Руководство Администратора
УКПМ

СОДЕРЖАНИЕ

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1 Используемые в документе сокращения и термины

Термин / Аббревиатура	Определение
AD	Active Directory, платформа для управления удостоверениями и обеспечения их безопасности
HTTPS	Протокол, обеспечивающий безопасность и конфиденциальность при обмене информацией между сайтом и устройством пользователя
ITSM	Информационная система ГМК НН, обеспечивающая доступ сотрудников к IT-услугам и сервисам.
OAuth 2.0	Протокол авторизации, позволяющий выдать одному сервису (приложению) права на доступ к ресурсам пользователя на другом сервисе
SSL-сертификат	Виртуальный документ, который содержит данные об организации, её владельце и подтверждает их существование.
SSO	Технология единого входа
УКПМ	Автоматизированная система «Управление корпоративной процессной моделью»
ИБ	Информационная безопастность
ИС	Информационная система
КСПД	Корпоративная сеть передачи данных
СУБД	Система управления базами данных
НН-ОЦО	ООО «Норникель – Общий Центр Обслуживания»

1.2 Назначение документа

Документ «Руководство администратора» предназначен для Администраторов ИС и Администраторов ИБ и содержит описание действий по настройке и контролю параметров безопасности в части информационной безопасности и защите информации.

2. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ АДМИНИСТРАТОРА В ЧАСТИ ОБЕСПЕЧЕНИЯ ИБ

2.1 Управление ролевой моделью

УКПМ обеспечивает разделение прав доступа на основе ролевой модели. Ролевая модель включает в себя следующие роли:

- Пользователь;
- Методолог БП;
- Эксперт КПМ;
- Бизнес-администратор;
- Технический администратор.

Пользователи системы формируются на основании данных Active Directory. Для доступа к ИС используется доменная учетная запись пользователя, сформированная средствами Active Directory. В УКПМ производится авторизация пользователей посредством использования сервисов корпоративного SSO провайдера по протоколу OAuth 2.0. После подтверждения авторизации пользователь получает доступ в соответствии с членством в группе AD. Для обеспечения доступа к системе учетные записи пользователей AD должны быть включены в соответствующие группы, определяющие роль пользователя в системе. Настройка и наименование групп индивидуальны для каждого заказчика

Добавление пользователей в группы Active Directory производится на основании согласованной владельцем ИС заявки.

В ИС обеспечивается разделение (запрет на совмещение) полномочий (ролей):

- выполняющих функции разработки (разработчики, проектировщики) и эксплуатации (администраторы);
- выполняющих функции разработки (разработчики, проектировщики) и использования (пользователи);
- выполняющих функции сопровождения и эксплуатации;
- выполняющих функции эксплуатации (администраторы) и использования (пользователи);
- выполняющих функции администратора ИС и администратора ИБ;
- выполняющих функции разработки, эксплуатации, сопровождения и функции их контроля.

2.2 Управление доступом к ИС и передача данных

При обмене данными УКПМ использует протокол HTTPS с поддержкой криптографических алгоритмов шифрования.

Администратору ИС необходимо поддерживать ИС в рамках выбранной политики безопасности, обеспечивать конфиденциальность и целостность данных, с учетом реализации требований к ИБ УКПМ..

Аутентификация клиента управляется файлом конфигурации /var/lib/pgsql/13/data/pg_hba.conf. В настройках СУБД в файле /var/lib/pgsql/13/data/pg_hba.conf указан доступ по логину и паролю для всех пользователей с ограничением подключения с ip сервера приложения. Каждая запись определяет тип соединения, диапазон IP-адресов клиента (если это актуально для типа соединения), имя базы данных, имя пользователя и метод аутентификации, который будет использоваться для соединений, соответствующих этим параметрам. Первая запись с совпадающим типом соединения, адресом клиента, запрошенной базой данных и именем пользователя используется для аутентификации Доступ к указанному файлу имеет УЗ postgres. Подключение происходит при помощи протокола SSH через 22 порт.

2.3 Настройка и проверка журналов событий

Система журналирования обеспечивает регистрацию действий пользователей в ИС и запись событий, происходящих в системе, таким образом позволяя проследить историю изменений системы.

Администратору ИС необходимо проводить просмотр журналов событий с целью анализа фактов событий безопасности, действия пользователей, привилегированных пользователей и администраторов ИС. Для этого необходимо осуществить вход под учетными данными Администратора ИС, затем осуществить переход к местам хранения журналов, которые указаны Таблица 1.

Места хранения журналов указаны Таблица 1.

Таблица **1**. Места хранения журналов

Наименование	**Место хранения**
БД	/var/lib/pgsql/13/data/log/
Системные журналы	/var/log/
Системный журнал аудита	/var/log/audit/audit.log
Интеграция АСУП	/opt/<название папки>/logs/asup/asup.log
Интеграция ARIS	/opt/<название папки>/logs/aris/aris.log
Интеграция Active Directory	/opt/<название папки>/logs/ad/ad.log
Почтовый сервер	/opt/<название папки>/logs/smpt/smtp.log
Журнал приложения	/opt/<название папки>/<название папки>.log

Команда для просмотра журналов предоставляются при инсталяции.

