АО «БАРС Груп»

Прогрраммa для ЭВМ БАРС.Мониторинг-Здравоохранение

Инструкция для системных администраторов

Версия 5.3.11

2024

Содержание

Определения, обозначения и сокращения

В настоящем документе применяют следующие термины и сокращения с соответствующими определениями и обозначениями:

Термин, сокращение	Определение
.NET	Модульная платформа для разработки программного обеспечения с открытым исходным кодом
API	Дополнительный функционал в рамках определенного проекта, который расширяет возможности программа для ЭВМ (файлы формата .dll)
AVX2	Advanced Vector Extensions 2 – расширение системы команд процессора, разработанное компанией Intel в дополнение к набору инструкций AVX
AW, Компонент анализа данных	Компонент анализа данных программы для ЭВМ БАРС.Мониторинг-Здравоохранение
ClickHouse	Колоночная аналитическая СУБД с открытым исходным кодом
CPU	Central Processing Unit – центральное процессорное устройство
HDD	Hard (magnetic) Disk Drive – накопитель на жестких магнитных дисках, жесткий диск − запоминающее устройство (устройство хранения информации), основанное на принципе магнитной записи
HTTP	HyperText Transfer Protocol – протокол передачи гипертекста – протокол прикладного уровня передачи данных
ID	Уникальный признак объекта, позволяющий отличать его от других объектов
IP	Уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу TCP/IP
IP-адрес	Internet Protocol Address – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP
LAN	Локальная вычислительная сеть
LDAP	Lightweight Directory Access Protocol – протокол прикладного уровня для доступа к службе каталогов X.500. LDAP – протокол, использующий TCP/IP и позволяющий производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей
OIDC	OpenID Connect – расширение, предназначенное для обеспечения идентификации и аутентификации пользователя посредством протокола OAuth 2.0
OLAP	OnLine Analytical Processing – технология обработки данных, заключающаяся в подготовке суммарной информации на основе больших массивов данных, структурированных по многомерному принципу
OpenID	Система единого входа (авторизации) на сайты, порталы, блоги и форумы
OpenLDAP	Открытая реализация LDAP, разработанная одноимённым проектом, распространяется под собственной свободной лицензией OpenLDAP Public License
OpenSSL	Криптографическая библиотека с открытым исходным кодом

Термин, сокращение	Определение
POST	Метод запроса для получения информации от web-сервера, используемый HTTP протоколом сети Интернет, при котором web-сервер принимает данные, заключенные в тело запроса, для хранения. Он часто используется для загрузки файла или представления заполненной web-формы
PostgreSQL	Свободная объектно-реляционная система управления базами данных
RAM	Random Access Memory – оперативная память – энергозависимая часть системы компьютерной памяти, в которой во время работы компьютера хранится выполняемый машинный код (программы), а также входные, выходные и промежуточные данные, обрабатываемые процессором
Redis	Нереляционная резидентная СУБД, хранящая данные в виде пар «ключ-значение».
SAS	Serial Attached SCSI (Small Computer System Interface) – последовательный компьютерный интерфейс, разработанный для подключения различных устройств хранения данных, например, жестких дисков и ленточных накопителей
SDK	Software Development Kit – набор инструментов для разработки программного обеспечения в одном устанавливаемом пакете
SOAP	Simple Object Access Protocol – протокол обмена структурированными сообщениями в формате XML в распределённой вычислительной среде
SQL	Structured Query Language (язык структурированных запросов) – язык программирования, предназначенный для управления данными в системах управления реляционными базами данных
SSD	Solid State Drive – накопитель информации, основанный на чипах энергонезависимой памяти, которые сохраняют данные после отключения питания
SSH	Сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов)
SSL	Криптографический протокол, обеспечивающий безопасную передачу данных по сети Интернет. При его использовании создается защищенное соединение между клиентом и сервером.
SSO	Single Sign-On – технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации
SWAP	Механизм виртуальной памяти, при котором отдельные фрагменты памяти перемещаются из оперативной памяти во вторичное хранилище (жесткий диск или другой внешний накопитель), освобождая оперативную память для загрузки других активных фрагментов памяти
TCP/IP	Набор сетевых протоколов передачи данных, используемых в сетях, включая сеть Интернет. Протоколы работают друг с другом в стеке (англ. stack, стопка) – это означает, что протокол, располагающийся на уровне выше, работает «поверх» нижнего, используя механизмы инкапсуляции. Например, протокол TCP работает поверх протокола IP
UI	User Interface – интерфейс, обеспечивающий передачу информации между пользователем-человеком и программно-аппаратными компонентами компьютерной системы
UNIX	Многопользовательская операционная система

