



**ПРОГРАММНЫЙ КОМПЛЕКС
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ»**

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

RU.33654484.0004-02 90 01

Листов 40

СОДЕРЖАНИЕ

1 Введение.....	4
1.1 Область применения.....	4
1.2 Краткое описание возможностей.....	4
1.3 Уровень подготовки администратора.....	5
1.4 Перечень эксплуатационной документации для ознакомления.....	5
2 Назначение и условия работы СКДПУ.....	7
2.1 Назначение СКДПУ.....	7
2.2 Требования к техническим и программным средствам.....	7
2.3 Требования к аппаратному обеспечению.....	8
2.4 Требования к программному обеспечению.....	8
3 Интерфейс пользователя.....	10
3.1 Доступ к веб-интерфейсу СКДПУ.....	10
3.2 Изменение настроек профиля пользователя.....	10
3.2.1 Изменение адреса электронной почты и языка интерфейса.....	11
3.2.2 Изменение пароля.....	12
3.2.3 Загрузка открытого ключа SSH.....	12
3.2.4 Загрузка GPG ключа.....	13
3.2.5 Просмотр списка доступных устройств.....	13
3.3 Меню «Сессии».....	13
3.4 Меню «Пароли».....	13
4 Вход в целевые устройства.....	15
4.1 Проверка подлинности по паролю и ключу.....	15
4.2 Генерирование ключа в ОС Linux.....	15
4.3 Генерирование ключа в ОС Windows.....	16
4.4 Вход в систему по SSH.....	21
4.4.1 Вход в систему по SSH с рабочей станции Unix/Linux.....	21
4.4.2 Вход в систему по SSH с рабочей станции Windows.....	23
4.5 Вход в систему через RDP.....	27
4.5.1 С рабочей станции Windows (XP, Vista, 7, 10).....	27
4.5.2 С рабочей станции Linux.....	30
5 Действия в нестандартных ситуациях.....	33
5.1 Проблемы, связанные с входом в систему.....	33
5.2 Автоматизированный сеанс SSH.....	33
6 Рекомендации по освоению.....	35
Перечень сокращений.....	36
Перечень рисунков.....	38

Перечень таблиц.....	39
Лист регистрации изменений.....	40

1 ВВЕДЕНИЕ

1.1 Область применения

Настоящий документ предназначен для администраторов СКДПУ для доступа к администрируемым устройствам (серверы, сетевые устройства, устройства обеспечения безопасности, веб-интерфейсам администрирования и т.д.).

В настоящем документе приводится подробное описание действий, необходимых для ретрансляции подключений SSH или RDP на целевые устройства, мониторинга подключений в соответствии с правами, заданными в профиле, записи действий.

1.2 Краткое описание возможностей

Основные возможности СКДПУ приведены в [таблица 1](#).

Таблица 1 – Основные возможности СКДПУ

Основные возможности	Описание
Контроль доступа	СКДПУ позволяет создать политику управления доступом на основе прав пользователей: целевые учетные записи, протоколы, интервалы времени и типы сеансов.
Единая точка входа в систему (SSO)	Для доступа к учетным записям достаточно предоставить имя пользователя и пароль в СКДПУ.
Поддержка нескольких протоколов администрирования	СКДПУ поддерживает следующие протоколы администрирования устройств и серверов: RDP/TSE, SSH, TELNET, VNC, SFTP/SCP и т.д.
Отслеживание активности и запись сеансов	Регистрация и возможность записи всех действий, выполненных на управляемых устройствах в течение графического сеанса (RDP/TSE или VNC) или сеанса командной строки (SSH, TELNET).
Управление паролями	СКДПУ позволяет изменять пароли на управляемых устройствах по запросу или через заданные интервалы времени.
Работа без использования агентов	СКДПУ работает без использования специальных агентов на администрируемых устройствах или на рабочих станциях администраторов.

Основные возможности	Описание
Статистика и отчеты о действиях	Возможность формировать рабочую статистику/отчеты и экспортировать эти данные в формате CSV через интерфейс администратора.
Делегирование функций администрирования СКДПУ	Средства управления профилями позволяют определить, какие действия будут доступны каждому пользователю СКДПУ (например, создание пользователей, управление правами и т.д.)
Анализ потока и распознавание текста	СКДПУ позволяет в реальном времени обнаруживать определенные строки символов в сессиях SSH и анализировать содержимое сеансов подключения к удаленному рабочему столу (RDP/TSE).
Контроль в реальном времени	Администраторы СКДПУ могут просматривать активные сеансы подключения к удаленному рабочему столу и SSH в СКДПУ в реальном времени.
Поддержка Web Service	Вся информация о пользователях, учетных записях, устройствах, правах доступа в СКДПУ может вводиться или быть доступна с помощью Web Service API.

1.3 Уровень подготовки администратора

Администратор должен обладать следующими знаниями:

- Системное администрирование ОС Windows/Linux и активного сетевого оборудования;
- Базовые знания сетевых протоколов;
- Администрирование СКДПУ и умение с его помощью реализовывать корпоративную политику безопасности, в части относящейся к информационному обмену;
- Знание и соблюдение требований конфиденциальности (секретности) при проведении работ.

1.4 Перечень эксплуатационной документации для ознакомления

Администратор СКДПУ должен ознакомиться с настоящим документом и со следующими эксплуатационными документами:

Таблица 2 – Перечень эксплуатационной документации для ознакомления

Номер документа	Название документа
RU.33654484.0004-02 91 01	Программный комплекс «Система контроля действий поставщиков ИТ-услуг» Руководство администратора

2 НАЗНАЧЕНИЕ И УСЛОВИЯ РАБОТЫ СКДПУ

2.1 Назначение СКДПУ

СКДПУ предназначена для мониторинга и аудита действий поставщиков ИТ-услуг и других третьих лиц на администрируемых устройствах с целью контроля доступа внутренних и внешних поставщиков ИТ-услуг, владельцев учетных записей с расширенными правами и пользователей с повышенными рисками.

СКДПУ своевременно уведомляет Администратора о любых попытках подключения к устройствам, определенным как критичные, о неудачных попытках входа в СКДПУ или о невозможности автоматического входа с использованием заданной учетной записи.

СКДПУ предназначена для записи рабочих сеансов для последующего просмотра с целью аудита, управления инцидентами и проведения расследований.

СКДПУ анализирует все команды, вводимые в ходе сеансов SSH, в реальном времени и в случае обнаружения запрещенных строк отправляет соответствующее уведомление или разрывает сеанс подключения. Кроме того, СКДПУ использует технологию оптического распознавания символов (OCR) сеансов подключения к удаленному рабочему столу (RDP и VNC) в реальном времени, что упрощает процесс выявления причин сбоев или инцидентов безопасности.

СКДПУ поддерживает следующие протоколы передачи данных:

- HTTP (RFC 2616) и HTTPS (HTTP Over TLS – RFC 2818);
- SSH (RFC 4250 – 4256) и подсистемы указанного протокола;
- TELNET (RFC 854);
- RLOGIN (RFC 1282);
- произвольные TCP протоколы (RAWTCPIP) в рамках сессий SSH;
- RDP (v. 5 – 8.1) и VNC (на основе RFB 3.8, RFC 6143) в домене пользователя.