Для каждого регистрируемого события безопасности производится фиксация данных:

- дата и время возникновения события безопасности;
- идентификатор источника безопасности;
- результат события безопасности;

– тип отправленного запроса сервису (вызвавшего негативный ответ) с идентификатором пользователя или процесса, выполнявшего действие.

УКПМ в автоматическом режиме производит архивирование лог-файлов с ежедневной периодичностью.

Срок хранения информации о событиях безопасности в журналах регистрации событий ИС в течение не менее 3 (трех) месяцев, согласно настройкам БД ИС.

2.4 Восстановление и резервное копирование

Для предотвращения потери данных УКПМ предусмотрена процедура резервного копирования данных.

Резервному копированию подлежат виртуальные машины серверов и БД УКПМ.

Резервное копирование и восстановление конфигураций УКПМ описаны в Регламенте сопровождения УКПМ и осуществляется Корпоративными средствами резервного копирования.

Резервное копирование виртуальных машин серверов УКПМ осуществляется регламентированными средствами резервного копирования, используемыми в Компании (vmware – veeam). Этапы и процедуры описаны в пункте 4.4.

Также, выполнение резервного копирования данных ИС может выполняться штатными средствами СУБД.

Описание процедуры:

На сервере СУБД создать скрипт для выполнения в планировщике ежедневного бекапа:

nano daily_backup.sh
Содержимое файла:

```
cat <<EOF >  daily_backup.sh
#!/bin/sh
# пользователь базы данных
USER=username
# сервер база данных
HOST=localhost
# заменяем your-dababase на имя архивируемой базы данных
DB=your-database
# заменяем your-password на ваш пароль к базе данных
PASSWORD=your-password
# формируемое имя файла
FILENAME=\${DB}_\$(date +%Y_%m_%d_%H_%M_%S).dump
# путь к каталогу с архивными копиями
BACKUPDIR=/backup/dump/
# команда зупуска
PGPASSWORD=\$PASSWORD pg_dump -U \$USER -h \$HOST -O -Fc \$DB > \$BACKUPDIR\$FILENAME
EOF
```

Открываем фаил для редактирования nano daily_backup.sh для изменения переменных
Сохраняем файл, и присваиваем ему статус исполняемого chmod u+x daily_backup.sh.
Этот файл можно добавить в сервис Cron для автоматического создания резервных копий.
Управлять cron нужно с помощью команды 'crontab'.

Команда crontab -l покажет список текущих заданий, crontab -e автоматически запустит текстовый редактор и загрузит в него файл конфигурации cron. После выхода из редактора, новая конфигурация cron будет установлена (вступит в силу) автоматически.

Конфигурационный файл содержит последовательность командных строк и расписание их вызова. Пустые строки и строки, начинающиеся с символа '#' игнорируются. Остальные строки являются установками переменных окружения и командами cron.

Добавляем задание

```
0 1 * * * /backup/scripts/backup_daily.sh
- - - - -
| | | | |
| | | | ----- день недели (0–7) (воскресенье = 0 или 7)
| | | ------- месяц (1–12)
| | --------- день (1–31)
| ----------- час (0–23)
------------- минута (0–59)

Пример задания, которое будет выполняться ежедневно в 01:00
```

```
echo "0 1 * * * /backup/scripts/backup_daily.sh" >> /var/spool/cron/root
# перезапускаем службу cron
systemctl restart crond
```

В случае возникновения ошибок в работе Системы необходимо провести процедуру по восстановлению работоспособности.

Для восстановления необходимо выполнить команду на сервере СУБД под пользователем postgres:

Если база данных уже существует, следующая команда восстановит ее:

```
pg_restore -U username -Fc -d your-database < /backup/dump/your-database_date_YYYY_mm_dd_HH_MM_SS.dump
```

Если база данных еще не существует , следующая команда создаст и восстановит ее:

```
pg_restore -U username -C -Fc -d your-database < /backup/dump/your-database_date_YYYY_mm_dd_HH_MM_SS.dump
```

```
# пользователь базы данных
username
# сервер база данных
localhost
# заменяем your-dababase на имя архивируемой базы данных
your-database
# фаил резервной копии
your-database_date_YYYY_mm_dd_HH_MM_SS.dump
```

```
[root@vmshqkpm02 scripts]# pg_restore -U postgres -C -Fc -d nn_portal < /backup/dump/nn_portal_date_2022_03_30_10_10_00.dump
```

/opt/<название папки> - местоположение папки для восстановления настроек системы, а также файлов (изображения, файлы БЗ), на которые в БД есть ссылки.

УКПМ обеспечивает тестирование резервных копий и возможности восстановления в случае нештатных ситуаций. Тестирование резервных копий и

возможности восстановления в случае нештатных ситуаций описано в Регламенте сопровождения УКПМ в разделе 4.3.3. Настройки резервного копирования виртуальных серверов указаны в Приложении 2 настоящего документа ().

Хранение резервных копий обеспечивает СРК.

2.5 Управление техническими уязвимостями ИБ

После ввода Системы в промышленную эксплуатацию администратору ИБ рекомендуется отслеживать выполнение процедуры периодического сканирования на наличие уязвимостей средствами корпоративного сканера анализа защищенности MaxPatrol.

Администратор УКПМ осуществляет выявление, анализ уязвимостей ИТ-инфраструктуры, ИС и их оперативное устранение.

