фильтре **Класс ресурса** выберите **Плагин браузера**, а в фильтре **Наличие** выберите **В наличии**. Введите название расширения в поле **Быстрый поиск** и нажмите **Применить**
4. Для найденного компьютера откройте свойства устройства и перейдите в **Дополнительная информация → Плагины браузера**. В строке расширения указан браузер, в котором оно обнаружено

Примечание

В списке видны только включённые расширения по данным последней инвентаризации. Поиск охватывает все профили браузера. Если нужного устройства нет в результатах, проверьте дату и результат последнего сбора

ГЛАВА 14

Контроль количества лицензий на ПО

У организации есть лицензия на программу для **10 устройств**. Администратору нужно проверить количество установок, найти лишние и настроить уведомления о новых расхождениях

В примере используется одна запись ПО и одна лицензия. Если лицензий несколько, правила объединения мест описаны в разделе Лицензии ПО

14.1 Что подготовить

- Сведения о приобретённой лицензии: название, ключ и количество мест
- Права на создание и изменение лицензий ПО, просмотр аудита ПО и устройств
- Возможность выполнить инвентаризацию на проверяемых устройствах
- Для уведомлений — UEM и настроенный канал доставки

Важно

Для проверки всего парка использовать учётную запись с доступом ко всем устройствам. Превышение проверяется по всему серверу, а список установок и счётчики показывают только доступные пользователю устройства

14.2 Собрать данные и добавить лицензию

1. Выполнить политику Инвентаризация со сбором **Установленных приложений** на проверяемых устройствах
2. Проверить завершение задания и ошибки по устройствам
3. Открыть **Инвентаризация → Аудит ПО**, найти программу и сверить её ОС и дистрибутив
4. Проверить, нет ли уже лицензий, связанных с этим ПО, чтобы не учесть одни и те же приобретённые места повторно
5. В разделе **Инвентаризация → Лицензии ПО** добавить запись, выбрать найденное **ПО**, заполнить название и ключ, указать **Количество мест: 10**
6. Сохранить лицензию и посмотреть столбец **Установлено**

Подсказка

Без связи с **ПО** лицензия не участвует в проверке установок. При ошибке инвентаризации старые данные устройства могут не отражать фактический состав программ

14.3 Разобрать превышение

Предположим, программа обнаружена на **12 устройствах**. При лимите 10 значение **Установлено** выделяется красным

1. Нажать на счётчик **Установлено**, чтобы открыть список устройств
2. Определить, на каких компьютерах программа действительно нужна
3. Удалить ненужные установки либо внести сведения о дополнительно приобретённых местах: обновить существующую лицензию или добавить новую, связанную с тем же ПО
4. После удаления программы повторно выполнить инвентаризацию на изменённых устройствах
5. Вернуться к списку лицензий и проверить результат

Если две установки удалены и инвентаризация подтвердила удаление, счётчик **Установлено** станет равен 10, а красное выделение исчезнет

Примечание

Изменение количества мест или назначений в RuDesktop само по себе не удаляет, не устанавливает и не активирует программу на компьютерах

14.4 Проверить назначения устройств

Этот шаг нужен, если организация закрепляет лицензии за конкретными компьютерами

1. Открыть лицензию и заполнить **Назначенные устройства**
2. При необходимости воспользоваться кнопкой **Добавить устройства с выбранным ПО**, затем оставить только нужные компьютеры. Для лицензии на 10 мест назначить больше 10 устройств нельзя
3. Сохранить запись и проверить **Установлено без назначения**
4. Если значение больше нуля, открыть список по счётчику и проверить назначения

Например, программа установлена на 10 компьютерах, а назначены только 9 из них. Превышения количества мест нет, но **Установлено без назначения** покажет 1. Если оставшийся компьютер должен использовать эту лицензию, добавить его в назначения

Подсказка

Если назначения вообще не используются, столбец **Установлено без назначения** показывает прочерк. Контроль общего количества мест при этом продолжает работать

Назначения ведутся отдельно от сведений об установках. После удаления программы проверить, нужно ли также убрать устройство из **Назначенных устройств**

14.5 Настроить уведомления и проверить результат

1. В UEM открыть **Организация → Уведомления** и создать уведомление
2. Выбрать получателей и канал доставки: Email, телефон, Telegram или MAX
3. На вкладке **Инвентаризация** включить **Уведомлять о превышении количества лицензий на ПО**
4. Сохранить правило, выполнить инвентаризацию и дождаться обработки результатов. Для дальнейшего контроля настроить её запуск по расписанию

Уведомление сообщает о впервые обнаруженном превышении и об увеличении числа установок по сравнению с последним отправленным оповещением.

Если используются назначения, оно также сообщает о новых установках на устройствах, которым не назначена соответствующая лицензия

Подсказка

Сообщения формируются после фоновой обработки результатов инвентаризации, а не сразу при сохранении правила. Уже известные установки без назначения проверить по счётчику: включение уведомления не вызывает их повторную рассылку. Обновление версии уже установленной программы не считается новой установкой

Примечание

Отсутствие нового сообщения не означает, что расхождение устранено: неизменившееся превышение не рассылается после каждой инвентаризации. Результат исправления проверять по актуальным счётчикам и спискам устройств

На странице **Кейсы** вы найдете разнообразные практические сценарии и пошаговые инструкции, которые помогут вам эффективно использовать продукт **RuDesktop**. Каждый кейс разработан, чтобы упростить выполнение определенных действий и достижение нужных результатов. **Наши кейсы** - это ваши помощники в повседневной работе и инструменты для решения специфических задач

Двухфакторная авторизация

Включение второго фактора при входе на сервер: SMS, Email, Telegram, MAX, TOTP, FIDO2, ЭЦП Рутокен

MDM

Регистрация и управление Android-устройствами в режиме Device Owner: настройка через QR-код или `adb`, киоск, сброс, геолокация, блокировка камеры

Настройка прав и доступов

Типовые роли через группы, подключение без подтверждения, мастер-пароль, доступы через динамические группы

Установка ПО

Установка стороннего ПО через политики UEM: Kaspersky Endpoint Security, Yandex Telemost, eXpress, PIX Task, 1С, публикация в магазине приложений

Запись видеосессий и логи передачи файлов

Включение автоматической видеозаписи удалённых сессий и подробных логов передачи файлов для группы пользователей

Развёртывание клиентов

Поиск устройств и установка клиента по сети, клонирование из общего образа и настройка hostname в качестве ID

Мобильный клиент

Типовые сценарии работы с Android-клиентом: подключение, передача файлов, раздача экрана, запись сессий, голосовой вызов, прокси

Пригласительные ссылки

Создание одноразовых URL для подключения к устройству без ID и пароля - в веб-интерфейсе, десктопном и мобильном клиенте

Миграция Windows → Linux

Полный путь миграции парка устройств с Windows на Linux через PXE: подготовка, создание сценария, запуск, настройка после переустановки

Удалённая печать

Печать документа с удалённого устройства на локальном принтере оператора: виртуальный принтер **RuDesktop**, права и параметры приёма заданий

Обновление ОС

Поиск и выборочная установка обновлений Windows в закрытой сети, подготовка пакетов и проверка результата

Поиск установленного ПО по категориям

Сбор инвентаризации, поиск программ на устройствах и разбор записей без классификации

Подключение сетевой папки с установщиками

Подключение общей папки, проверка файлов и выбор новой версии установщика в политике

На каких устройствах включено расширение браузера

Поиск компьютеров по названию расширения и проверка браузера на

устройстве

Контроль количества лицензий на ПО

Поиск превышения числа установок, проверка назначений устройств и настройка уведомлений