Термин, сокращение	Определение
URL	Uniform Resource Locator – стандартизированный способ записи адреса ресурса в сети Интернет
USB-порт	Последовательный интерфейс для подключения периферийных устройств к вычислительной технике
UTF-8	Unicode Transformation Format, 8-bit – распространенный стандарт кодирования символов, позволяющий более компактно хранить и передавать символы Юникода, используя переменное количество Б (от 1 до 4), и обеспечивающий полную обратную совместимость с 7-битной кодировкой ASCII
WDSL	Язык описания web-сервисов и доступа к ним, основанный на языке XML
Web-браузер	Прикладное программное обеспечение для просмотра web-страниц, содержания web-документов, компьютерных файлов и их каталогов; управления web-приложениями
Web-приложение, приложение	Клиент-серверное приложение, в котором клиентом выступает web-браузер, а сервером – web-сервер
XML	Расширяемый язык разметки
АО «БАРС Груп»	Акционерное общество «БАРС Груп»
БД	База данных
ГАР	Государственный адресный реестр
ГБ	Гигабайт
ГГц	Гигагерц
ГОСТ	Государственный стандарт
ЕСИА, ИА	Единая система идентификации и аутентификации
ИС	Информационная система
МБ	Мегабайт
ОС	Операционная система
ПО	Программное обеспечение
Приложение.барс	Файл с подключением к базе данных
Сервис отчетных форм	Приложение, отвечающее за открытие/закрытие отчетных форм и выполнение операций над ними.
ПП МЗ	Программа для ЭВМ БАРС.Мониторинг-Здравоохранение
СУБД	Система управления базами данных
Суперпользователь	Root. Специальный аккаунт (и группа пользователей) в UNIX-подобных системах, владелец которого имеет право на выполнение всех операций
ФИО	Фамилия, имя, отчество
ЭВМ	Электронная вычислительная машина

Термин, сокращение	Определение
ЭП	Электронная подпись

1 Введение

1.1 Область применения

Программа для ЭВМ БАРС.Мониторинг-Здравоохранение (далее – ПП МЗ) представляет собой программный комплекс, предназначенный для выполнения задачи автоматизации процессов централизованного сбора, сведения и анализа отчетности.

ПП МЗ обеспечивает возможность ведения единой централизованной БД в Центральном Офисе, ответственном за сбор и консолидацию отчетности.

Вся информация собирается и консолидируется в разрезе отчетных периодов. Средства ПП МЗ позволяют представить данные в удобной для пользователя форме (Рисунок 1).

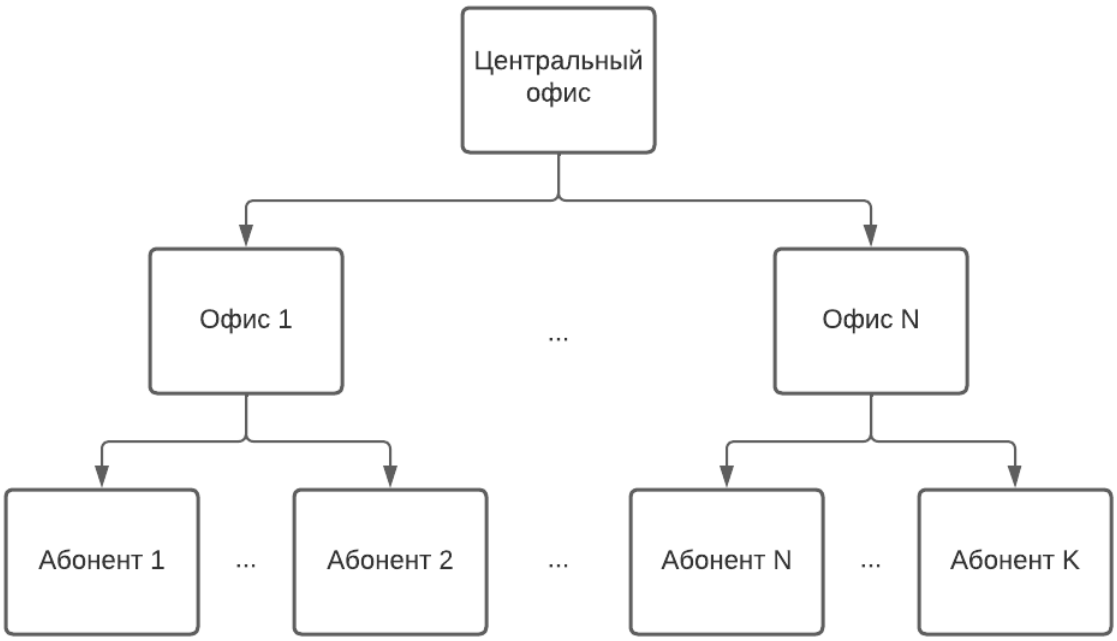


Рисунок 1 – Пример формирования цепочки сдачи отчетности

Центральный офис – это единственное учреждение, которое формирует итоговый отчет, единый по всей цепочке сдачи отчетности (то есть по всем отчетам, собранным по подчиненным учреждениям (офисам и абонентам)).

