ООО «Прикладные системы»

РУКОВОДСТВО АДМИНИСТОРАТОРА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ «ATOMIC KEEPER» v.2.0

Минск, 2023

СОДЕРЖАНИЕ

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сокращение (обозначение)	Расшифровка (пояснение)
АСУиК ЯМ	Автоматизированная система учета и контроля ядерных материалов
АЭС	Атомная электростанция
ЗБМ	Зона баланса материалов
ИС	Изотопный состав
КТИ	Ключевая точка измерений
МАГАТЭ	Международное агентство по атомной энергии
МБО	Материально-балансовый отчет
ОИИК	Отчет об изменении инвентарного количества
ОС	Операционная система
СУБД	Система управления базами данных
УЕ	Учетная единица
ЯМ	Ядерный материал
ЯМ МК	Ядерный материал малых количеств
ICR	Inventory Change Report
MBR	Material Balance Report
PIL	Physical Inventory Listing

1. ОБЩИЕ ПОЛОЖЕНИЯ

Руководство администратора автоматизированной системы учёта и контроля ядерных материалов «Atomic Keeper» v.2.0 (далее — Руководство) содержит пошаговые инструкции и пояснения по основным операциям, выполняемым администратором системы.

1.1. Область применения

Автоматизированная система учета и контроля ядерных материалов «Atomic Keeper» v.2.0 (далее – АСУиК ЯМ 2.0.) предназначена для автоматизации процедур учета и контроля ядерных материалов малых количеств, централизованного хранения и обработки данных по обращению с ЯМ МК на АЭС, формирования отчетной и учетной документации, а также предоставления достоверной информации о местоположении ЯМ МК на территории АЭС.

1.2. Основные возможности и функции АСУиК ЯМ 2.0.

АСУиК ЯМ 2.0. предоставляет следующие основные возможности:

сбора, обработки и хранения информации о свойствах и характеристиках ЯМ МК, используемых на атомной электростанции;

формирования и ведения учетных и отчетных документов;

предоставления информации о текущем местоположении и количестве ЯМ МК в местах их нахождения.

К основным функциям АСУиК ЯМ 2.0. относятся:

1. учет характеристик каждой учетной единицы, ведение их истории изменения;
2. учет местоположения каждой учетной единицы;
3. регистрация операций и работ, выполняемых с учетными единицами;
4. регистрация всех перемещений учетных единиц;
5. формирование документации, необходимой специалистам АЭС до, во время или после выполнения работ с ЯМ МК;
6. предоставление данных о количестве ядерных материалов в ЗБМ малых количеств;
7. формирование документации о наличии ядерных материалов количеств и их местоположения, а также учетных отчетов установленной формы (ICR, PIL, MBR, ОИИК ЯМ МК);
8. ведение учетных документов (Главный и Вспомогательный журналы, журнал структурного подразделения, учетные карточки);
9. обеспечение информационного сопровождения инспекций и физических инвентаризаций, проводимых в ЗБМ малых количеств на АЭС;

10. обеспечение проверки вводимых (выбираемых) данных на соответствие валидационным критериям.

1.3. Уровень подготовки администратора.

Администратор обязан знать:

настоящее Руководство и иметь представление о работе основных интернет-технологий;

соответствующую терминологию настоящего документа;

основные принципы работы сайтов.

Администратор системы должен обладать следующими знаниями и навыками:

настройка и диагностирование работы системы;

обслуживание технического и системного программного обеспечения системы;

администрирование баз данных;

резервное копирование и восстановление данных;

обеспечение регламентных работ и анализ результатов регламентных операций.

сопровождение и администрирование локальной вычислительной сетей, протокола TCP/IP;

настройка рабочих станций локальной вычислительной сети;

инсталляция, общесистемное сопровождение и администрирование;

администрирование СУБД.

2. ОСНОВНОЕ ОПИСАНИЕ АРХИТЕКТУРЫ СИСТЕМЫ

2.1. Построение архитектуры.

Построение архитектуры системы реализовано по MVC-шаблону («Model-View-Controller» паттерн) с разделением данных приложения, пользовательского интерфейса и управляющей логики на три отдельных компонента. Таким образом, в системе можно выделить следующие уровни:

1. Уровень пользовательского интерфейса;
2. Уровень бизнес-логики;
3. Уровень базы данных.

Верхним уровнем является уровень интерфейса пользователя. На этом уровне система содержит формы ввода/вывода информации, функции проверки корректности вводимых данных до их обработки на стороне сервера. Интерфейс реализуется на языке разметки HTML5/CSS3 и с помощью языков программирования TypeScript, JavaScript.

На уровне бизнес-логики система содержит программные коды, выполняющие функции поддержки необходимых операций. Уровень бизнес-логики написан на языке C#.

Уровень базы данных состоит из таблиц необходимых для полноценной работы системы учета и контроля. Связь уровня бизнес-логики и уровня базы данных происходит с помощью O/RM от Microsoft Entity Framework и синтаксиса LINQ.

2.2. Техническое и программное обеспечение.

Система реализована с использованием следующих технологий:

1. NET 6;
2. ASP.NET Core 6;
3. СУБД MS SQL Server или PostgreSQL;
4. HTML5, CSS3
5. C#, Transact-SQL, TypeScript, JavaScript, Angular 12.

Функционирование системы обеспечивается следующим программным обеспечением:

1. Серверная часть

1.1. Для Windows:

Операционная система Windows Server 2019;

СУБД MS SQL Server 2019 или PostgreSQL 14;

1.2. Для Linux:

Linux Astra Smolensk 1.6;

PostgreSQL 9.X

2. Клиентская часть

Операционная система Windows 10;

Веб-обозреватель Chrome (105 и выше);

Средства создания и редактирования документации MS Office (2016 и выше).

2.3. Информация по безопасности АСУиК ЯМ 2.0.

Все действия пользователей, выполняемые в АСУиК ЯМ 2.0. регистрируются и хранятся в журнале событий бессрочно. Для исключения переполнения журнала аудита и потери записей из-за нехватки дискового пространства администратору необходимо своевременно контролировать достаточный объем памяти на сервере, где установлена АСУиК ЯМ 2.0. (См. п.5.4.)

Конфиденциальная информация, ключи API и пароли не содержаться в исходном коде или репозиториях исходного кода, кроме одной учетной записи администратора (логин: admin, пароль: admin) используемой для первоначального входа в АСУиК ЯМ 2.0. после ее установки. Данные стандартной учетной записи администратора персонализируются при первом входе в систему.

В АСУиК ЯМ 2.0. используются следующие роли пользователей:

Роль	Назначение
Администратор	Выполнение функций администрирования АСУиК ЯМ 2.0. описанных в главе 4.
Настройщик	Назначается пользователю для редактирования (добавления/изменения/удаления) информации (при возможности) в разделах модуля «Справочники».
Учетчик	Назначается пользователю для выполнения основного функционала АСУиК ЯМ 2.0. связанного непосредственно с учетом и контролем ЯМ МК.

Для реализации раздельного хранения системных файлов и файлов конфигурации, принадлежащие АСУиК ЯМ 2.0., а также журнала событий от пользовательских данных, необходимо установить АСУиК ЯМ 2.0. и базу данных в разные места (каталог, системный раздел и т. д.). Экспортированный журнал событий хранить так же отдельно.

Для аутентификации пользователей используется современный протокол Oauth 2.0.

Доступ пользователя к функциональности АСУиК ЯМ 2.0. обеспечивается использованием персонального компьютера и IP-адреса, который входит в перечень доверенных IP-адресов.

Ввод пароля в интерфейсе системы скрыт, и не виден другим лицам.

Для предотвращения ввода вредоносных команд в АСУиК ЯМ 2.0. реализована валидация вводимых пользователем данных.

Пользовательская сессия завершается по таймауту, заданному настройками администратора или после нажатия кнопки «Выход».

3.ПОДГОТОВКА К УСТАНОВКЕ И ИНСТАЛЯЦИЯ «ATOMIC KEEPER» V.2.0

Подготовка к установке АСУИК ЯМ 2.0. включает в себя установку и настройку на сервере в зависимости от ОС (Windows или Linux) следующих программных продуктов:

MS SQL server (только для Windows) или PostgreSQL.

(опционально) SSL certificate

ПО АСУиК ЯМ «Atomic Keeper» v.2.0.

