



УТВЕРЖДЕН

RU.33654484.0004-04 90 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ
ПОСТАВЩИКОВ ИТ-УСЛУГ»

РУКОВОДСТВО ПО УСТАНОВКЕ

RU.33654484.0004-04 90 01

Листов 66

Име. №подл.	Подпись и дата	Взам. инв №	Инв. № дубл.	Подпись и дата

АННОТАЦИЯ

В данном документе приведено руководство пользователя программного комплекса «Система контроля действий поставщиков ИТ-услуг» далее по тексту – ПК СКДПУ, СКДПУ, Система, Изделие). В документе описываются действия пользователя по осуществлению настройки СКДПУ, подключению к целевым устройствам через СКДПУ, а также аудита действий, ранее выполненных пользователем, а также представлены описания:

- режимов работы СКДПУ;
- принципов безопасной работы СКДПУ;
- функций и интерфейсов функций СКДПУ, доступных каждой роли пользователей;
- параметров (настроек) безопасности СКДПУ, доступных роли пользователя, и их безопасных значений;
- типов событий безопасности, связанных с доступными пользователю функциями СКДПУ;
- действий после сбоев и ошибок эксплуатации СКДПУ.

СОДЕРЖАНИЕ

1. Общие сведения	5
1.1. Назначение и область применения	5
1.2. Требования к уровню подготовки пользователя СКДПУ	6
1.3. Рекомендуемые характеристики АРМ пользователя	6
1.4. Обеспечение безопасности	8
1.4.1. Режимы работы средства (СКДПУ).....	8
1.4.2. Принципы безопасной работы средства (СКДПУ)	8
1.4.3. Функций и интерфейсы функций СКДПУ, доступные каждой роли пользователей	8
1.4.4. Параметры (настроек) безопасности средства (СКДПУ), доступные роли пользователя, и их безопасных значений	8
1.4.5. Типы событий безопасности, связанных с доступными пользователю функциями средства	9
1.4.6. Действия после сбоев и ошибок эксплуатации средства.....	9
1.5. Общие сведения	9
2. Доступ к веб-интерфейсу СКДПУ	11
3. Веб-интерфейс пользователя	13
3.1. Раздел меню Мои настройки	13
3.2. Раздел меню Мои авторизации	16
3.3. Доступ к целевым устройствам.....	27
3.3.1. Доступ к целевым устройствам из веб-интерфейса пользователя.....	27
3.3.2. Авторизация пользователя на СКДПУ через клиент удаленного доступа PuTTY	33
3.4. Доступ к целевым устройствам через клиент удаленного доступа PuTTY	35
4. Действия в нестандартных ситуациях	38
4.1. Проблемы, связанные с входом в систему	38
4.2. Возможные проблемы при автоматизированном сеансе SSH.....	38
Приложение 1 Примеры генерации и использования SSH-ключей.....	40

Приложение 2 Вход в систему и способы переноса файловой информации между АРМ пользователя и целевыми устройствами	46
Перечень терминов	57
Перечень сокращений.....	60
Перечень рисунков.....	62
Перечень таблиц.....	64
Лист регистрации изменений.....	66

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и область применения

СКДПУ является программным средством для мониторинга, аудита и оперативного контроля действий зарегистрированных внешних пользователей (поставщиков ИТ-услуг) на администрируемых устройствах домена, контролируемых АС, использующим методы распознавания и анализа информации сессий авторизации.

СКДПУ анализирует команды, вводимые в ходе сеансов протокола SSH, в режиме реального времени, а в случае обнаружения запрещенных наборов команд отправляет соответствующее уведомление администратору об инциденте и/или разрывает сеанс подключения в соответствии с правилами безопасности. Для анализа данных сеансов RDP и VNC в СКДПУ используется технология оптического распознавания символов (OCR) в режиме реального времени.

Изделие позволяет реализовывать различные схемы идентификации/аутентификации пользователей в СКДПУ и в контролируемых АС. В СКДПУ реализована дискреционная система контроля и управления доступом с элементами ролевой модели.

Изделие также позволяет внедрять и поддерживать политики управления паролями пользователей СКДПУ. Для локально заданных на СКДПУ учетных записей поддерживается настраиваемая политика паролей. Для учетных записей целевых систем *nix и windows, сохраненных на СКДПУ, система позволяет реализовать режим автоматической замены паролей в соответствии с заданными параметрами политики.

СКДПУ позволяет реализовать следующие функции безопасности:

- идентификация и аутентификация пользователей;
- управление доступом субъектов доступа к объектам доступа;
- регистрация событий безопасности.

СКДПУ, устанавливаемый на аппаратные средства информационных и автоматизированных систем, предназначен для обработки конфиденциальной информации и может использоваться:

- в государственных информационных системах (ГИС) до 1-го класса защищенности включительно в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утв. приказом ФСТЭК России от 11.02.2013 г. № 17 (далее по тексту – [1]);

– в информационных системах персональных данных (ИСПД) до 1–го уровня защищенности включительно в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. приказом ФСТЭК России от 18.02.2013 г. № 21 (далее по тексту – [2]);

– в автоматизированных системах управления производственными и технологическими процессами (АСУПиТП) до 1–го класса защищенности включительно в соответствии с документом «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденным приказом ФСТЭК России от 14 марта 2014 г. № 31 (далее по тексту – [3]);

– в информационных системах на объектах критической информационной инфраструктуры (ИС КИИ) до 1–ой категории значимости включительно в соответствии с документом «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденным приказом ФСТЭК России от 25.12.2017 г. № 239 (далее по тексту – [4]).

1.2. Требования к уровню подготовки пользователя СКДПУ

Пользователь СКДПУ должен обладать практическими навыками работы в командной строке терминала среды функционирования и клиентами для различных протоколов удаленного доступа (SSH, Telnet, Rlogin и др.).

1.3. Рекомендуемые характеристики АРМ пользователя

Действия пользователя СКДПУ осуществляются с АРМ, рекомендуемые характеристики аппаратного обеспечения которого представлены в таблице 1.

Т а б л и ц а 1 – Рекомендуемые характеристики аппаратного обеспечения АРМ пользователя

Компонент	Характеристика
Процессор	архитектура x86-64 с тактовой частотой 2 ГГц
Оперативная память	6 ГБ

Компонент	Характеристика
Жесткий диск	20 ГБ и более
Интерфейсы	– интерфейс для подключения к LAN
Монитор	разрешение экрана при работе с управляющим интерфейсом 1280x1024.
<p>Примечание. Здесь и далее в настоящем документе для обозначения объемов памяти и дискового пространства используется единица измерения ГБ (гигабайт) = 2^{30} байт. Приставка гига- в значении 10^9 байт не применяется</p>	

Требования к среде функционирования и программным средствам АРМ пользователя представлены в таблице 2.

Т а б л и ц а 2 – Программные средства АРМ пользователя

Компонент	Характеристика
ОС	Unix, Windows, Mac OS X
Веб-обозреватель	Веб-обозреватели Mozilla Firefox 80.0, Google Chrome 10.0 – 80.0, Microsoft Edge 44.18362.449.0 указанных версий и выше, обеспечивающие поддержку стандартов HTTP 1.1, TLS 1.2 и выше.
Другое ПО	Свободно распространяемый клиент для различных протоколов удаленного доступа, включая SSH, Telnet, Rlogin. В качестве таких клиентов могут быть использованы «PuTTY», «WinSCP», «FileZilla»

Браузер должен быть установлен перед началом работы с СКДПУ. Для корректной работы СКДПУ рекомендуется в настройках браузера разрешить выполнение javascript и сохранение файлов cookies.

1.4. Обеспечение безопасности

1.4.1. Режимы работы средства (СКДПУ)

Пользователь СКДПУ, в общем случае, при подключении к целевому устройству осуществляет первичную авторизацию на СКДПУ, а затем, для подключения к целевому устройству, выполняет авторизацию вторичную.

Примечание. В зависимости от настроек подключения к целевому устройству, вторичная авторизация может быть отключена.

Способы и порядок авторизации пользователя назначаются администратором СКДПУ.

После выполнения первичной авторизации на СКДПУ пользователю могут быть доступны функции по настройке своего профиля, изменению пароля, загрузке публичного ключа SSH и ключа GPG, просмотру информации о доступных целевых устройствах, формированию заявок на доступ к целевым устройствам и просмотру параметров авторизации, формированию и просмотру подтвержденных/запрещенных разрешений на доступ к целевым устройствам и параметров авторизации, скачиванию ярлыков для быстрого доступа к СКДПУ и целевым устройствам, а также просмотру информации о выполненных ранее авторизациях на целевые устройства.

1.4.2. Принципы безопасной работы средства (СКДПУ)

Действия пользователя СКДПУ должны осуществляться на АРМ пользователя с характеристиками аппаратного обеспечения не ниже рекомендуемых.

Среда функционирования и программные средства АРМ пользователя должны соответствовать рекомендуемым.

1.4.3. Функций и интерфейсы функций СКДПУ, доступные каждой роли пользователей

Пользователь СКДПУ в общем случае осуществляет авторизацию (первичную и вторичную) а также настройку СКДПУ, подключение к целевым устройствам, аудит действий, ранее выполненных пользователем через веб – интерфейс, из командной строки терминала или клиента удаленного доступа.

1.4.4. Параметры (настроек) безопасности средства (СКДПУ), доступные роли пользователя, и их безопасных значений

Пользователю доступна единственная роль – пользователь СКДПУ.

Параметры (настройки) безопасности Изделия, доступные пользователю СКДПУ и их безопасные значения, задаются Администратором СКДПУ.

Для осуществления работы пользователя СКДПУ администратор СКДПУ должен передать ему следующие сведения:

- порядок и параметры авторизации;
- дополнительную служебную информацию (сроки действия паролей, разрешенные пользователю периоды доступа на целевые устройства, сроки проведения регламентных работ и др.).

1.4.5. Типы событий безопасности, связанных с доступными пользователю функциями средства

События безопасности, связанные с доступными пользователю функциями Изделия:

- успешно установленные сессии пользователя;
- отключенные сессии;
- передача файлов в рамках сессии;
- ошибки аутентификации;
- отсутствие доступа к целевому устройству.

1.4.6. Действия после сбоев и ошибок эксплуатации средства

Восстановление работоспособности СКДПУ может быть выполнено путем принудительной перезагрузки, которая выполняется администратором; участие пользователя не требуется.

В случае, когда Изделие не может восстановить свою работу, требуется разорвать текущее соединение и повторно авторизоваться. Также следует обратиться с описанием проблемы к администратору СКДПУ.

Действия пользователя при возникновении нестандартных ситуаций приведены в разделе 4 настоящего документа

1.5. Общие сведения

Первичная авторизация пользователя осуществляется через веб-интерфейс или из командной строки терминала клиента удаленного доступа и может быть выполнена несколькими способами (порядок и параметры авторизации пользователю назначает администратор):

- путем использования логина и пароля;
- путем использования логина и публичного ключа SSH;
- путем использования токенов.

Локальная проверка подлинности SSH в СКДПУ выполняется с помощью пароля и ключа. В случае проверки подлинности по ключу СКДПУ не запрашивает пароль для входа SSH, однако пользователь в любом случае должен ввести пароль для входа в веб-интерфейс СКДПУ для администрирования и на устройства RDP.

Открытый ключ SSH пользователя должен ввести либо администратор посредством веб-интерфейса для администрирования, либо пользователь на странице Мои настройки (п.1.7.3 данного руководства).

П р и м е ч а н и е . Примеры генерации SSH-ключа приведены в приложении 1.

П р и м е ч а н и е . При авторизации на СКДПУ и (или) целевых устройствах (системах) с помощью токенов, пользователи руководствуются эксплуатационной документацией на данные устройства

2. ДОСТУП К ВЕБ-ИНТЕРФЕЙСУ СКДПУ

Для доступа к веб-интерфейсу СКДПУ необходимо на АРМ пользователя выполнить следующую последовательность действий:

Шаг 1. Открыть веб-браузер.

Шаг 2. В адресной строке веб-браузера ввести следующее значение:

`https://skdpu_ip_address`

где `skdpu_ip_address` – IP-адрес СКДПУ.

В окне веб-браузера появится окно авторизации СКДПУ (см. рисунок 1).

Примечание. Веб-браузер должен быть настроен для принятия файлов cookies и запуска JavaScript.

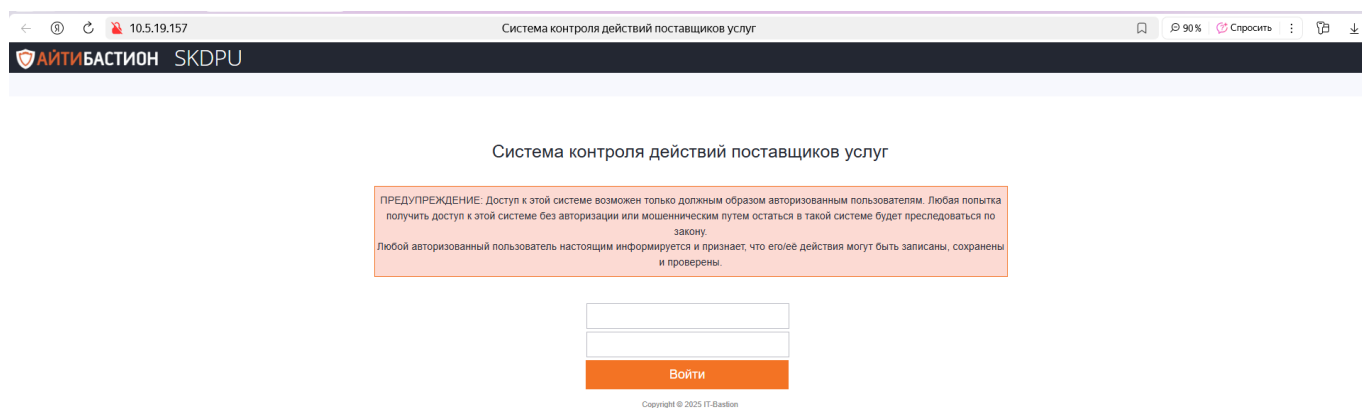


Рисунок 1 - Окно авторизации СКДПУ

Шаг 3. В окне авторизации необходимо указать в верхнем поле ввода - Имя пользователя (логин) и в нижнем поле ввода - Пароль, предоставленные администратором СКДПУ (см. рисунок 2).

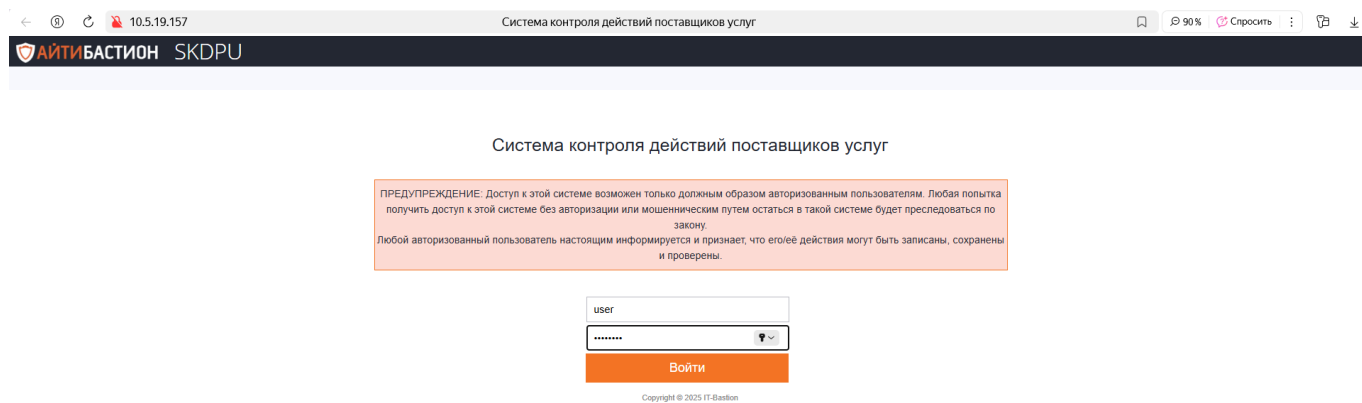


Рисунок 2 - Авторизация пользователя СКДПУ

Шаг 4. Шаг 4. Нажать кнопку Войти.

При успешном входе в систему на экране отобразится главная страница СКДПУ (см. рисунок 3).

При неактивности пользователя в течение установленного периода времени (по умолчанию 15 минут) происходит блокировка сеанса пользователя. При выполнении любых действий пользователя после блокировки сеанса отобразится соответствующее уведомление; главное окно СКДПУ будет закрыто; пользователю отобразится окно как на рисунке 2; для возобновления сеанса следует повторно произвести авторизацию.




3. ВЕБ-ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ



Рисунок 3 - Главная страница СКДПУ

Интерфейс СКДПУ имеет три основных области (см. рисунок 3):

- Главное меню (обозначена цифрой «1»);
- Боковое меню для доступа к разрешенным функциям СКДПУ (обозначена цифрой «2»);
- Рабочая область (обозначена цифрой «3»).

Главное меню (1) содержит панель авторизации, отображающую информацию о пользователе, выполнившем вход в СКДПУ, кнопку для выхода из интерфейса , кнопку для вызова справки  и кнопку для отображения уведомлений .

Боковое меню (2) содержит следующие пункты меню:

- 1. Мои настройки** – предназначен для изменения настроек профиля пользователя;
- 2. Мои авторизации** – предназначен для отображения доступных аккаунтов и сервисов для доступа к ресурсам и содержит следующие подразделы:

- **Сессии** – описание доступных сессий;
- **Пароли** – модуль управления паролями различных соединений.

В рабочей области (3) отображаются страницы интерфейса пользователя, соответствующие выбранным из бокового меню (2) позициям

3.1. Раздел меню Мои настройки

При выборе пункта **Мои настройки** в рабочей области отображаются параметры, которые могут быть внесены/изменены пользователем (см. рисунок 4).

10.5.19.157 Система контроля действий поставщиков услуг user (exit)

АЙТИБАСТИОН SKDRU

Мои настройки

Мои настройки
Мои авторизации

Профиль

Имя пользователя * user

Видимое имя user

Предпочитаемый язык * Russian

Предпочитаемый язык

E-mail * cia_cia@mail.ru

E-mail пользователя

Применить

Пароль SKDRU

Текущий пароль *

Новый пароль *

Политика паролей: минимум 8 символов, минимум 1 большой буква, как минимум 1 буква нижнего регистра, минимум 1 цифр, минимум 1 специальных символов, отличаться от имени пользователя

Применить

Публичный ключ SSH

Загрузить публичный ключ: Выберите файл | Файл не выбран

Или вставить публичный ключ

Рисунок 4 - Страница «Мои настройки»

Меню **Мои настройки** доступно всем пользователям вне зависимости от прав доступа.