Офис – это учреждение, которое сводит и консолидирует отчеты, составленные абонентами.

Абонент – это учреждение, которое подлежит сдаче отчетности, то есть составляет отчет по своим данным.

Пассивный абонент – это учреждение, за которое сдают отчетность вышестоящие учреждения.

1.2 Краткое описание возможностей

В рамках ПП МЗ реализованы следующие функциональные возможности, относящиеся к централизованному сбору отчетности:

- централизация первичных и сводных отчетных данных в единой БД;
- оперативный доступ к первичным и сводным данным отчетности из пункта сбора отчетности;
- ведение единых справочников и классификаторов, необходимых для обеспечения процесса сдачи отчетности;
- контроль данных, введенных в отчетную форму, с помощью внутриформенных, межформенных и внутривкладочных контрольных соотношений. Контроль гарантирует соответствие отчетной формы параметрам, установленным в пункте сбора отчетности;
- настройка цепочек сдачи отчетности, которые позволяют организовать сборку разнородных отчетных данных в рамках одного экземпляра ПП МЗ;
- контроль своевременности и корректности сдачи отчетных форм по всем уровням цепочки сдачи отчетности;
- импорт в формате .bxml и экспорт форм отчетности в формате файлов .xlsx, .docx, .pdf, .html, .bxml, .xlsm и других;
- формирование аналитических выборок (аналитических отчетов) по заданным параметрам;
- контроль корректности заполнения отчетных форм с помощью экспертизы;
- подписание форм отчетности с электронной подписью.

1.3 Уровень подготовки пользователя

Пользователи ПП МЗ должны обладать навыками:

- работы с рекомендованными web-браузерами (Яндекс.Браузер, Google Chrome);
- работы с КриптоПро 5 версии (при необходимости использования ЭП);
- офисным ПО для работы с файлами формата .docx, .xlsx, .pdf.

Перед началом работы с ПП МЗ пользователи, не обладающие такими навыками, должны пройти соответствующие курсы.

Администратор ПП МЗ должен иметь опыт разворачивания и настройки .net-приложения на операционной системе, которая будет установлена на web-сервере, опыт установки и настройки PostgreSQL, Redis, опыт работы с Крипто ПРО CSP, опыт работа с Docker. Необходимость навыков зависит от конфигурации разворота приложения и типа ОС на сервере web-приложения.

1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться

Для работы с ПП МЗ администратору необходимо ознакомиться с данной инструкцией и материалами, на которые ссылается данное руководство, а также с мануалами поставщиков ПО, которое устанавливается на сервера.

2 Условия применения

2.1 Требования к обеспечению клиентских рабочих мест

Компьютеры на рабочих местах должны обеспечивать комфортную работу в web-браузере.

Для клиентских машин устанавливаются следующие технические требования:

- процессор с тактовой частотой от 2,5 ГГц и 4 и более ядра;
- объем оперативной памяти от 8 ГБ;
- клавиатура;
- монитор (графический режим должен быть не менее 1024 x 768, рекомендуемое разрешение 1920x1080);
- манипулятор типа «мышь».

Дополнительное обеспечение для возможности подписания ЭП – USB-порт.

Аппаратное обеспечение должно соответствовать типу используемого web-браузера для комфортной работы с сетью Интернет. Требования к каналам связи представлены в таблице (Таблица 1).

Таблица 1 – Каналы связи

Требование к количеству пользователей, подключенных к каналу связи	**Требование к каналу связи**
1 пользователь	Канал связи: от 100 Мбит/с

Примечание – Подразумевается стабильный канал связи.

Программные средства, необходимые для обеспечения работы на клиентском рабочем месте ПП МЗ:

- один из следующих web-браузеров:
  - Google Chrome 122 версия и выше;
  - «Яндекс.Браузер» версия 22.7 и выше.
- программный продукт, поддерживающий форматы .xlsx, .docx, .pdf.