Для автоматизированного сканирования уязвимостей ИС создана учетная запись mpuser с привилегией sudo.

2.6 Процедура обновления ИС

Для обновления ИС необходимо:

- Остановить приложение: sudo systemctl stop <название папки>
- Создать архив текущей установки приложения: sudo mv /opt/<название папки>/<название папки>.jar /opt/<название папки>/<название папки>_{текущая дата}.jar.bak
- Заменить файл /opt/<название папки>/<название папки>.jar обновленным файлом
- Запустить приложение: sudo systemctl start <название папки>
- Проверить добавлено ли приложение в автозагрузку: systemctl is-enabled <название папки>. Если приложение не добавлено, добавить его командой: systemctl enable <название папки>
- В логе /opt/<название папки>/logs/<название папки>.log должна появится строка "Started PortalApplication in" тогда приложение считается запущенным - обновление успешно

Если приложение не запустилось (обновление считается не успешным) восстановить приложение из архива - sudo mv /opt/<название папки>/<название папки>_{текущая дата}.jar.bak /opt/<название папки>/<название папки>.jar

Проводимая процедура обновления ИС должна отвечать следующим требованиям:

- Все применимые обновления безопасности компонентов ИС и ее СЗИ устанавливаются в течение рекомендуемого производителем срока с момента их выпуска.
- Получение обновлений безопасности осуществляется только из доверенных источников

- Перед установкой обновлений проводится их тестирование на тестовой группе перед их тиражированием на все ИС.
- Разработку и тестирование изменений ИС необходимо производить только в тестовой среде ИС. Перед установкой обновлений на продуктивный контур производится полное тестирование на тестовой среде.
- Установка средств разработки запрещена, и не должна использоваться как на этапе тестирования, так и в продуктивной среде.

2.7 Обновление справочников с использованием файла-шаблона

Большинство справочных таблиц УКПМ обновляются посредством автоматизированного получения данных с использованием интеграционных решений со смежными информационными системами.

Для справочника «Организации» в УКПМ предусмотрен дополнительный инструмент, позволяющий дополнить таблицу данными, отсутствующими в системе-источнике.

Администрирование/Настройка НСИ/Справочник «Организации» => Добавить организации.

В модальном окне «Добавление организации» необходимо:

1. Нажать на кнопку «Выбрать файл» и загрузить заполненный файл-шаблон.
2. Нажать кнопку «Применить».

После выполнения процедуры дополнения справочника «Организации» Технический Администратор УКПМ производится выборочная проверка корректности загрузки данных (поиск загруженных организаций в справочнике УКПМ).

2.8 Управление конфигурациями

УКПМ развернута на ИТ-инфраструктуре Компании. Настройка компонентов ИТ-инфраструктуры выполняется согласно корпоративным методическим документам по конфигурированию систем и компонентов. При настройке ИС должны использоваться максимальные версии стороннего ПО, учитываться рекомендации производителей ПО.

Администратору ИБ необходимо осуществлять контроль изменений в конфигурации ИТ-инфраструктуры, включая СЗИ, в рамках проведения процедуры аудита ИБ.

Разработка и тестирование изменений ИС на продуктивном экземпляре ИС не допускается.

2.9 Управление инцидентами ИБ

Администратором ИС обеспечивается своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов ИБ пользователями и администраторами.

Администратору ИБ необходимо проводить анализ инцидентов ИБ, в ходе которого определяются источники и причины возникновения инцидентов ИБ, а также

проводится оценка их последствий, а также принимаются меры по устранению последствий инцидентов ИБ.

После проведения анализа инцидентов ИБ администратору ИБ необходимо запланировать и принять меры по предотвращению повторного возникновения инцидентов ИБ.

2.10 Замена SSL-сертификата

Администратору ИС рекомендуется отслеживать дату окончания действия SSL-сертификата и своевременно проводить процедуру замены.

Рекомендуемая процедура замены:

В папке приложения отредактировать файл application.yaml, прописать путь (текущее местоположение сертификата- application.yaml, файл enabled-protocols) и зашифрованный пароль (см. пункт 2.10.3) к сертификату pfx. Пароль сертификата в формате pfx должен отвечать требованиям для паролей технических УЗ (см. пункт 2.11.1).

2.11 Настройки ИС

Настройки и их описание представлены в Приложении №1.

Для просмотра всех настроек, реализованных в УКПМ, необходимо перейти к архиву /opt/<название папки>/<название папки>.jar и открыть файл:

cat ./BOOT-INF/classes/META-INF/spring-configuration-metadata.json

в котором содержится актуальные настройки в системе с описанием, в виде JSON

{

"name": "portal.aris.url",

"type": "java.lang.String",

"description": "Aris WS URL",

"sourceType": "ru.baccasoft.nn.portal.aris.ArisProperties"