Пользователю доступны следующие возможности:

- указание адреса электронной почты и выбор языка интерфейса (для отображения сообщений прокси-сервера);
- смена пароля (только если пользователь был объявлен локально);
- загрузка открытого ключа SSH;
- загрузка GPG-ключа.

Если проверка подлинности пользователя реализована посредством службы каталогов (LDAP, LDAP/AD), то форма для изменения пароля будет недоступна.

3.1.1. Изменение адреса электронной почты и языка интерфейса

Для изменения адреса электронной почты или языка интерфейса необходимо в области Профиль (см. рисунок 4) выполнить следующие действия:

Шаг 1. Для изменения языка интерфейса из раскрывающегося списка Предпочитаемый язык выбрать необходимый язык.

Шаг 2. Для изменения адреса электронной почты в поле E-mail ввести адрес электронной почты.

Шаг 3. Для сохранения внесенных изменений нажать кнопку Применить.

Поля Предпочитаемый язык и E-mail помечены символом «*» и являются обязательными для заполнения.

3.1.2. Изменение пароля

Пользователю может потребоваться изменение пароля в следующих случаях:

– срок действия пароля истекает в ближайшее время (при входе пользователя в веб-интерфейс отображается соответствующее сообщение);

– пароль входит в список паролей, запрещенных парольной политикой, настроенной администратором СКДПУ;

– пароль слишком короткий или включает недостаточно специальных символов, цифр или букв в верхнем регистре;

– пароль совпадает с именем пользователя;

– пароль совпадает с предыдущим паролем.

Для изменения пароля необходимо в области Пароль SKDPU выполнить следующие действия:

Шаг 1. Ввести текущий пароль в поле Текущий пароль.

Шаг 2. Ввести новый пароль и подтверждение пароля в двойное поле Новый пароль.

Примечание. Новый пароль должен удовлетворять параметрам, которые указаны в подсказке ниже поля подтверждения нового пароля.

Шаг 3. Для сохранения внесенных изменений нажать кнопку Применить.

Поля Текущий пароль и Новый пароль помечены символом * и являются обязательными для заполнения.

3.1.3. Загрузка открытого ключа SSH

Для загрузки открытого ключа SSH необходимо в области Публичный ключ SSH выполнить следующие действия:

Шаг 1. Нажать кнопку Выберите файл для вызова окна выгрузки файла и в открывшемся окне навигатора выбрать файл ключа
либо

Скопировать из текстового редактора содержимое публичного ключа SSH и вставить его в поле Или вставить публичный ключ.

Шаг 2. Нажать кнопку Применить.

3.1.4. Загрузка GPG-ключа

Для загрузки GPG-ключа необходимо в области GPG-ключ (см. рисунок 5 выполнить следующие действия:)

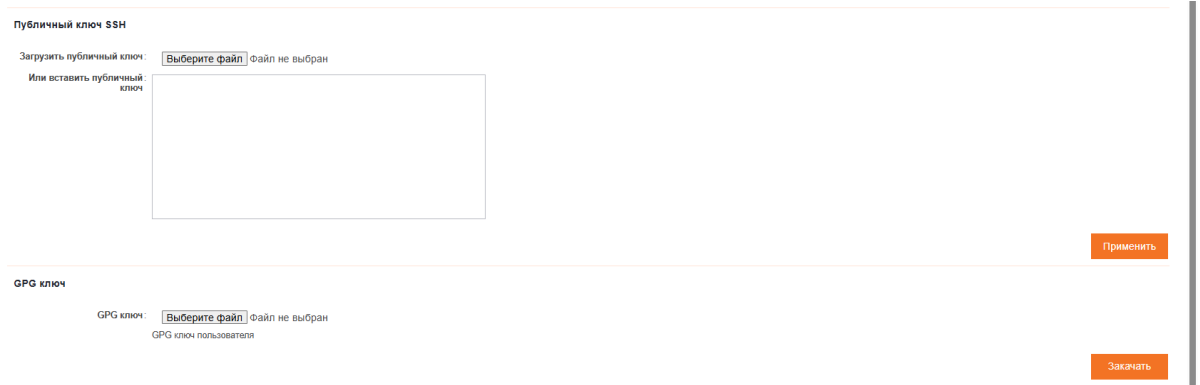


Рисунок 5 - Страница «Мои настройки», область GPG-ключ

Шаг 1. Нажать кнопку **Выберите файл** для вызова окна выгрузки файла и в открывшемся окне навигатора выбрать файл GPG-ключа.

Шаг 2. Нажать кнопку **Закачать**.

3.2. Раздел меню Мои авторизации

В разделе меню **Мои авторизации** пользователю предоставляется возможность:

– просмотреть информацию о своих ранее выполненных подключениях к целевым учетным записям и доступным сервисам;

– получить доступ к разрешенным ресурсам и сервисам.

3.2.1. Страница меню «Сессии»

При выборе пункта **Сессии** из бокового меню интерфейса, в рабочей области отображается перечень доступных сервисов (см. рисунок 6).

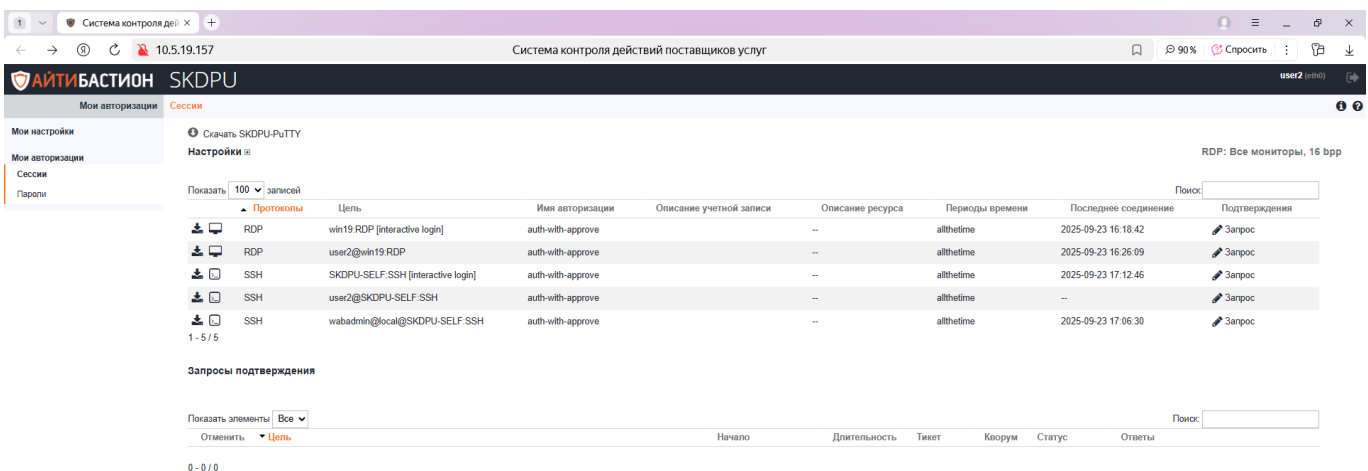



Рисунок 6 - Страница «Сессии»

На странице «Сессии» пользователю доступны действия по скачиванию клиентского приложения SKDPU-PuTTY(включен в состав СКДПУ); для этой цели необходимо нажать на значок  слева от надписи «Скачать SKDPU-PuTTY».

Для настройки разрешения и глубины цвета клиентского окна (окон) при доступе к целевым устройствам по протоколу RDP следует нажать «+» справа от надписи «Настройки» (см. рисунок 7).

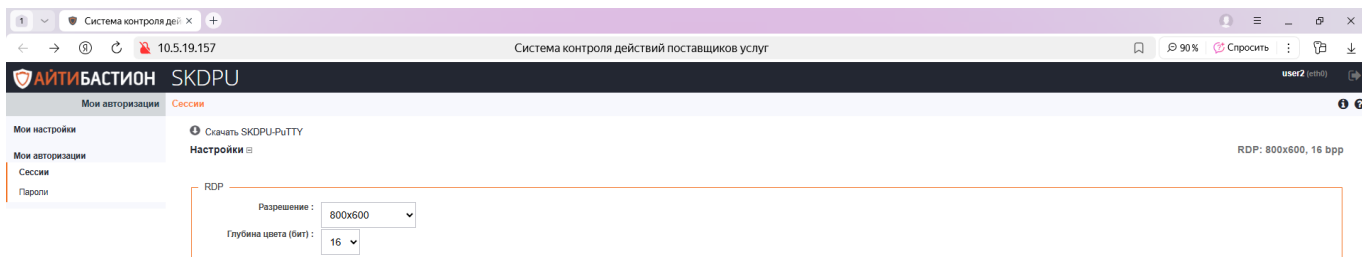



Рисунок 7 - Настройка параметров клиентского окна (окон) при доступе к целевым устройствам по протоколу RDP

В раскрывшемся окне RDP из выпадающих списков следует выбрать желаемые настройки.


В центральной части страницы «Сессии» пользователю отображаются параметры целевых учетных записей (см. рисунок 6).


Имеется возможность настроить количество отображаемых записей на странице (следует выбрать из выпадающего списка «Показать ... записей»), отфильтровать отображаемый список записей, задав начальные символы в поле «Поиск».


Параметры целевых учетных записей представлены в полях:

- «Протокол» - наименование протокола подключения;
- «Цель» - наименование целевого устройства;
- «Имя авторизации» - условное наименование имени авторизации;
- «Описание учетной записи» - краткое описание учетной записи (необязательный параметр);
- «Описание ресурса» - краткое описание целевого устройства (необязательный параметр);
- «Периоды времени» - условное наименование периода времени, когда пользователю может быть разрешен доступ к целевому устройству;
- «Последнее соединение» - информация в формате «дата, время» о последнем подключении пользователя к целевому устройству;
- «Подтверждения» - в данном поле пользователю может быть доступен функционал для формирования запроса на подключение к целевому устройству (когда в данном поле присутствует запись «  Запрос »).

В левой области записей размещаются элементы управления для осуществления доступа к целевым устройствам, минуя веб – интерфейс СКДПУ:

 - элемент управления для скачивания файлов настроек (соединение по протоколу RDP)/ конфигурационных файлов (соединение по протоколу SSH);

 - элемент управления для организации быстрого доступа к целевому устройству (соединение по протоколу RDP);


 - элемент управления для организации быстрого доступа к целевому устройству (соединение по протоколу SSH).

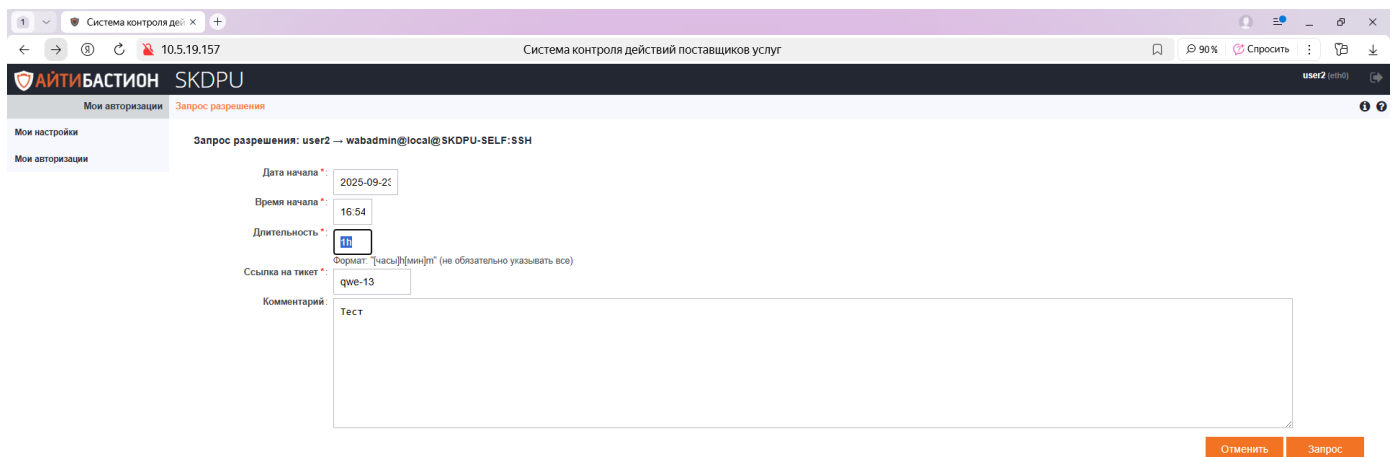
Порядок осуществления доступа к целевым устройствам описан в разделе 3.3. и приложении 2.

При желании, записи о целевых устройствах можно упорядочить по отдельным полям в порядке убывания или возрастания.

Пользователь может сформировать запрос на подключение к целевому устройству. Разрешение согласуется администратором (администраторами) СКДПУ в соответствии с настроенным порядком согласования.

Для формирования запроса на подключение к целевому устройству необходимо выполнить следующие действия.

Шаг 1. В строке необходимого целевого устройства в поле «Подтверждения» нажать на элемент управления  **Запрос** , откроется окно для формирования запроса (см. рисунок 8).



Скриншот веб-интерфейса системы контроля действий поставщиков услуг (СКДПУ). В центре экрана отображается форма «Запрос разрешения» для пользователя user2 к устройству wabadmin@local@SKDPU-SELF:SSH по протоколу SSH. Форма содержит следующие поля:

- Дата начала: 2025-09-25
- Время начала: 16:54
- Длительность: 15 минут (с выпадающим списком и подсказкой формата «часы|минуты»)
- Ссылка на тикет: qwe-13
- Комментарий: Тест

В нижней правой части формы расположены кнопки «Отменить» и «Запрос».

Рисунок 8 - Окно запроса разрешения на доступ к целевому устройству

Шаг 2. В открывшемся окне следует ввести параметры разрешений (обязательные параметры отмечены звездочкой «*»):

– «Дата начала» - начальная дата подключения к целевому устройству;

– «Время начала» - начальное время подключения к целевому устройству;

– «Длительность» - длительность подключения к целевому устройству в часах и (или) минутах;

– «Ссылка на тикет» - условное обозначение задачи, в рамках которой запрашивается текущее подключение;

– «Комментарий» - при необходимости указываются комментарии, пояснения и т.д. к формируемому запросу.

Шаг 3. Для формирования запроса после заполнения необходимых полей следует задействовать кнопку «Запрос» (Для отмены формирования запроса следует задействовать кнопку «Отменить»).

Поле нажатия кнопки «Запрос» текущее окно закроется и отобразится страница «Сессии» (см. рисунок 9).

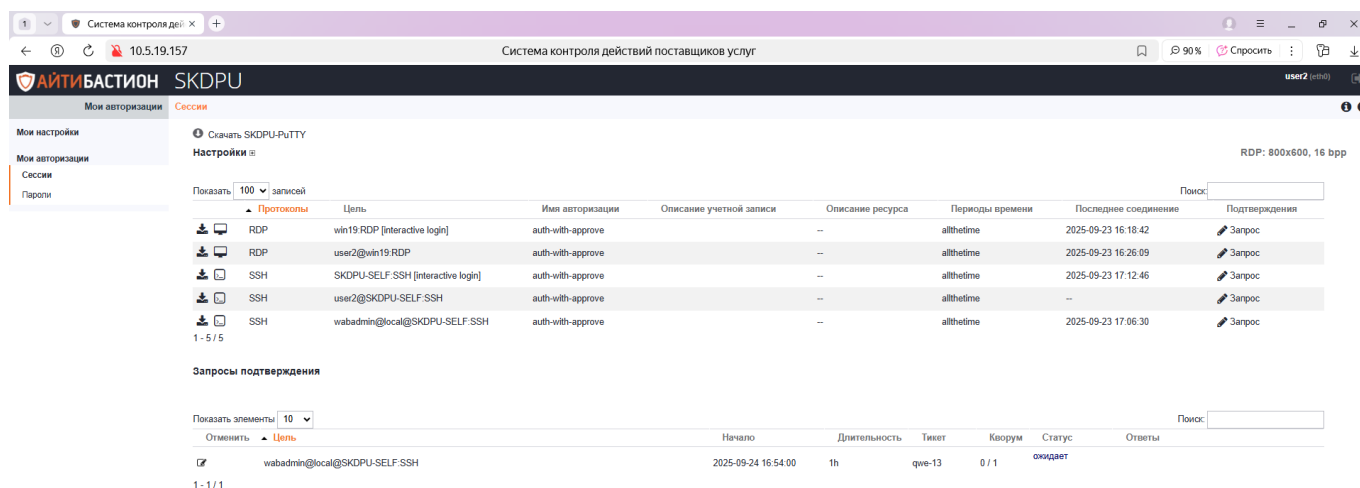


Рисунок 9 - Страница «Сессии»; сформированный запрос находится в статусе «Ожидает»

Сформированный запрос будет отображен в области «Запросы подтверждения». Параметры запроса отображаются в полях:

– «Цель» - условное наименование целевого устройства;

– «Начало» - начальная дата подключения к целевому устройству;

– «Длительность» - длительность подключения к целевому устройству в часах и (или) минутах;

– «Тикет» - условное обозначение задачи, в рамках которой запрашивается подключение;

– «Кворум» - отображается в формате n/m, где n - количество положительных согласований, m - количество согласующих лиц (положительное решение по согласованию запроса достигается, когда все согласующие лица дадут разрешение, т.е. n=m);

– «Статус» - текущий статус запроса.

– «Ответы» - комментарии согласующих лиц к их решению по согласованию текущего запроса.

Имеется возможность настроить количество отображаемых записей в данной области (следует выбрать из выпадающего списка «Показать ... записей»), отфильтровать отображаемый список записей, задав начальные символы в поле «Поиск».

Также при желании, записи в области «Запросы подтверждения» можно упорядочить по отдельным полям в порядке убывания или возрастания.

В случае согласования запроса администратором (администраторами), его статус изменится на «Принято» (см. рисунок 10).

Длительность доступа к целевому устройству может быть отредактирована администратором при согласовании в сторону уменьшения.