3.1. Подготовка к установке и инсталляция «Atomic Keeper» v.2.0 для Windows.

3.1.1 Настройка MSSQL Server

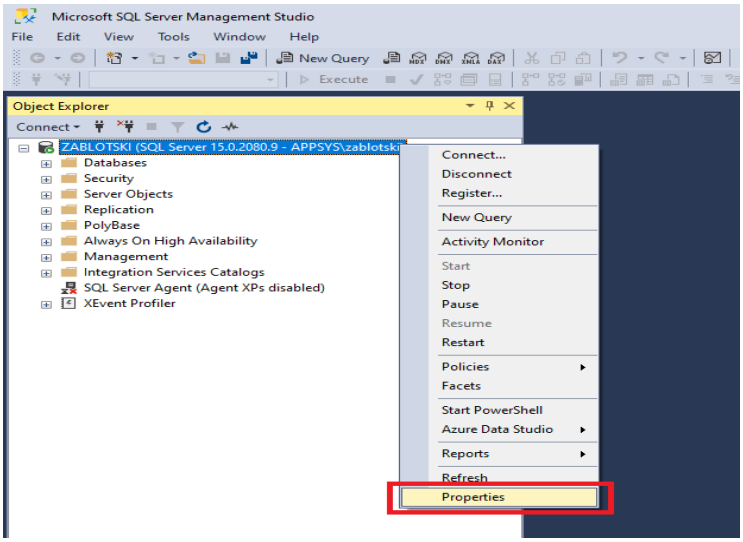
SQL Server – это программное обеспечение от компании Microsoft. Представляет собой комплексный продукт, который содержит функционал, необходимый для создания и управления базами данных. Необходим здесь для хранения данных, генерируемых или вводимых пользователем, в процессе работы АСУИК ЯМ 2.0.

Для настройки SQL Server необходимо выполнение следующих предварительных условий:

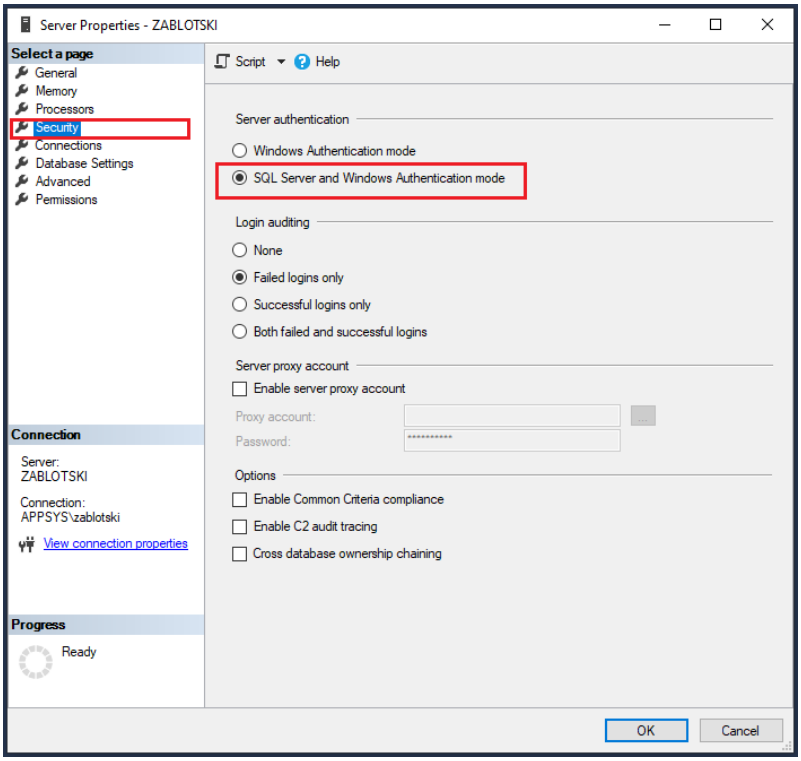
1. **SQL Server 2016+** установлен с полным функционалом (на вкладке **Feature Selection** активирована опция **Select All**).
2. Установлен **SQL Server Management Studio**.

Выполнение настройки MSSQL Server производится следующим образом:

1. Открыть SQL Server Management Studio.
2. На странице **Object Explorer**, правым щелчком выделить сервер, затем выбрать **Properties:**



3. На странице **Select a page**, выбрать **Security → Server authentication → SQL Server and Windows Authentication mode** и нажать **OK**:

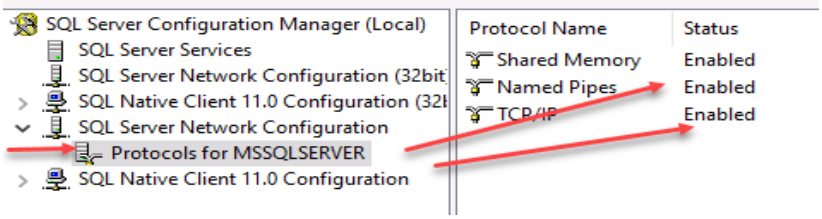


4. Активировать поддержку протоколов **Named pipes** и **TCP.**

4.1. Открыть **SQL Server Configuration Manager.**

4.2. Развернуть **SQL Server Network Configuration -> Protocols for MSSQLSERVER.**

4.3. Активировать (enable) поддержку протоколов **Named Pipes** and **TCP/IP**, если они не были выбраны ранее. Для этого правым щелчком выбрать протокол, а затем **Enabled**:

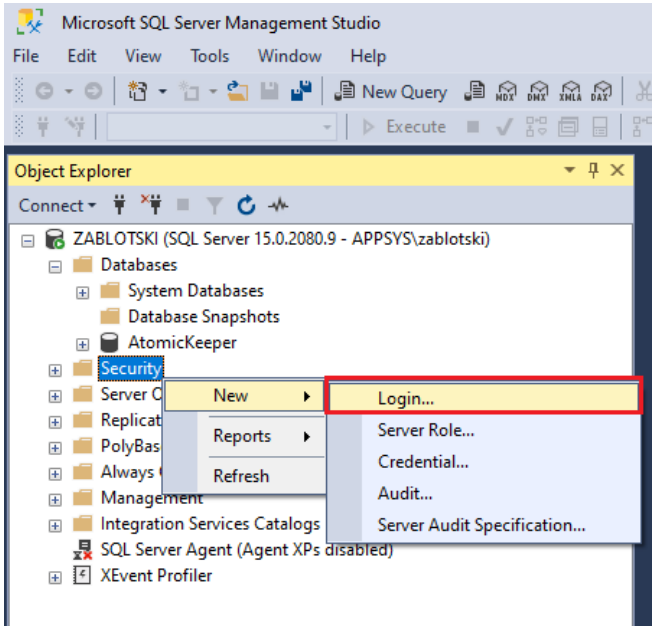


4.4. Перезапустить **SQL Server services** или компьютер.

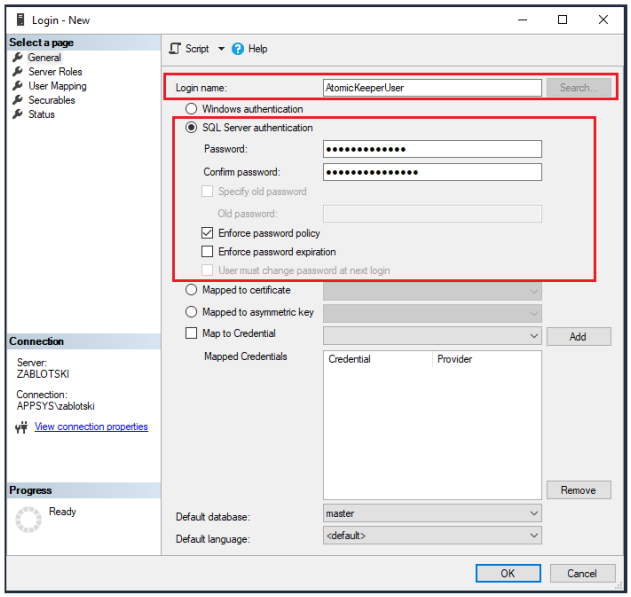
5. Создать пользователя для SQL:

5.1. Открыть SQL Server Management Studio.