Примечание – Если пользователь использует версию web-браузера, не поддерживаемую ПП МЗ, то ему не будет обеспечена корректная работа в ПП МЗ и доступ к полному набору функций.

Программные средства, необходимые для подписания отчетных форм электронной подписью:

- web-браузер (см. выше);

Примечание – Функция «Подписать форму» действует только при использовании рекомендованного web-браузера. Подробнее процедура подписания документа при помощи ЭП описана в руководстве пользователя ПП МЗ.

- «CryptoPro CSP 5» и выше – криптопровайдер, вспомогательная программа, используемая для генерации электронных подписей, работы с сертификатами и так далее. В частности, для подписания отчетных форм может использоваться КриптоПро CSP;
- плагин «КриптоПро CSP» – ПО, обеспечивающее кроссбраузерную работу с ЭП;
- сертификат ключа ЭП.

Примечания

1 Сертификат ЭП не должен содержать запрещенные символы - "=", "#", "$", "&", ">", "<".

2.2 Требования к обеспечению клиентских рабочих мест для работы с Компонентом анализа данных

2.2.1 Требования к техническому обеспечению

Аппаратное обеспечение должно соответствовать типу используемого web-браузера для комфортной работы с сетью Интернет.

Для клиентских машин устанавливаются следующие минимальные технические требования:

- процессор с тактовой частотой от 2,5 ГГц;
- объем оперативной памяти 8 ГБ и выше;
- объем жесткого диска – 100 ГБ, объем свободного места на диске – не менее 5 ГБ;
- сетевая карта 1 ГБ/с;
- монитор, поддерживающий разрешение не менее 1920x1080;
- клавиатура;
- манипулятор типа «мышь».

2.2.2 Требования к программному обеспечению

Требования к обеспечению клиентских рабочих мест:

- один из следующих web-браузеров:
  - Google Chrome версия 122 и выше;
  - Яндекс.Браузер версия 22.7 и выше.

– программный продукт, поддерживающий форматы .xlsx, .docx, .pdf.

Примечания

1 Если используется версия web-браузера, не поддерживаемая Компонентом анализа данных, не будет обеспечена корректная работа в Компоненте анализа данных и доступ к полному набору функций.

2 Для корректного отображения окон, масштаб в web-браузере и на компьютере пользователя должен быть 100%.

2.3 Требования к обеспечению сервера БД

Минимальные требования к обеспечению сервера БД:

- процессор от 8 CPU ядер x 2.7 ГГц;
- объем оперативной памяти 16 ГБ и выше;
- рекомендуем размещать БД на SSD-дисках. На 1 млн ячеек в одной отчетной форме, хранящих данные в XML-файлах в несжатом виде, требуется ~30 МБ, в сжатом виде: 5 МБ – 18 МБ. Для отчетных форм, хранящих данные в БД, требования указаны в таблице (Таблица 2). В таблице указан общий размер памяти на диске, зарезервированный БД Postgres под таблицы данных отчетных форм, индексы и внутренние структуры.

Таблица 2 – Требования памяти для отчетной формы с хранящимися данными в БД

Тип хранящихся данных	**Число строк**	**pg_total_relation_size после vacuum full**
1 млн ячеек в одной отчетной форме	1 100 500	337 МБ
bool	110 050	12 МБ
date	110 050	14 МБ
dec (числовые)	440 200	55 МБ
dict	220 100	228 МБ
long	110 050	14 МБ
str	110 050	14 МБ

Характеристики каналов связи представлены ниже (Таблица 3).

Таблица 3 – Каналы связи

Количество пользователей, подключенных к каналу связи	Характеристика канала связи
До 300 пользователей	Канал связи: 100 Мбит/с
От 300 пользователей	Канал связи: 1 Гбит/с

Примечание – Подразумевается стабильный канал связи.

Операционная система, на которой работает СУБД:

- PostgreSQL 11 и выше, Postgres Pro Standard 11 и выше, Postgres Pro Enterprise 11 и выше.

2.4 Требования к обеспечению сервера web-приложений

Минимальные требования к обеспечению сервера web-приложений на 300 одновременных подключений на сервере с программным обеспечением Linux представлены в таблице (Таблица 4).