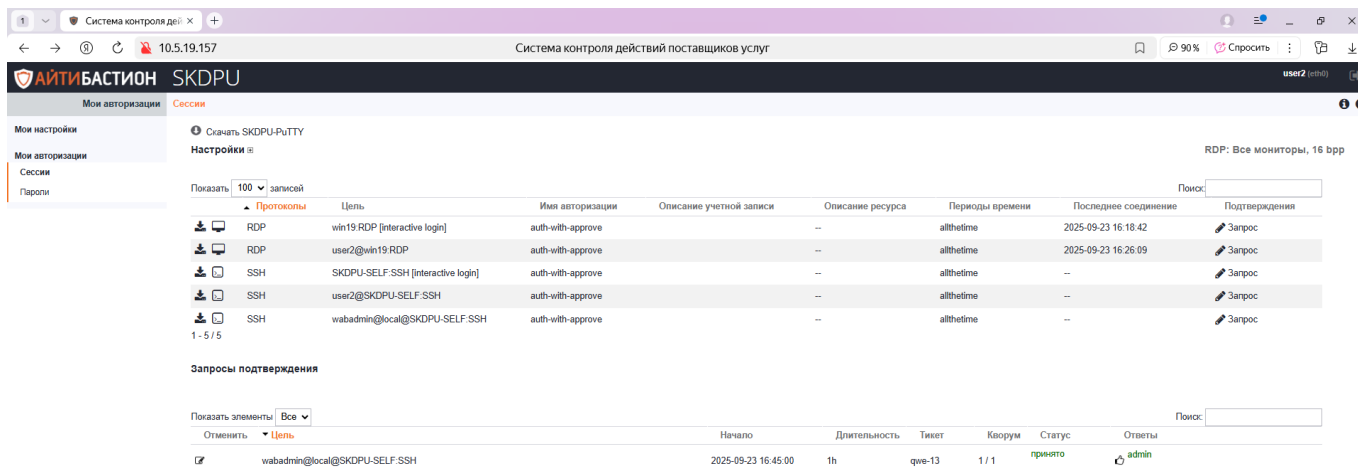


Рисунок 10 - Страница «Сессии»; сформированный запрос находится в стадии «Принято»

Для отмены сформированного запроса следует выполнить следующие действия.

Шаг 1. В левой области записи запроса подтверждения задействовать кнопку «Посмотреть данные», после чего отобразится окно с параметрами запроса (См. рисунок 11).

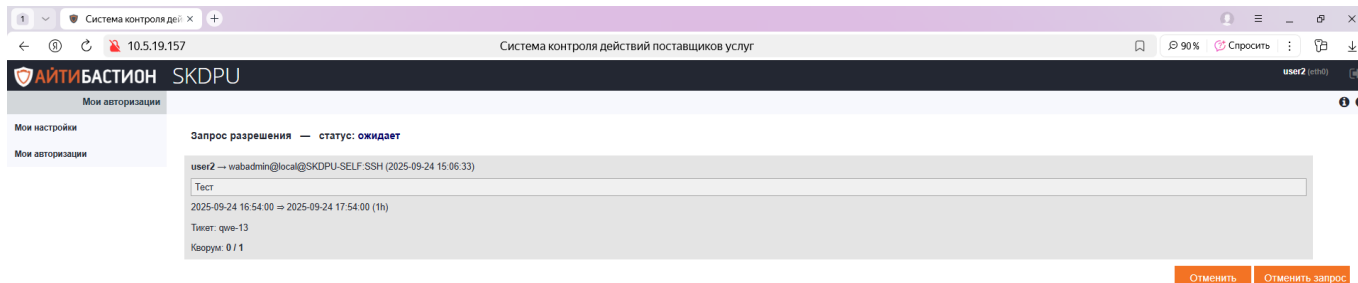


Рисунок 11 - Параметры текущего запроса

Шаг 2. Задействовать кнопку «Отменить запрос» (Чтобы отказаться от удаления запроса следует задействовать кнопку «Отменить»).

В случае задействия кнопки «Отменить запрос» текущем окне отобразится уведомление «Запрос разрешения был отклонен» и статус запроса изменится на «Отменено» (см. рисунок 12).

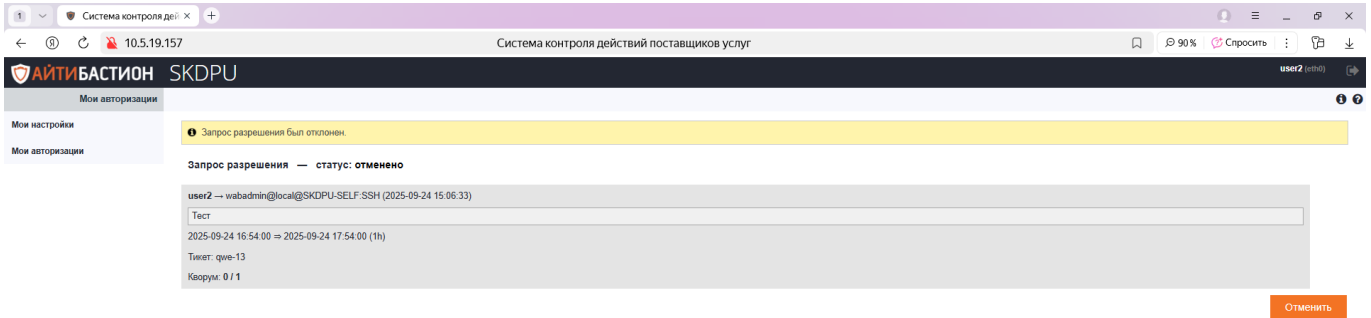


Рисунок 12 - Отмена запроса разрешения

На странице «Сессии» в области «Запросы подтверждения» статус запроса также изменится на «Отменено» (см. рисунок 13).

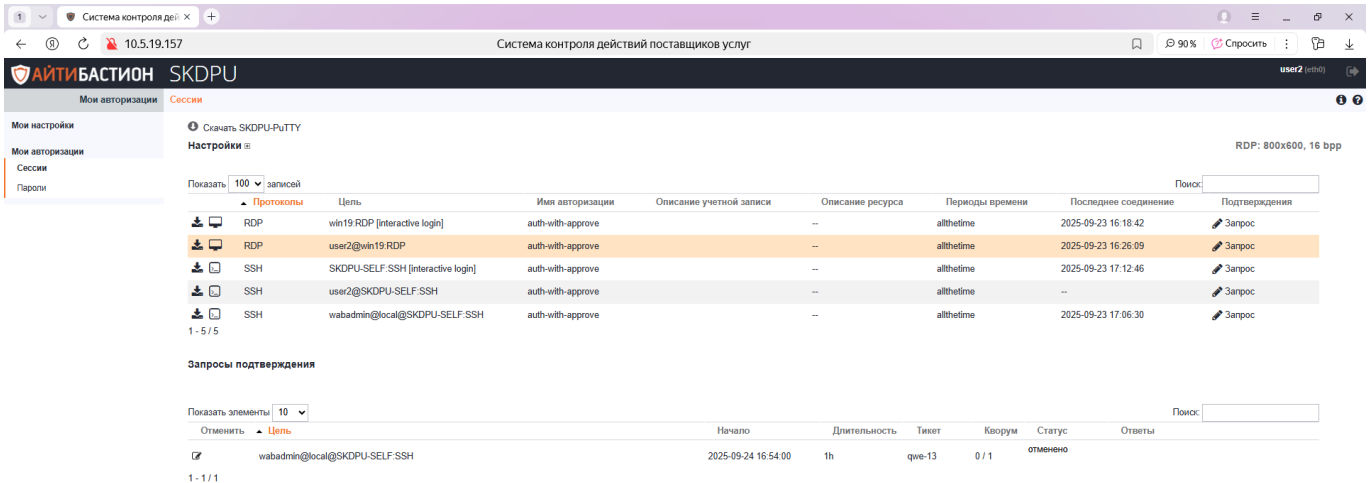


Рисунок 13 - Страница «Сессии»; статус запроса – «Отменено»

Примечание. Так же возможно отменить уже согласованные запросы со статусом «Принято», порядок действий аналогичен описанному выше.

3.2.2. Страница меню «Пароли»

При выборе пункта Пароли из бокового меню интерфейса, в рабочей области отображается перечень доступных сервисов (см. рисунок 14).

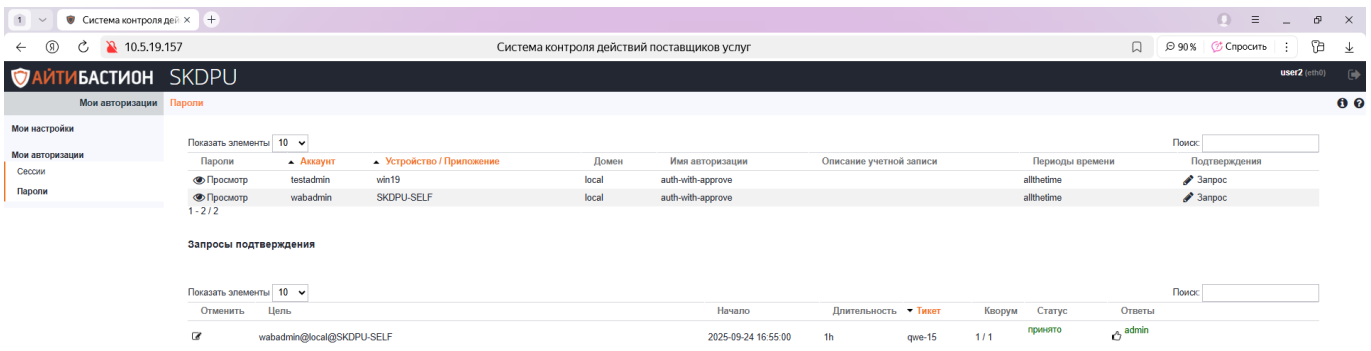



Рисунок 14 - Страница «Пароли»

В разделе меню «Пароли» пользователю предоставляется возможность получить доступ к просмотру назначенных администратором СКДПУ паролей для доступа к целевым учетным записям.

На странице отображаются следующие поля записей

– «Пароли» - в данных полях располагаются элементы управления  Просмотр для просмотра паролей доступа к соответствующим целевым учетным записям;

– «Аккаунт» - условное наименование аккаунта;


– «Устройство/приложение» - наименование целевого устройства;

– «Домен» - условное наименование домена;


– «Имя авторизации» - условное наименование имени авторизации;

– «Описание учетной записи» - краткое описание учетной записи (необязательный параметр);

– «Периоды времени» - условное наименование периода времени, когда пользователю может быть разрешен доступ к целевому устройству;

– «Подтверждения» - в данном поле пользователю может быть доступен функционал для формирования запроса на просмотр паролей для доступа к целевым учетным записям (когда в данном поле присутствует запись «  Запрос »).

При желании, записи можно упорядочить по отдельным полям в порядке убывания или возрастания.

В том случае, когда у пользователя при нажатии на элемент управления  Просмотр нет подтвержденных разрешений на просмотр пароля, ему отображается соответствующее уведомление (см. рисунок 15).

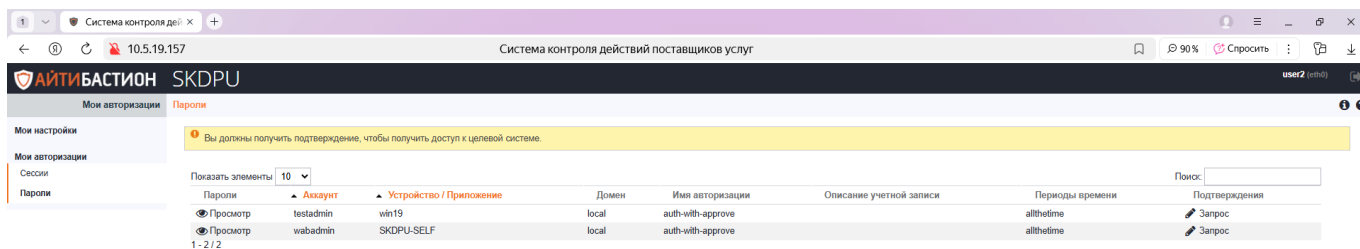
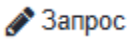


Рисунок 15 - Страница «Пароли»; уведомление о необходимости получить подтверждение для доступа к целевому устройству (для отображения пароля доступа)

Пользователь может сформировать запрос на просмотр паролей для доступа к целевым учетным записям. Разрешение согласуется администратором (администраторами) СКДПУ в соответствии с настроенным порядком согласования.

Для формирования запроса на просмотр паролей для доступа к целевым учетным записям необходимо выполнить следующие действия.

Шаг 1. В строке необходимого целевого устройства в поле «Подтверждения» нажать на элемент управления  , откроется окно для формирования запроса (см. рисунок 16).

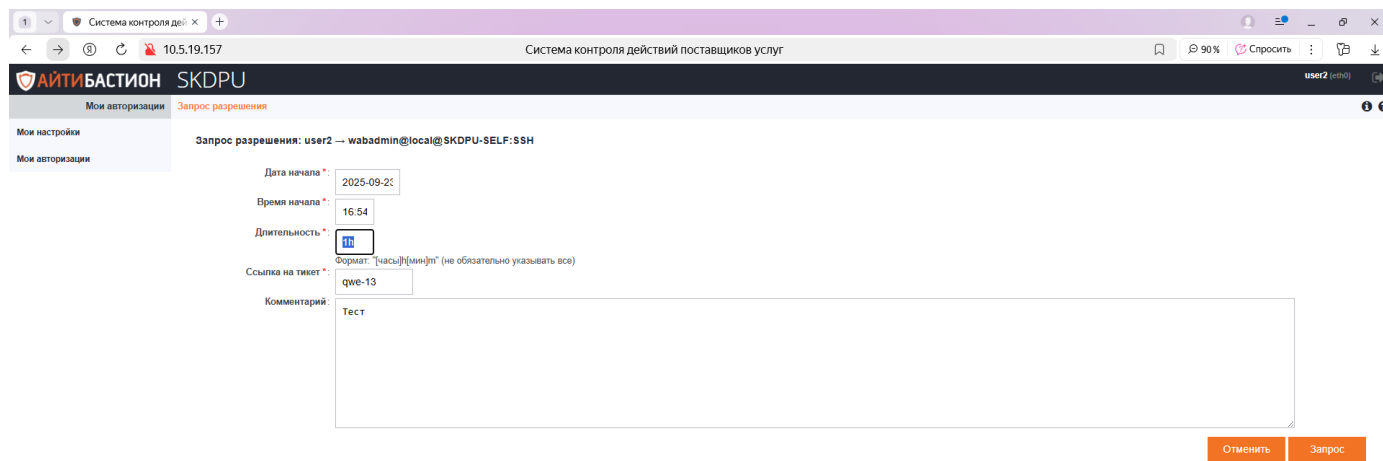


Рисунок 16 - Окно запроса разрешения на просмотр пароля доступа к целевому устройству

Шаг 2. В открывшемся окне следует ввести параметры разрешений (обязательные параметры отмечены звездочкой «*»):

- «Дата начала» - начальная дата подключения к целевому устройству;
- «Время начала» - начальное время подключения к целевому устройству;
- «Длительность» - длительность подключения к целевому устройству в часах и (или) минутах;
- «Ссылка на тикет» - условное обозначение задачи, в рамках которой запрашивается текущее подключение;
- «Комментарий» - при необходимости указываются комментарии, пояснения и т.д. к формируемому запросу.

Шаг 3. Для формирования запроса после заполнения необходимых полей следует задействовать кнопку «Запрос» (Для отмены формирования запроса следует задействовать кнопку «Отменить»).

Поле нажатия кнопки «Запрос» текущее окно закроется и отобразится страница «Пароли» (см. рисунок 17).

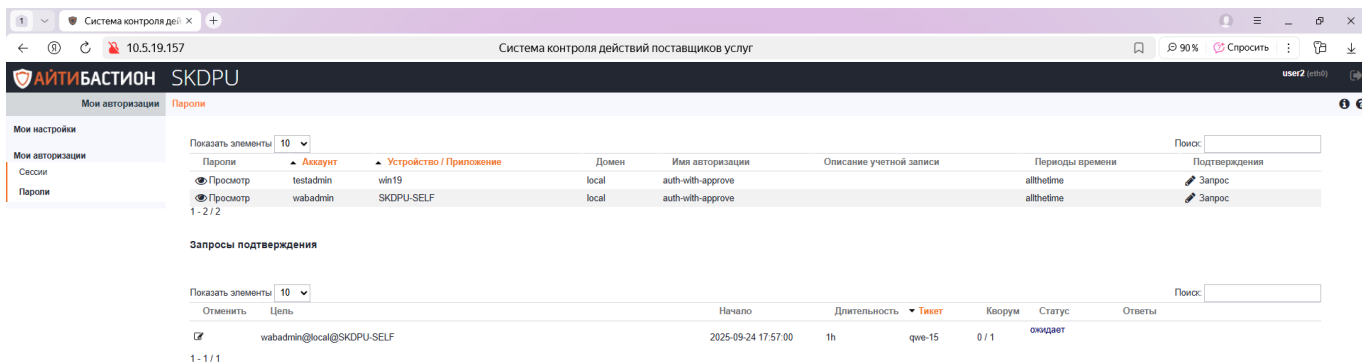


Рисунок 17 - Страница «Пароли»; сформированный запрос находится в статусе «Ожидает»

Сформированный запрос будет отображен в области «Запросы подтверждения».

Параметры запроса отображаются в полях:

- «Цель» - условное наименование целевого устройства;
- «Начало» - начальная дата подключения к целевому устройству;
- «Длительность» - длительность подключения к целевому устройству в часах и (или) минутах;
- «Тикет» - условное обозначение задачи, в рамках которой запрашивается подключение;
- «Кворум» - отображается в формате n/m, где n - количество положительных согласований, m- количество согласующих лиц (положительное решение по согласованию запроса достигается, когда все согласующие лица дадут разрешение, т.е. n=m);
- «Статус» - текущий статус запроса.
- «Ответы» - комментарии согласующих лиц к их решению по согласованию текущего запроса.

Имеется возможность настроить количество отображаемых записей в данной области (следует выбрать из выпадающего списка «Показать ... записей»), отфильтровать отображаемый список записей, задав начальные символы в поле «Поиск».

Также при желании, записи в области «Запросы подтверждения» можно упорядочить по отдельным полям в порядке убывания или возрастания.

В случае согласования запроса администратором (администраторами), его статус изменится на «Принято» (см. рисунок 18).

Длительность действия пароля доступа к целевому устройству может быть отредактирована администратором при согласовании в сторону уменьшения.

