СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ

Инструкция по установке и настройке

Система санкционирования и защищенной передачи команд дистанционного управления

2022

Оглавление

Термины и сокращения

Заказчик	–	Акционерное общество «Системный оператор Единой энергетической системы»;
ДУ	–	дистанционное управление;
ЕЭС	–	Единая энергетическая система;
ЗДУ	–	защищенное дистанционное управление
ОС	–	операционная система;
СБПК	–	сервис биометрического подтверждения команды
СКЗИ	–	средство криптографической защиты информации
СУБД	–	система управления базами данных;
ЦП	–	центральный процессор;
UID	–	уникальный идентификатор.

1. Общая информация

Полное наименование системы: система санкционирования и защищенной передачи команд дистанционного управлении.

Сокращенное наименование системы: ЗДУ, Система.

Разработчиком Системы является АО «ЛАНИТ» на основании договора № 22/01/31 от 03 февраля 2022 года.

ЗДУ обеспечивает контроль пользователей, которым разрешена отправка команд ДУ на объект электроэнергетики, посредством использования Биометрического сканера. СБПК обрабатывает полученные биометрические данные и разрешает/отклоняет отправку команды ДУ на объект электроэнергетики.

2. Технические требования к серверу

Программные компоненты ЗДУ размещаются на двух физических серверах, которые представляют из себя группу горячего резервирования. Подключаемыми аппаратными компонентами системы являются Биометрический сканер и АРМ Администратора. Описание взаимодействия компонентов Системы представлено в документе «Общее описание системы».

Технические требования серверов ЗДУ указаны в Таблице 1.

Таблица 1. Технические требования серверов ЗДУ

Оборудование	Минимальные требования	Рекомендуемые требования
Сервер-1	Оперативная память: 16 Гб Количество ядер ЦП: 8 Частота ЦП: 2.4 ГГц Postgres Pro Astra Linux SE* Объем хранилища: 400 Гб	Оперативная память: 32 Гб Количество ядер ЦП: 12 Частота ЦП: 3,2 ГГц Postgres Pro Astra Linux SE* Объем хранилища: не менее 1 Тб
Сервер-2	Оперативная память: 16 Гб Количество ядер ЦП: 8 Частота ЦП: 2.4 ГГц Postgres Pro* Astra Linux SE* Объем хранилища: 400 Гб	Оперативная память: 32 Гб Количество ядер ЦП: 12 Частота ЦП: 3,2 ГГц Postgres Pro 13 Astra Linux SE* Объем хранилища: не менее 1 Тб

ЗДУ совместима со средством антивирусной защиты Kaspersky для Linux.

3. Установка и настройка системного ПО

Для установки программных компонентов ЗДУ на сервере под управлением ОС Astra Linux SE (версия не ниже 1.7) должны быть установлены следующие компоненты:

- СУБД – Postgresql (не ниже версии 11);
- Веб-сервер – Apache2;
- Библиотеки .NET;
- СКЗИ «КриптоПро CSP».

Для выполнения установки компонентов на ОС Astra Linux должен быть подключен носитель с ОС Astra Linux. Установка компонентов должна выполняться с правами sudo. Перечень переносимых на сервер компонентов, должен выглядеть следующим образом:

- ASP.NET Core Runtime (раздел 3.3.2);
- СКЗИ «КриптоПро CPS» (раздел 3.4);
- Сертификат и ключ сертификата для «КриптоПро CSP»;
- Установочный компонент СБПК.

3.1. Установка СУБД PostgreSQL

1. Для хранения данных ЗДУ используется СУБД PostgreSQL версии не ниже 11. Для установки базы данных необходимо выполнить команду:

```
sudo apt install postgresql-11
```

2. После выполнения команды, необходимо подтвердить свое действие и дождаться окончания установки. В случае успешной установки PostgreSQL Вы увидите сообщение в терминале:

```
Готово. Теперь вы можете запустить сервер баз данных
```

3. После установки PostgreSQL необходимо установить пароль пользователю *postgres*. Для входа в учетную запись пользователя БД выполните команду:

```
sudo su - postgres
```

4. Вы успешно вошли в учетную запись пользователя. Для изменения пароля необходимо использовать команду psql -c в следующем формате:

```
psql -c "alter user postgres with password 'пароль'"
```

где вместо «пароль» Вы указываете необходимый пароль.