5.2. В **SQL Server Management Studio Object Explorer**, правым щелчком выбрать **Security** > **New** > **Login**:



5.3. На вкладке **General** выбрать **SQL Server authentication**, ввести **Login name**, затем заполнить поля **Password** и **Confirm password**. Деактивировать опции **Enforce password expiration** и **User must change password at next login**.

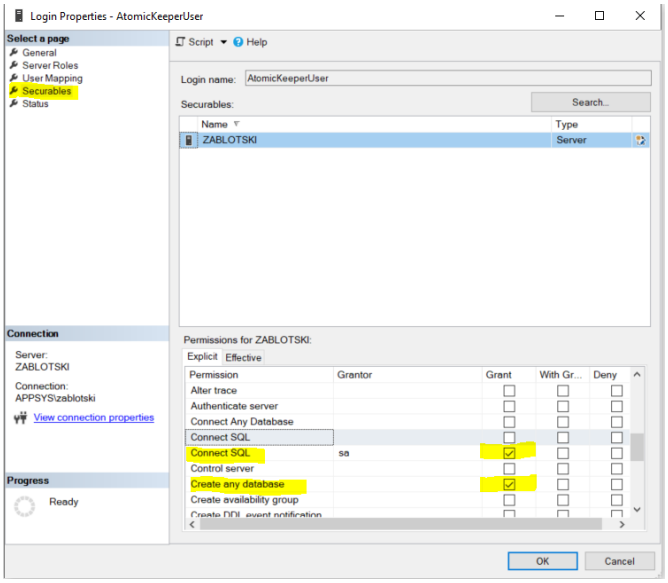


5.4. Нажать OK

5.5. В окне **Object Explorer** разверните **Security > Logins**. Найдите здесь созданного пользователя на шаге 5, щелкните его правой кнопкой мыши и перейдите в раздел **Properties > Securables**.

5.6. В разделе **Securables** включите разрешения **Create any database** и **Connect SQL**, если они не включены. Нажмите **ОК.**

ПРИМЕЧАНИЕ. После установки AtomicKeeper права на создание базы данных могут быть удалены.



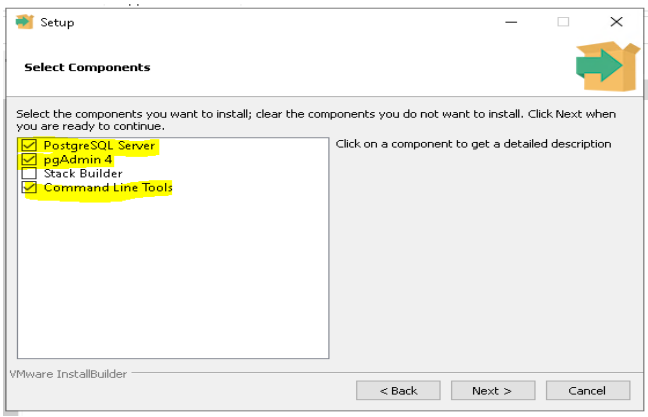
3.1.2 Настройка PostgreSQL.

PostgreSQL — это мощная система объектно-реляционных баз данных с открытым исходным кодом, которая использует и расширяет язык SQL в сочетании со многими функциями, позволяющими безопасно хранить и масштабировать самые сложные рабочие нагрузки данных. PostgreSQL имеет множество функций, призванных помочь разработчикам создавать приложения, администраторам защищать целостность данных и создавать отказоустойчивые среды, а также помогать управлять своими данными, независимо от того, насколько велик или мал набор данных.

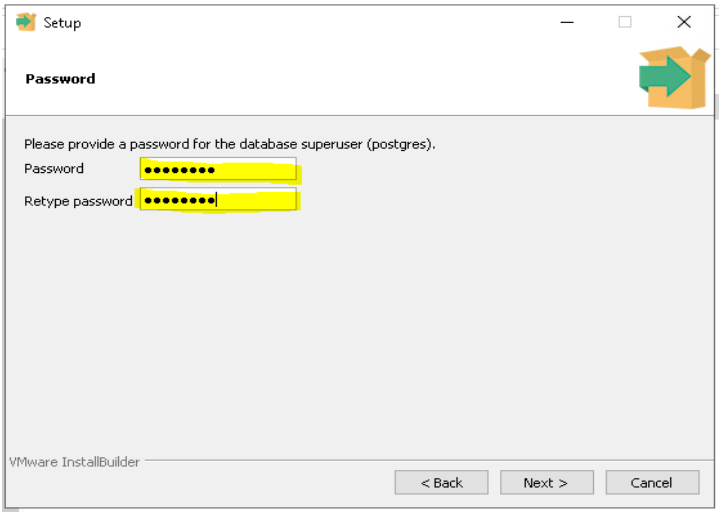
1. Установка PostgreSQL.

1.1. Загрузить и запустить установочный пакет Postgresql 14.x.

1.2. В процессе установки выберите следующие функции: **PostgreSQL Server, pgAdmin 4, Command Line Tools.**



1.3. В диалоговом окне «Пароль» ввести пароль PostgreSQL (этот пароль будет вашим мастер-паролем при первом входе в систему) и нажать кнопку **Next**.



1.4. В диалоговом окне «Порт» оставить значение по умолчанию (5432), нажать **Next** и завершить установку.

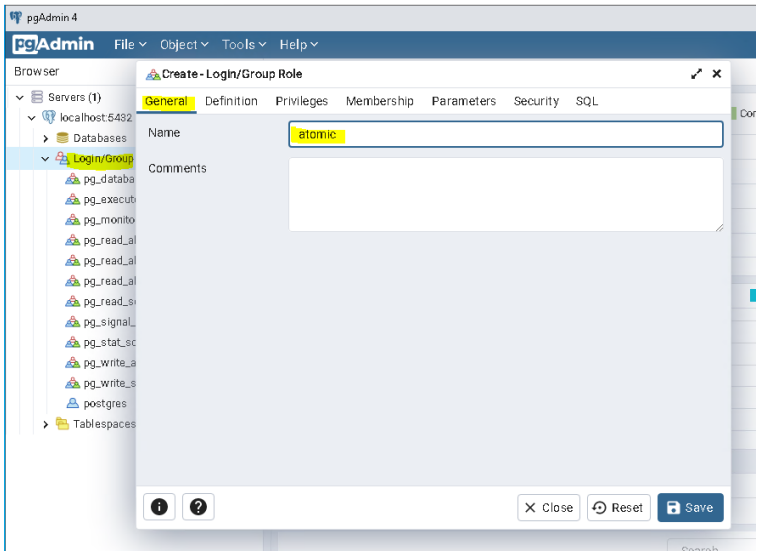
2. Создание пользователя базы данных.

2.1. Запустить утилиту pgAdmin (установлена из установочного пакета Postgresql).

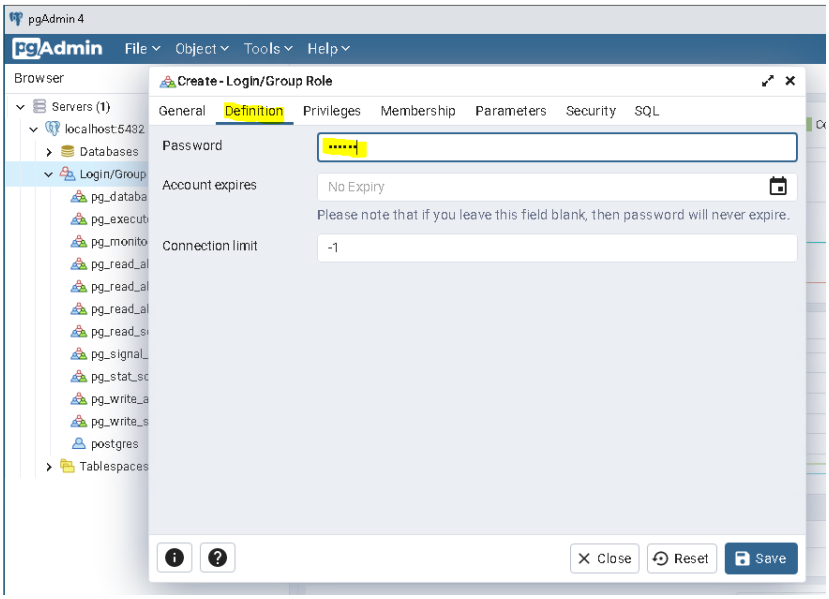
2.2. Подключится к серверу localhost через pgAdmin (при первом входе введите мастер-пароль указанный в п.1.3).