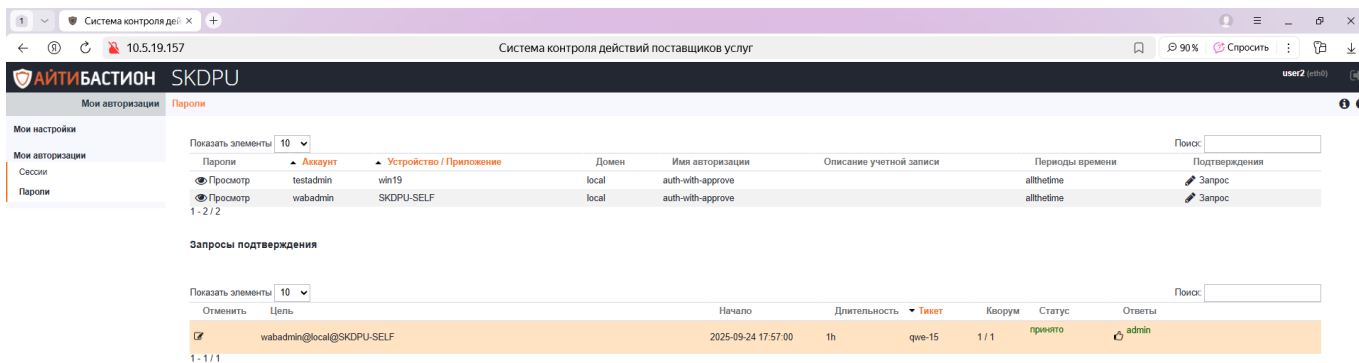



Рисунок 18 - Страница «Пароли»; сформированный запрос находится в статусе «Принято»

После согласования запроса пользователю будет доступен к просмотру пароль доступа к соответствующему целевому устройству.

Для просмотра пароля следует нажать на элемент управления  «Просмотр» в записи соответствующего целевого устройства, после чего откроется окно (см. рисунок 19).

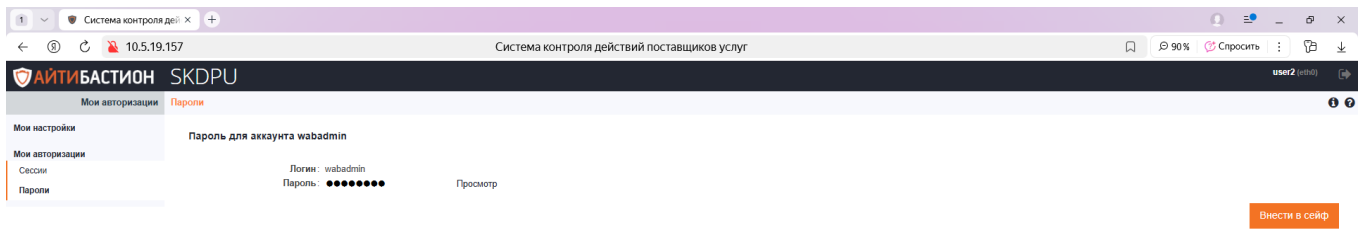


Рисунок 19 - Окно для просмотра пароля (аккаунт wabadmin)

Чтобы отобразить пароль следует нажать на элемент управления «Просмотр» (см. рисунок 20).

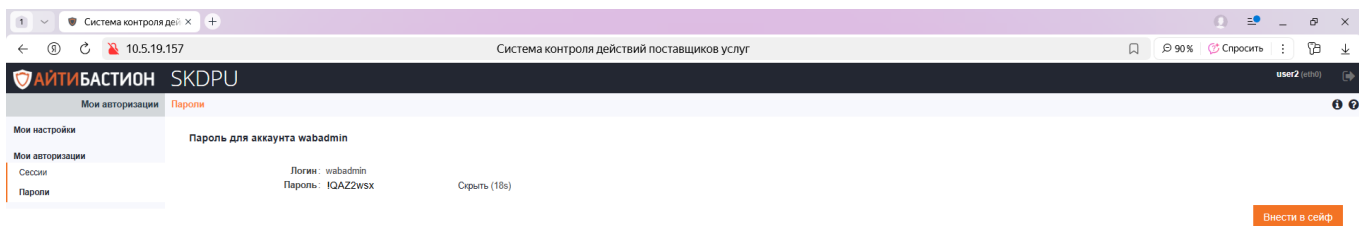



Рисунок 20 - Отображение пароля (аккаунт wabadmin)

Отображение пароля закроется по истечении 20 секунд, в окне будет отображаться обратный отсчет этого периода. На время отображения пароля администратор СКДПУ не имеет возможности редактировать данный пароль. Для того, отмены данного запрета пользователю следует нажать кнопку «Внести в сейф».

Для отмены сформированного запроса следует выполнить следующие действия.

Шаг 1. В поле «Отменить» задействовать кнопку  «Посмотреть данные», после чего отобразиться окно с параметрами запроса (см. рисунок 21).

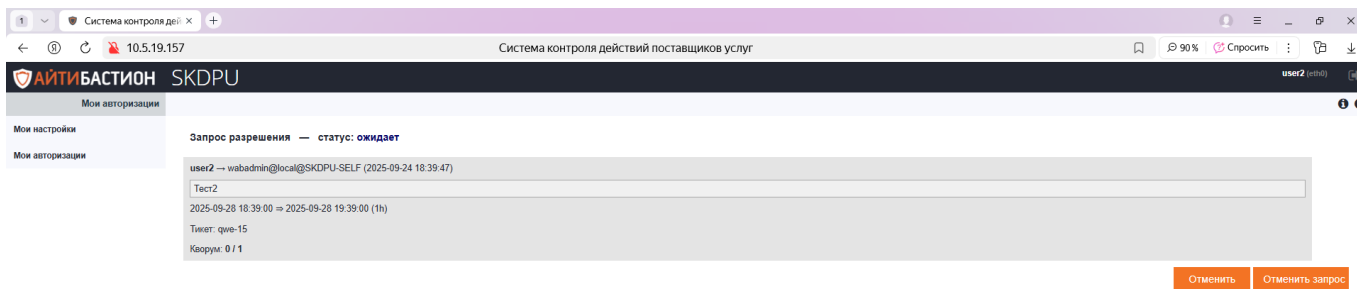


Рисунок 21 - Параметры текущего запроса.

Шаг 2. Задействовать кнопку «Отменить запрос» (Чтобы отказаться от удаления запроса следует задействовать кнопку «Отменить»).

В случае задействования кнопки «Отменить запрос» текущем окне отобразится уведомление «Запрос разрешения был отклонен» и статус запроса изменится на «Отменено» (см. рисунок 22).

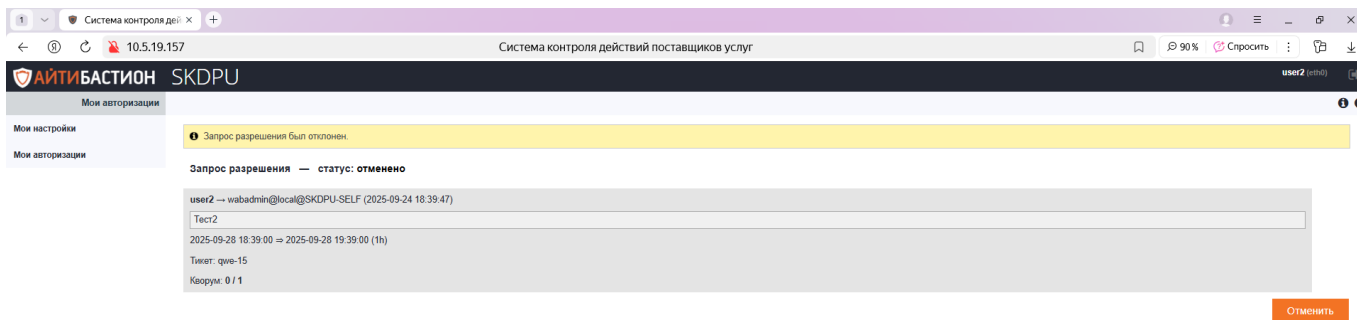


Рисунок 22 - Отмена запроса разрешения

На странице «Пароли» в области «Запросы подтверждения» статус запроса также изменится на «Отменено» (см. рисунок 23).

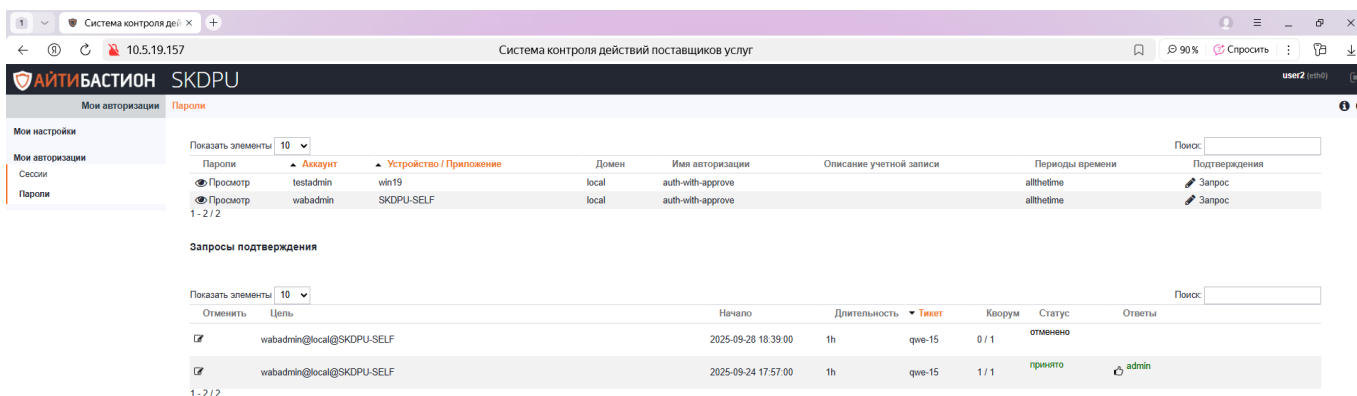


Рисунок 23 - Страница «Пароли»; статус запроса на 2025-09-28 18:39:00 – «Отменено»

Примечание. Так же возможно отменить уже согласованные запросы со статусом «Принято», порядок действий аналогичен описанному выше.

3.3. Доступ к целевым устройствам

Доступ к целевым устройствам (системам) через СКДПУ, может быть реализован различными способами и зависит от:


- способов авторизации на целевых устройствах, которые в свою очередь определяются:
 - настройками авторизации, назначаемые Администраторами СКДПУ;
 - средствами, используемыми при авторизации (веб-интерфейс СКДПУ, клиенты удаленного доступа, терминал командной строки, токены);
- используемых протоколов подключения к целевым устройствам;
- среды функционирования (ОС) АРМ пользователей.

В данном разделе описаны действия пользователей по доступу к целевым устройствам из веб-интерфейса СКДПУ, авторизации на СКДПУ и доступу к целевым устройствам через клиент удаленного доступа PuTTY.

Апробированные варианты входа в систему и способы переноса файловой информации между АРМ пользователя и целевыми устройствами с учетом их вариативности описаны в приложении 2.

3.3.1. Доступ к целевым устройствам из веб-интерфейса пользователя

Для доступа к целевому устройству (системе) пользователю необходимо перейти на страницу «Сессии» меню «Мои авторизации».

В строке целевого устройства из списка для получения доступа к целевым учетным записям необходимо нажать на значок  для скачивания файлов настроек в виде ярлыка (соединение по протоколу RDP)/ конфигурационных файлов (соединение по протоколу SSH) на АРМ пользователя.

В дальнейшем, для доступа целевому устройству (системе) пользователю нет необходимости осуществлять вход на СКДПУ через веб-интерфейс; достаточно двойным нажатием на скачанный файл запустить процесс авторизации (первичной и (или) вторичной, в зависимости от выполненным администратором СКДПУ настроек авторизации).

Пользователю отобразится окно авторизации СКДПУ (см. рисунок 24).

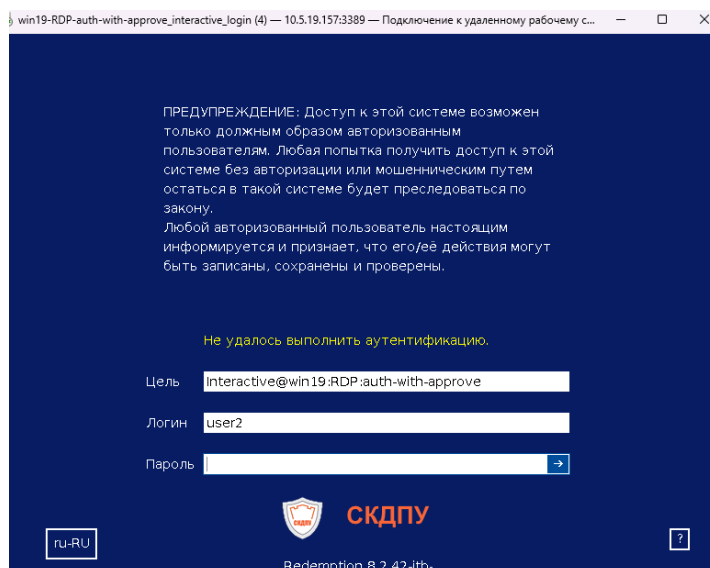


Рисунок 24 - Окно авторизации СКДПУ

В окне авторизации отображаются предупреждения, элементы управления для выбора языка ввода и получения справочной информации, а также поля для указания:

- «Цель» - наименования целевого устройства;
- «Логин»;
- «Пароль».

В окне авторизации в полях «Цель» и «Логин» будут указаны наименование целевого устройства и логин пользователя, которые соответствуют параметрам, указанным в скачанном ранее файле настроек.

При желании, при авторизации в окне можно ввести иные корректные параметры целевого устройства, пользователя и соответственно пароля доступа.

В случае, успешной авторизации на СКДПУ и при условии, что пользователю согласован доступ на целевое устройство, ему отображается окно с соответствующим уведомлением (см. рисунок 25).

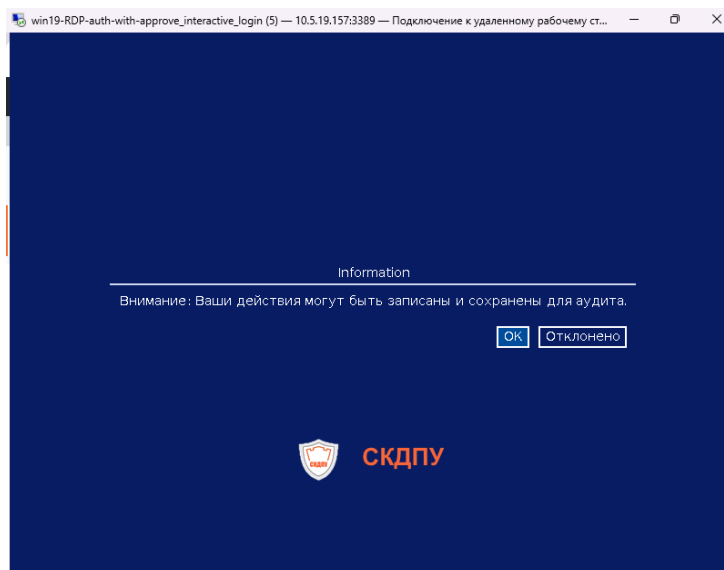


Рисунок 25 - Уведомление СКДПУ

Для дальнейшей авторизации на целевом устройстве следует нажать кнопку «Ок», в противном случае, нажать «Отклонено».

При нажатии кнопки «Ок» отобразится окно с уведомлением о времени, до которого пользователю будет доступно целевое устройство (см. рисунок 26).

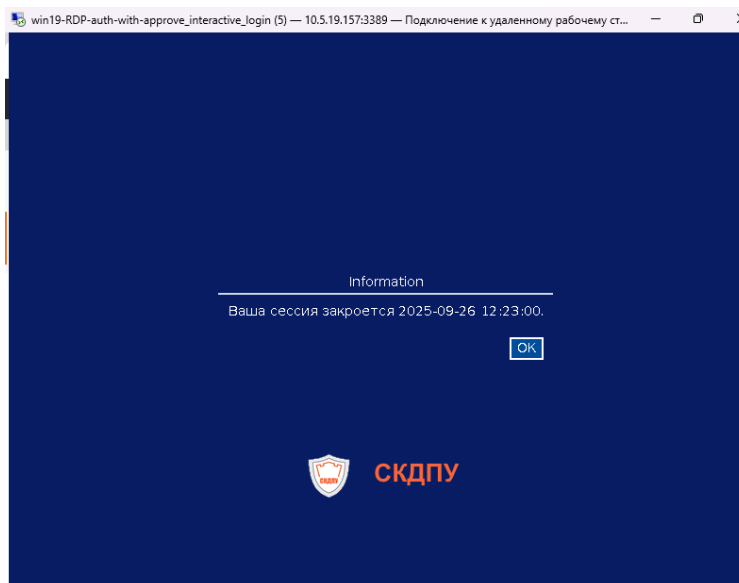


Рисунок 26 - Уведомление о времени, до которого пользователю доступно целевое устройство

Для дальнейшей авторизации на целевом устройстве следует нажать кнопку «Ок», после чего отобразится окно авторизации на целевом устройстве (см. рисунок 27).

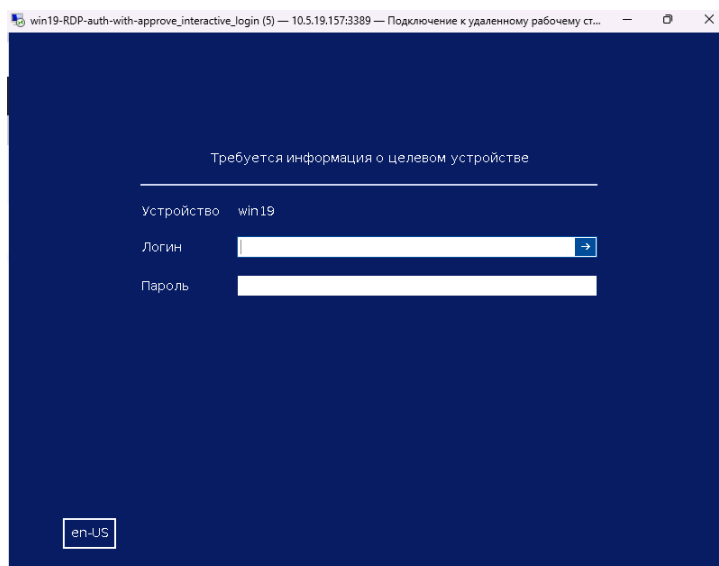


Рисунок 27 - Окно авторизации на целевом устройстве

И, наконец, следует ввести логин и пароль для авторизации на целевом устройстве (системе), далее нажать кнопку Enter.

В случае успешной авторизации, будет осуществлен доступ к целевому устройству (пример см. на рисунке 28).