ВНИМАНИЕ! Данный пароль будет использоваться для подключения компонентов ЗДУ в дальнейшем.

5. В случае успешной смены пароля, в терминале появится сообщение «ALTER ROLE». После смены пароля необходимо выйти из учетной записи postgres командой *exit*.

6. Для проверки работоспособности СУБД и корректности установки необходимо выполнить команду:

```
sudo systemctl status postgresql
```

В появившейся информации, в параметре Active должен быть установлен статус «Active». Пример представлен на Рисунке 1.

Рисунок 1. Работоспособность СУБД

7. В случае, если в параметре Active указан статус «inactive» необходимо выполнить команду следующую команду, для активации службы СУБД:

```
sudo systemctl start postgresql
```

8. После запуска службы, необходимо убедиться в работоспособности службы командой:

```
sudo systemctl status postgresql
```

После выполнения вышеописанных пунктов установка СУБД завершена и не требует дополнительных действий.

3.2. Установка веб-сервера

Управление сервисом биометрического подтверждения команды будет осуществляться через Web-интерфейс. Для использования web-панели необходимо установить веб-сервер Apache2. Для установки необходимо выполнить команду:

```
sudo apt install apache2
```

После выполнения команды, необходимо подтвердить свое действие и дождаться окончания установки.

Для проверки работоспособности веб-сервера и корректности установки необходимо выполнить команду:

```
sudo systemctl status apache2
```

В появившейся информации, в параметре Active должен быть установлен статус «Active».

В случае, если в параметре Active указан статус «inactive» необходимо выполнить команду следующую команду, для активации службы Apache2:

```
sudo systemctl start apache2
```

После запуска службы, необходимо убедиться в работоспособности службы командой:

```
sudo systemctl status apache2
```

Для корректной работы сервера, необходимо открыть конфиг веб-сервера Apache2 и прописать переменные ServerName следующим образом: sudo nano /etc/apache2/apache2.conf

В самом конце файла добавить строчку или, если необходимо, строчки для корректной маршрутизации.

В первом параметре необходимо указать ip-адрес текущего сервера, во втором указать его dns-имя в случае, если планируется доступ к веб-панели по сетевому имени.

3.3. Установка библиотек .NET

Компоненты СБПК разработаны на модульной платформе .NET. Для работоспособности компонентов, необходимо установить на сервер библиотеки .NET.

3.3.1. Установка библиотек .NET

Для установки .NET необходимо:

1 На сервере Astra Linux создать в папке /usr/bin каталог dotnet:

```
sudo mkdir /usr/share/dotnet
```

2. Скопировать или переместить архив ASP.NET Core Runtime 6.0.* (версия для Linux Binaries x64) в созданный каталог /usr/share/dotnet.

```
sudo cp /*путь к архиву*/*название архива*.tar.gz /usr/share/dotnet
```

3. Перейти в директорию и распаковать архив:

```
cd /usr/share/dotnet
```

```
sudo tar xf *название архива*.tar.gz
```

44. Создать символьную ссылку для использования библиотек компонентами СБПК:

```
cd /usr/bin
```

```
ln -s /usr/share/dotnet/dotnet
```

В случае правильного выполнения всех пунктов установка библиотек .Net завершена.

3.4. Установки СКЗИ «КриптоПро CPS»

В ЗДУ обеспечивается хранение отпечатков пальцев работников в зашифрованном виде. Шифрование в Системе производится с помощью средства криптографической защиты «КриптоПро CSP». Для установки СКЗИ «КриптоПро CSP» необходимо выполнить следующие пункты:

1. Архив с «КриптоПро CSP» необходимо загрузить с официального сайта, предварительно зарегистрировавшись (или

воспользоваться уже имеющейся в организации учетной записью). В случае, если у Вас имеется экземпляр ПО версии 5.0, необходимо перейти к пункту 4.