2.3. Создать пользователя (правой кнопкой мыши выбрать вкладку **Login/Group** и выберите **Create Login/Group Role**):

2.4. На вкладке **General** ввести имя пользователя (например: **atomic**)



2.5. На вкладке **Definition** ввести пароль (**Connection limit** равен -1, **Account expires** оставить пустым (означает отсутствие срока действия)).



2.6. На вкладке **Privileges** включить следующие переключатели: **Can login** и **Create databases** и нажать кнопку **Save.**

3.1.3 Генерация сертификата SSL с собственной подписью

В целях обеспечения безопасного и конфиденциального обмена данными между АСУИК ЯМ 2.0. и пользовательскими ПК в систему была добавлена поддержка протокола HTTPS. Безопасная передача данных по указанному протоколу обеспечивается при помощи SSL сертификата. Поэтому в инсталляционный пакет интегрирован SSL сертификат.

В инсталляционный пакет АСУИК ЯМ 2.0. добавлена возможность указания пользовательского сертификата. Если пользовательский сертификат не указан - система будет установлена с сертификатом по умолчанию («default SSL certificate»). Сертификат по умолчанию представляет из себя само-подписанный сертификат, созданный на стороне компании-разработчика (как создать само-подписанный сертификат см. инструкцию ниже). Сертификата по умолчанию будет достаточно для обеспечения безопасности во внутренней сети. Единственный его недостаток заключается в том, что пользователи, которые будут подключаться к АСУИК ЯМ 2.0. через браузер, будут видеть предупреждение о том, что сертификат не является доверенным. В качестве пользовательского сертификата может быть использован не только само-подписанный, но и любой другой сертификат (доменный, публичный, приобретенный у доверенной сертификационной организации, и др.). Единственное требование — это формат сертификата. Сертификат должен быть в формате .**pfx**.

Предварительные условия для создания сертификата –Установлена утилита **openssl**.

Для создания сертификата SSL с собственной подписью необходимо:

1. Открыть командную строку (**cmd**) и выполнить следующие команды:

1.1. Создание сертификата с собственной подписью в формате (.crt) и ключа (.key):

openssl req -x509 -sha256 -nodes -days NDAYS -newkey rsa:2048 -keyout KEYPATH -out CRTPATH

Где используются следующие параметры:

NDAYS - срок действия сертификата в днях.

KEYPATH - путь для сохранения ключа (пример: D:\mycert.key).

CRTPATH - путь для сохранения сертификата (пример: D:\mycert.crt).

1.2. Конвертация сертификата в формате (.crt) и ключа (.key) в .pfx формат:

Важно: после выполнения команды система запросит у вас ввести и подтвердить пароль для защиты сертификата. **ЗАПОМНИТЕ ЕГО**. Он понадобится для дальнейшего использования сертификата.

openssl pkcs12 -export -out PFXPATH -inkey KEYPATH -in CRTPATH

Где используются следующие параметры:

PFXPATH - путь для сохранения сертификата в формате pfx (пример: D:\mycert.pfx).

KEYPATH - путь для сохранения ключа (пример: D:\mycert.key).

CRTPATH - путь для сохранения сертификата (пример: D:\mycert.crt).

3.1.4 Инсталляция «Atomic Keeper» v.2.0.

Инсталляция приложения «Atomic Keeper» v.2.0. делится на две части:

a. установка платформы;

b. установка конфигурации;

и могут выполняться двумя способами:

1) инсталляция по умолчанию (с использованием UI) предоставляет пользователю удобный интерфейс для простой навигации по процессу установки;

2) автоматизированная инсталляция (через командную строку).

1. Инсталляция по умолчанию (с использованием UI):

1.1. Установка платформы.

Платформа является неотъемлемой частью установки «Atomic Keeper» v.2.0 и служит для установки и настройки следующих параметров:

a. установка общих файлов конфигурации;

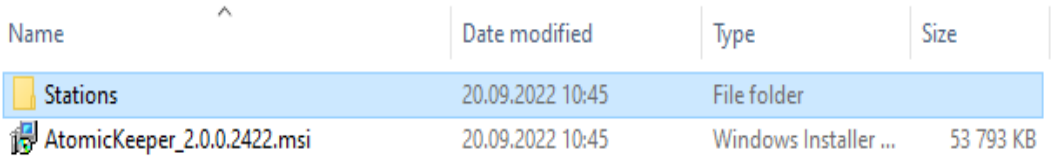
b. установка бинарных файлов и библиотеки;

c. настройка и проверка подключения к базе данных;

d. настройка и проверка параметров доступа к приложению.

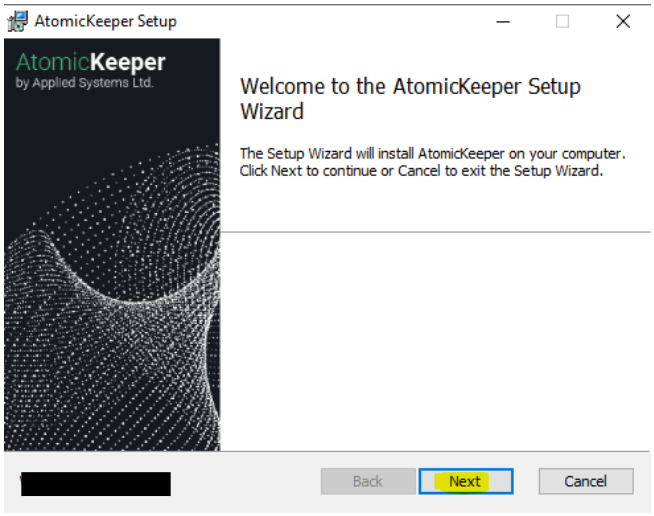
1.1.1. Для установки Платформы «Atomic Keeper» v.2.0 необходимо выполнить следующее:

1) Распаковать архив поставки («AtomicKeeper_X.X.X.XXXX.zip») в любую папку. Пример распакованного архива выглядит примерно так:

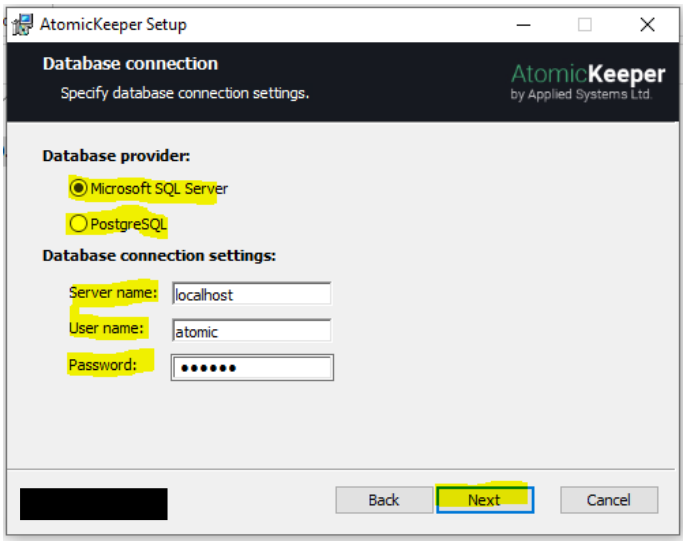


2) Запустить файл установки с расширением *.msi (пример: AtomicKeeper_2.0.0.2422.msi) двойным щелчком.

3) В диалоговом окне нажмите **Next**.



4) В диалоговом окне **Database connection** ввести настройки для подключения к соответствующей базе данных



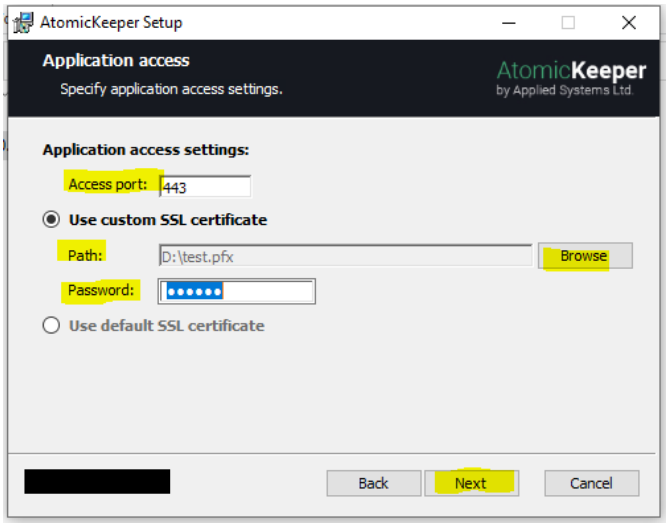
Database provider – поставщик базы данных в зависимости от выбранного в п. 4.1.