}

Таблица 2 – Описание настроек ИС по интеграциям

Код	Описание
Параметры для интеграции с Aris	
portal.aris.connect-timeout	Тайм-аут подключения для HTTP-клиента Aris
portal.aris.password	Пароль Aris WS для базовой аутентификации
portal.aris.published-only	Какие ПБ отправлять в ARIS: только опубликованные или все (по умолчанию только опубликованные)
portal.aris.read-timeout	Тайм-аут чтения для HTTP-клиента Aris (soTimeout)
portal.aris.trust-store	Aris WS trust store location. Используется для закрытых сертификатов CA

portal.aris.trust-store-password	Aris WS доверенное хранилище пароля
portal.aris.trust-store-type	Aris WS тип доверенного хранилища
portal.aris.url	Aris WS URL
portal.aris.username	Пользователь Aris WS для базовой аутентификации
Параметры для интеграции с AD	
portal.auth.adfs.attrs.email	Атрибутное имя E-Mail
portal.auth.adfs.attrs.groups	Имя атрибутов групп AD
portal.auth.adfs.groups	Сопоставление идентификаторов групп и ролей ADFS
portal.auth.adfs.logout-url	Пользовательский URL для входа. Используется для ADFS тестирования
portal.auth.adfs.url	Базовый URL-адрес сервера ADFS
portal.auth.adfs.use-db-roles	Не используйте группы ADFS и выбирайте роли непосредственно из базы данных. Используется для тестирования. Don't use ADFS groups and pick roles directly from database. Useful for testing
Параметры для интеграции с почтовой системой	
portal.mail.connect-timeout	SMTP Connection Timeout
portal.mail.default-encoding	TBD
portal.mail.filter	Регулярное выражение для фильтрации получателей. Используется для тестирования
portal.mail.host	SMTP хост
portal.mail.password	SMTP пароль
portal.mail.port	SMTP порт
portal.mail.read-timeout	SMTP Read Timeout (soTimeout)
portal.mail.sender	Используется, если в сообщении нет отправителя (от)
portal.mail.test	Включена конечная точка POST / api / mail. Используется для тестирования SMTP
portal.mail.username	SMTP имя пользователя

2.12 Смена паролей

2.12.1 Смена паролей технических учетных записей

Обязанностью Администратора ИС является периодическая смена паролей технических учетных записей. Процедура смены паролей технических учетных записей должна выполняться не реже 1 раза в год. При вводе ИС в промышленную эксплуатацию пароли учетных записей, использовавшихся на стадии проектирования и реализации, изменяются администраторами соответствующих ИС. Перечень технических учетных записей приведен в Паспорте ИС.

При смене пароля технических учетных записей необходимо учитывать, что пароли технических учетных записей должны отвечать следующим требованиям:

- сгенерированы случайным образом специальными утилитами для генерации паролей;

- длина пароля составляет не менее 12 (двенадцати) символов;
- пароль содержит буквы в верхнем и нижнем регистрах, цифры, специальные символы (@, #, $, &, *, % и т.п.), не включают очевидных слов и комбинаций;
- новый пароль не совпадает с пятью предыдущими;
- количество попыток неудачного ввода – не более 7 (семи), после 5 (пятой) попытки усложняющие техники вода: CAPTCHA, увеличение времени ожидания;
- блокировка учетной записи после исчерпания лимита попыток неудачного ввода, без возможности автоматического разблокирования по таймауту;
- возможность копирования и вставки в поле ввода;
- срок действия пароля не более 12 (двенадцати) месяцев;
- пароли не включают очевидных слов и комбинаций, повторяющихся символов, сочетаний символов (более трех), последовательно расположенных на клавиатуре, контекста (имени, фамилии пользователя, даты рождения, названия приложения и т.д.), не входят в общедоступные словари часто используемых паролей.
- Примеры запрещенных к использованию паролей: дата рождения, имя, набор цифр, последовательность близко расположенных на клавиатуре букв и т.п.

2.12.2 Смена паролей административных/третьих лиц учетных записей

Пароли учетных записей: техническая/административная/административная третьего лица отличны от всех других паролей учетных записей данного пользователя.

Пароли учетных записей: административная/административная третьего лица должны отвечать следующим требованиям:

- длина пароля составляет не менее 12 (двенадцати) символов;
- пароль содержит буквы в верхнем и нижнем регистрах, цифры и при необходимости специальные символы (@, #, $, &, *, % и т.п.) не включают очевидных слов и комбинаций;
- новый пароль не совпадает с пятью предыдущими;
- количество попыток неудачного ввода – не более 7 (семи), после 5 (пятой) попытки усложняющие техники вода: CAPTCHA, увеличение времени ожидания;
- время блокировки учетной записи после исчерпания лимита попыток неудачного ввода - не менее 15 (пятнадцати) минут;
- возможность копирования и вставки в поле ввода;
- срок действия пароля не более 45 (сорока пяти) дней;

- пароли не включают очевидных слов и комбинаций, повторяющихся символов, сочетаний символов (более трех), последовательно расположенных на клавиатуре, контекста (имени, фамилии пользователя, даты рождения, названия приложения и т.д.), не входят в общедоступные словари часто используемых паролей.
- Примеры запрещенных к использованию паролей: дата рождения, имя, набор цифр, последовательность близко расположенных на клавиатуре букв и т.п.