Таблица 4 – Минимальные требования к обеспечению сервера web-приложений на 300 одновременных подключений на сервере с программным обеспечением Linux

Параметр	Значение	Примечание
RAM (если используются формы, хранящиеся в БД)	8 ГБ независимо от числа форм на всех экземплярах сервиса	Можно снизить до 4 ГБ свободной памяти на экземпляр приложения, если приложение сервиса и приложение ПП МЗ разворачиваются на одном сервере
RAM (если используются формы, хранящиеся в в формате .xml)	8 ГБ независимо от числа форм на всех экземплярах сервиса	Можно снизить до 4 ГБ свободной памяти на экземпляр приложения, если приложение сервиса и приложение ПП МЗ разворачиваются на одном сервере
CPU	От 8 CPU core x 2.7 ГГц	Если разворачивается на одном сервере с сервисом отчетных, удваивать количество ядер не нужно. На одном сервере можно разворачивать при количестве пользователей до 300
HDD	50 ГБ	Дополнительно 40 ГБ, если планируется использовать ГАР
LAN	1 Гбит/с	

В случае если пользователей больше 300, то можно увеличить мощности сервера приложения, либо использовать балансировщик.

Согласно официальной документации при использовании Nginx в качестве балансировщика рекомендуются следующие характеристики для сервера балансировки:

- до 4000 подключений – 2 CPU, 4 ГБ RAM;
- до 7500 подключений – 4 CPU, 4 ГБ RAM;
- до 14000 подключений – 8 CPU, 4 ГБ RAM;
- до 27000 подключений – 16 CPU, 4 ГБ RAM;
- до 48000 подключений – 32 CPU, 8 ГБ RAM;
- до 64000 подключений – 44 CPU, 16 ГБ RAM;

Дополнительные требования к серверу балансировки:

- дисковое пространство: от 50 ГБ (SAS/SSD), зависит от объемов логов на сервере и периодов их очистки;
- канал связи: 1 Гбит/с, проводное подключение.

Требования к программному обеспечению сервера web-приложений:

- сервер web-приложений на ОС Linux:
  - версия ОС согласно https://github.com/dotnet/core/blob/main/release-notes/6.0/supported-os.md;
  - CryptoPro CSP 5 или выше (для возможности подписания отчетных форм электронной подписью);
  - OpenSSL 1.1.0 для работы с сертификатами;
  - .NET 6;
  - Nginx / HAProxy 1.8.17 и выше;
  - LibreOffice.

Примечания

1 В случае использования HAProxy на сервере балансировки дополнительных настроек конфигурации проводить не нужно. Далее в описании предоставлены настройки Nginx, т.к. при его использовании необходимо задавать дополнительные параметры.

2 В случае невозможности разнести все необходимые компоненты для работы ПП МЗ на разные сервера, то необходимо придерживаться следующим рекомендациям:

- сервер для работы Компонента анализа данных всегда должен идти отдельно;
- сервер для сервиса отправки сообщений и сервер для дизайнера отчетных форм можно объединить;
- если у вас всего несколько администраторов, которые работают в дизайнере отчетных форм, а пользователей на web-сервере меньше, чем максимальное количество возможных, на основании технических характеристик, то их тоже можно объединить;
- при объединении необходимо отслеживать состояние сервера и при необходимости разнести компоненты по разным серверам.

2.5 Требования к обеспечению сервера Redis

Минимальные требования к обеспечению сервера Redis:

- ОС Linux;
- процессор: 4 ядра, 2,6 ГГц;
- оперативная память: 4 ГБ (из расчета ~150 МБ на 1 форму. 4 ГБ обеспечивает ~30 одновременно выгружаемых печатных форм);
- свободное дисковое пространство: 10 ГБ;
- канал связи: 1 Гбит/с, проводное подключение.

Для уменьшения количества серверов Redis можно поставить на сервер приложения.

Для обеспечения работоспособности ПП МЗ версия Redis должна быть 7.2.0.

Примечание – По умолчанию в данном руководстве описывается установка сервера Redis совместно с web-сервером на одну машину. В случае если нагрузка крайне высока, может возникнуть необходимость выносить сервер Redis на отдельную машину.

2.6 Требования к обеспечению сервера форм

Минимальные требования к обеспечению сервера форм на сервере с программным обеспечением Linux представлены в таблице (Таблица 5).

Таблица 5 – Минимальные требования к обеспечению сервера форм на сервере с программным обеспечением Linux

Параметр	Значение	Примечание
RAM (если используются формы, хранящиеся в БД)	От 8 ГБ ~30 МБ / форма + буфер для операций с отчетной формой из расчета предполагаемого числа параллельных операций	Буфер ~ 300 МБ / форма. 16 ГБ ~ 550 отчетных форм (без буфера)
RAM (если используются формы, хранящиеся в в формате .xml)	От 12 ГБ ~60 МБ / форма + буфер для операций с отчетной формой из расчета предполагаемого числа параллельных операций	12 ГБ, исходя из формулы: (4 ГБ ПП МЗ + 12 ГБ отчетные формы = 16 ГБ – минимальные требования). Буфер ~ 350 МБ / форма. 12 ГБ ~ 200 форм (без буфера). 16 ГБ ~ 270 форм (без буфера)
CPU	От 8 CPU core x 2.7 ГГц	До 500 отчетных форм без учета нагрузки по памяти.