2.2 Требования к техническим и программным средствам

Минимальные характеристики программного и аппаратного обеспечения для развертывания сервера СКДПУ см. [таблица 3](#).

Таблица 3 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ

Компонент	Описание
Процессор	архитектура x86-64 с тактовой частотой 2.6 ГГц
Оперативная память	6 ГБ
Жесткий диск	500 ГБ, SCSI или SATA
Интерфейсы	интерфейс для подключения к LAN
ОС	ОС Astra Linux 1.6 Special Edition
Веб-сервер	HTTP Apache 2.4

Компонент	Описание
База данных	СУБД PostgreSQL версии 9.6
Брокер сообщений	RabbitMQ версии 3.6
Другое ПО	Интерпретаторы языка программирования Python 2.7, Python 3.5
	Библиотеки Python, обеспечивающие удовлетворение зависимостей для *.py части ПО

2.3 Требования к аппаратному обеспечению

АРМ пользователя СКДПУ должно быть оборудовано компьютером, обладающим следующим характеристиками:

Таблица 4 – Минимальные характеристики аппаратного обеспечения сервера СКДПУ

Компонент	Описание
Процессор	архитектура x86-64 с тактовой частотой 2.6 ГГц
Оперативная память	6 ГБ
Жесткий диск	500 ГБ, SCSI или SATA
Интерфейсы	Интерфейс для подключения к LAN
Разрешение экрана	От 1280x1024

2.4 Требования к программному обеспечению

В состав программного обеспечения АРМ пользователя СКДПУ должна входить программа-клиент, предоставляющая возможность навигации и просмотра веб-ресурсов - веб-браузер.

Таблица 5 – Минимальные характеристики программного обеспечения АРМ пользователя СКДПУ

Компонент	Описание
Веб-обозреватель	Mozilla Firefox 80.0 и выше, Google Chrome 10.0 – 80.0, Microsoft Edge версии 44.18362.449.0. и выше . Обеспечивающий поддержку стандарта HTTP 1.1, TLS 1.2 и лучше
Брокер сообщений	Свободно распространяемый клиент для различных протоколов удаленного доступа, включая SSH, TELNET, RLOGIN. В качестве таких клиентов могут быть использованы «PuTTY», «WinSCP», «FileZilla»

Веб-браузер должен быть установлен перед началом работы с СКДПУ. Описание установки веб-браузера приведено в документации поставщика ПО.

3 ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

3.1 Доступ к веб-интерфейсу СКДПУ

Для доступа к веб-интерфейсу необходимо 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.



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

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

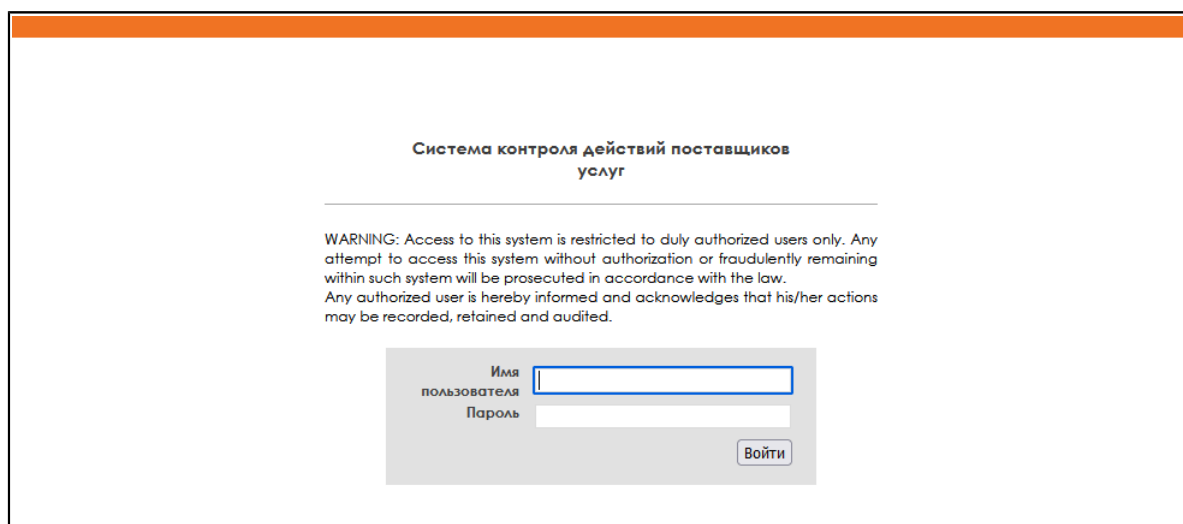


Рисунок 1 – Страница входа

Шаг 3. Для получения доступа к веб-интерфейсу пользователя в окне авторизации необходимо указать имя пользователя (логин) в поле **Имя пользователя** и пароль в поле **Пароль**, предоставленные администратором СКДПУ.

Шаг 4. Нажать кнопку **Войти**.

Если вход в систему будет выполнен успешно, то на экране отобразится главная страница СКДПУ.

В боковом меню представлены доступные действия. Содержимое бокового меню зависит от профиля пользователя и от назначенных прав доступа

3.2 Изменение настроек профиля пользователя

При выборе пункта **Мои настройки** из бокового меню интерфейса пользователя, в рабочей области отображаются настройки профиля, которые могут быть изменены пользователем (см. рисунок 2).