2.12.3 Смена паролей в настройках ИС

- Скачать и распаковать архив wget https://github.com/jasypt/jasypt/releases/download/jasypt-1.9.3/jasypt-1.9.3-dist.zip
- Для шифрования пароля выполнить команду в командной строке:
- unzip jasypt-1.9.3-dist.zip

sh ./jasypt-1.9.3/bin/encrypt.sh \

algorithm=PBEWITHHMACSHA512ANDAES_256 \

saltGeneratorClassName=org.jasypt.salt.RandomSaltGenerator \

ivGeneratorClassName=org.jasypt.iv.RandomIvGenerator \

password="*JASYPT_ENCRYPTOR_PASSWORD*" \

input="*NEW_PASSWORD*"

Параметры: NEW_PASSWORD – новый пароль, JASYPT_ENCRYPTOR_PASSWORD – переменная окружения сервера приложения, также она хранится в файле /etc/systemd/system/<название папки>.service.d/override.conf.

- Полученный зашифрованный пароль сохранить в nano /opt/<название папки>/BOOT-INF/classes/application.yaml на сервере приложения в формате ENC(Шифрованный пароль).
- Перезапускаем приложение:

systemctl restart <название папки>

2.12.4 Смена пароля, хранящегося в переменной окружения JASYPT_ENCRYPTOR_PASSWORD

- Скачать и распаковать архив https://github.com/jasypt/jasypt/releases/download/jasypt-1.9.3/jasypt-1.9.3-dist.zip
- Расшифровать все пароли, хранящиеся в настройках /opt/<название папки>/application.yaml,
- Получить все пароли можно командой: cat /opt/<название папки>/BOOT-INF/classes/application.yaml | grep ENC

– заданные в формате: ENC(Шифрованный пароль) с помощью команды, ввести в командной строке:

sh ./jasypt-1.9.3/bin/decrypt.sh \

algorithm=PBEWITHHMACSHA512ANDAES_256 \

saltGeneratorClassName=org.jasypt.salt.RandomSaltGenerator \

ivGeneratorClassName=org.jasypt.iv.RandomIvGenerator \

password="*JASYPT_ENCRYPTOR_PASSWORD*" \

input="*ENC_PASSWORD*"

Параметры: ENC_PASSWORD – зашифрованный пароль, JASYPT_ENCRYPTOR_PASSWORD – переменная окружения сервера приложения, также она хранится в файле /etc/systemd/system/<название папки>.service.d/override.conf.

– Выполняем команду для изменения:

systemctl edit <название папки>

– - Изменяем переменную окружения JASYPT_ENCRYPTOR_PASSWORD.

[Service]

Environment="JASYPT_ENCRYPTOR_PASSWORD=<new_password>"

Переменная окружения JASYPT_ENCRYPTOR_PASSWORD должна отвечать требованиям для паролей технических УЗ (см. пункт 2.10.1). Настройка сохраняется в файл: /etc/systemd/system/<название папки>.service.d/override.conf

– Обновляем пароли в настройках приложения ИС для новой переменной окружения JASYPT_ENCRYPTOR_PASSWORD см. 2.10.3.

– Перезапускаем приложение:

systemctl restart <название папки>

2.12.5 Настройка синхронизации с NTP серверами

Для настройки синхронизации с NTP серверами необходимо выполнить следующие действия:

1) Отредактировать файл /etc/chrony.conf;
2) Перезагрузить службу синхронизации командой systemctl restart chronyd.

2.13 Настройка фильтрации ЭЦП

Администратору ИС, необходимо отслеживать и вести файл конфигурации/

```
qeds:
  caList:
    - "Тестовый УЦ им.\"Семашко\""
    - "\"АО \"\"ПФ \"\"СКБ Контур\"\"\""
    - "Препродуктовый УЦ"

```

3. ПОРЯДОК ПРОВЕДЕНИЯ АУДИТА В ЧАСТИ ИБ

В обязанности администратора УКПМ входит проведение мероприятий, направленных на:

- осуществление контроля соответствия состава технических средств, программного обеспечения приведенному в эксплуатационной документации с целью поддержания актуальной конфигурации ИС и принятие мер, направленных на устранение выявленных недостатков;
- проведение аудита состава технических средств, программного обеспечения на соответствие сведениям эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков и уязвимостей ИС;
- исключение или восстановление из состава ИС несанкционированно установленных или удаленных технических средств, программного обеспечения и средств защиты информации;
- проверки актуальности документации и, при необходимости, ее корректировка.

Контроль состава технических средств, программного обеспечения рекомендуется проводить с периодичностью 1 (один) раз в квартал. Все изменения необходимо фиксировать в паспорте ИС УКПМ.

4. УСТРАНЕНИЕ НЕПОЛАДОК В РАБОТЕ ИС

4.1 Действия в случае несоблюдения условий выполнения технологического процесса, в том числе при длительных отказах технических средств

В случае сбоя в работе аппаратуры восстановление нормальной работы Системы должно быть произведено после:

- перезагрузки операционной системы;
- перезапуска ИС УКПМ

В ходе работы с Системой могут возникнуть следующие неисправности, приводящие к аварийным ситуациям:

- несоблюдение условий выполнения технологического процесса, в том числе при длительных отказах технических средств;
- отказ магнитных носителей или обнаружение ошибок в данных;

– обнаружение несанкционированного вмешательства в данные.

4.2 Действия по восстановлению программ и/или данных при отказе магнитных носителей или обнаружении ошибок в данных

При отказе магнитных носителей для восстановления программ и/или данных необходимо осуществить:

– восстановление инфраструктуры и программно-аппаратной конфигурации серверов;

– восстановление базы данных из резервной копии;

4.3 Действия в случаях обнаружения несанкционированного вмешательства в данные

В случае обнаружения несанкционированного вмешательства в данные установите логин пользователя, под которым была произведена аутентификация, затем смените пароль пользователя и проинформируйте пользователя о смене пароля.