Server name – имя сервера, на котором установлена база данных ((local), если база данных находится на том же компьютере).

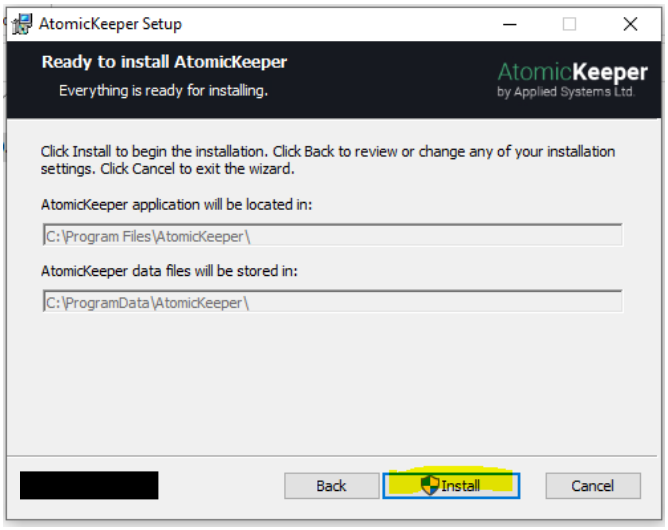
User name – имя пользователя для соединения с базой данных

Password – пароль пользователя для соединения с базой данных

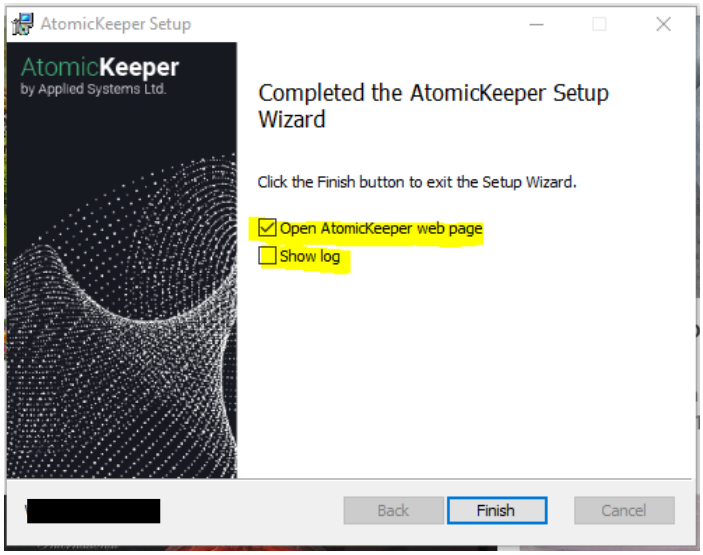
5) В диалоговом окне **Application access** ввести порт для доступа к веб-приложению и активировать одну из следующих опций: **Use custom SSL certificate** либо **Use default certificate** и нажать кнопку **Next**. При использовании опции **Use custom SSL certificate** придется указать путь к вашему сертификату в формате **.pfx** (созданному в п.3.5.), а также пароль, которым защищен сертификат. Использование опции **Use default SSl certificate** означает использование сертификата SSL по умолчанию, чтобы использовать встроенный самозаверяющийся сертификат.



6) В диалоговом окне **Ready to install** нажать **Install**.



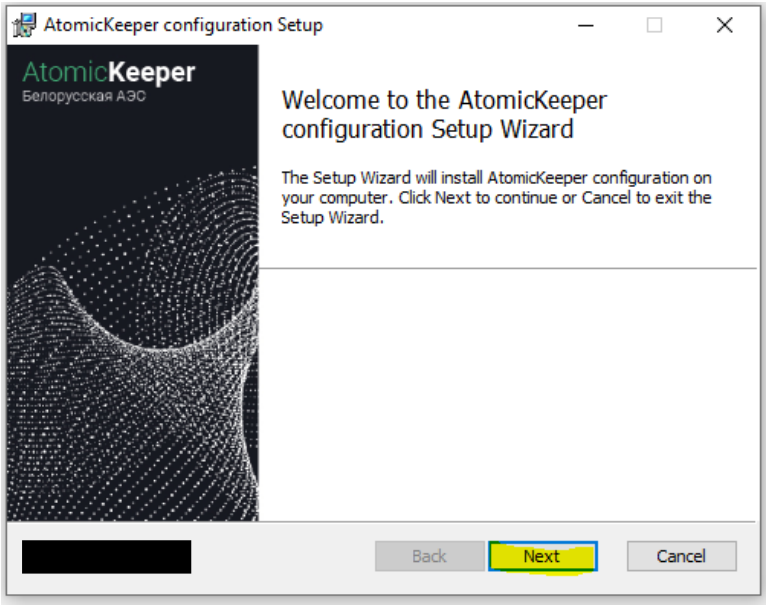
7) Дождитесь окончания процесса установки и в диалоговом окне **Final** по желанию выбрав параметры **Show log** (Показать журнал установки) и **Open AtomicKeeper web page** (Открыть веб-страницу AtomicKeeper по окончанию установки) установив соответствующий флажок и нажать кнопку **Finish**:



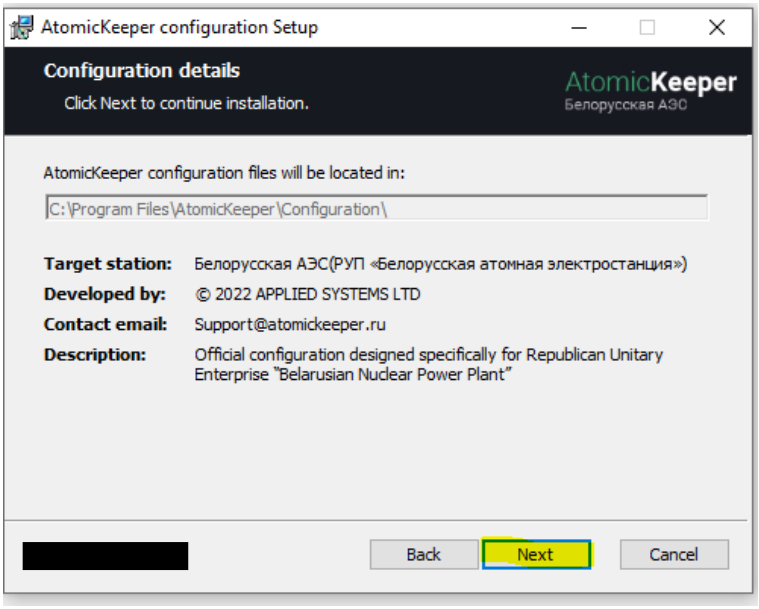
1) Установка конфигурации «Atomic Keeper» v.2.0 Убедится, что установка Платформы завершена успешно.

2) Перейти в папку **Stations** в распакованной папке поставки и запустить установочный файл конфигурации (например: AtomicKeeper_Akkuyu_x.x.x.x.msi).

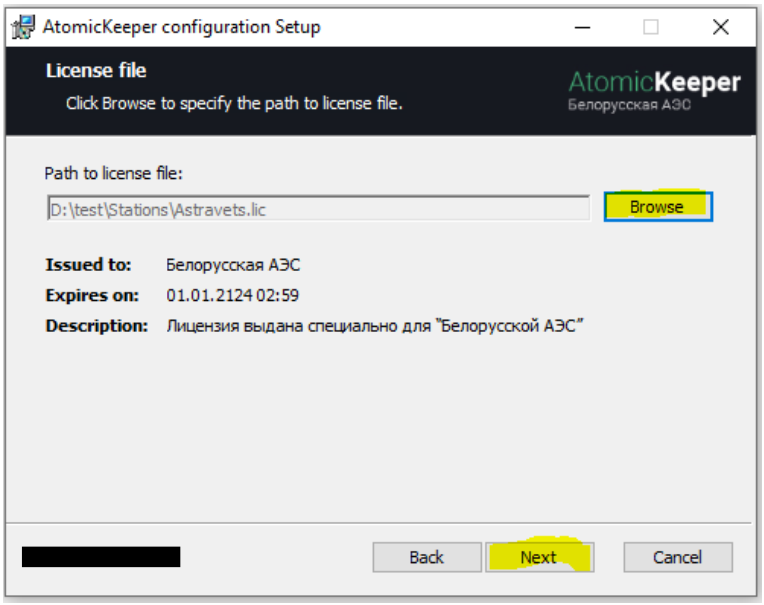
3) В диалоговом окне нажмите Next.