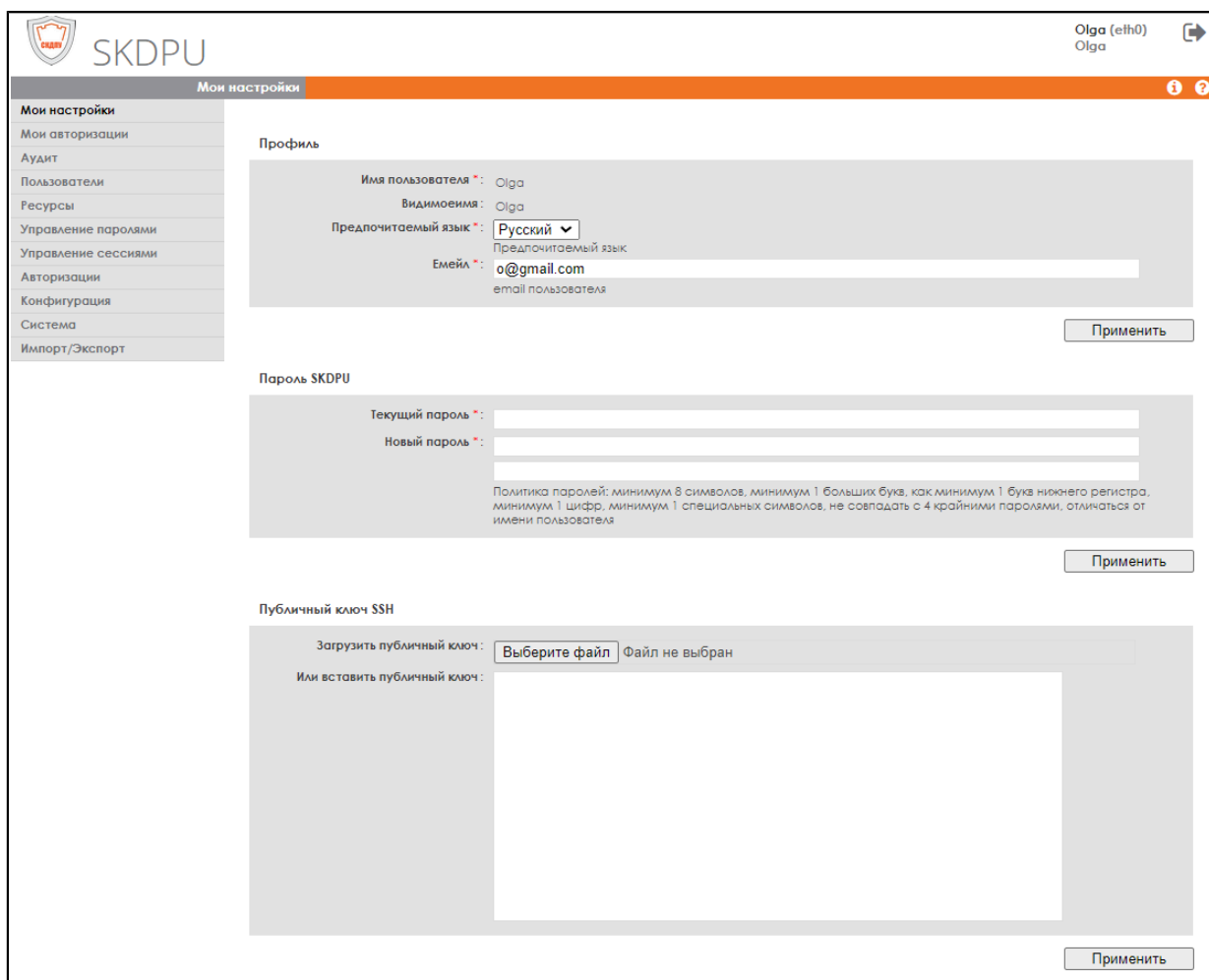


Рисунок 2 – Страница "Мои настройки"

В данном разделе веб-интерфейса пользователь может:

- Изменить адрес электронной почты и язык интерфейса (для отображения сообщений прокси-сервера);
- Изменить пароль (только если пользователь был объявлен локально);
- Загрузить открытый ключ SSH;
- Загрузить GPG ключ.



Меню **Мои настройки** доступно всем пользователям вне зависимости от прав доступа. Если проверка подлинности пользователя связана с каталогом компании, то форма для изменения пароля будет недоступна.

3.2.1 Изменение адреса электронной почты и языка интерфейса

Для изменения адреса электронной почты или языка интерфейса необходимо перейти в раздел **Профиль** (см. [рисунок 2](#)) и 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.

3.2.2 Изменение пароля

В зависимости от параметров СКДПУ пользователю может потребоваться изменение пароля в следующих случаях:

- Если срок действия пароля истекает в ближайшее время (при входе пользователя в веб-интерфейс отображается сообщение о том, что срок действия пароля истекает);
- Если пароль для доступа к устройствам изменен в первый раз. Некоторые пароли могут быть отклонены в соответствии с настройками конфигурации СКДПУ;
- Если пароль входит в список паролей, запрещенных парольной политикой, настроенной администратором СКДПУ;
- Если пароль слишком короткий или включает недостаточно специальных символов, цифр или букв в верхнем регистре;
- Если пароль совпадает с именем пользователя;
- Если пароль совпадает с предыдущим паролем.

Для изменения пароля необходимо перейти в раздел **Пароль SKDPU** (см. [рисунок 2](#)) и 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**.

Шаг 3. Для сохранения внесенных изменений нажать кнопку **Применить**.



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

3.2.3 Загрузка открытого ключа SSH

Для загрузки открытого ключа SSH необходимо перейти в раздел **Публичный ключ SSH** (см. [рисунок 2](#)) и выполнить следующие действия:

Шаг 1. Нажать кнопку **Выберите файл** для вызова окна выгрузки файла и выбрать необходимый файл ключа.

Шаг 2. Для загрузки нажать кнопку **Применить**.

3.2.4 Загрузка GPG ключа

Для загрузки GPG ключа необходимо в разделе **GPG ключ** (см. [рисунок 2](#)) нажать кнопку **Закачать**, выбрав требуемый файл.

3.2.5 Просмотр списка доступных устройств

С помощью пункта меню **Мои авторизации** пользователь может:

- Просмотреть информацию по своим доступам к целевым учетным записям и доступным сервисам;
- Получить доступ к разрешенным ресурсам и сервисам.

3.3 Меню «Сессии»

При выборе пункта **Сессии** из бокового меню интерфейса, в рабочей области отображается перечень доступных сервисов (см. [рисунок 3](#)).

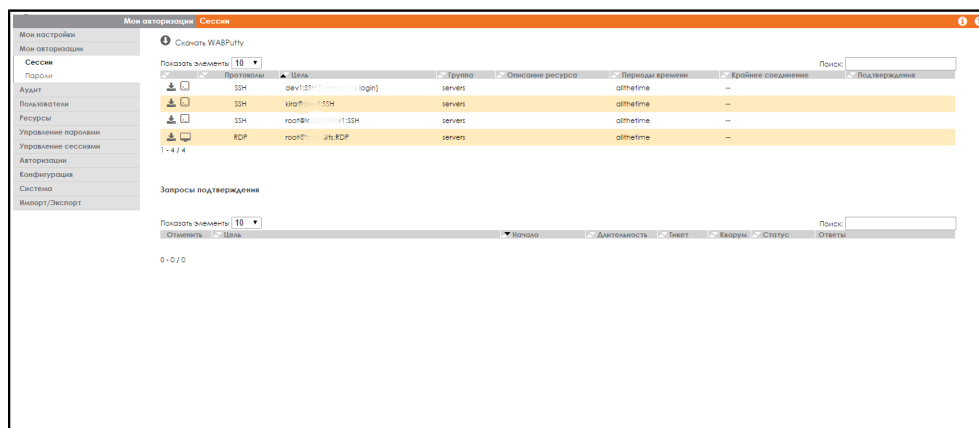



Рисунок 3 – Страница "Сессии"

Чтобы получить доступ к целевым учетным записям по протоколу RDP необходимо нажать на значок  для загрузки связанного файла RDP для того, чтобы напрямую открыть клиент Microsoft RDP.

Для доступа к HTTP/HTTPS необходимо нажать на значок, чтобы напрямую перейти к ресурсам через пользовательский веб-интерфейс.

3.4 Меню «Пароли»

При выборе пункта **Пароли** из бокового меню интерфейса администратора отображается перечень доступных целевых учетных записей (см. [рисунок 4](#)).