4.4 План восстановления системы

Восстановление ВМ происходит по запросу в службу ITSM и распределяется на Направление инфраструктурных приложений.

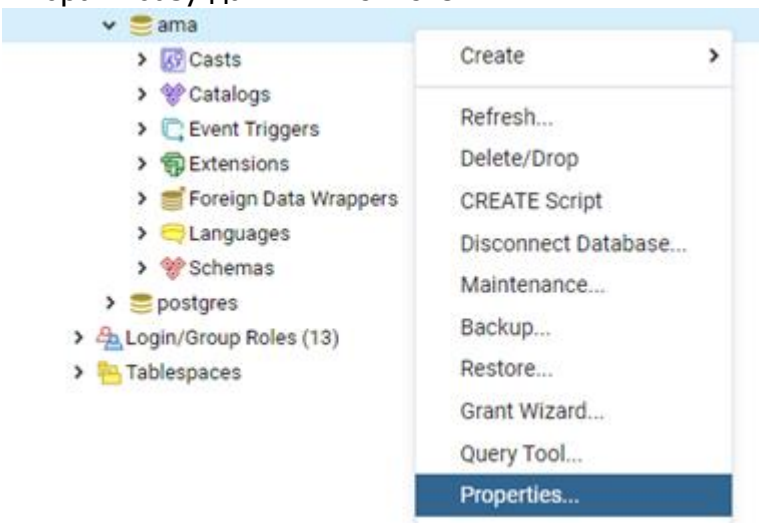
Правила отключения/неотключения автоматизированных систем формируются внутренним регламентом организации и регламентом обслуживания и профилактических работ.

Восстановление системы производится в соответствии с регламентом резервного копирования.

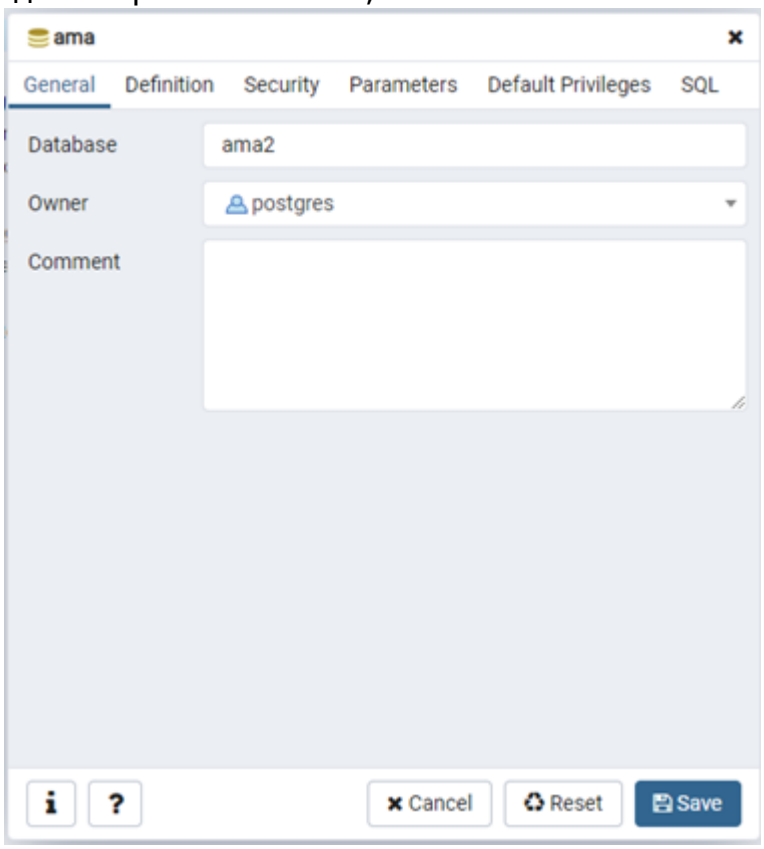
4.5 Локальное восстановление БД из бэкапа через pgAdmin

1. Необходимо запустить «pgAdmin».
2. Подключиться к серверу базы данных, используя пароль.

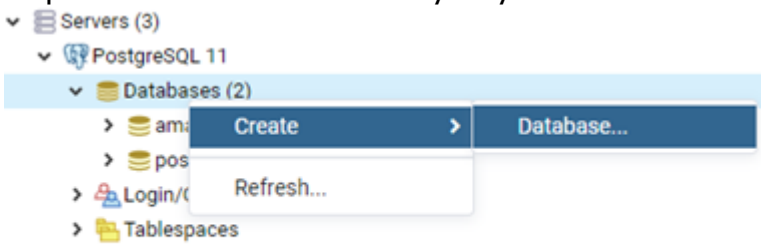
   Выбрать базу данных в списке.