2. Перейдя по ссылке, необходимо выбрать «КриптоПро CSP». В разделе сертифицированные версии использовать КриптоПро CSP 5.0 для UNIX систем. В открывшемся списке доступных версий, необходимо выбрать «КриптоПро CSP 5.0 для Linux (x64, deb)». В случае, если Вы используете другую архитектуру, необходимо скачать архив для используемой архитектуры.

3. Перенести скачанный архив на сервер Astra Linux.

4. Разархивировать полученный архив в терминале командой:

```
tar -zxf linux-amd64_deb.tgz
```

5. Перейти в каталог с разархивированным ПО:

```
cd linux-amd64_deb
```

6. Запустить установки ПО с помощью команды:

```
sudo ./install_gui.sh
```

7. В окне CryptoPro CSP Setup выбрать необходимые модули и библиотеки. Для работы компонентов СБПК достаточно выбрать модуль KC1 Cryptographic Service Provider.

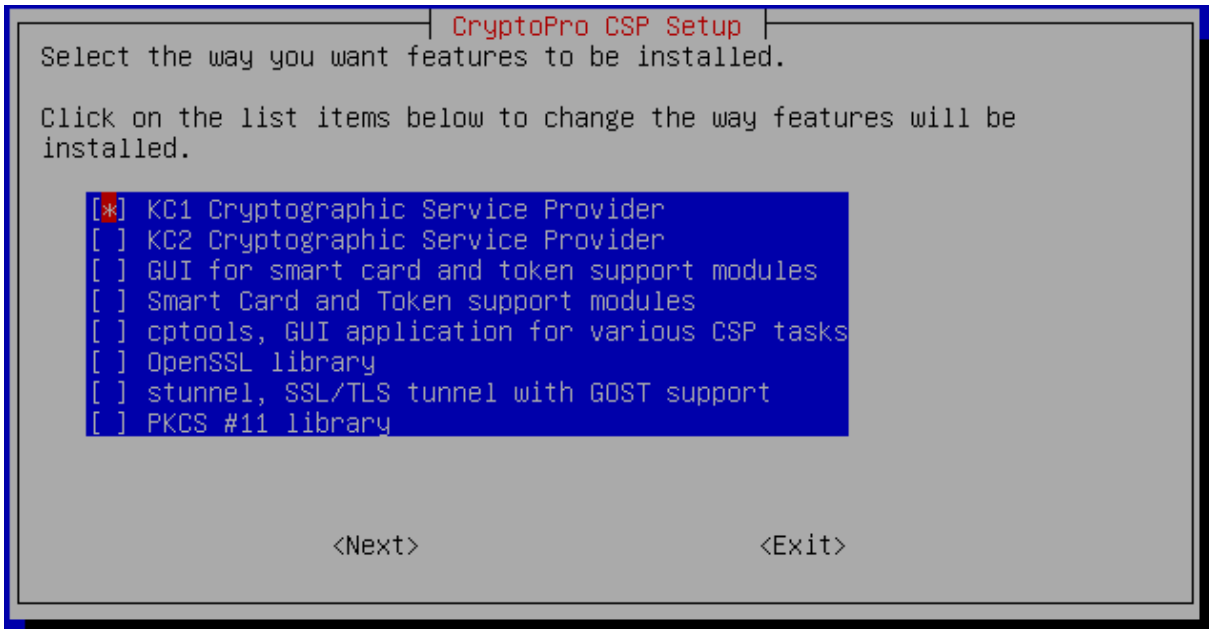

Рисунок 2. Выбор необходимых модулей и библиотек.

8. После успешной установки компонентов должно появиться сообщение «CSP packages have been successfully installed».

9. Следующим шагом необходимо ввести ключ лицензии на «КриптоПро CSP» и продолжить установку. После ввода ключа лицензии необходимо выйти из установщика.