Параметр	Значение	Примечание
		Если нужно больше отчетных форм, рекомендуется развернуть дополнительный экземпляр сервиса и выделить ему аналогичные ресурсы
HDD	100 ГБ	
LAN	1 Гбит/с	

Примечания

1 Буфер для операций с отчетными формами – размер дополнительной оперативной памяти, используемой процессом сервиса для выполнения операций с данными формы (предусмотренных стандартным функционалом). После выполнения операции данная память переиспользуется процессом сервиса для других операций, других отчетных форм. Общий объем буфера оперативной памяти на сервере следует определять исходя из предполагаемого числа операций над формами, которые будут выполняться параллельно в один момент времени. Для новых установок рекомендуется принимать число параллельных операций = 0,2*(макс одновременно открытых форм (окно работающие пользователи));

2 Указанные требования по оперативной памяти учитывают работу только функционала ПП МЗ при работе с отчетными формами и не учитывают объем оперативной памяти, который может потребоваться при запуске некоторых макросов.

Для возможности подписания отчетных форм электронной подписью на сервере форм должны быть установлены:

- CryptoPro CSP 5 или выше;
- Корневые и промежуточные сертификаты ЭП.

2.7 Требования к обеспечению сервера Компонента анализа данных

Минимальные технические требования к серверу Компонента анализа данных:

- процессор: 8 ядер, 2.7 ГГц;
- оперативная память: 16 ГБ;
- свободное дисковое пространство: 200 ГБ (SAS/SSD);
- канал связи: 1 Гбит/с, проводное подключение.

Примечание – Технические требования к серверу Компонента анализа данных рассчитываются индивидуально от потребности клиента.

Программные требования к серверу Компонента анализа данных:

- версия ОС, которая поддерживает работу Docker 20.10.1;
- Docker, версия 20.10.1 и выше;

– процессор с поддержкой AVX2.

Примечание – Для получения информации о требованиях для работы Docker можно воспользоваться документацией, расположенной по адресу https://docs.docker.com/engine/install/.

3 Подготовка к работе

3.1 Состав и содержание дистрибутивного носителя данных

Дистрибутивный носитель данных включает в себя архива web-приложения, внутри которого лежит папка updater, содержащая утилиту для создания и обновления приложения – DBUpdater.

3.2 Порядок загрузки данных и программ

ПП М3 поставляется в виде дистрибутива, в соответствии с типом операционной системы на сервере web-приложения:

- Bars.Svody.Linux-5.3.0.zip – это архив с web-приложением ПП М3, собранный под ОС Linux x64;
- Bars.Svody.Linux.Forms.Service -5.3.0.zip – это архив с приложением сервиса форм, собранный под ОС Linux x64, предназначен для обработки запросов пользователей при работе с отчетными формами;
- Bars.Svody.Linux.Updater.5.3.0.zip – это архив с утилитой DbUpdater, собранный под ОС Linux x64, предназначен для обновления ПП М3, установки лицензии;
- Bars.Svody.Windows.Updater.5.3.0.zip – это архив с утилитой DbUpdater, собранный под ОС Windows x64, предназначен для обновления ПП М3, установки лицензии;
- AddInLib.zip – это архив с набором проектных библиотек (может отсутствовать на Вашем проекте);
- apiJs.zip – это архив с проектными файлами для переопределения/доработки клиентской части приложения (может отсутствовать на Вашем проекте).

Для создания нового web-приложения с нуля:

а) определите, что сервера соответствует техническим требованиям ПП М3. Подробнее в п. 2.4;
б) настройте сетевую связанность между всеми серверами;
в) настройте web-сервер для запуска web-приложения (установите требуемое ПО – например, .NET, Nginx и т.п.);
г) установите Redis, по умолчанию предполагается отдельный сервер. При необходимости других конфигураций, требуется дополнительная консультация;

д) скачайте подходящий дистрибутив (в зависимости от ОС) на сервер web-приложения;

е) распакуйте дистрибутив в папку на web-сервере;

ж) настройте сервер форм для запуска сервиса форм (установите требуемое ПО – например, .NET, Nginx и т.п.);

з) скачайте подходящий дистрибутив (в зависимости от ОС) на сервер форм;

и) распакуйте дистрибутив в папку на сервере форм;

к) создайте БД для работы приложения. В дистрибутиве ПП М3 находится консольное приложение BARS.Svody.DbUpdater (в папке updater в корне архива);

л) установите лицензию. Установку лицензии можно выполнить с помощью DBUpdater. Подробнее в п. 8.3;

Примечание – Без установки лицензии обновление невозможно.