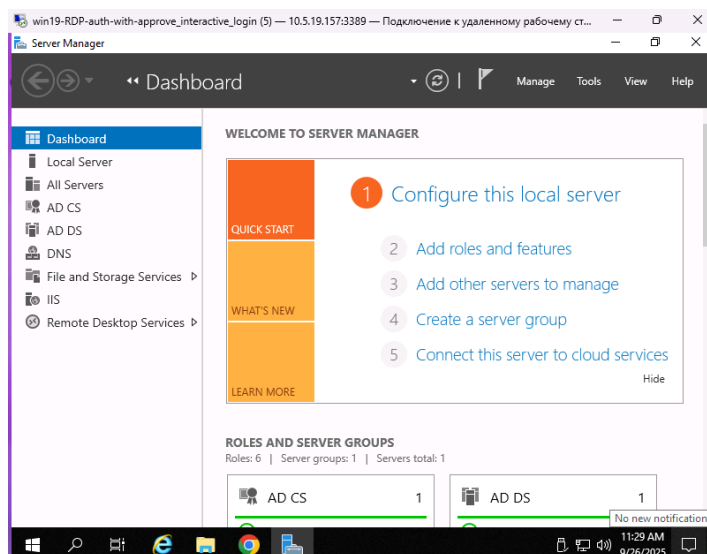


Рисунок 28 - Осуществлен доступ к целевому устройству

Выход из сессии доступа к целевому устройству осуществляется путем закрытия окна удаленного доступа.

В том случае, когда авторизация на СКДПУ прошла успешно, но пользователю не согласован доступ на целевое устройство, ему отображается окно с соответствующим уведомлением (см. рисунок 29) и предлагается сформировать запрос на доступ.

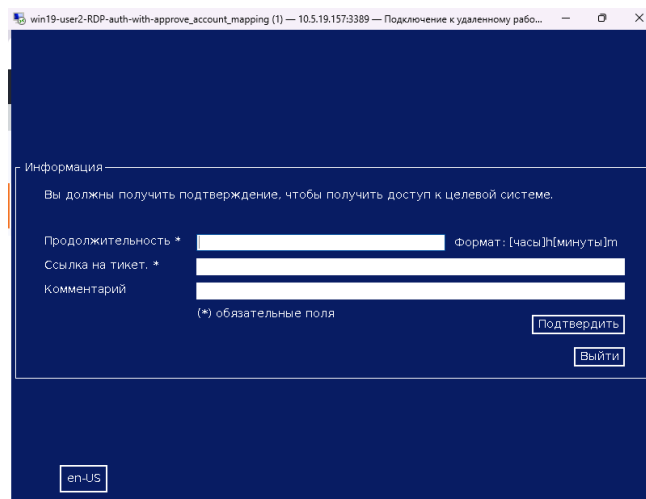


Рисунок 29 - Пользователю не согласован доступ на целевое устройство (систему)

Для формирования запроса на подтверждение доступа к целевому устройству следует выполнить следующие действия.

Шаг 1. В поле «Продолжительность» ввести запрашиваемую длительность времени на доступ к целевому устройству в часах и (или) минутах в формате <часы>h<минуты>m.

Шаг 2. В поле «Ссылка на тикет» ввести условное наименование задачи, в рамках которой планируется доступ к целевому устройству.

Шаг 3. При необходимости, в окне «Комментарий» ввести описание планируемого подключения, иную информацию.

Шаг 4. Чтобы окончательно завершить формирование запроса на доступ, следует нажать кнопку «Подтвердить», либо кнопку «Выйти», чтобы отказаться от его формирования.

Система отслеживает формат введенных параметров запроса и при некорректном вводе выдает пользователю соответствующее предупреждение.

В результате корректно выполненных действий будет сформирован запрос на доступ к целевому устройству (см. рисунок 30).

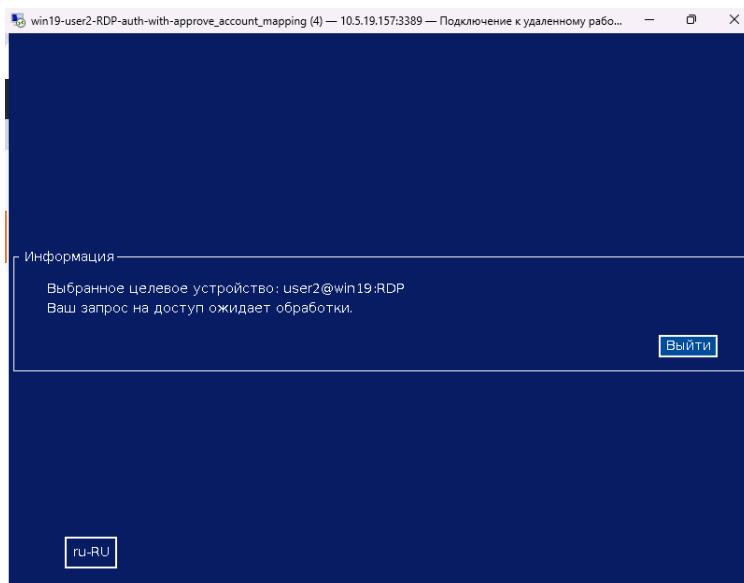


Рисунок 30 - Запрос на доступ сформирован, ожидает обработки

В случае, если запрос на доступ будет отклонен, пользователю отобразится соответствующее уведомление (см. рисунок 31).

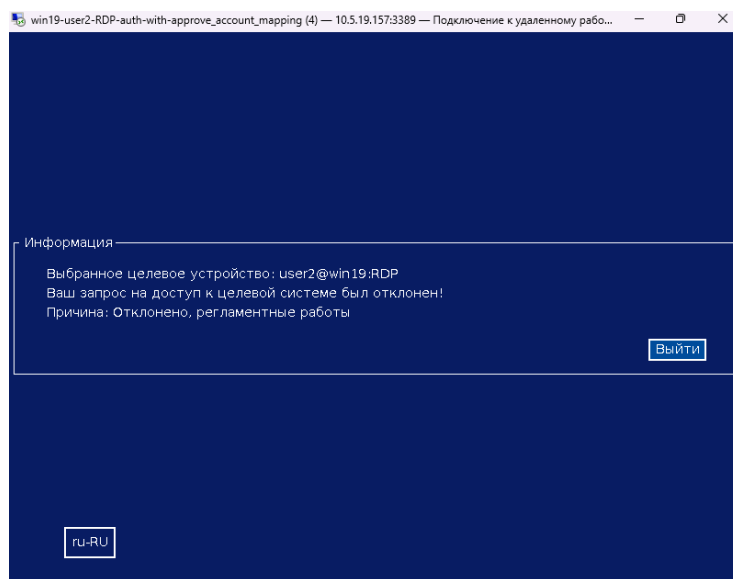




Рисунок 31 - Запрос на доступ отклонен

Для быстрого доступа к целевому устройству (системе) необходимо на странице «Сессии» меню «Мои авторизации» в строке целевого устройства из списка нажать на значок  - элемент управления для организации быстрого доступа к целевому устройству (соединение по протоколу RDP); или нажать на значок  - элемент управления для организации быстрого доступа к целевому устройству (соединение по протоколу SSH).

Двойным нажатием на скачанный файл запускается процесс авторизации. Его отличие от предыдущего варианта авторизации заключается в том, что авторизация выполняется, минуя

авторизацию на СКДПУ, а также, авторизация на целевом устройстве (системе) должна быть выполнена в течение 30 секунд с момента ее инициации, в противном случае, доступ к целевому устройству будет запрещен.

3.3.2. Авторизация пользователя на СКДПУ через клиент удаленного доступа PuTTY

Для доступа к СКДПУ из командной строки терминала клиента удаленного доступа PuTTY (протокол подключения SSH) следует выполнить следующие действия.

Шаг 1. Осуществить запуск клиента удаленного доступа (см. рисунок 32).

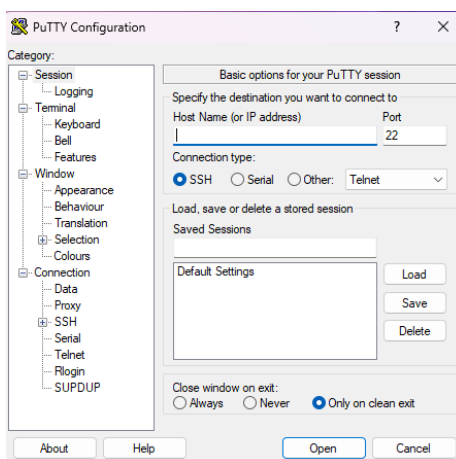


Рисунок 32 - Интерфейс клиента PuTTY

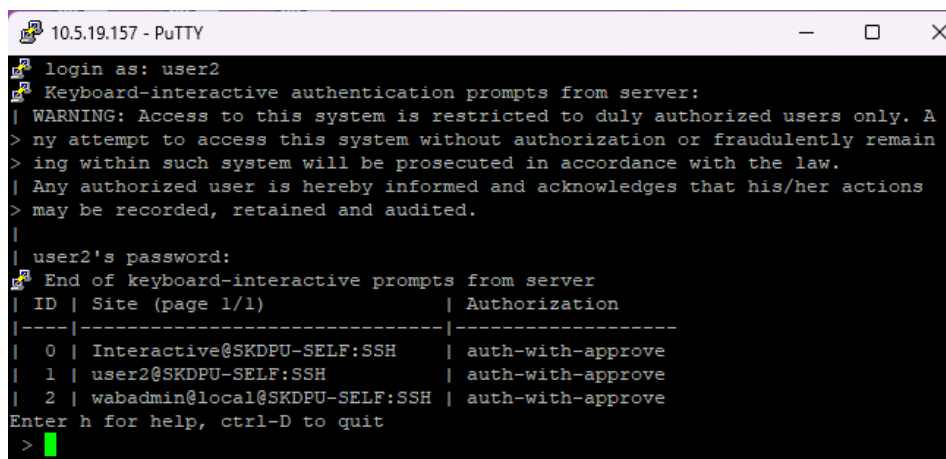
Шаг 2. В поле «Host Name (or IP address)» ввести IP-адрес СКДПУ, в поле «Port» задать значение параметра - 22 и нажать кнопку «Open».

В результате данных действий откроется окно клиента с приглашением ввести логин пользователя (см. рисунок 33).



Рисунок 33 - Окно клиента с приглашением ввести логин пользователя

Шаг 3. Ввести логин пользователя, задействовать клавишу Enter (в результате выполненных действий в окне клиента отобразится предупреждение и приглашение ввести пароль); далее следует ввести пароль и задействовать клавишу Enter; при корректно введенных параметрах будет выполнена авторизация пользователя на СКДПУ (см. рисунок 34).



```

10.5.19.157 - PuTTY
login as: user2
Keyboard-interactive authentication prompts from server:
| WARNING: Access to this system is restricted to duly authorized users only. A
| ny attempt to access this system without authorization or fraudulently remain
| ing within such system will be prosecuted in accordance with the law.
| Any authorized user is hereby informed and acknowledges that his/her actions
| may be recorded, retained and audited.
|
| user2's password:
End of keyboard-interactive prompts from server
| ID | Site (page 1/1) | Authorization
|----|-----|-----
| 0 | Interactive@SKDPU-SELF:SSH | auth-with-approve
| 1 | user2@SKDPU-SELF:SSH | auth-with-approve
| 2 | wabadmin@local@SKDPU-SELF:SSH | auth-with-approve
Enter h for help, ctrl-D to quit
>

```

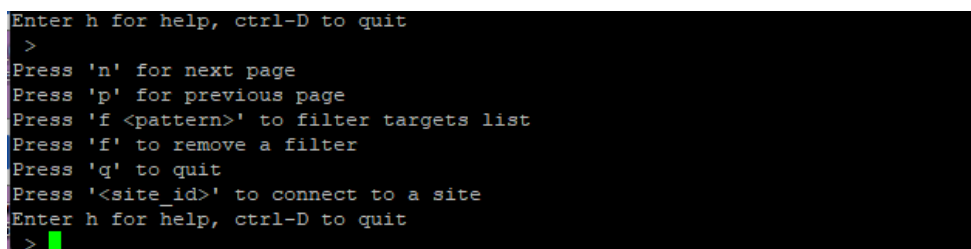
Рисунок 34 - Интерфейс СКДПУ при авторизации пользователя с клиента

Пользователю в табличном виде будет отображен список целевых устройств, где полях записей представлены:

- «ID» - идентификационный номер (идентификатор) целевого устройства;
- «Site» - условное наименование целевого устройства;
- «Authorization» - условное наименование авторизации.

Также отобразятся подсказки по получению справочной информации и порядку выхода из сеанса СКДПУ.

Для получения справочной информации в окне клиента следует ввести h (см. рисунок 35).



```

Enter h for help, ctrl-D to quit
>
Press 'n' for next page
Press 'p' for previous page
Press 'f <pattern>' to filter targets list
Press 'f' to remove a filter
Press 'q' to quit
Press '<site_id>' to connect to a site
Enter h for help, ctrl-D to quit
>

```

Рисунок 35 - Справка по командам СКДПУ

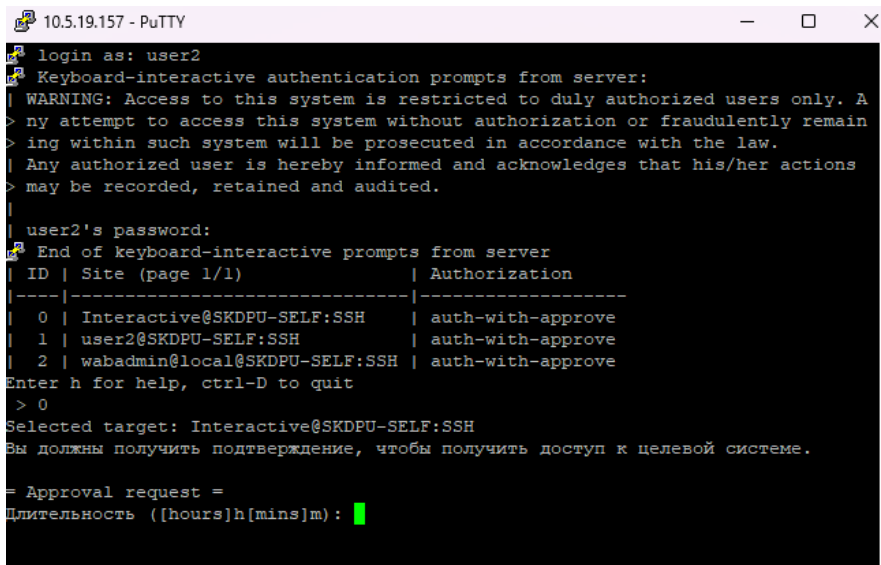
Команды СКДПУ предназначены для выполнения следующих задач:

- n – перейти к следующей странице списка;
- p – перейти к предыдущей странице списка;
- f – поиск контекста в списке по комбинации символов;
- q – закрыть сеанс клиента удаленного доступа;
- <site id> – переход (переход к процедуре авторизации) на целевое устройство по его идентификатору;
- <ctrl-D> – комбинация клавиш для закрытия сеанса клиента удаленного доступа.

3.4. Доступ к целевым устройствам через клиент удаленного доступа PuTTY

Для доступа к целевому устройству окне клиента следует ввести его идентификатор и нажать клавишу Enter.

В случае, если администратором СКДПУ не выполнены разрешения на доступ пользователя к данному целевому устройству (системе), то ему отобразится соответствующее предупреждение и будет предложено сформировать запрос на разрешение (см. рисунок 36).



```
10.5.19.157 - PuTTY
login as: user2
Keyboard-interactive authentication prompts from server:
| WARNING: Access to this system is restricted to duly authorized users only. A
| ny attempt to access this system without authorization or fraudulently remain
| ing within such system will be prosecuted in accordance with the law.
| Any authorized user is hereby informed and acknowledges that his/her actions
| may be recorded, retained and audited.
|
| user2's password:
End of keyboard-interactive prompts from server
| ID | Site (page 1/1) | Authorization
|----|-----|-----
| 0 | Interactive@SKDPU-SELF:SSH | auth-with-approve
| 1 | user2@SKDPU-SELF:SSH | auth-with-approve
| 2 | wabadmin@local@SKDPU-SELF:SSH | auth-with-approve
Enter h for help, ctrl-D to quit
> 0
Selected target: Interactive@SKDPU-SELF:SSH
Вы должны получить подтверждение, чтобы получить доступ к целевой системе.
= Approval request =
Длительность ([hours]h[mins]m): █
```

Рисунок 36 - Предупреждение о необходимости сформировать запрос на подтверждение доступа к целевому устройству

Для формирования запроса на подтверждение доступа к целевому устройству следует выполнить следующие действия.

Шаг 1. Ввести запрашиваемую длительность времени на доступ к целевому устройству в часах и (или) минутах в формате <часы>h<минуты>m, нажать клавишу Enter. Система отслеживает формат введенного параметра и при некорректном вводе выдает пользователю соответствующее предупреждение.

Шаг 2. Ввести условное наименование задачи (позиция в окне клиента «Заявка»), в рамках которой планируется доступ к целевому устройству, нажать клавишу Enter.

Шаг 3. При необходимости, в позиции «Описание (optional)» ввести описание планируемого подключения, иную информацию, нажать клавишу Enter.

В результате выполненных действий будет сформирован запрос на доступ к целевому устройству (см. рисунок 37).

```

10.5.19.157 - PuTTY
> ny attempt to access this system without authorization or fraudulently remain
> ing within such system will be prosecuted in accordance with the law.
> | Any authorized user is hereby informed and acknowledges that his/her actions
> may be recorded, retained and audited.
> |
> | user2's password:
> | End of keyboard-interactive prompts from server
> | ID | Site (page 1/1) | Authorization
> |-----|-----|-----|
> | 0 | Interactive@SKDPU-SELF:SSH | auth-with-approve
> | 1 | user2@SKDPU-SELF:SSH | auth-with-approve
> | 2 | wabadmin@local@SKDPU-SELF:SSH | auth-with-approve
> Enter h for help, ctrl-D to quit
> 0
Selected target: Interactive@SKDPU-SELF:SSH
Вы должны получить подтверждение, чтобы получить доступ к целевой системе.

= Approval request =
Длительность ([hours]h[mins]m): 1h30m
Заявка: qwe-55
Описание (optional): Test
Ваш запрос на доступ ожидает обработки.

```

Рисунок 37 - Сформирован запрос на подтверждение доступа к целевому устройству; ожидает обработки

В случае отклонения запроса на подтверждение доступа к целевому устройству администратором СКДПУ пользователю отобразится соответствующее уведомление (см. рисунок 38) и приглашение сформировать запрос повторно.

```

Ваш запрос на доступ к целевой системе был отклонен!
Причина: Идут регламентные работы. Запрос отклонен.

Вы должны получить подтверждение, чтобы получить доступ к целевой системе.

= Approval request =
Длительность ([hours]h[mins]m):

```

Рисунок 38 - Запрос на подтверждение доступа к целевому устройству отклонен

В случае положительного решения на подтверждение доступа к целевому устройству администратором СКДПУ пользователю, в зависимости от настроек авторизации на целевом устройстве, может быть предоставлен либо доступ к целевому устройству (без авторизации) либо будет предоставлена возможность осуществить доступ путем прохождения авторизации на целевом устройстве (вторичная авторизация, см. рисунок 39).

```

= Approval request =
Длительность ([hours]h[mins]m): 1h30m
Заявка: qwe-55
Описание (optional): Test
Ваш запрос на доступ ожидает обработки.

Account successfully checked out

Connecting to Interactive@SKDPU-SELF:SSH...
Target login:

```

Рисунок 39 - Запрос на подтверждение доступа к целевому устройству удовлетворен; необходимо пройти авторизацию на целевом устройстве.