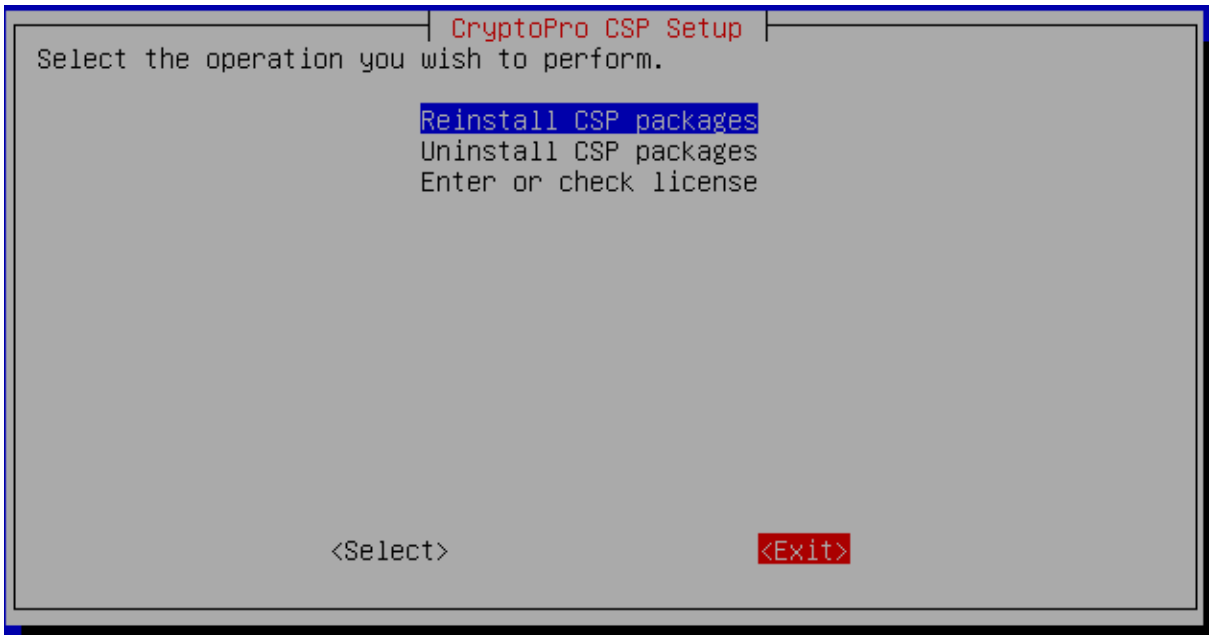

Рисунок 3. Выход из установщика.

10. Если вы пропустили установку лицензии в системе, необходимо выполнить следующую команду для ввода ключа:

```
sudo /opt/cprocsp/sbin/amd64/cpconfig -license -set <ваш_лицензионный_номер>
```

Проверить установленный ключ лицензии можно командой:

```
sudo /opt/cprocsp/sbin/amd64/cpconfig -license -view
```

11. Следующим шагом необходимо установить сертификат и его ключи. Сертификаты необходимо получить от УЦ. Полученный сертификаты перенести на сервер ЗДУ. Установить ключ расширения .pfx в Систему можно следующей командой, где, 1111 – это пин-код Вашего ключа.:

```
sudo /opt/cprocsp/bin/amd64/certmgr -install -pfx -file /*путь к файлу*/*название ключа*.pfx -pin <pin code>
```

После выполнения команды необходимо установить пароль на контейнер или оставить пароль пустым. Далее этот пароль потребуется ввести в настройках веб-панели СБПК. ***Важно**, для работоспособности горячего резервирования, на оба сервера должны устанавливаться одинаковые ключи.*

12. После установки ключа на сервер необходимо установить сертификаты с доступных контейнеров последовательно выполненными командами:

```
sudo /opt/cprocsp/bin/amd64/csptestf -absorb -certs -autoprov
```

```
sudo /opt/cprocsp/bin/amd64/csptestf -absorb -certs -pattern ''
```

13. Проверить информацию по установленному контейнеру. Получить имя сертификата можно в разделе KP_CERTIFICATE, в параметре Subject. Необходимо запомнить имя сертификата, он потребуется для ввода в веб-панели СБПК:

```
sudo /opt/cprocsp/bin/amd64/csptestf -keyset -container '\\.\HDIMAGE' -info
```

14. Для проверки работоспособности КриптоПро CSP, необходимо создать файл Input.txt с содержанием «12345» и выполнить команду, где в *название сертификата* указать название Вашего сертификата, полученного в пункте 13:

```
sudo /opt/cprocsp/bin/amd64/cryptcp -encr -dn '*название сертификата*' -encryptionalg 1.2.643.2.2.21 Input.txt output.txt
```

В рамках выполнения команды, Вам будет предложено согласиться на шифрование файла с выбранным сертификатом. После успешного шифрования файла, появится сообщение в терминале «Зашифрованное сообщение успешно создано».