м) обновите БД (проведите миграции). Обновление также выполняется с помощью DBUpdater. Подробнее в п. 8.2;

н) обновите прикладные библиотеки (при их наличии);

о) обновите проектные файлы apiJs (при их наличии);

п) настройте соответствующие конфигурационные файлы;

р) при необходимости подключения Компонента анализа данных:

- настроить сервер и SSO-приложение (п. 13);
- настроить сервер для Компонента анализа данных и развернуть AW (п. 15);
- настроить конфигурационные файлы для совместной работы связки ПП М3-SSO-AW (п. 15.4).

3.3 Разметка дисков

При разметке диска рекомендуется использовать схемы разметки, при которых все файлы в одном разделе. Название подобных пунктов меню разметки диска могут незначительно отличаться между собой при установке различных ОС.

Например, для ОС Astra Linux:

- в разделе «Разметка дисков» выберите пункт «Авто – использовать весь диск» (Рисунок 2);

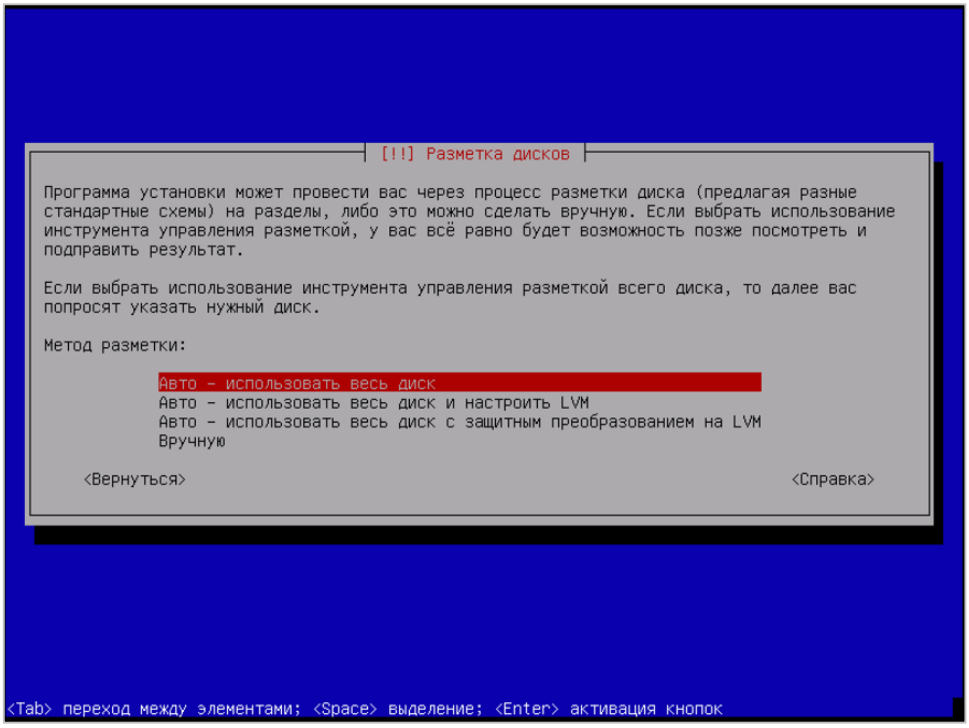


Рисунок 2 – Разметка дисков

Примечание – Если на сервере объем оперативной памяти будет превышать размер диска, куда устанавливается ОС, то метод разметки «Авто – использовать весь диск» выдаст ошибку и не выполнит автоматическую разметку диска, т.к. не сможет создать на диске SWAP-раздел, равный объему оперативной памяти сервера. Потребуется выбрать метод разметки «Вручную».