Для авторизации на целевом устройстве следует в позиции «Target login» ввести логин, нажать клавишу Enter, затем в позиции «password» ввести пароль и нажать клавишу Enter.

В случае успешной авторизации пользователь осуществит вход на целевое устройство.

В случае заданного администратором СКДПУ количества неудачных попыток авторизации на целевом устройстве сессия клиента удаленного доступа будет закрыта.

Для возобновления авторизации на целевом устройстве пользователю необходимо повторно выполнить процедуру авторизации на СКДПУ и целевом устройстве.

4. ДЕЙСТВИЯ В НЕШТАТНЫХ СИТУАЦИЯХ

4.1. Проблемы, связанные с входом в систему

Причины, связанные с входом целевую систему, могут быть следующими:

Проблема	Возможное решение
Служба СКДПУ недоступна	Перезагрузить систему командой reboot
Введен неверный идентификатор и/или пароль пользователя	Необходимо обратиться к администратору с запросом о смене пароля
Целевое устройство недоступно	Убедиться, что целевое устройство функционирует
Неверный пароль целевой учетной записи	Проверить корректность вводимого пароля целевой учетной записи
Пользователь не прошел авторизацию для доступа к целевой учетной записи	Обратиться к администратору с запросом исправить права доступа для выбранной авторизации, куда входит пользователь, (раздел Авторизации > Управление авторизациями)
Попытка входа в систему вне периода времени, определенного авторизацией	Следует использовать доступ с подтверждением
Протокол не авторизован	Указать для выбранного целевого устройства требуемый протокол соединения (раздел Ресурсы > Устройства)
Достигнуто максимальное количество одновременных авторизованных подключений	Обратиться к администратору с запросом о возможном отключении отдельных пользователей

4.2. Возможные проблемы при автоматизированном сеансе SSH

На некоторых целевых платформах символы, используемые целевым устройством, не отображаются на экране и не выводятся при нажатии соответствующих клавиш.

Данная проблема зарегистрирована, в частности, на следующих целевых платформах:

- Серверы Telnet Open Solaris;
- Серверы Telnet Solaris 8.

Для решения этой проблемы следует выполнить следующие действия:

Шаг 1. Ввести команду для удаления выделения псевдотерминала (tty):

```
$ ssh -T root@obelix:martin@wab.mycorp.lan  
root@obelix:martin@wab.mycorp.lan's password:
```

Шаг 2. В ОС Windows, запустить «PuTTY», перейти в подменю **SSH > TTY**, снять флажок **Don't allocate a pseudo-terminal** (см. рисунок 40).

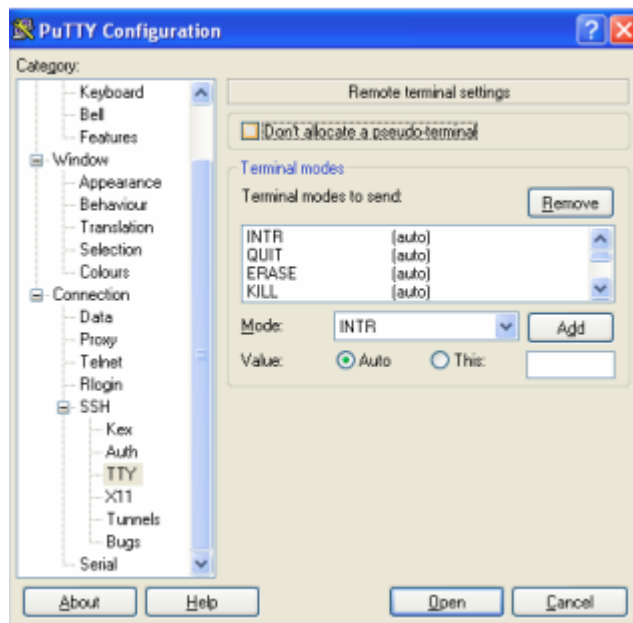


Рисунок 40 - Настройки PuTTY

ПРИЛОЖЕНИЕ 1

Примеры генерации и использования SSH-ключей

1) Генерирование ключей в ОС Linux

Для того, чтобы сгенерировать и использовать ключи с OpenSSH в ОС Linux, следует выполнить следующие действия:

Примечание. Можно использовать файл `~/.ssh/id_rsa` - файл идентификации, по умолчанию используемый всеми командами OpenSSH. В этом случае, если файл уже существует, следует пропустить первые два шага, описанные в данном разделе, и импортировать файл `~/.ssh/id_rsa.pub` в СКДПУ (см. п.1.7.3 Загрузка открытого ключа SSH). В приведенном примере файл идентификации закрытого ключа имеет имя `wab_rsa2048`, однако возможно использовать любое другое допустимое имя файла. Рекомендуется сохранить данный ключ в каталоге `.ssh` файла HOME.

Шаг 1. На терминале выполнить следующую команду, чтобы сгенерировать пару открытого и закрытого ключей (см. рисунок 1):

```
$ ssh-keygen -t rsa -f ~/.ssh/wab_rsa2048
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/martin/.ssh/
wab_rsa2048.
Your public key has been saved in /home/martin/.ssh/
wab_rsa2048.pub.
```

Рисунок 1 - Генерирование открытого и закрытого ключей SSH

Также можно изменить размер ключа с помощью параметра `-b size`. По умолчанию ключ RSA в текущей версии `ssh-keygen` имеет размер 2048 бит, что подходит для большинства случаев.

Шаг 2. Импортируйте файл `~/.ssh/wab_rsa2048.pub` в СКДПУ (см. п.1.7.3 Загрузка открытого ключа SSH).

Шаг 3. Если агент проверки подлинности не используется, то команды SSH, SCP и SFTP будут напрямую использовать ключ идентификации по умолчанию `~/.ssh/id_rsa` либо закрытый ключ, который обращается к данному аргументу при помощи параметра `-i key`, например (см. рисунок 2):

```
$ ssh -t -i ~/.ssh/wab_rsa2048 martin@wab.mycorp.lan
root@asterix:SSH_22
Enter passphrase for key '/home/martin/.ssh/wab_rsa2048':
```

Рисунок 2 - Генерирование открытого и закрытого ключей SSH

Шаг 4. Если используется агент проверки подлинности, то закрытый ключ необходимо импортировать при каждом перезапуске данного агента (см. рисунок 3):

```
$ ssh-add ~/.ssh/wab_rsa2048
Enter passphrase for /home/martin/.ssh/wab_rsa2048:
Identity added: /home/martin/.ssh/wab_rsa2048 (/home/
martin/.ssh/wab_rsa2048)
```

Рисунок 3 - Импорт закрытого ключа SSH при перезапуске агента

Шаг 5. Затем необходимо войти в прокси SSH, не вводя пароль еще раз и не используя аргумент `-i` в командной строке (SSH автоматически использует все идентификационные данные, добавленные в агент).

Шаг 6. Вход в систему SSH осуществляется согласно инструкциям, приведенным в разделе Вход в систему по SSH.

2) Генерирование ключей в ОС Windows

Чтобы сгенерировать и использовать ключи SSH с помощью «PuTTY» в ОС Windows, необходимо выполнить следующие действия:

Шаг 1. В Windows открыть меню Пуск и запустить «PuTTY».

Шаг 2. Перейти в меню Settings (Настройки) и изменить параметры указанным ниже образом, чтобы сгенерировать 2048-битный ключ SSH-2 RSA (см. рисунок 4):



Рисунок 4 - Генерирование ключа SSH в «PuTTY»

– в разделе **Parameters** (Параметры) установить переключатель в положение **SSH-2 RSA**;

– в поле **Number of bit in a generated key** (Количество бит для генерации ключа) указать значение **2048**.

Примечание. В данном примере файл идентификации закрытого ключа имеет имя `wab_rsa2048`, однако возможно использовать любое другое допустимое имя файла.

Шаг 3. Нажать кнопку **Generate** (Сгенерировать) и сдвинуть указатель «мыши» в любую сторону для того, чтобы ускорить процесс и сделать его менее предсказуемым.

Шаг 4. После того, как «PuTTY» сгенерирует ключ, необходимо ввести выбранный пользователем пароль в поле **Key passphrase** и подтверждение пароля в поле **Confirm passphrase**, а также можно ввести краткий комментарий в поле **Key comment** (см. рисунок 5)



Рисунок 5 - Подтверждение сгенерированного в «PuTTY» ключа

Шаг 5. Нажать кнопку **Save public key** (Сохранить открытый ключ) и сохранить ключ в пользовательском каталоге, например, `My Documents\wab_rsa2048.ppk`.

Шаг 6. В поле **Public key for pasting into OpenSSH authorized_keys file** необходимо выделить весь текст (с помощью контекстного меню или сочетания клавиш `CTRL +A`), скопировать выделенный текст в буфер обмена (с помощью контекстного меню или сочетания клавиш `CTRL+C`).

Шаг 7. В Windows открыть меню Пуск и запустить «Блокнот», для создания пустого текстового документа.

Шаг 8. Вставить сохраненный в буфере обмена текст в созданный документ (с помощью контекстного меню или сочетания клавиш `CTRL+V`).

Шаг 9. Сохранить документ с открытым ключом, например, `My Documents \wab_rsa2048.ppk.txt`, а затем закрыть «PuTTY» и «Блокнот».

Шаг 10. Импортировать файл открытого ключа в СКДПУ (см. п.1.7.3 Загрузка открытого ключа SSH).

Шаг 11. Импортировать закрытый ключ в клиент SSH. Закрытый ключ возможно использовать для входа в систему одним из следующих способов:

– **При проверке подлинности «Pageant»:**

Шаг 1. Запустите приложение «Pageant» в меню Пуск, если оно не было запущено, а затем дважды нажмите на значок «Pageant» в области уведомлений на панели задач ОС Windows.

Шаг 2. Откроется окно «Pageant Key List» (см. рисунок 6).

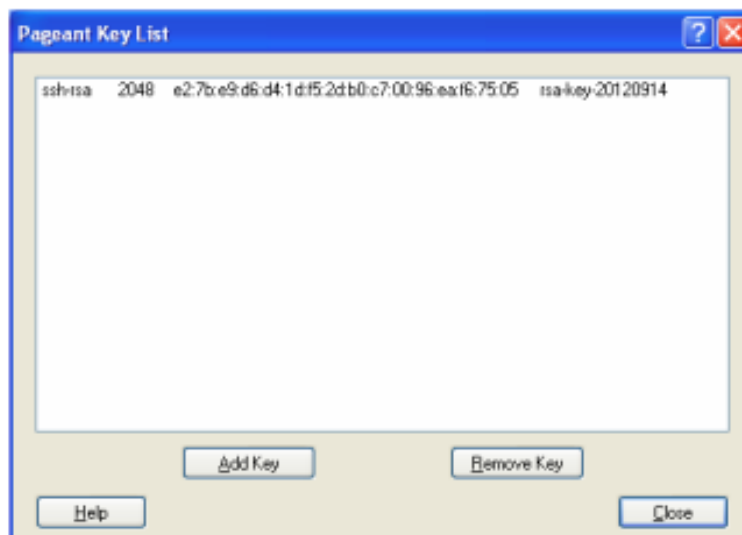


Рисунок 6 - Проверка подлинности «Pageant»

Шаг 3. Нажмите кнопку **Add Key** (Добавить ключ) и выберите файл закрытого ключа (`My Documents \wab_rsa2048.ppk`).

После выполненных действий возможно получить доступ к прокси-серверу с помощью «PuTTY», «PSCP», «PSFTP», «Filezilla» или «WinSCP» (если параметры последнего не запрещают использовать проверку подлинности «Pageant»).

Примечание. Ключ также можно добавить двойным нажатием на имени файла закрытого ключа в Проводнике. Для этого тип файлов с расширением `.ppk` сначала необходимо связать с «Pageant».

– **При использовании «PuTTY» в «Pageant»:**

Шаг 4. Откройте меню Пуск и запустите PuTTY. В дереве параметров конфигурации следует выбрать `Connection > SSH > Auth`, в разделе **Authentication parameters**, нажать кнопку **Обзор** и выбрать файл закрытого ключа (`My Documents \wab_rsa2048.ppk`).

Примечание. Для повторного использования необходимо сохранить настройки сеанса.

– При использовании «FileZilla» в «Pageant»:

Шаг 5. Запустите «FileZilla», откройте меню Edit > Settings и выберите страницу SFTP. Нажмите Add keyfile... и выберите файл закрытого ключа (My Documents\wab_rsa2048.ppk) (см. рисунок 7).

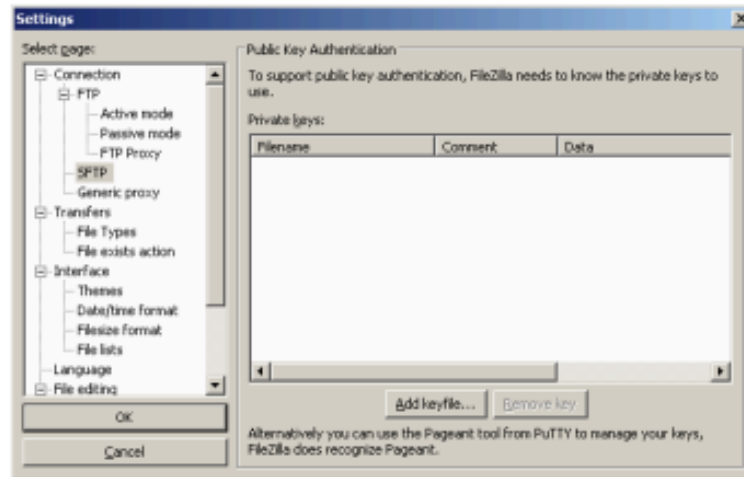


Рисунок 7 - Проверка подлинности «FileZilla»

– При использовании «WinSCP» в «Pageant»:

Шаг 6. Запустите «WinSCP», на странице параметров сеанса (см. рисунок 47) нажмите кнопку в поле Private key file и выберите файл My Documents \wab_rsa2048.ppk.

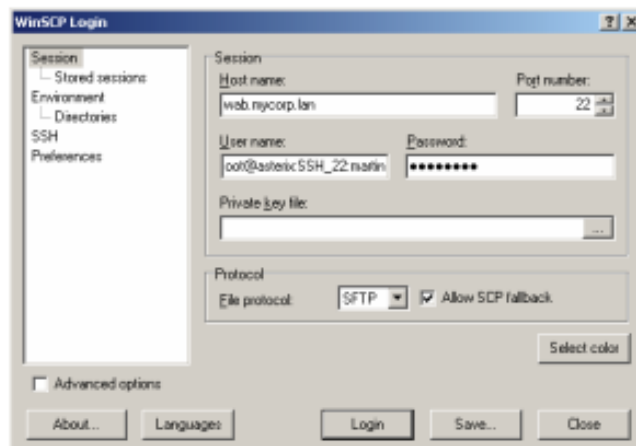


Рисунок 8 - Настройка параметров сеанса WinSCP

Выполните процедуру входа в систему по SSH.

– При использовании PSCP или PSFTP без «Pageant»:

Шаг 1. Добавьте в командную строку параметр -i key (см. рисунок 48):

```
$ pscp -scp -i "C:\Documents and Settings\martin\My
Documents\wab_rsa2048.ppk
myfile martin@wab.mycorp.lan:root@asterix:SSH_22:/tmp
Passphrase for key "rsa-key-20120914":
```

Рисунок 9 - Использование PSCP без «Pageant»

Выполните процедуру входа в систему по SSH.

ПРИЛОЖЕНИЕ 2

Вход в систему и способы переноса файловой информации между АРМ пользователя и целевыми устройствами

1. Вход в систему по SSH

SSH распределен на подсистемы:

- SSH_SHELL_SESSION - запуск сеанса оболочки;
- SSH_SCP_UP - перемещение файлов на целевое устройство;
- SSH_SCP_DOWN - перемещение файлов с целевого устройства;
- SFTP_SESSION - двунаправленная передача файлов посредством SFTP;
- SSH_REMOTE_COMMAND - выполнение удаленных команд;
- SSH_X11_SESSION - настройка перенаправления на АРМ отображения результатов

выполнения команд или приложений на целевом устройстве, имеющих графическую часть вывода для протокола SSH.

Каждой из этих подсистем требуется отдельный вид авторизации в СКДПУ.

Примечание. Если у пользователя нет прав на доступ к необходимой подсистеме, то функции запуска удаленного сеанса оболочки или передачи файла могут быть недоступны. Некоторые клиенты также требуют авторизации SSH_SHELL_SESSION для отображения списка каталогов, если используются в режиме SCP. Подпротоколы SCP и SFTP будут работать, только если для целевой учетной записи включена функция автоматического входа в систему, поскольку данные протоколы не позволяют ввести дополнительный пароль в интерактивном режиме.

1.1 Вход в систему по SSH с рабочей станции Unix/Linux

1.1.1 Сеанс оболочки

Для входа в СКДПУ следует выполнить команду:

```
$ ssh -t martin@wab.mycorp.lan root@asterix:SSH_22  
martin@wab.mycorp.lan's password:
```

где

`martin` - пользователь, настроенный в СКДПУ с авторизацией SSH_SHELL_SESSION;

`wab.mycorp.lan` - полное доменное имя СКДПУ;

`root@asterix:SSH_22` - целевая учетная запись, устройство и служба.

Примечание. В зависимости от настроек устройства, заданных администратором, для пользователей может отображаться запрос на проверку подлинности для входа в `root@asterix:SSH_22`.

Далее на приглашение системы следует ввести пароль доступа пользователя.

1.1.2 Удаленное выполнение команд

СКДПУ позволяет удаленно выполнять команды на одном или нескольких компьютерах при наличии у пользователя прав на использование SSH_REMOTE_COMMAND.

```
$ ssh martin@wab.mycorp.lan root@asterix:SSH_22 halt.  
martin@wab.mycorp.lan's password:
```

Команда `halt` выполняется на компьютере **asterix**, затем начинается сеанс оболочки.

Далее на приглашение системы следует ввести пароль доступа пользователя.