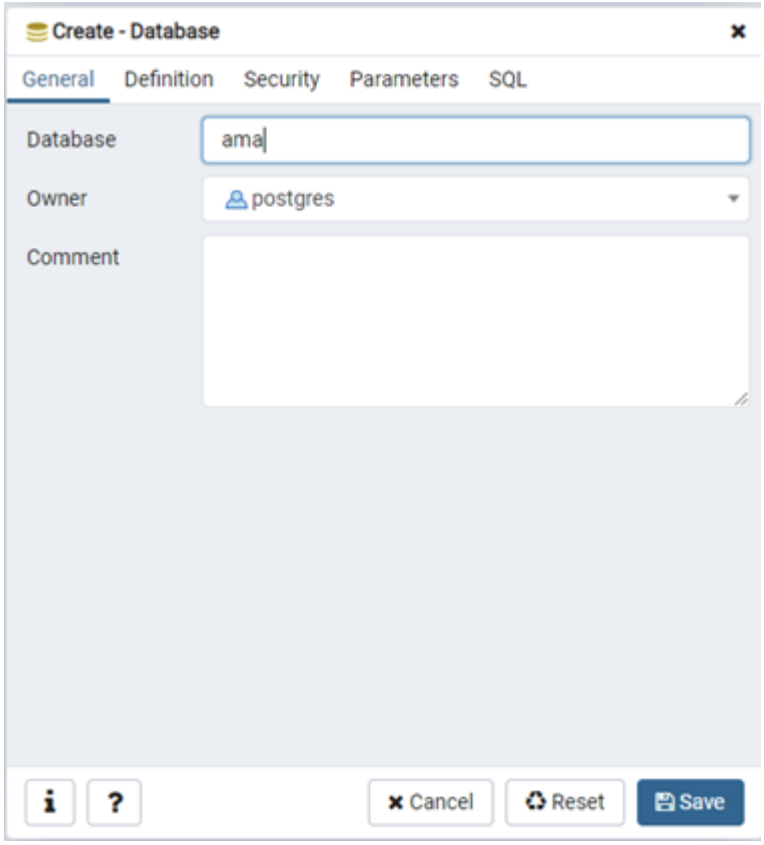
3. Необходимо переименовать её, нажать Save.



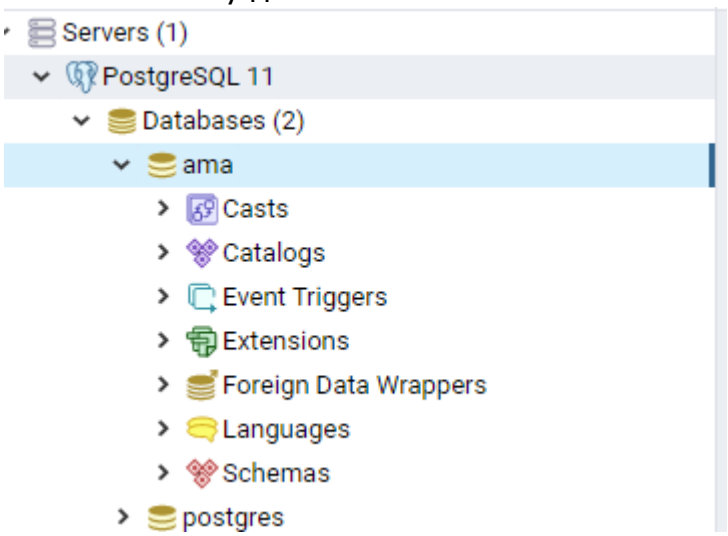
4. Нажать правой кнопкой мыши по пункту Databases -> Create -> Database…



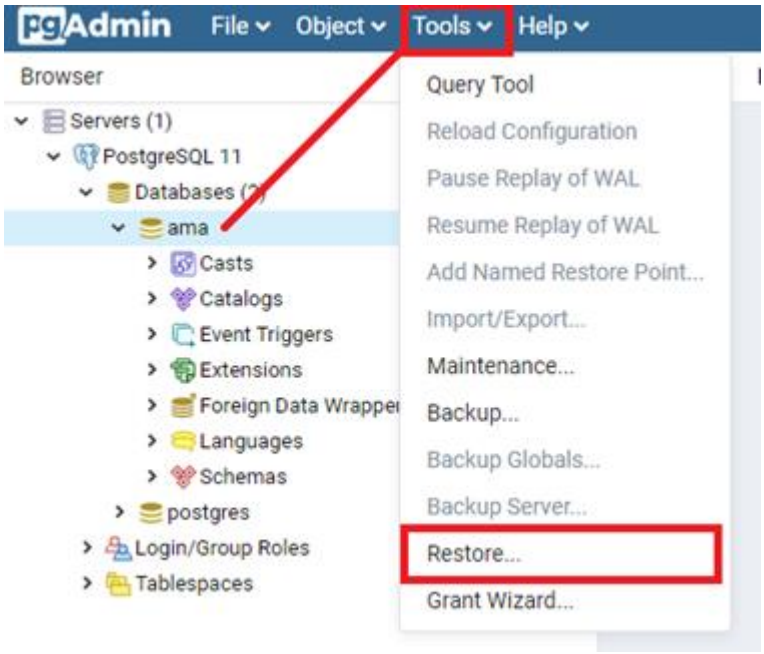
5. Ввести изменённое название базы данных, нажать Create.