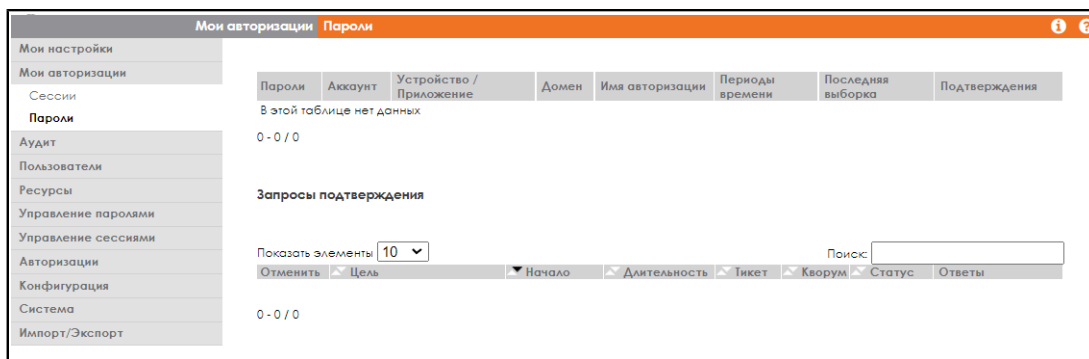


Рисунок 4 – Страница "Пароли"

Для просмотра данных учетной записи необходимо перейти по ссылке **Просмотр**, расположенной в первом столбце таблицы (см. [рисунок 4](#)). Откроется страница с параметрами учетной записи. На странице с данными учетной записи для просмотра пароля учетной записи необходимо перейти по ссылке **Просмотр**, расположенной справа от поля **Пароль**. Для загрузки ключа SSH перейти по ссылке **Скачать**, для того, чтобы скопировать ключ необходимо перейти по ссылке **Копировать в буфер обмена**.

4 ВХОД В ЦЕЛЕВЫЕ УСТРОЙСТВА

Для подключений между СКДПУ и целевыми устройствами, т.к. они находятся в безопасной зоне, можно использовать протоколы: SSH, RDP, VNC, TELNET, RLOGIN.

Для подключения между СКДПУ и рабочими станциями, т.к. они находятся в опасной зоне, можно использовать только зашифрованные протоколы: SSH, RDP.

В сочетании с СКДПУ допускается применять стандартные средства: клиенты SSH в текстовом или графическом режиме либо клиент RDP на платформах Unix, Windows, Mac OS X.

4.1 Проверка подлинности по паролю и ключу

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** (см. [рисунок 2](#)).

4.2 Генерирование ключа в ОС Linux

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



Можно использовать файл `~/.ssh/id_rsa`, файл идентификации, по умолчанию используемый всеми командами OpenSSH. В этом случае, если файл уже существует, можно пропустить первые два шага, описанные в данном разделе, и импортировать файл `~/.ssh/id_rsa.pub` в СКДПУ (см. [Загрузка открытого ключа SSH](#)).

В данном примере файл идентификации закрытого ключа имеет имя `wab_rsa2048`, однако вы можете использовать любое другое допустимое имя файла. Рекомендуется сохранить данный ключ в каталоге `.ssh` файла HOME.

Шаг 1. На терминале выполните следующую команду, чтобы сгенерировать пару открытого и закрытого ключей:

```
$ 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.
```

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. [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:

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

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

```
$ 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)
```

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

Шаг 6. Приступите к процедуре входа в систему SSH согласно инструкциям, приведенным в [Вход в систему по SSH](#) настоящего документа.

4.3 Генерирование ключа в ОС Windows

Чтобы сгенерировать и использовать ключ 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 5**):



Рисунок 5 – Генерирование ключа SSH

- 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**.



В данном примере файл идентификации закрытого ключа имеет имя `wab_rsa2048`, однако вы можете 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 6](#)).

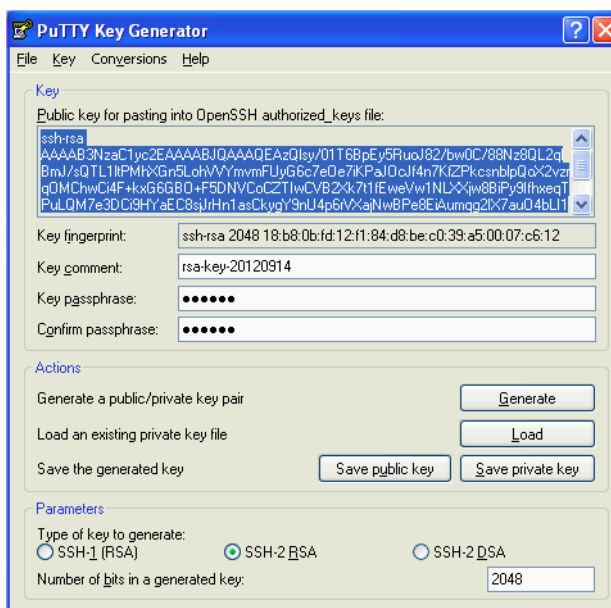


Рисунок 6 – Подтверждение сгенерированного ключа

- Шаг 5.** Нажать кнопку **Save public key (Сохранить 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 того, чтобы создать пустой текстовый документ.
- 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. [Загрузка открытого ключа SSH](#)).

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

I При проверке подлинности «Pageant»:

Шаг 1. Запустите приложение «Pageant» в меню **Пуск**, если оно еще не 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 7](#)).

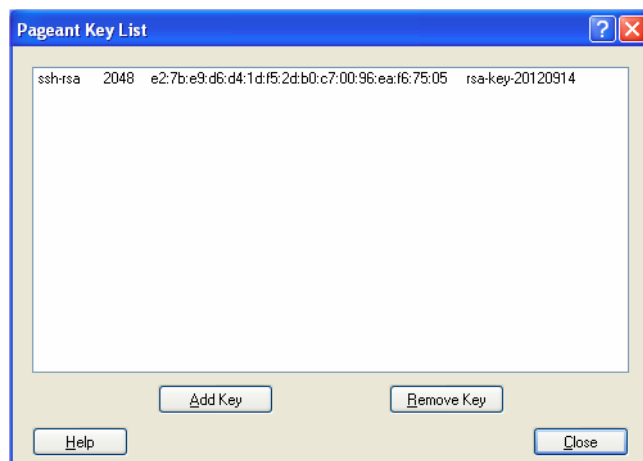


Рисунок 7 – Проверка подлинности «Pageant»

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

Шаг 4. Теперь можно получить доступ к прокси-серверу с помощью «PuTTY», «PSCP», «PSFTP», «Filezilla» или «WinSCP» (если параметры последнего не запрещают использовать проверку подлинности «Pageant»).



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

II При использовании «PuTTY» в «Pageant»:

Откройте меню **Пуск** и запустите PuTTY. В дереве параметров конфигурации выберите **Connection > SSH > Auth**, в разделе **Authentication parameters**

нажмите кнопку **Обзор** и выберите файл закрытого ключа (My Documents \wab_rsa2048.ppk).



Для повторного использования необходимо сохранить настройки сеанса.

III При использовании «FileZilla» в «Pageant»:

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 8](#)).

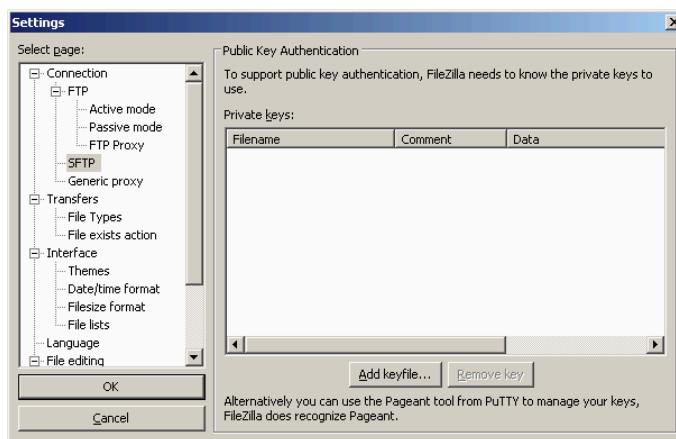


Рисунок 8 – Проверка подлинности «FileZilla»

IV При использовании «WinSCP» в «Pageant»:

Запустите «WinSCP», на странице параметров сеанса (см. [рисунок 9](#)) нажмите кнопку в поле **Private key file** и выберите файл My Documents \wab_rsa2048.ppk.