4) В появившемся диалоговом окне **Configuration details** нажать **Next**



5) В диалоговом окне **License file** нажать **Browse** и указать путь к лицензионному файлу (например: **Akkuyu.lic)**, который находится в папке поставки **Stations**, затем нажать **Next**. Если лицензионный файл недействительный, кнопка **Next** будет неактивна.



6) В диалоговом окне **Ready to install** нажать кнопку **Install**.

7) Дождитесь окончания процесса установки и в диалоговом окне **Final** по желанию выбрав параметр **Show log** (Показать журнал установки) установив соответствующий флажок нажать кнопку **Finish**:

2. Автоматизированная инсталляция (через командную строку).

Для проведения автоматизированной инсталляции необходимо:

2.1.Установка Платформы:

2.1.1. Запустить командную строку от имени Администратора.

2.1.2. Выполнить команду:

Msiexec /I $(PATH_TO_MSI) /QN /L*V $(PATH_TO_LOG_FILE) Arg1=Value1 Arg2=Value2 … ArgN=ValueN

Где используются следующие параметры:

PATH_TO_MSI – путь к msi-файлу AtomicKeeper_X.X.X.X..msi.

PATH_TO_LOG – путь к папке, где будет сохранен log-файл.

Список аргументов:

1) **USE_DEFAULT_CERT** (по умолчанию: False) — установить для этого значения значение True, чтобы установить msi с SSL-сертификатом по умолчанию.

2) **CERTIFICATE_PATH** (по умолчанию: empty) — путь к пользовательскому SSL-сертификату в формате pfx.

3) **CERTIFICATE_PASSWORD** (по умолчанию: empty) — пароль для пользовательского SSL-сертификата.

4) **ACCESS_PORT** (по умолчанию: 443) - порт для доступа к веб-приложению через браузер.

5) **DB_PROVIDER** (по умолчанию: MSSQL. Возможные значения: MSSQL или POSTGRESQL) - провайдер базы данных.

6) **DB_SERVER** (по умолчанию: localhost) - имя сервера SQL.

7) **DB_USER** (по умолчанию: atomic) - имя пользователя для подключения приложения «Atomic Keeper» к базе данных

8) **DB_PASSWORD** (по умолчанию: atomic) — пароль пользователя, используемый приложением «Atomic Keeper» для подключения к базе данных SQL.

2.2. Установка конфигурации АСУиК ЯМ 2.0:

2.2.1. Запустить командную строку от имени Администратора.

2.2.2. Выполнить команду:

Msiexec /I $(PATH_TO_MSI) /QN /L*V $(PATH_TO_LOG_FILE) Arg1=Value1 Arg2=Value2 … ArgN=ValueN

Где используются следующие параметры:

PATH_TO_MSI – путь к msi-файлу (пример: AtomicKeeper_Akkuyu_ x.x.x.x.msi).

PATH_TO_LOG – путь к папке, где будет сохранен log-файл.

Список аргументов:

1) **LICENSE_PATH** (по умолчанию: empty) – путь к файлу лицензии.

3.2. Подготовка к установке и инсталляция «Atomic Keeper» v.2.0 для Linux Astra Smolensk 1.6.

3.2.1 Настройка PostgreSQL.

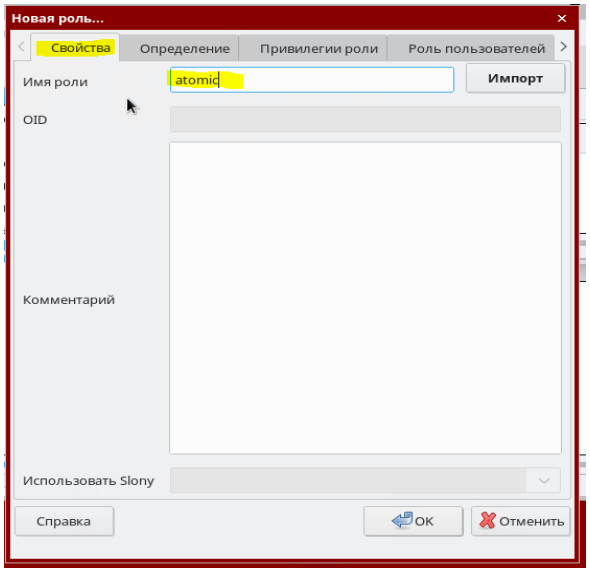
1. Установить PostgreSQL.

2. Создать пользователя базы данных:

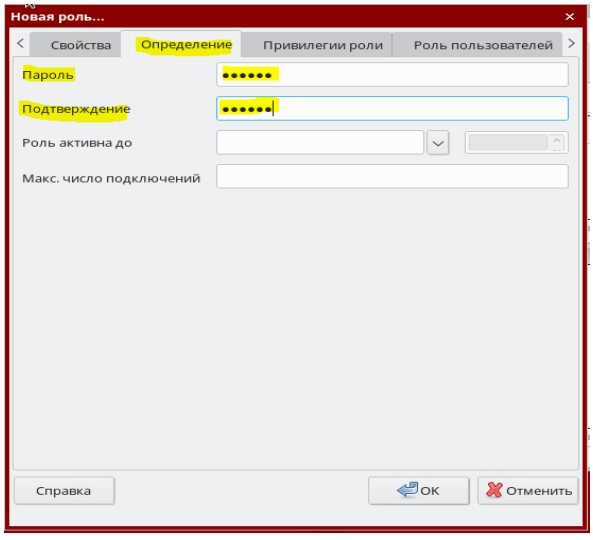
2.1. Откройте pgAdmin утилиту.

2.2. Разверните вкладку Серверы, затем разверните вкладку **localhost**. Найти «Роли входа» секцию, кликните по ней правой кнопкой мыши и выберите пункт «Новая роль…».

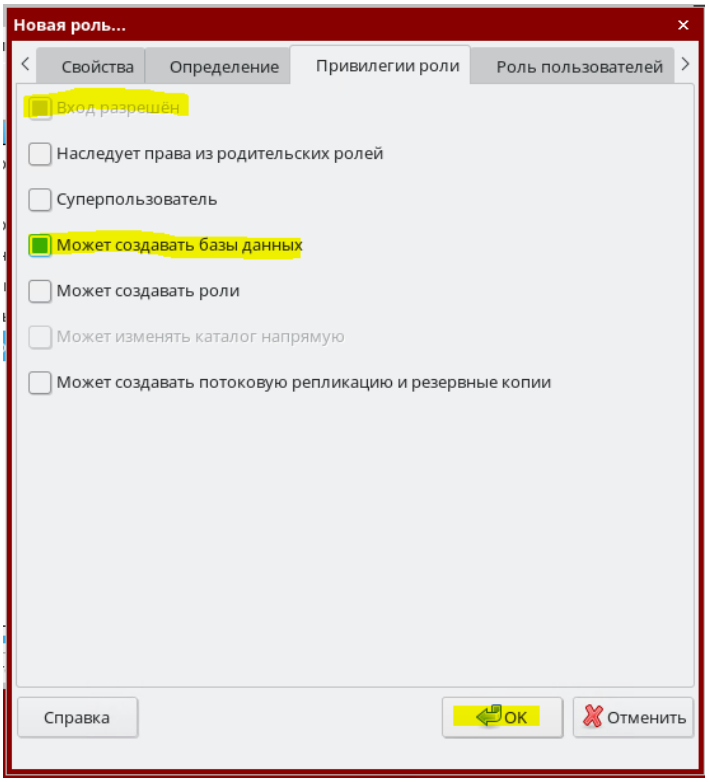
2.3. В открывшемся окне на вкладке «Свойства» введите имя пользователя в поле «Имя роли», например **atomic**.