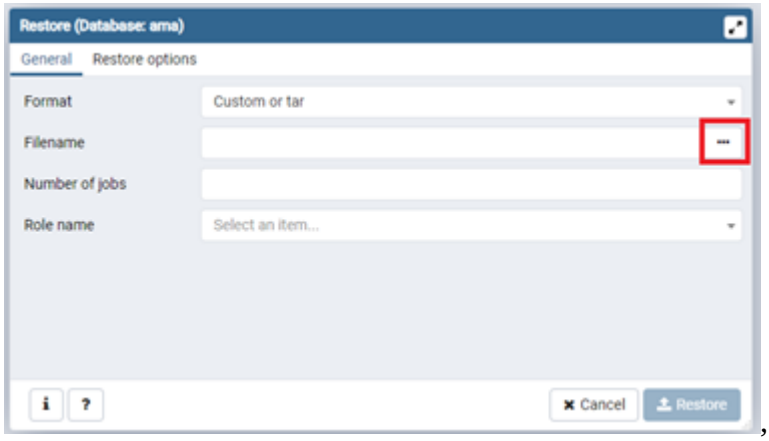
6. Выбрать в списке базу данных.



7. Нажать на пункт меню «Tools» и выбрать пункт «Restore».

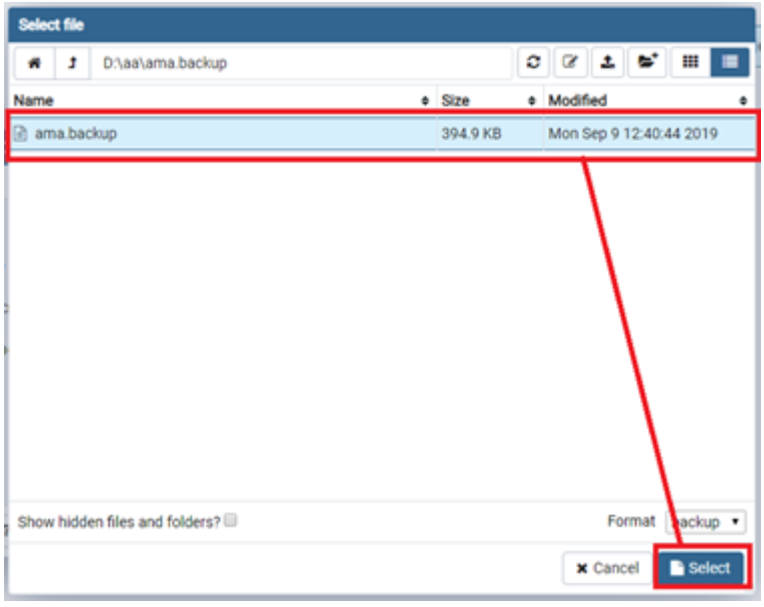


8. В появившемся окне нажать на «...» в поле Filename.

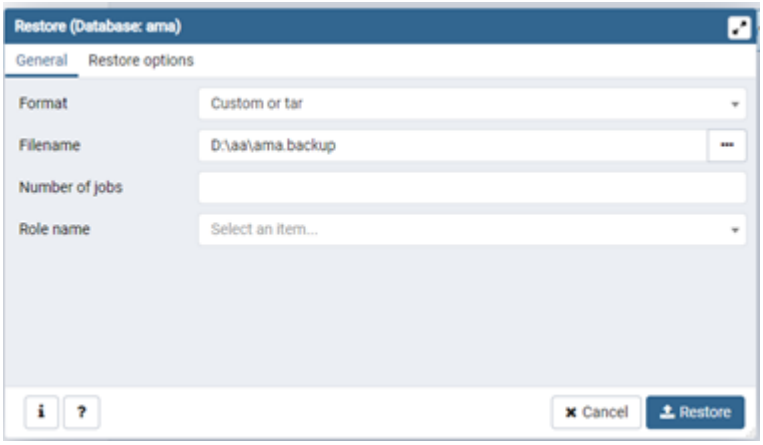


,

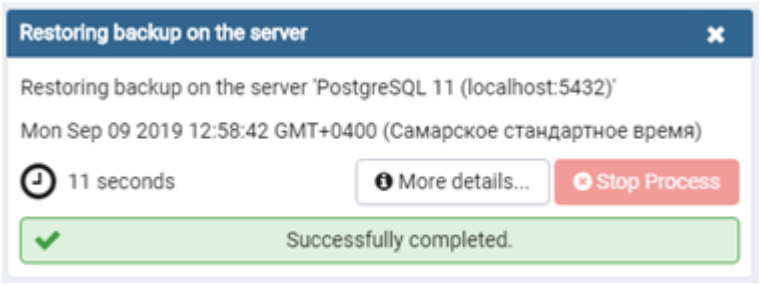
9. В окне выбора файла необходимо задать формат резервной копии «backup», затем найти файл резервной копии, выбрать его, нажать «Select».



10. Затем вернуться в окно настроек резервной копии, нажать «Restore».



11. Далее запустится процесс восстановления базы данных, затем появится окно:



12. Далее необходимо снова подключиться к базе данных для продолжения работы.

5. ОПИСАНИЕ ЗАПИСЕЙ ЛОГОВ ИС

В таблице 4 представлено описание событий. которые записываются в файлы логов:

- По действия пользователей (файл логов security.log).
- По интеграции Active Directory (файл /logs/ad/ad.log).
- По REST-интеграции SharePoint (файл /logs/sp/sp.log).