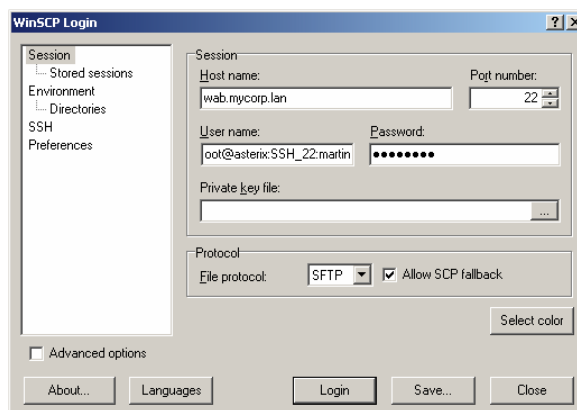


Рисунок 9 – Настройка параметров сеанса WinSCP

Выполните процедуру входа в систему по SSH, описание которой приведено в разделе [Вход в систему по SSH с рабочей станции Windows](#).

V При использовании PSCP или PSFTP без «Pageant»:

Добавьте в командную строку параметр **-i key**:

```
$ 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":
```

Шаг 12. Выполните процедуру входа в систему по SSH, описание которой приведено в [Вход в систему по SSH с рабочей станции Windows](#) настоящего документа.

4.4 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.

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.

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

4.4.1.1 Сеанс оболочки

Для входа в СКДПУ необходимо выполнить следующую команду:

```
$ ssh -t martin@wab.mycorp.lan root@asterix:SSH_22
martin@wab.mycorp.lan`s password:
```

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.



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

4.4.1.2 Удаленное выполнение команд

СКДПУ позволяет удаленно выполнять команды на одном или нескольких компьютерах при наличии у пользователя прав на использование `SSH_REMOTE_COMMAND` (см. [Вход в систему по SSH](#)).

```
$ 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.

4.4.1.3 Вход без ввода имени целевого объекта

СКДПУ может отобразить список устройств, доступных пользователю, для этого введите следующую 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, введите его номер.

4.4.1.4 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:
```

martin

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

root@asterix:SSH_22:/tmp

целевая учетная запись, компьютер, служба и каталог.

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

martin

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

root@asterix:SSH_22:/tmp/myfile

целевая учетная запись, компьютер, служба, каталог и файл.

В учетной записи необходимо включить автоматический вход в систему.

4.4.1.5 Перенос файлов с помощью SFTP

Для переноса файлов с помощью SFTP необходимо выполнить следующую команду:

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

martin

пользователь, настроенный в СКДПУ, с авторизацией SFTP_SESSION.

root@asterix:SSH_22

целевая учетная запись, компьютер и служба.

В учетной записи необходимо включить автоматический вход в систему.

4.4.1.6 Сеанс X11

Для запуска сеанса X11 необходимо выполнить следующую команду:

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

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 сообщает СКДПУ о желании начать сеанс X11 Forwarding, при этом на рабочей станции будут отображаться графические приложения, выполняемые на целевом устройстве во время данного сеанса.

4.4.2 Вход в систему по SSH с рабочей станции Windows

4.4.2.1 Сеанс оболочки и «PuTTY»

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

Шаг 1. Задать целевую систему, к которой требуется подключиться, для этого (см. рисунок 10):

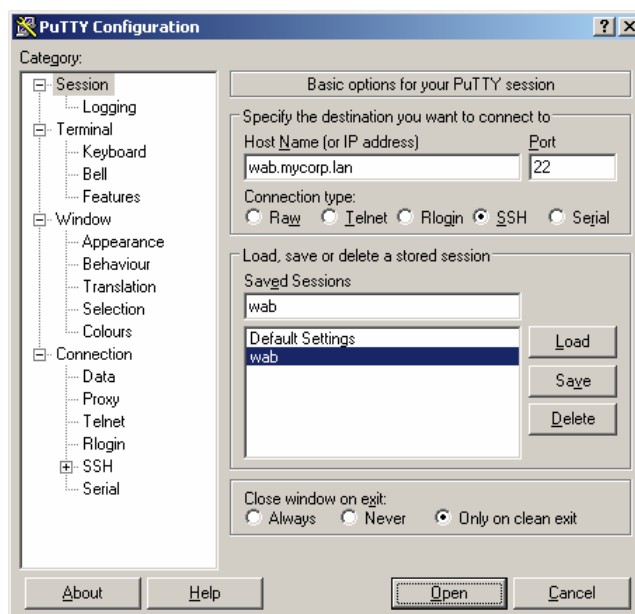


Рисунок 10 – Задание целевой системы

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

Шаг 2. Перейдите в раздел **Connection > SSH** и введите имя целевой учетной записи, устройство и службу в поле **Remote command:** (см. рисунок 11).

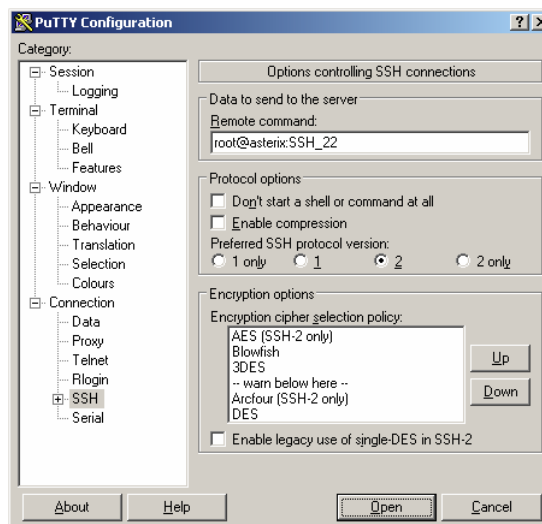


Рисунок 11 – Конфигурирование PuTTY

4.4.2.2 Перенос файлов с помощью PSCP

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

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

В учетной записи необходимо включить автоматический вход в систему.