1.1.3 Вход без ввода имени целевого объекта

СКДПУ может отобразить список устройств, доступных пользователю, для этого следует ввести команду

```
$ ssh -t martin@wab.mycorp.la  
martin@wab.mycorp.lan's password:  
| ID | Site  
|----|-----  
| 0  | root@centos:SSH_22  
| 1  | root@asterix:SSH_22  
Connect to (ctrl-D to quit):
```

Для того чтобы выбрать целевой объект, следует ввести его номер.

1.1.4 Перенос файлов с помощью SCP

Для переноса файлов с помощью SCP необходимо выполнить следующие команды:

```
$ scp myfile martin@wab.mycorp.lan:root@asterix:SSH_22:/tmp  
martin@wab.mycorp.lan's password:
```

где

`martin` - пользователь, настроенный в СКДПУ, с авторизацией `SSH_SCP_UP`.

`root@asterix:SSH_22:/tmp` - целевая учетная запись, компьютер, служба и каталог.

Далее на приглашение системы следует ввести пароль доступа пользователя.

```
$ scp martin@wab.mycorp.lan:root@asterix:SSH_22:/tmp/myfile /tmp  
martin@wab.mycorp.lan's password:
```

где

`martin` - пользователь, настроенный в СКДПУ, с авторизацией `SSH_SCP_DOWN`.

`root@asterix:SSH_22:/tmp/myfile` - целевая учетная запись, компьютер, служба, каталог и файл.

Далее на приглашение системы следует ввести пароль доступа пользователя.

Примечание. В учетной записи должен быть включен автоматический вход в систему.

1.1.5 Перенос файлов с помощью SFTP

Для переноса файлов с помощью SFTP следует выполнить команду:

```
$ sftp root@asterix:SSH_22:martin@wab.mycorp.lan
Connecting to wab.mycorp.lan...
martin@wab.mycorp.lan's password:
sftp>
```

где

martin - пользователь, настроенный в СКДПУ, с авторизацией SSH_X11_SESSION.
root@asterix:SSH_22 - целевая учетная запись, компьютер и служба.

Параметр -X в командной строке SSH инициирует начало сеанса X11 Forwarding, при этом на рабочей станции будут отображаться графические приложения, выполняемые на целевом устройстве во время данного сеанса.

Далее на приглашение системы следует ввести пароль доступа пользователя.

1.2 Вход в систему по SSH с рабочей станции Windows

1.2.1 Сеанс оболочки и «PuTTY»

Для входа в систему по SSH с рабочей станции Windows необходимо запустить «PuTTY» и выполнить следующие настройки:

Шаг 1. Задать целевое устройство, к которому требуется подключиться, для этого (см. рисунок 1):

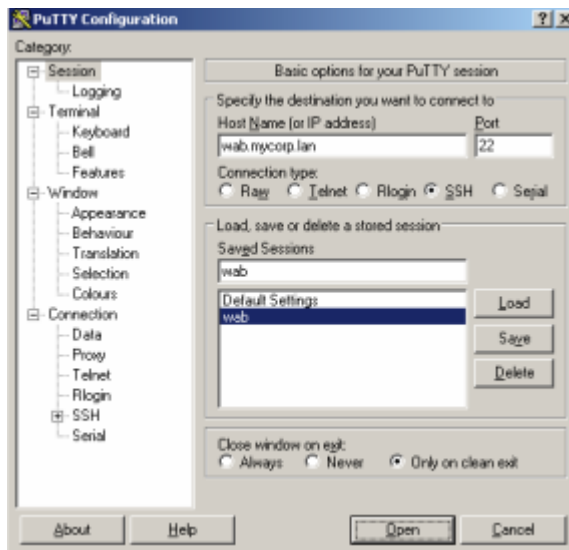


Рисунок 1 - Задание целевого устройства

- В поле **Host Name** следует ввести полное доменное имя СКДПУ;
- В поле **Port** ввести 22 (порт прослушивания прокси SSH СКДПУ).

Шаг 2. Перейти в раздел **Connection > SSH** и ввести имя целевой учетной записи, устройство и службу в поле **Remote command:** (см. рисунок 2).

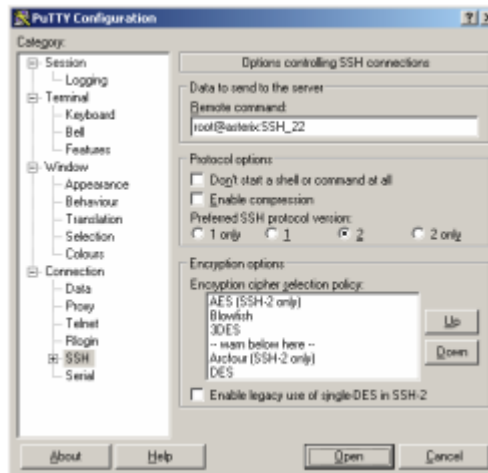


Рисунок 2 - Конфигурирование PuTTY

Далее следует нажать кнопку «Open».

1.2.2 Перенос файлов с помощью PSCP

Переместить файл `myfile` с локальной рабочей станции в каталог `/tmp` с помощью учетной записи `root` на компьютере `asterix` возможно с помощью следующей команды:

```
C:\> pscp -scp myfile martin@wab.mycorp.lan:root@asterix:SSH_22:/tmp
martin@wab.mycorp.lan's password :
```

Далее на приглашение системы следует ввести пароль доступа пользователя.

Примечание. В учетной записи должен быть включен автоматический вход в систему.

1.2.3 Перенос файлов с помощью FileZilla

Для переноса файлов с помощью «FileZilla» необходимо:

Шаг 1. Запустить «FileZilla» и ввести следующую информацию (см. рисунок 3):

- В поле **Host** ввести полное доменное имя СКДПУ;
- В поле **Port** ввести 22 (порт прослушивания TCP прокси SSH);
- В поле **Protocol** выбрать из выпадающего списка тип сервера SFTP - SSH File Transfer Protocol;
- В поле **Logon Type** выбрать из выпадающего списка тип входа в систему Normal;
- В поле **User** ввести данные пользователя в следующем формате:

```
root@asterix:SSH_22: martin
```

где

`martin` - пользователь, настроенный в СКДПУ, с авторизацией `SFTP_SESSION`.

`root@asterix:SSH_22` - целевая учетная запись, компьютер и служба.

- В поле **Password** ввести пароль пользователя СКДПУ.

Шаг 2. Нажать кнопку Connect

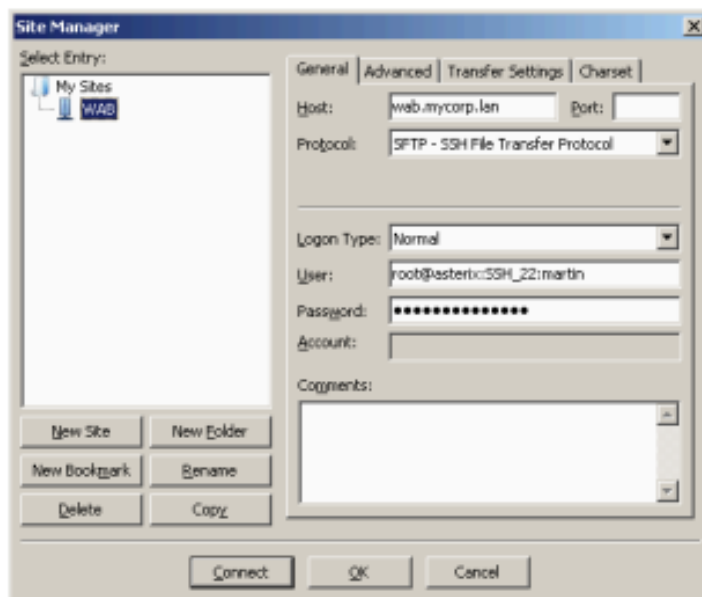


Рисунок 3 - Перенос файлов с помощью FileZilla

1.2.4 Перенос файлов с помощью WinSCP

Для переноса файлов с помощью «WinSCP» необходимо:

Шаг 1. Запустить «WinSCP», перейти в раздел Session и ввести следующую информацию (см. рисунок 4):

- В поле **Host** name ввести полное доменное имя СКДПУ;
- В поле **Port number** выбрать 22 (порт прослушивания TCP прокси SSH);
- В поле **User name** введите данные пользователя в следующем формате:

```
root@asterix:SSH_22: martin
```

где

martin – пользователь, настроенный в СКДПУ, с авторизацией SFTP_SESSION;

root@asterix: SSH_22 – целевая учетная запись, компьютер и служба;

– В поле **Password** ввести пароль пользователя СКДПУ;

– Из выпадающего списка **File protocol** выбрать протокол передачи файлов SFTP.

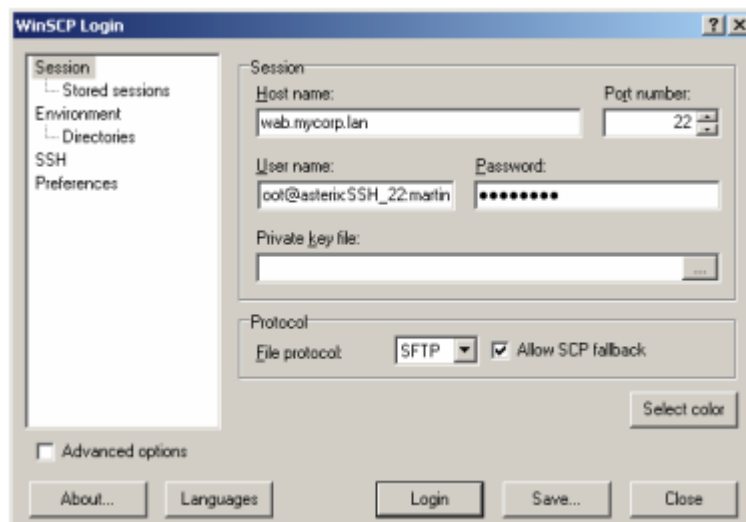


Рисунок 4 - Параметры сессии WinSCP

Шаг 2. Перейти в раздел Preferences > Transfer (см. рисунок 5):

– В разделе **Upload options** установите флаг Ignore permission errors;

– В разделе Common options снять флаг Preserve timestamp.

Примечание. Эти действия необходимо выполнять в указанном выше порядке, т.к. если флаг Preserve timestamp не установлен, параметр Ignore permission errors невозможно изменить.

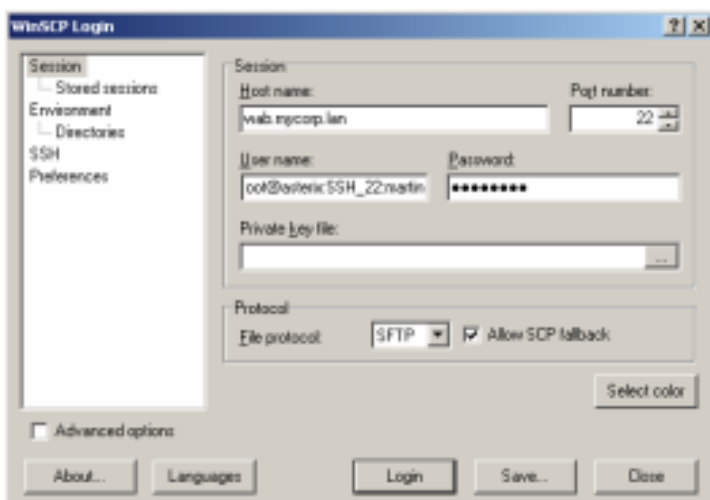


Рисунок 5 - Настройка параметров сеанса WinSCP


2. Вход в систему через RDP

2.1 Вход в систему через RDP с рабочей станции Windows

Запустить сеанс RDP с рабочей станции Windows можно двумя способами: из веб-интерфейса пользователя или напрямую из клиента Terminal Server (Remote desktop connection).

2.1.1 Вход в систему из веб-интерфейса пользователя

Для входа в систему через веб-интерфейс пользователя необходимо:

Шаг 1. Открыть страницу Мои авторизации> Сессии (см. рисунок 6) и для необходимого устройства из списка нажать на значок  для загрузки связанного файла RDP с помощью которого можно войти в прокси СКДПУ RDP и получить доступ к удаленной рабочей станции Windows (см. рисунок 6).

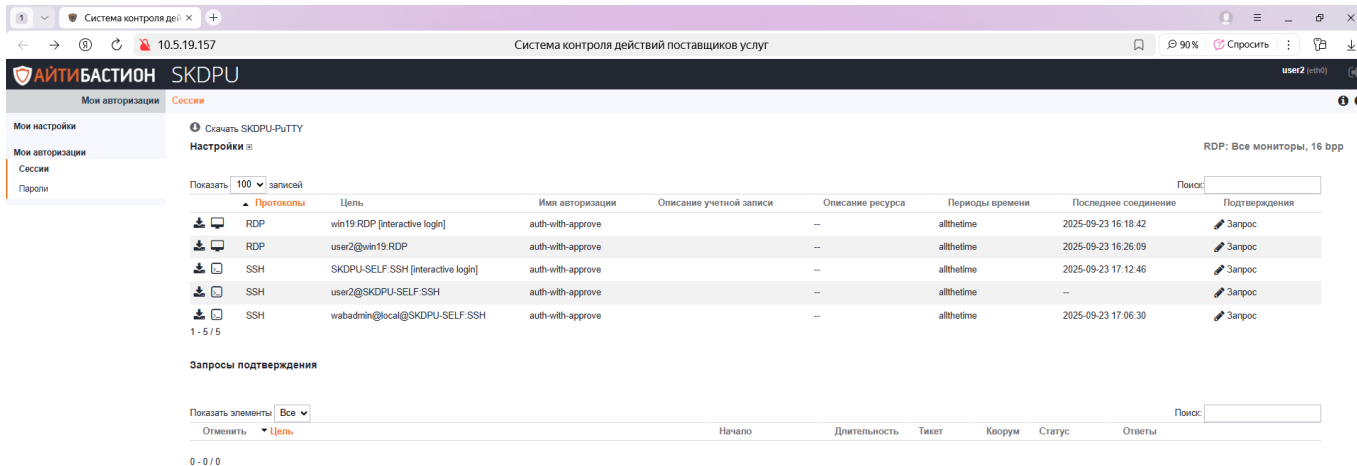


Рисунок 6 - Страница "Сессии"

Шаг 2. Шаг 2. Нажать кнопку Открыть для того, чтобы запустить клиент Terminal Server рабочей станции (см. рисунок 7).

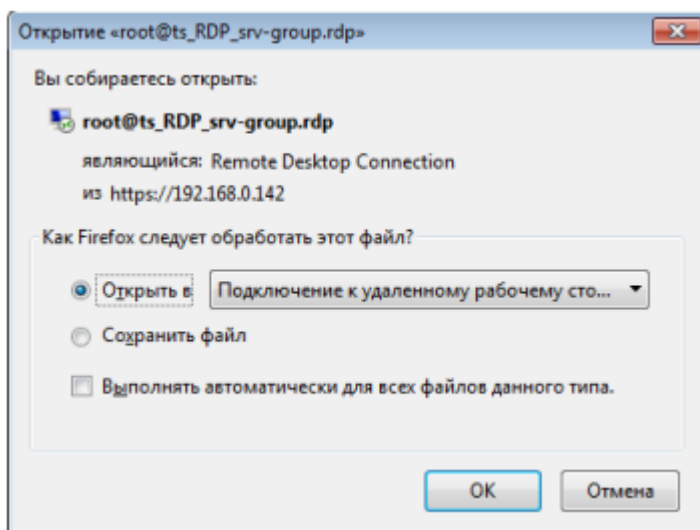


Рисунок 7 - Загрузка связанного файла RDP

Далее следует нажать кнопку «ОК»

2.1.2 Вход в систему из клиента Terminal Server

Для входа в систему с помощью клиента «Terminal Server» необходимо:

Шаг 1. Войти в прокси СКДПУ через клиента «Terminal Server» под именем пользователя

```
administrator@win2003:RDP_3389:martin
```

где

`martin` – пользователь, настроенный в СКДПУ, с авторизацией RDP;
`administrator@win2003:RDP_3389` – целевая учетная запись в СКДПУ, на доступ к которой у пользователя есть права.

Шаг 2. Ввести пароль пользователя и нажать кнопку `Connect` (см. рисунок 8), после чего на экране отобразится сеанс ОС Windows.

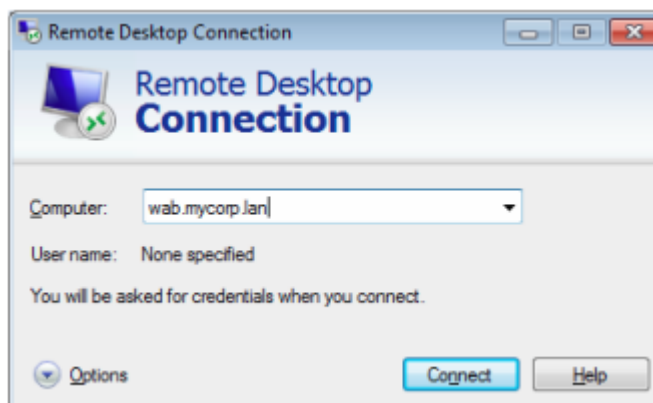


Рисунок 8 - Подключение к удаленной рабочей станции с помощью клиента Terminal Server

Шаг 3. В СКДПУ ввести имя пользователя, после чего откроется промежуточная страница, отображающая список доступных серверов (см. рисунок 9).