Для расшифрования файла необходимо выполнить команду:

```
sudo /opt/cprocsp/bin/amd64/cryptcp -decr -dn '*название сертификата*' output.txt output1.txt
```

После успешной расшифровки файла, в терминале появится сообщение «Сообщение успешно расшифровано».

В случае, если расшифровка файла прошла успешна, установка «КриптоПро CSP» завершена. Можно приступать к установке компонентов СБПК.

4. Установка и настройка компонентов СБПК

4.1. Установка/обновление компонентов СБПК

Установка и обновление компонентов происходит в автоматическом режиме путем установки deb-пакета. Для начала установки/обновления необходимо скопировать на сервер актуальную версию ПО.

1. Для выполнения установки/обновления на сервере, необходимо выполнить команду:

```
sudo dpkg -i /*путь к файлу*/sbpk.deb
```

2. В процессе установки/обновления будет запрошен Логин пользователя базы данных. В случае, если Вы не меняли его при установке СУБД, необходимо указать postgres. После ввода логина, необходимо указать пароль, который Вы использовали в пункте 4, раздела 3.1 настоящего руководства. В случае успешной установки будет отображена информация в терминале «Установка компонентов СБПК завершена».

Установка компонентов СБПК завершена. Для того, чтобы проверить работоспособность компонентов, необходимо со стороннего ПК в браузере ввести ip-адрес или dns-имя сервера. После успешного открытия веб-панели, необходимо произвести попытку авторизации под технической учетной записью, логин admin, пароль необходимо оставить пустым. В случае корректной установки компонентов, появится предложение сменить пароль. Необходимо нажать кнопку «Отменить» и перейти к разделу 4 настоящего руководства. В случае, если авторизация под технической учетной записью не проходит, необходимо проверить корректность установки библиотек .NET согласно разделу 3.3 настоящего руководства.

4.2. Настройка компонентов СБПК

ВНИМАНИЕ! Перед выполнением настройки компонентов необходимо перейти к установке второго сервера. Выполнять настройку компонентов необходимо при двух установленных серверах ЗДУ.

Для настройки системы, необходимо авторизоваться под технической учетной записью. Логин: admin, пароль оставить пустым. При первом входе

в техническую учетную запись, будет предложено сменить пароль. После успешной смены пароля, потребуется войти в систему с новым паролем.