4.4.2.3 Перенос файлов с помощью FileZilla

Для переноса файлов с помощью «FileZilla» необходимо:

Шаг 1. Запустить «FileZilla» и ввести следующую информацию (см. рисунок 12):

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

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

martin

это пользователь, настроенный в СКДПУ, с авторизацией SFTP_SESSION.

root@asterix:SSH_22

это целевая учетная запись, компьютер и служба

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

Шаг 2. Нажать кнопку **Connect**

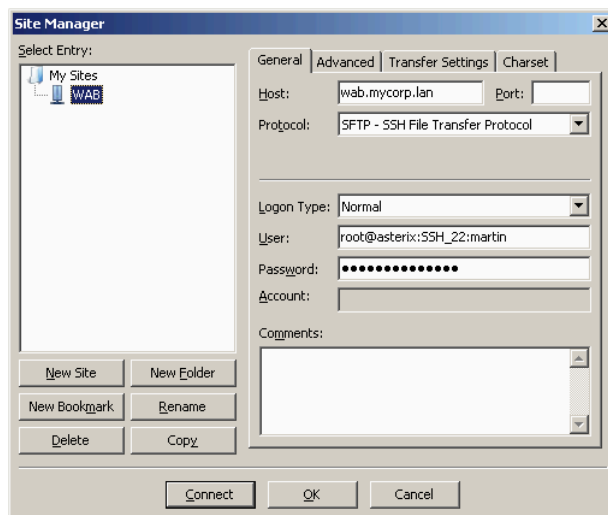


Рисунок 12 – Перенос файлов с помощью FileZilla

4.4.2.4 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 13](#)):

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

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

martin

это пользователь, настроенный в СКДПУ, с авторизацией SFTP_SESSION;

root@asterix: SSH_22

это целевая учетная запись, компьютер и служба;

- В поле **Password** введите пароль пользователя СКДПУ;
- Из выпадающего списка **File protocol** выберите протокол передачи файлов SFTP.

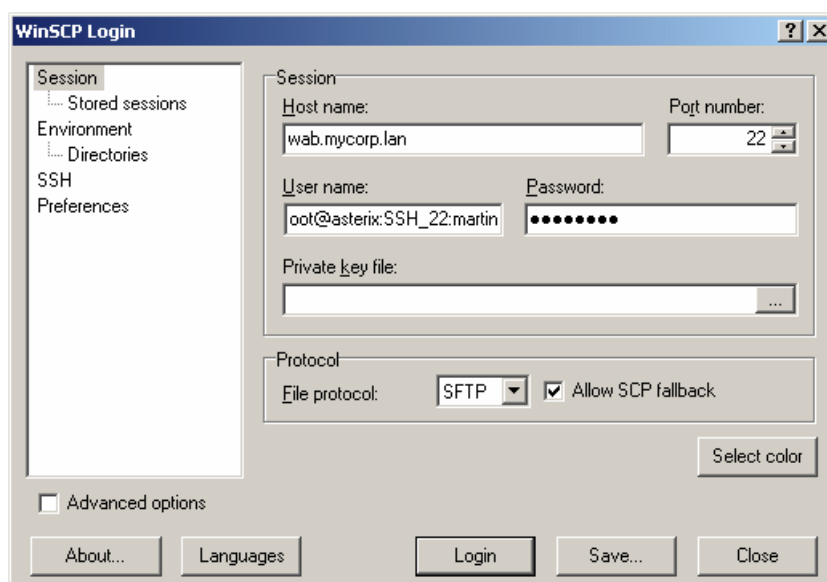


Рисунок 13 – Параметры сессии WinSCP

Шаг 2. Перейдите в раздел **Preferences > Transfer** (см. [рисунок 14](#)):

- В разделе **Upload options** установите флаг **Ignore permission errors**;
- В разделе **Common options** снимите флаг **Preserve timestamp**.



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

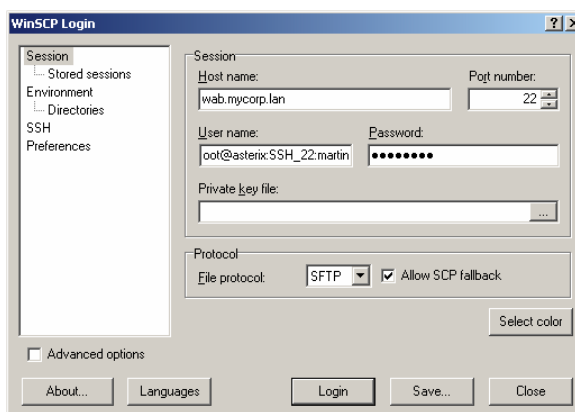


Рисунок 14 – Настройка параметров сеанса WinSCP


4.5 Вход в систему через RDP

4.5.1 С рабочей станции Windows (XP, Vista, 7, 10)

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

4.5.1.1 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 15) 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 15).

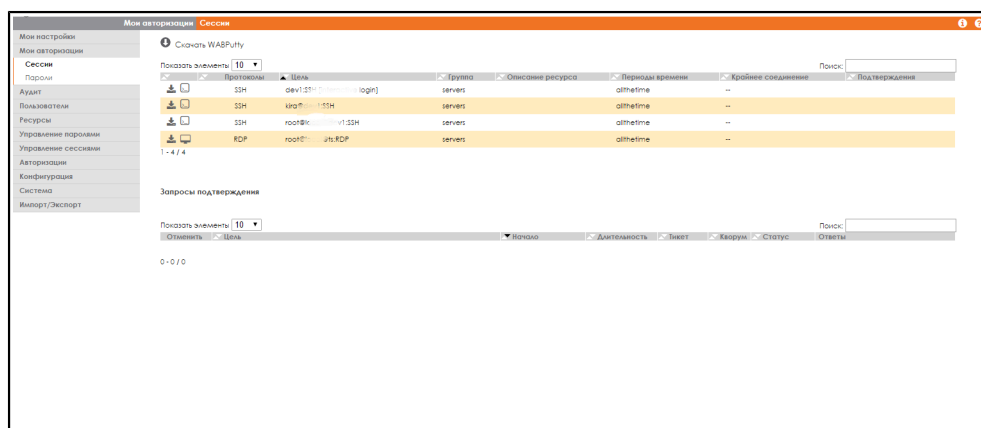


Рисунок 15 – Страница "Сессии"

Шаг 2. Нажать кнопку **Открыть** для того, чтобы запустить клиент Terminal Server рабочей станции (см. рисунок 16).