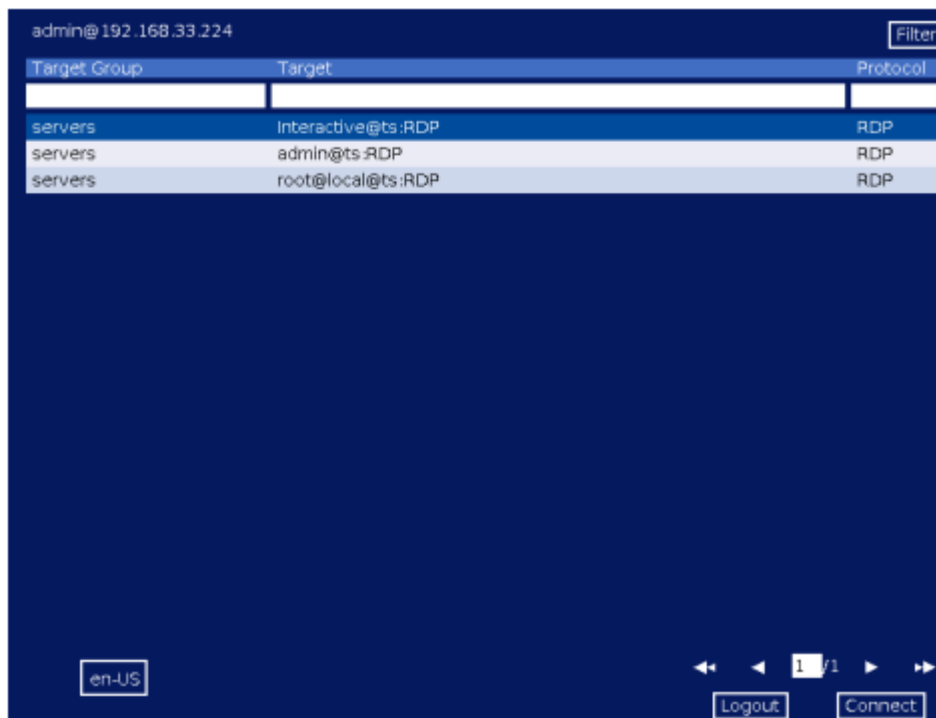


Рисунок 9 - Список доступных устройств

На странице отображены все доступные ресурсы, группа, к которой они принадлежат, тип удаленного сервера (VNC или RDP) и время автоматического прерывания подключения. Если доступный сервер относится к различным группам, в списке отобразится несколько записей для

одного и того же удаленного ресурса. Длинный список можно отфильтровать по группе или учетной записи, чтобы сузить область поиска, для этого выберите (выделенной строкой) нужный сервер и нажмите кнопку Connect для того, чтобы войти на удаленный сервер.

Прежде чем соединение будет фактически установлено, система может отобразить несколько диалоговых окон и/или запросить подтверждение. Это значит, что пользователь получит предупреждение о записи сеанса, о скором истечении срока действия его пароля или о времени автоматического прерывания сеанса.

Примечание. Также можно войти в удаленную консоль, для этого необходимо открыть клиент MSTSC в ОС Windows (меню Пуск > Выполнить) и ввести `mstsc/admin` либо `mstsc/console` в зависимости от используемой версии Windows (`/admin` используется для всех версий, начиная с Windows Vista SP3) (см. рисунок 10).

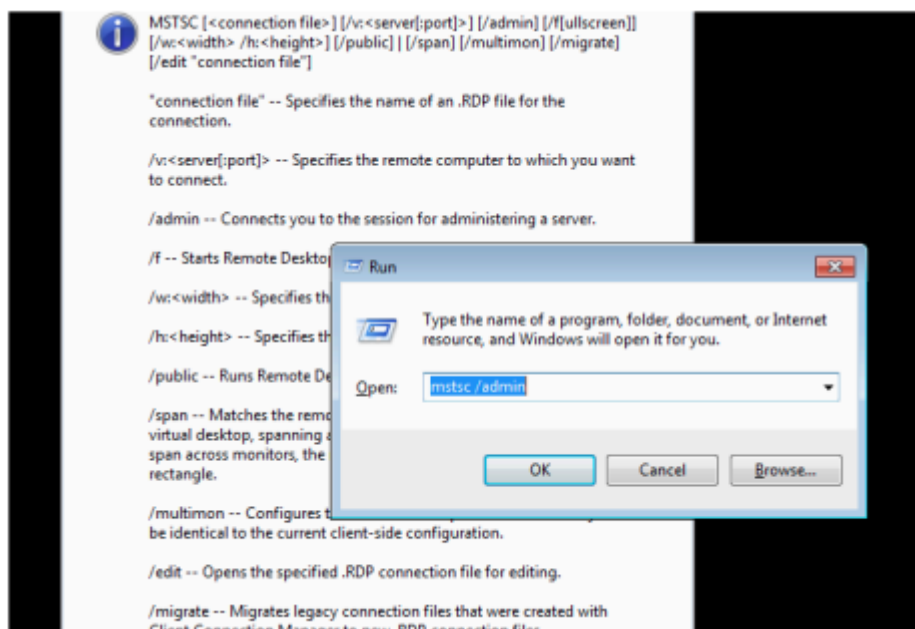


Рисунок 10 - Вход в удаленную консоль с помощью клиента MSTSC

2.1.3 Перенаправление на устройство

Встроенный прокси RDP СКДПУ поддерживает перенаправление на устройство - функцию отображения ресурсов локальной рабочей станции: принтера, каталога, приложения Блокнот и т.п. на рабочей станции в удаленном сеансе Windows.

Эта функция позволяет переносить файлы с одного компьютера с ОС Windows на другой путем перетаскивания, даже в пределах одного сеанса RDP, а также копировать и вставлять текст с локального компьютера на удаленный и наоборот.

Примечание. Данную функцию требуется включить в интерфейсе клиента «Terminal Server».

2.2 Вход в систему через RDP с рабочей станции Linux

Для входа в RDP с рабочей станции в ОС Linux возможно использовать клиент rdesktop RDP или аналогичный ему клиент, для этого:

Шаг 1. Выполнить команду:

```
$rdesktop wab.mycorp.lan
```

где

wab.mycorp.lan - полное доменное имя СКДПУ.

Шаг 2. В открывшемся окне авторизации для сеанса RDP в поле **login** ввести имя пользователя в следующем формате:

```
administrator@win2003:RDP_3389:martin
```

где

martin - пользователь, настроенный в СКДПУ, с авторизацией RDP;

administrator@win2003:RDP_3389- целевая учетная запись в СКДПУ, на доступ к которой у пользователя есть права.

Шаг 3. В поле **password** ввести пароль для пользователя.

Шаг 4. Нажать кнопку ОК для входа в систему удаленной рабочей станции, на экране отобразится сеанс ОС Windows.

Шаг 5. Ввести в командной строке следующую команду:

```
$rdesktop -u administrator@win2003:RDP_3389:martin  
wab.mycorp.lan
```

Ниже приведены параметры, которые могут быть использованы для клиента rdesktop:

-u предназначен для ввода имени пользователя;

-g 1024x768 предназначен для выбора разрешения экрана (разрешение 1024x768 можно заменить на необходимое разрешение);

-a 24 предназначен для выбора глубины цвета (битов на пиксель). Поддерживаемые значения: 8, 15, 16 и 24;

-0 предназначен для подключения к консоли удаленной рабочей станции.

Шаг 6. Для того чтобы установить соединение с удаленной рабочей станцией в окне авторизации следует ввести пароль пользователя и нажать кнопку ОК.

Шаг 7. В СКДПУ ввести имя пользователя, после чего откроется промежуточная страница, отображающая список доступных серверов (см. рисунок 11).

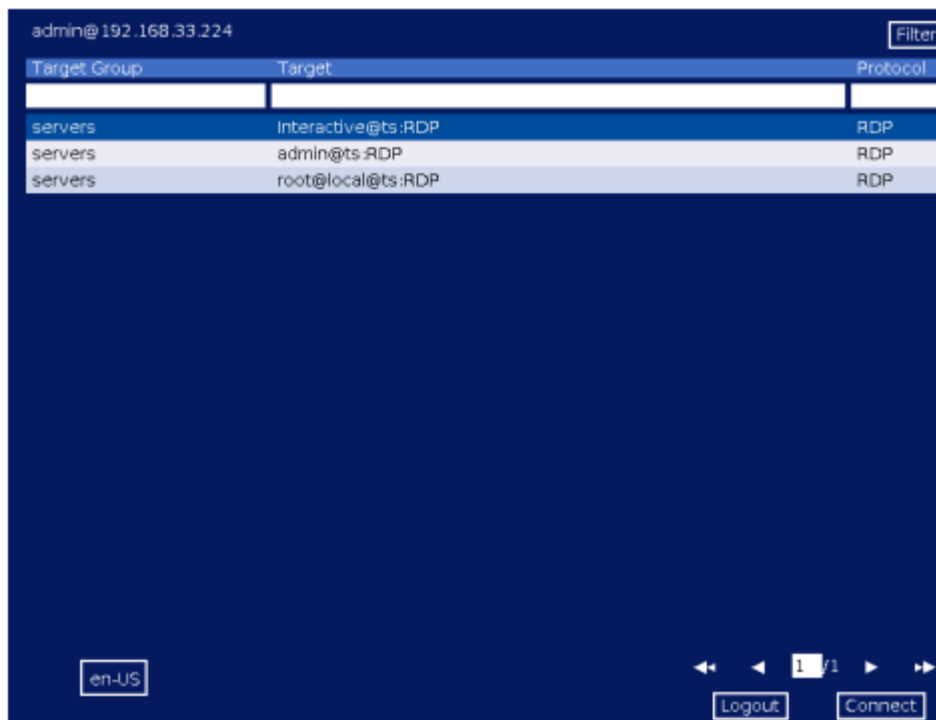


Рисунок 11 - Список доступных устройств

На странице отображены все доступные ресурсы, группа, к которой они принадлежат, тип удаленного сервера (VNC или RDP) и время автоматического прерывания подключения. Если доступный сервер относится к различным группам, в списке отобразится несколько записей для одного и того же удаленного ресурса. Длинный список можно отфильтровать по группе или учетной записи, чтобы сузить область поиска, для этого выберите (выделенной строкой) нужный сервер и нажмите кнопку «Connect» для того, чтобы войти на удаленный сервер.

Прежде чем соединение будет фактически установлено, система может отобразить несколько диалоговых окон и/или запросить подтверждение. Это значит, что пользователь получит предупреждение о записи сеанса, о скором истечении срока действия его пароля или о времени автоматического прерывания сеанса.

ПЕРЕЧЕНЬ ТЕРМИНОВ

Автоматизированная система	Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
Авторизация	Предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом
Аудит	Проверка данных на предмет соответствия критериям качества и безопасности их сбора, хранения и дальнейшего использования
Аутентификация	Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации
Вторичная авторизация	Получение доступа пользователем к целевому устройству после первичной авторизации
Домен	Область пространства доменных имен, включающая информационные системы, в том числе содержащие данные о доменных именах, выделенных в домене, в том числе в Интернете
Идентификация	Процесс установления соответствия между чем-то (объектом, человеком, процессом) и его именем или уникальным идентификатором, позволяющий отличить его от других подобных объектов
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Информационная технология	Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных
Ключ	Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор

одного преобразования из совокупности всевозможных для данного алгоритма преобразований

Критически важные объекты	Объекты, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики страны, субъекта или административно-территориальной единицы или к существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях длительный период времени
Логин	Уникальное имя пользователя (идентификатор) для входа в компьютерные системы, приложения и онлайн-сервисы
Локальная проверка подлинности	Проверка подлинности, управляемая СКДПУ
Пароль	Идентификатор субъекта доступа, который является его (субъекта) секретом
Парольная политика	Набор правил, определяющих требования к паролям и способам их создания и изменения, а также правила использования паролей в информационной системе
Первичная авторизация	Получение доступа пользователем к СКДПУ
Персональные данные	Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)
Профиль пользователя	Набор настроек и информации, связанных с пользователем
Сессия (пользовательская сессия)	Временной период взаимодействия пользователя с системой, приложением или сайтом
Событие безопасности	Идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее

неизвестную ситуацию, которая может быть значимой для безопасности информации

Учетная запись (аккаунт)	Совокупность данных субъекта, хранимая в компьютерной системе (приложении, онлайн-сервисе), необходимая для его опознавания (идентификации и аутентификации), предоставления доступа и использования им данной компьютерной системы
Целевая система	Операционная система, функционирующая на целевом устройстве
Целевая учетная запись (аккаунт)	Совокупность данных, которая позволяет целевой системе распознавать пользователя и предоставлять ему доступ к определенным функциям или данным
Целевое устройство	Устройство, к которому осуществляется доступ через СКДПУ
IP-адрес	Уникальный числовой идентификатор устройства в компьютерной сети
SSH2	Вторая версия протокола SSH, являющаяся текущим стандартом, используемая для создания безопасного зашифрованного соединения между компьютерами по незащищенной сети

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИТ	Информационные технологии
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
СКДПУ	Программный комплекс «Система контроля действий поставщиков ИТ-услуг»
AD	Active Directory – службы каталогов корпорации Microsoft для операционных систем семейства Windows Server
CSV	Comma-Separated Values – текстовый формат, предназначенный для представления табличных данных
GPG	GNU Privacy Guard (GnuPG, GPG) – свободная программа для шифрования информации и создания электронных цифровых подписей
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
ID	IDentifier – идентификатор
LAN	Local Area Network – компьютерная сеть, которая соединяет компьютеры на ограниченной территории
LDAP	Lightweight Directory Access Protocol – протокол прикладного уровня, который используется для доступа к службам каталогов
OCR	Optical Character Recognition – механический или электронный перевод изображений рукописного, машинописного или печатного текста в текстовые данные – последовательность кодов, использующихся для представления символов в компьютере (например, в текстовом редакторе)
OpenSSH	Open Secure Shell – набор программ, предоставляющих шифрование сеансов связи по компьютерным сетям с использованием протокола SSH
RDP	Remote Desktop Protocol, протокол удаленного рабочего стола
RLOGIN	Remote LOGIN (удаленный вход в систему)

RSA	RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел
SCP	Secure Copy Protocol — утилита и протокол копирования файлов между компьютерами, использующий, в отличие от утилиты RCP, в качестве транспорта не RSH, а зашифрованный
SFTP	SSH File Transfer Protocol — протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надежного и безопасного соединения
SSH	Secure SHell (безопасная оболочка), протокол защищенной передачи данных
TCP	Transmission Control Protocol (TCP, протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета
TELNET	TErminaL NETwork – сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP)
TLS	Transport Layer Security – протокол защиты транспортного уровня
VNC	Virtual Network Computing – система удаленного доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удаленный кадровый буфер)

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 - Окно авторизации СКДПУ	11
Рисунок 2 - Авторизация пользователя СКДПУ	11
Рисунок 3 - Главная страница СКДПУ	13
Рисунок 4 - Страница «Мои настройки»	14
Рисунок 5 - Страница «Мои настройки», область GPG-ключ	16
Рисунок 6 - Страница «Сессии»	16
Рисунок 7 - Настройка параметров клиентского окна (окон) при доступе к целевым устройствам по протоколу RDP	17
Рисунок 8 - Окно запроса разрешения на доступ к целевому устройству	18
Рисунок 9 - Страница «Сессии»; сформированный запрос находится в статусе «Ожидает»	19
Рисунок 10 - Страница «Сессии»; сформированный запрос находится в стадии «Принято»	20
Рисунок 11 - Параметры текущего запроса	20
Рисунок 12 - Отмена запроса разрешения	21
Рисунок 13 - Страница «Сессии»; статус запроса – «Отменено»	21
Рисунок 14 - Страница «Пароли»	22
Рисунок 15 - Страница «Пароли»; уведомление о необходимости получить подтверждение для доступа к целевому устройству (для отображения пароля доступа)	22
Рисунок 16 - Окно запроса разрешения на просмотр пароля доступа к целевому устройству	23
Рисунок 17 - Страница «Пароли»; сформированный запрос находится в статусе «Ожидает»	24
Рисунок 18 - Страница «Пароли»; сформированный запрос находится в статусе «Принято»	25
Рисунок 19 - Окно для просмотра пароля (аккаунт wabadmin)	25
Рисунок 20 - Отображение пароля (аккаунт wabadmin)	25
Рисунок 21 - Параметры текущего запроса	26
Рисунок 22 - Отмена запроса разрешения	26
Рисунок 23 - Страница «Пароли»; статус запроса на 2025-09-28 18:39:00 – «Отменено»	26
Рисунок 24 - Окно авторизации СКДПУ	28
Рисунок 25 - Уведомление СКДПУ	29
Рисунок 26 - Уведомление о времени, до которого пользователю доступно целевое устройство... ..	29
Рисунок 27 - Окно авторизации на целевом устройстве	30
Рисунок 28 - Осуществлен доступ к целевому устройству	30
Рисунок 29 - Пользователю не согласован доступ на целевое устройство (систему)	31
Рисунок 30 - Запрос на доступ сформирован, ожидает обработки	32
Рисунок 31 - Запрос на доступ отклонен	32

Рисунок 32 - Интерфейс клиента PuTTY	33
Рисунок 33 - Окно клиента с приглашением ввести логин пользователя	33
Рисунок 34 - Интерфейс СКДПУ при авторизации пользователя с клиента	34
Рисунок 35 - Справка по командам СКДПУ	34
Рисунок 36 - Предупреждение о необходимости сформировать запрос на подтверждение доступа к целевому устройству	35
Рисунок 37 - Сформирован запрос на подтверждение доступа к целевому устройству; ожидает обработки.....	36
Рисунок 38 - Запрос на подтверждение доступа к целевому устройству отклонен	36
Рисунок 39 - Запрос на подтверждение доступа к целевому устройству удовлетворен; необходимо пройти авторизацию на целевом устройстве.	36
Рисунок 40 - Настройки PuTTY	39
Рисунок 1 - Генерирование открытого и закрытого ключей SSH	40
Рисунок 2 - Генерирование открытого и закрытого ключей SSH	40
Рисунок 3 - Импорт закрытого ключа SSH при перезапуске агента	41
Рисунок 4 - Генерирование ключа SSH в «PuTTY»	41
Рисунок 5 - Подтверждение сгенерированного в «PuTTY» ключа.....	42
Рисунок 6 - Проверка подлинности «Pageant»	43
Рисунок 7 - Проверка подлинности «FileZilla»	44
Рисунок 8 - Настройка параметров сеанса WinSCP	44
Рисунок 9 - Использование PSCP без «Pageant»	44
Рисунок 1 - Задание целевого устройства	48
Рисунок 2 - Конфигурирование PuTTY	49
Рисунок 3 - Перенос файлов с помощью FileZilla	50
Рисунок 4 - Параметры сессии WinSCP	51
Рисунок 5 - Настройка параметров сеанса WinSCP	51
Рисунок 6 - Страница "Сессии"	52
Рисунок 7 - Загрузка связанного файла RDP	52
Рисунок 8 - Подключение к удаленной рабочей станции с помощью клиента Terminal Server	53
Рисунок 9 - Список доступных устройств.....	53
Рисунок 10 - Вход в удаленную консоль с помощью клиента MSTSC	54
Рисунок 11 - Список доступных устройств.....	56

ПЕРЕЧЕНЬ ТАБЛИЦ

Т а б л и ц а 1	– Рекомендуемые характеристики аппаратного обеспечения АРМ пользователя .	6
Т а б л и ц а 2	– Программные средства АРМ пользователя	7

ПЕРЕЧЕНЬ СИМВОЛОВ И ЧИСЛОВЫХ КОЭФФИЦИЕНТОВ

Обозначение/Символ	Наименование/Пояснение
Единицы измерения	
ГБ	Гигабайт (единица измерения объема информации, равная 2^{30} байт)