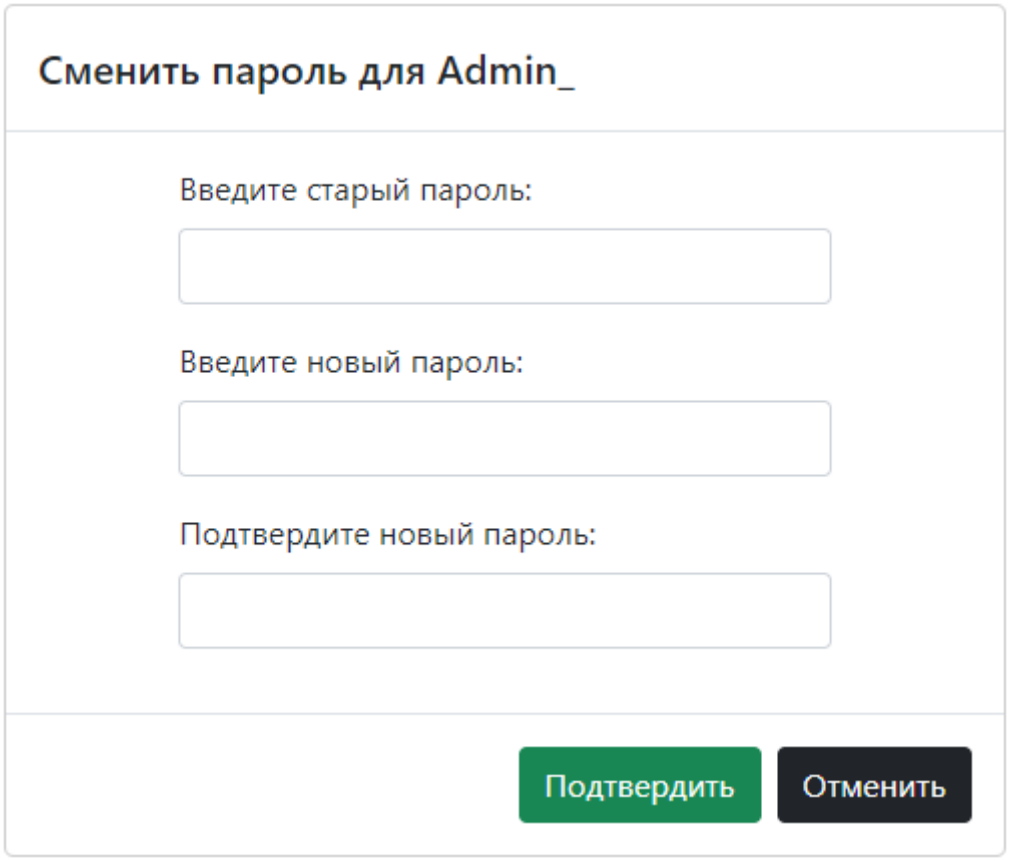

Рисунок 5. Окно смены пароля

Для первоначальной настройки необходимо перейти в раздел «Настройки» и указать ip-адрес зеркального сервера в формате *.*.*.*:5000. После обновления страницы статус подключения к зеркальному серверу изменится на доступен и будет отображаться слева от ip-адреса. После добавление IP-адреса зеркального сервера, необходимо выполнить аналогичные действия на втором сервере. После синхронизации двух серверов, необходимо продолжить настройку на любом из серверов, данные будут синхронизироваться.

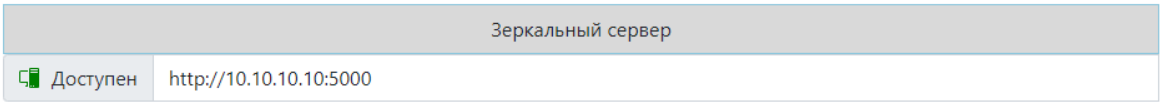

Рисунок 6. Проверка доступности зеркального сервера

Для завершения первоначальной настройки необходимо попробовать изменить любой параметр, сохранить изменения и убедиться, что на втором сервере применились настройки, указанные Вами на первом сервере.

После завершения настройки системы, необходимо в разделе «Администраторы» создать нового/новых пользователей, согласно матрице доступа. Для дальнейшей работы системы минимально необходим администратор с двумя ролями или два администратора с каждой из ролей.

Система имеет следующие разделы:

- Журнал;
- Работники;
- Администраторы;
- АРМ;
- Настройки.

Доступ к разделу «Настройки» имеют пользователи с ролью «Администратор ИБ». В данном разделе представлены следующие параметры для настройки компонентов СБПК и взаимодействия с компонентами NT_104.ProtoProxy:

- Токен;
- Время ожидания регистрации отпечатка, (сек.);
- Количество отпечатков для регистрации;
- Продолжительность смены диспетчера (сек.);
- Таймаут для серии команд, (сек.);
- Имя сертификата;
- Пароль контейнера;
- Зеркальный сервер;
- Использование отпечатка любого работника.

Перед изменением параметров необходимо убедиться в доступности зеркального сервера на двух серверах.

Для настройки взаимодействия компонентов NT_104.ProtoProxy и СБПК необходимо указывать токен, который настроен в ОИК СК-11. В поле уже указан предустановленный токен, но можно использовать собственный токен.

Взаимодействие Биометрического сканера происходит с использованием параметров, указанных в данном разделе. Для настройки взаимодействия сканера необходимо определить и установить «Время ожидания регистрации отпечатка». В данном параметре указывается время, которое сканер ожидает до отмены команды в секундах.

Каждый работник для подтверждения команды может использовать до 3-х отпечатков пальца. При регистрации отпечатков пальца работников сканер СБПК будет запрашивать количество отпечатков, указанное в данном параметре.