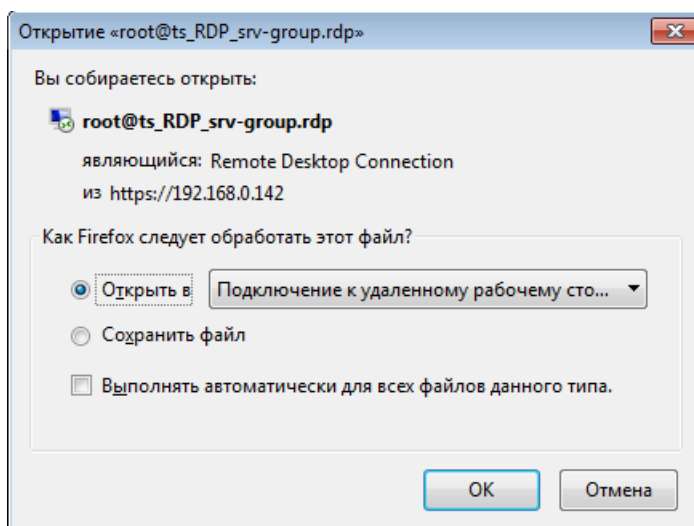


Рисунок 16 – Загрузка связанного файла RDP

4.5.1.2 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
```

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. Введите пароль пользователя и нажмите кнопку **Connect** (см. рисунок 17), после чего на экране отобразится сеанс ОС Windows.

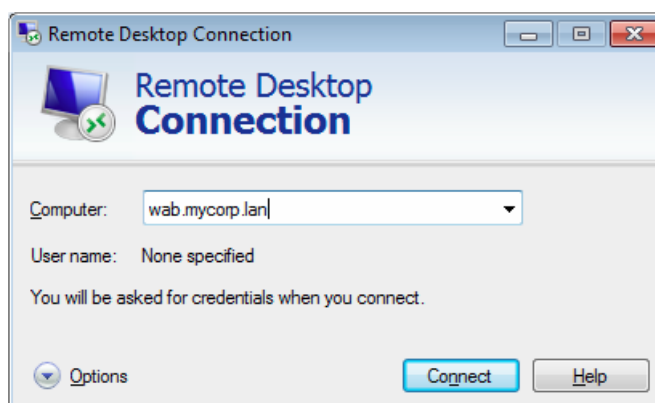


Рисунок 17 – Подключение к удаленной рабочей станции с помощью клиента Terminal Server

Шаг 3. В СКДПУ введите имя пользователя, после чего откроется промежуточная страница, отображающая список доступных серверов (см. рисунок 18).

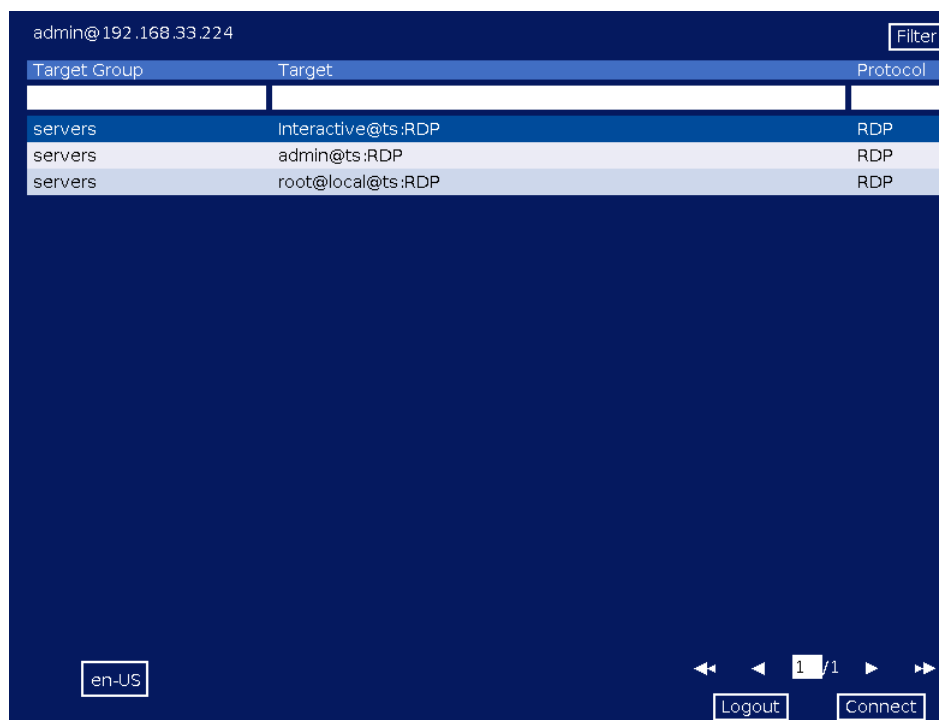


Рисунок 18 – Список доступных устройств

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.



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 19](#)).

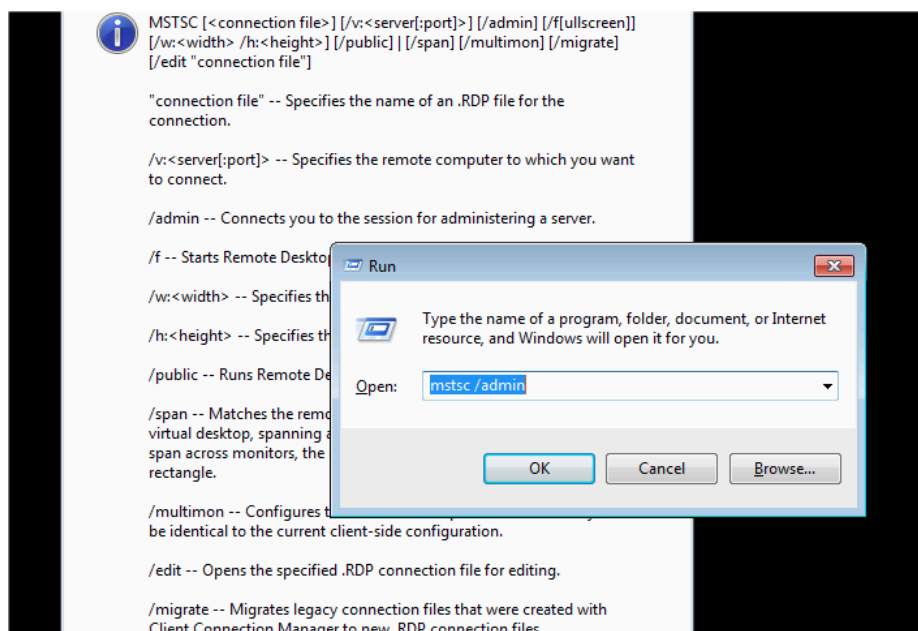


Рисунок 19 – Вход в удаленную консоль с помощью клиента MSTSC

4.5.1.3 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.



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

4.5.2 С рабочей станции Linux

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

Шаг 1. Выполнить команду:

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

wab.mycorp.lan

полное доменное имя СКДПУ.

Шаг 2. Откроется окно авторизации для сеанса RDP.

Шаг 3. В поле **login** необходимо ввести имя пользователя в следующем формате:

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

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 4. В поле **password** ввести пароль для пользователя.

Шаг 5. Нажать кнопку **ОК** для входа в систему удаленной рабочей станции, на экране отобразится сеанс ОС Windows.

Шаг 6. Введите 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 7. Для того чтобы установить соединение с удаленной рабочей станцией в окне авторизации введите пароль пользователя и нажмите кнопку **ОК**.

Шаг 8. В СКДПУ введите имя пользователя, откроется промежуточная страница, отображающая список доступных серверов (см. [рисунок 20](#)).

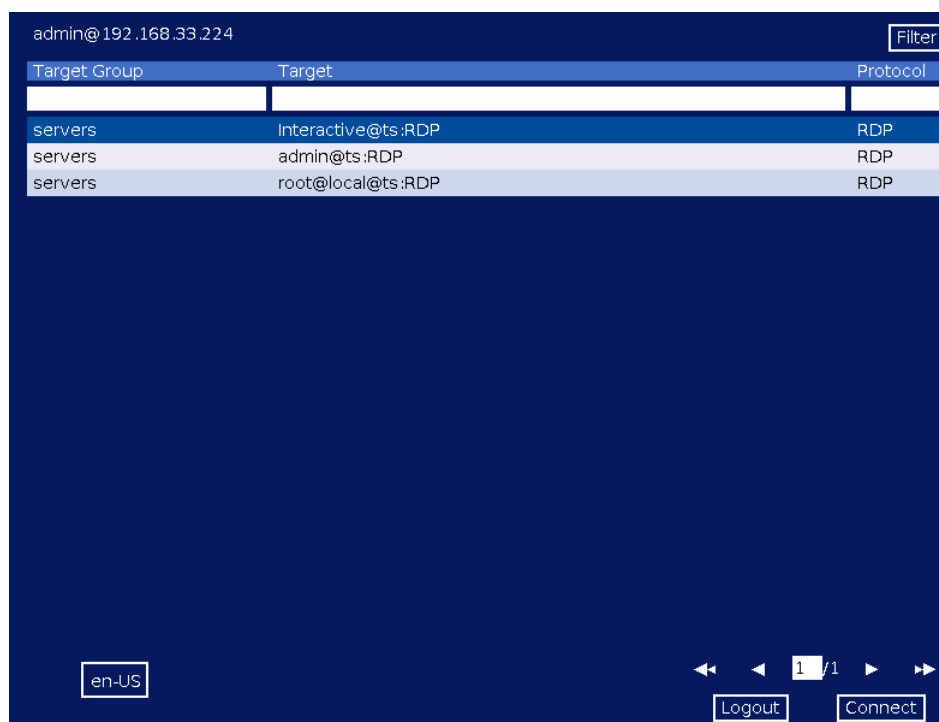


Рисунок 20 – Список доступных устройств

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.

5 ДЕЙСТВИЯ В НЕШТАТНЫХ СИТУАЦИЯХ

5.1 Проблемы, связанные с входом в систему

Причины сбоя входа в целевую учетную запись могут быть следующими:

Проблема	Возможное решение
Служба СКДПУ недоступна	Перезагрузить систему командой <code>reboot</code>
Введен неверный идентификатор и/или пароль пользователя	Свяжитесь с администратором для смены пароля
Целевое устройство недоступно	Проверить, что целевое устройство функционирует
Неверный пароль целевой учетной записи	Проверьте пароль целевой учетной записи
Пользователь не прошел авторизацию для доступа к целевой учетной записи	Исправить права доступа для выбранной авторизации, куда входит пользователь, в разделе 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 в разделе Ресурсы > Устройства
Достигнуто максимальное количество одновременных авторизованных подключений	Отключить часть пользователей

5.2 Автоматизированный сеанс 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 удалите выделение псевдотерминала (tty):

Шаг 1. Для решения этой проблемы удалите выделение псевдотерминала (tty):

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

Шаг 2. В ОС Windows, запустите «PuTTY», перейдите в подменю **SSH > TTY**, снимите флажок **Don't allocate a pseudo-terminal** (см. [рисунок 21](#)).

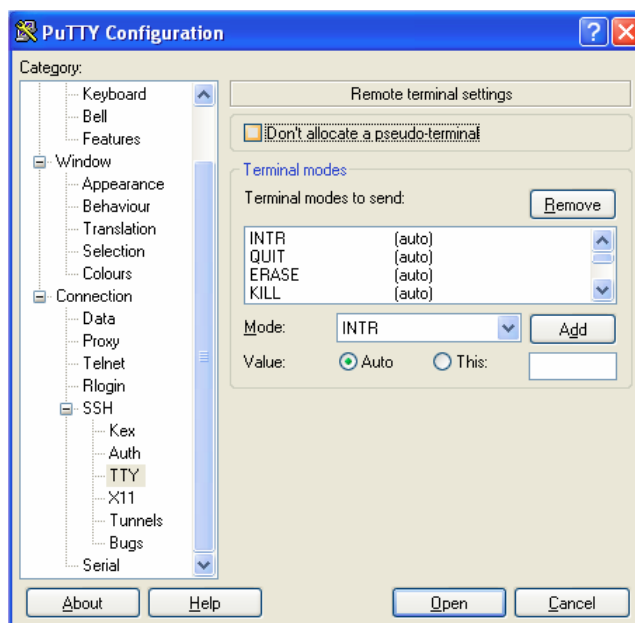


Рисунок 21 – Настройки PuTTY

6 РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