2.4. На вкладке «Определение» введите пароль для пользователя в поле «Пароль» и подтвердите его в поле «Подтверждение».



2.5. На вкладке "Привилегии роли" выберите "Вход разрешён"(если не выбрано) и "Может Создавать базы данных". Затем нажмите кнопку ОК:



3.2.2 Инсталляция «Atomic Keeper» v.2.0

Инсталляция «Atomic Keeper» v.2.0 делится на три части:

1. Установка платформы:

1.1. Создать папку для установки на Linux Astra Smolensk 1.6. (например: AtomicKeeper). Эта папка будет называться **InstallDir**

1.2.Скопируйте все файлы из папки **Setup.Linux/Platform** в **InstallDir**.

1.3. Настройте параметры доступа к веб-приложению:

Примечание: Шаги из списка ниже являются необязательными, и вы можете их пропустить, если хотите использовать настройки по умолчанию (Порт доступа по умолчанию 443):

1.3.1. Откройте файл **appsettings.json** в **InstallDir.**

1.3.2. Найти раздел «Порт» и заменить значение по умолчанию (443) на любой номер порта, который вы хотите, чтобы использовалось для АСУиК ЯМ 2.0.

```
"Kestrel": {
  "Port": "443",
  "Certificate": {
    "Path": "Security/Certificates/AtomicKeeper.pfx",
    "Password": "AtomicKeeper"
  }
},
```

Примечание: Если для порта установлено значение 443, АСУиК ЯМ 2.0. также будет доступен порт 80, чтобы включить автоматическое перенаправление с HTTP на HTTPS.

1.3.3. Сохранить изменения в файле **appsettings.json.**

1.4.Установка пользовательского SSL-сертификата:

Примечание: По умолчанию в систему уже встроен самозаверяющий сертификат.

1.4.1. Скопировать свой собственный сертификат в формате **PFX** в папку **InstallDir/Security/Certificates**.

2) Открыть файл **appsettings.json** в **InstallDir**.

3) Найти раздел **Certificate** задать имя пользовательского сертификата в подразделе **Path** и пароль к сертификату в подразделе **Password**:

```
"Kestrel": {
  "Port": "443",
  "Certificate": {
    "Path": "Security/Certificates/MyCustomCert.pfx",
    "Password": "MyCustomCertPassword"
  }
},
```

1.5.Настроить параметры подключения к базе данных:

Примечание: Пользователь создан в PostgreSql по инструкции описанной в п. 3.2.1.

1.5.1. Открыть файл **appsettings.json** в **InstallDir**.

1.5.2. Во всех подразделах раздела **ConnectionStrings** заменить идентификатор пользователя и пароль по умолчанию на соответствующие имя пользователя и пароль пользователя, которой был создан в PostgreSql.

2. Установка конфигурации.

2.1. Скопируйте содержимое из папки **Setup.Linux/Configurations/Target_Station** в папку **InstallDir/Configuration**.

Target_Station — имя станции, для которой вы хотите установить конфигурацию. (Пример: для установки конфигурации **Akkuyu**, нужно скопировать содержимое **Setup.Linux/Configurations/Akkuyu** в **InstallDir/Configuration)**.

2.2. Установить лицензию:

2.2.1. Скопировать файл лицензии из **Setup.Linux/Licenses/Target_Station.lic** в папку **InstallDir/Configuration**.

Target_Station — имя станции, для которой вы хотите установить лицензию. (Пример: для установки лицензии **Akkuyu**, нужно скопировать содержимое **Setup.Linux/Configurations/ Akkuyu.lic** в **InstallDir/Configuration)**.

3. Запуск «Atomic Keeper» v.2.0.

3.1. Предоставить права на выполнение исполняемому файлу **AtomicKeeper.Bootstrapper**:

3.1.1. Откройте командную строку и перейдите в **InstallDir**.

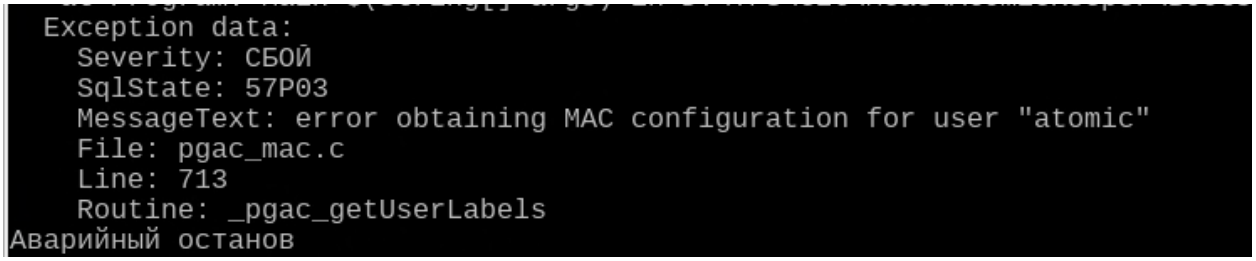
3.1.2. Выполните команду: *sudo chmod +x ./AtomicKeeper.Bootstrapper*

3.2.Запустить исполняемый файл **AtomicKeeper.Bootstrapper:**

3.2.1. Откройте командную строку и перейдите в **InstallDir.**

2. Выполните команду: *sudo ./AtomicKeeper.Bootstrapper*

Примечание: при первом запуске возможно появление сообщения об ошибке «ошибка получения конфигурации MAC для пользователя xxx».



Это сообщение означает, что установленный Postgresql пропустил некоторые настройки. Для исправления этой ошибки необходимо в файле **/etc/parsec/mswitch.conf** параметр, **zero_if_notfound** установить в **yes**.

3.3. Проверка работоспособности установленного ПО.

После успешной инсталляции ПО необходимо провести проверку основного функционала администратора.

Проверочное тестирование состоит из проведения тестов приведенных в приложении А и параллельной проверки пользовательского интерфейса администратора.

4. ОПИСАНИЕ ОПЕРАЦИЙ АДМИНИСТРАТОРА

4.1. Вход на страницу администрирования системы.

2.7. Для входа на страницу администрирования АСУиК ЯМ 2.0. необходимо:

1. В адресную строку браузера введите адрес приложения и нажмите на клавишу **Enter**. Произойдет переход на авторизационную страницу системы.
2. В поле **Логин** введите логин для входа в систему с ролью «Администратор».
3. В поле **Пароль** введите пароль.
4. Нажать на кнопку **Войти**. Произойдет переход на **Страницу** администрирования системы.

4.2. Создание группы прав для пользователей.

Группы прав используются для предоставления определенным пользователям с ролью «Учетчик» необходимых прав на проведение определенных операций по учету и контролю ЯМ МК в АСУиК ЯМ 2.0.

1. Войти в АСУиК ЯМ 2.0. с ролью «Администратор».
2. Перейти на вкладку «Группы прав».
3. Нажать кнопку «Добавить» и внести информацию о наименовании созданной группы прав.
4. Выбрать из списка областей, необходимую область которой будут владеть пользователи в созданной группе.
5. В правой части страницы выбрать необходимые права из списка для пользователей созданной группы выбранной области.
6. Нажать кнопку **Сохранить**.

4.3. Создание учетной записи пользователя с ролью «Настройщик».

Пользователь с ролью «Настройщик» имеет доступ только к модулю «Справочники» и предназначен для редактирования в нем информации.

1. Войти в АСУиК ЯМ 2.0. с ролью «Администратор».
2. Перейти на вкладку «Список пользователей» и нажать кнопку «Добавить».
3. Зарегистрировать нового пользователя с ролью «Настройщик»:

a. в полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;

a) добавить **IP адрес** компьютера пользователя;

b. остальные поля с персональными данными вводить необязательно;

c. нажать кнопку **Сохранить**.

В результате выполнения указанных действий произойдет добавление пользователя в систему с ролью «Настройщик». Первоначальный пароль передается администратором системы зарегистрированному пользователю для первого входа.

После первого входа в систему пользователю будет необходимо ввести новый персональный пароль.

4.4. Создание учетной записи пользователя с ролью «Учетчик».