В параметре «Продолжительность смены диспетчера» устанавливается время, в течении которого смена может быть открыта. После указанного времени, смена закрывается автоматически.

При выполнении серии команд, сканер СБПК запрашивает подтверждение на выполнение. Если серия команд выполняется дольше, чем указано в данном параметре, сканер СБПК запрашивает дополнительное подтверждение полномочий.

Для шифрования отпечатков пальцев работников используется СКЗИ «КриптоПро CSP». Установка выполняется согласно Инструкции по установке и настройке ЗДУ. В параметре «Имя сертификата» необходимо указать имя сертификата, полученное в ходе установки. В случае, если при установке СКЗИ использовался пароль для контейнера, необходимо указать его в соответствующем параметре.

Параметр «Зеркальный сервер» содержит в себе ip-адрес зеркального сервера, группа которых функционирует в режиме горячего резервирования. IP-адрес зеркального сервера необходимо указывать в формате *.*.*.*:5000 и убедиться в том, что статус сервера изменился на «Доступен».

ЗДУ позволяет использовать подтверждения выполнения команды или серии команд любым работником, находящимся на смене. В случае, если работник, запустивший выполнение команды, не может использовать отпечаток пальца, Система будет принимать подтверждение выполнения команды при включенном режиме «Использование отпечатка любого работника».

5. Резервное копирование

Для управления резервным копированием компонентов СБПК необходимо запустить утилиту SBPKDataBackup:

```
sudo ./SBPKDataBackup
```

5.1. Настройка резервного копирования компонентов СБПК

Настройка резервного копирования осуществляется путем выбора команды «1» утилиты SBPKDataBackup. После выполнения команды, необходимо указать логин и пароль пользователя базы данных, установленных в разделе 3.1 настоящего руководства. Указать путь хранения резервных копий в формате */usr/backups* и количество раз в сколько дней необходимо делать резервную копию. Например, при указании цифры 1, резервная копия будет создаваться каждый день в 01:00 по местному времени.

5.2. Восстановление из резервной копии

В случае необходимости восстановления данных из резервной копии необходимо воспользоваться пунктом «2» утилиты SBPKDataBackup. Для восстановления данных потребуется указать логин и пароль пользователя базы данных, указать путь до базы данных в формате */usr/backups/SBA01-01-2022_01:00.backsbpk* . После восстановления, в терминале появится сообщение «Процесс восстановления окончен» и данные в системе будут актуальны на время восстановления копии.

6. Настройка клиентского места

Для работы с ЗДУ требуется настройка Биометрического сканера, располагающегося вблизи АРМ диспетчера, а также АРМ Администратора для управления компонентами ЗДУ.

6.1. Настройка Биометрического сканера

Для настройки Биометрического сканера необходимо подключить сканер напрямую к АРМ Администратора через сетевой интерфейс и запустить утилиту ConfigScannerZKTeco:

```
sudo ./ConfigScannerZKTeco
```

Биометрическому сканеру по умолчанию присвоен определенный IP-адрес. Для смены IP-адреса необходимо подключиться к сканеру со стандартным IP-адресом набрав цифру «1» в терминале. В случае успешного подключения к сканеру, необходимо ввести новый ip-адрес сканера (необходимо указывать актуальный ip-адрес, который будет использовать сканер). Через некоторое время ip-адрес будет изменен. Проверить корректность изменения адреса можно использовав команду под номером «3». Изменение ip-адреса с иного адреса на необходимый доступно при выборе команды «2».

После изменения ip-адреса сканера, необходимо зафиксировать ip-адрес конкретного устройства. Данный адрес будет использоваться для привязки сканера к рабочему месту Диспетчера.

6.2. Настройка АРМ Администратора

Для соответствия требованиям информационной безопасности на АРМ Администратора должен функционировать под операционной системой Astra Linux Special Edition и на нем должно быть установлено средство защиты информации Kaspersky для Linux. Настройка АРМ Администратора выполняется в соответствии с регламентами, определенными в АО «СО ЕЭС».

Для работы с ЗДУ на АРМ Администратора должен быть установлен веб-браузер.