Для успешного освоения СКДПУ необходимо ознакомиться с документами, приведенными в [Перечень эксплуатационной документации для ознакомления](#).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

CLI	Command-Line Interface — — разновидность текстового интерфейса (TUI) между человеком и компьютером, в котором инструкции компьютеру даются в основном путём ввода с клавиатуры текстовых строк (команд), в UNIX-системах возможно применение мыши.
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.
GPL	General Public License лицензия на свободное программное обеспечение, созданная в рамках проекта GNU в 1988 г., по которой автор передаёт программное обеспечение в общественную собственность.
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	HyperText Transfer Protocol Secure - расширение протокола HTTP, поддерживающее шифрование.
LAN	Local Area Network (локальная компьютерная сеть)
LGPL	GNU Lesser General Public License — это лицензия свободного программного обеспечения за авторством Free Software Foundation (FSF).
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
RFB	Remote FrameBuffer — простой клиент-серверный сетевой протокол прикладного уровня для удалённого доступа к графическому рабочему столу компьютера, используемый в VNC.

RFC	Request for Comments, рабочее предложение – стандарты Интернета в части реализаций.
RLOGIN	Remote LOGIN (удалённый 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 SSH.
SFTP	SSH File Transfer Protocol — протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения.
SSH	Secure SHell (безопасная оболочка), протокол защищенной передачи данных
SSO	Single Sign-On — технология, при использовании которой пользователь переходит из одного раздела портала в другой, либо из одной системы в другую, не связанную с первой системой, без повторной аутентификации.
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 удалённого доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удалённый кадровый буфер).
APM	Автоматизированное рабочее место
ОС	Операционная система
ПО	Программное обеспечение

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Страница входа.....	10
Рисунок 2 – Страница "Мои настройки".....	11
Рисунок 3 – Страница "Сессии".....	13
Рисунок 4 – Страница "Пароли".....	14
Рисунок 5 – Генерирование ключа SSH.....	17
Рисунок 6 – Подтверждение сгенерированного ключа.....	18
Рисунок 7 – Проверка подлинности «Pegeant».....	19
Рисунок 8 – Проверка подлинности «FileZilla».....	20
Рисунок 9 – Настройка параметров сеанса WinSCP.....	20
Рисунок 10 – Задание целевой системы.....	24
Рисунок 11 – Конфигурирование PuTTY.....	24
Рисунок 12 – Перенос файлов с помощью FileZilla.....	25
Рисунок 13 – Параметры сессии WinSCP.....	26
Рисунок 14 – Настройка параметров сеанса WinSCP.....	27
Рисунок 15 – Страница "Сессии".....	28
Рисунок 16 – Загрузка связанного файла RDP.....	28
Рисунок 17 – Подключение к удаленной рабочей станции с помощью клиента Terminal Server.....	29
Рисунок 18 – Список доступных устройств.....	29
Рисунок 19 – Вход в удаленную консоль с помощью клиента MSTSC.....	30
Рисунок 20 – Список доступных устройств.....	32
Рисунок 21 – Настройки PuTTY.....	34

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Основные возможности СКДПУ.....	4
Таблица 2 – Перечень эксплуатационной документации для ознакомления.....	6
Таблица 3 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ.....	7
Таблица 4 – Минимальные характеристики аппаратного обеспечения сервера СКДПУ.....	8
Таблица 5 – Минимальные характеристики программного обеспечения АРМ пользователя СКДПУ.....	8