1. Войти в АСУиК ЯМ 2.0. с ролью «Администратор».
2. Перейти на вкладку «Список пользователей» и нажать кнопку «Добавить».
3. Зарегистрируйте нового пользователя с ролью «Учетчик»:

a. в полях **Логин** и **Временный пароль** укажите данные для аутентификации регистрируемого пользователя;

b) добавить **IP адрес** компьютера пользователя;

b. выбрать ФИО пользователя, которому будет принадлежать учетная запись из списка (список сотрудников и их данные регистрирует пользователь с правами «Настройщик» в модуле «Справочники»);

c. Выбрать группу прав для пользователя;

d. нажать кнопку **Сохранить**.

В результате выполнения указанных действий произойдет добавление пользователя в систему с ролью «Учетчик». Первоначальный пароль передается администратором системы зарегистрированному пользователю для первого входа. После первого входа в систему пользователю будет необходимо ввести новый персональный пароль.

4.5. Деактивация учетной записи

Во избежание несанкционированного доступа учётная запись может быть деактивирована. Администратор имеет возможность деактивировать учетную запись вручную (принудительно) следующими шагами:

1. Войти в АСУиК ЯМ 2.0. с ролью «Администратор».
2. Перейти на вкладку «Список пользователей».
3. Выбрать в таблице пользователя, которого необходимо деактивировать и в графе «Действия» нажать кнопку  (деактивировать).
4. Подтвердить деактивацию нажатием кнопки  .

4.6. Изменение данных в учетной записи пользователя.

Для изменения информации в учетной записи пользователя выполните следующие действия:

1. Войти в АСУиК ЯМ 2.0. с ролью «Администратор».
2. Перейти на вкладку «Список пользователей».
3. Выбрать в таблице пользователя, которого необходимо изменить информацию и в графе «Действия» нажать кнопку  (изменить).

4. Внести необходимые корректировки для выбранного пользователя и нажать кнопку **Сохранить**.

4.7. Сброс пароля записи пользователя.

1. Войти в АСУиК ЯМ 2.0. с ролью «Администратор».
2. Перейти на вкладку «Список пользователей».
3. Выбрать в таблице пользователя, которому необходимо сбросить пароль и в графе «Действия» нажать кнопку  (сбросить пароль).
4. В диалоговом окне ввести новый первоначальный пароль для пользователя или выбрать предложенный системой пароль.
5. Нажать кнопку **Сохранить**.

В результате выполнения указанных действий произойдет сброс пароля пользователя, после чего пользователь (при первоначальном входе в систему после сброса пароля) обязан ввести новый первоначальный пароль (переданный ему администратором), затем на странице входа в систему ввести личный персональный пароль.

4.8. Просмотр журнала действий пользователей (логирование).

1. Войти в АСУиК ЯМ 2.0. с ролью «Администратор».
2. На странице администрирования открыть главное навигационное меню и выбрать **Журнал аудита**.
3. Откроется страница со списком всех действий в системе с указанием данных о времени произведенных изменений и пользователе, вносившем изменения.

Журнал событий можно отфильтровать на определённый заданный период, а также имеется возможность экспорта данных журнала в файл *.xlsx.

4.9. Настройки аутентификации.

1. Войти в АСУиК ЯМ 2.0. с правами администрирования.
2. В главном навигационном меню выбрать **Настройки**.
3. Задать необходимые параметры для аутентификации.
4. Нажать **Сохранить.**

4.10. Снятие блокировки учётной записи.

Во избежание несанкционированного доступа учётная запись, может быть, автоматически заблокирована при заданных в Настройках параметрах аутентификации. Для снятия блокировки учетной записи пользователя необходимо:

1. Войти в АСУиК ЯМ 2.0. с ролью «Администратор».
2. В главном навигационном меню выбрать вкладку **IP-адреса** и выбрать **Заблокированные.**

3. Удалить из списка нужный IP Адрес и в главном меню перейти в **Список пользователей.**

4. Перейти на вкладку «Список пользователей», выбрать в таблице пользователя, которому необходимо активировать доступ, нажать кнопку  (активировать) в деактивированной учетной записи.

5. Нажать кнопку  (сохранить).

5. ДЕЙСТВИЯ ПРИ АВАРИЙНЫХ СИТУАЦИЯХ

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями администратора, неверным форматом или недопустимыми значениями входных данных. В указанных случаях администратору должны выдаваться соответствующие аварийные сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных. Аварийные ситуации могут возникать как из-за ошибок в программных продуктах, так и из-за неправильной настройки.

Основными признаками аварийной ситуации являются:

1. Отсутствие на экране необходимой страницы.
2. Окна с сообщениями о нештатной ситуации.
3. Окна с сообщениями на английском.
4. Ошибки, связанные с программным обеспечением.

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

После получения сообщения об ошибке необходимо выполнить рекомендации, указанные в сообщении, если таковы имеются, в противном случае перезагрузить страницу, проверить подключение к сети. В случае повторного возникновения сообщения об ошибке необходимо обратиться к разработчику АСУиК ЯМ 2.0. При обращении к разработчику необходимо указать порядок действий, приведший к возникновению ошибки, в том числе, предоставить вводимую в систему информацию, если ошибка произошла при ее вводе, данные журнала действий пользователя.

5.2. Действия по восстановлению программ и/или данных при отказе магнитных носителей информации или обнаружении ошибок в данных

При отказе магнитных носителей или обнаружения ошибок в данных администратор системы должен восстановить файлы и данные, необходимые для корректной работы системы из последней резервной копии. Если администратор не может устранить ошибки в данных, следует обратиться к разработчику АСУиК ЯМ 2.0. При этом необходимо указать перечень данных, содержащих ошибки и правильные значения искаженных атрибутов

5.3. Действия в случаях обнаружении несанкционированного вмешательства в данные

В случае обнаружения несанкционированного вмешательства в данные АСУиК ЯМ 2.0. администратор системы должен восстановить файлы и данные, необходимые для корректной работы системы из последней резервной копии. Также

следует обратиться к разработчику АСУиК ЯМ 2.0. и описать признаки и предполагаемый характер вмешательства, а также, указать перечень данных, подвергшихся вмешательству.

5.4. Действия в других аварийных ситуациях

В случае возникновения других аварийных ситуаций при работе с АСУиК ЯМ 2.0. и невозможности устранить их с помощью средств администрирования, системы управления базой данных, операционной системы следует обратиться к разработчику системы. При этом необходимо описать признаки аварийной ситуации и действия, которые были выполнены пользователем непосредственно перед возникновением аварийной ситуации. Ниже описаны основные возможные аварийные ситуации и способы их решения.

Аварийная ситуация	**Возможные потери информации**	**Способ ликвидации**	**Исполнитель**
Не добавляются записи в журнал аудита по причине нехватки памяти	Информация о действиях пользователей в журнале аудита.	Увеличить память на сервере, где установлена «Atomic Keeper» v.2.0. с помощью добавления дополнительных жестких дисков увеличенного объема или очистки ненужных файлов для освобождения необходимого объема памяти.	Администратор
Выход из строя аппаратных средств (за исключением жесткого диска)	Несохраненные пользователем данные	Повторный ввод и сохранение информации	Пользователь
Сбой операционной системы сервера	Вся информация, поступившая в Систему с момента окончания последнего резервного копирования данных.	Восстановление данных их резервных копий	Администратор
Выход из строя жесткого диска	Вся информация, поступившая в Систему с момента окончания последнего резервного копирования данных.	Восстановление данных их резервных копий	Администратор

Аварийная ситуация	Возможные потери информации	Способ ликвидации	Исполнитель
Отключение питания аппаратных средств	Несохраненные пользователем данные	Повторный ввод и сохранение информации	Пользователь
Сбой при передаче данных	Передаваемая информация	Повторная отправка данных на сервер	Пользователь
Отсутствие на экране необходимой страницы	Несохраненные пользователем данные	Перезагрузка страницы кнопкой «Обновить» интернет-браузера; возврат на предыдущую страницу и повторный клик по ссылке на необходимую страницу	Пользователь
Окна с сообщениями о нештатной ситуации	Несохраненные пользователем данные	Выполнить рекомендации, указанные в сообщении, если таковые имеются. При необходимости обратиться к администратору.	Пользователь
Окна с сообщениями на английском языке	Несохраненные пользователем данные	Обратиться к администратору	Пользователь
Ошибки, связанные с программным обеспечением	Информация, поступившая в систему с момента окончания последнего резервного копирования данных	Перезапуск соответствующего программного обеспечения, перезагрузка сервера, восстановление данных из резервных копий	Администратор