– выберите подготовленный диск для установки ОС (Рисунок 3);

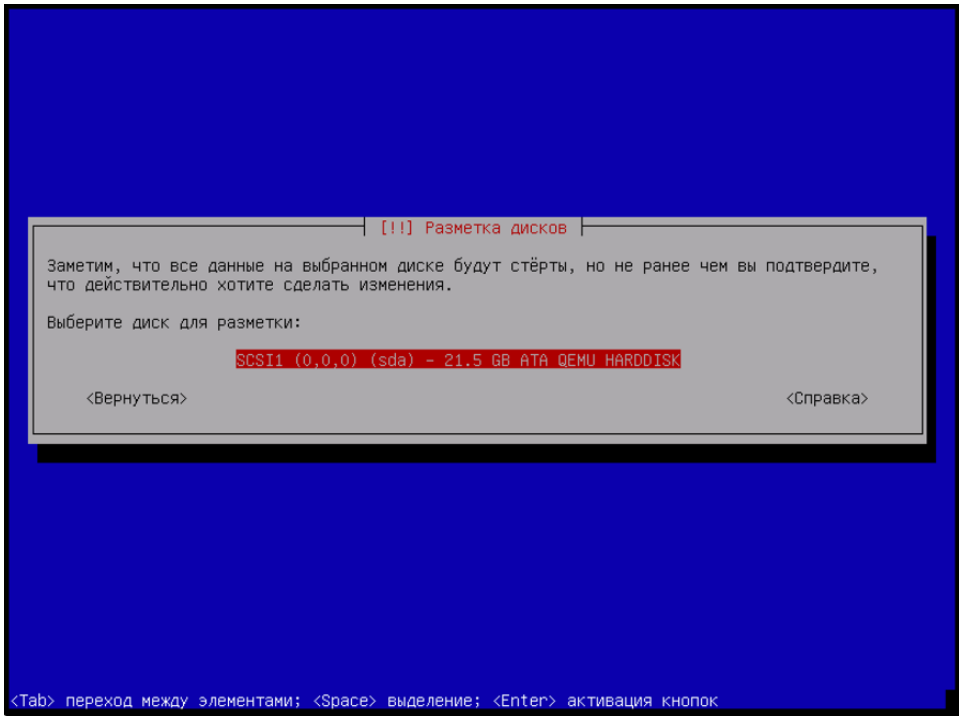


Рисунок 3 – Выбор диска

– выберите схему разметки диска «Все файлы в одном разделе (рекомендуется новичкам)» (Рисунок 4).

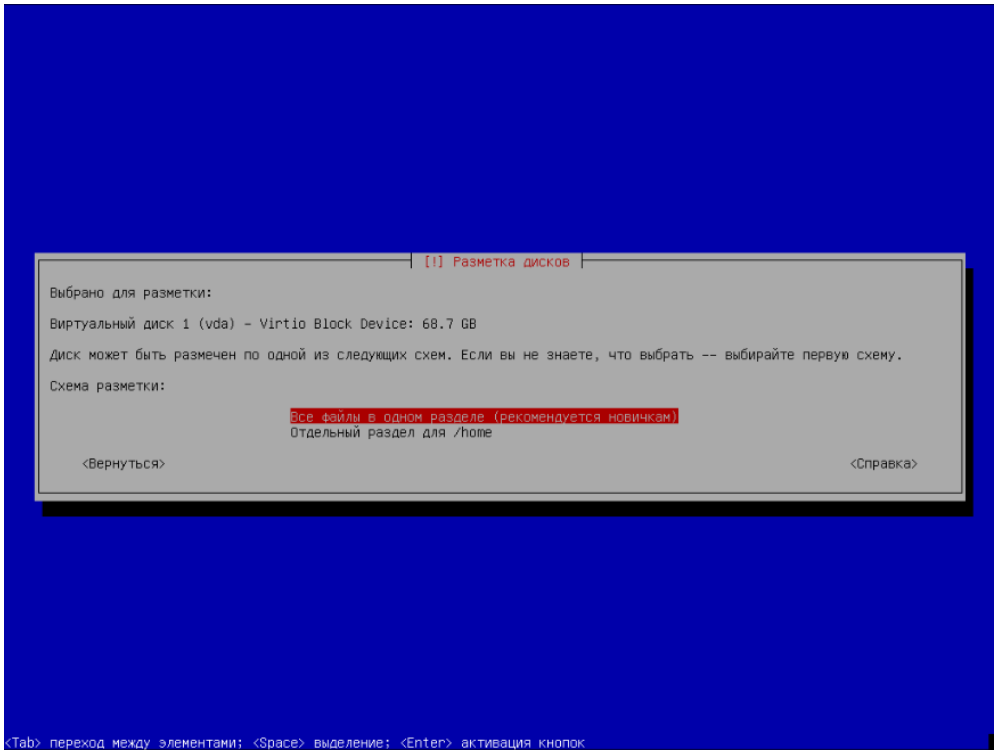


Рисунок 4 – Выбор схемы разметки

4 Настройка ПП МЗ версии 5.3.x на ОС AstraLinux Orel

Примечание – Протестировано на версии Astra Linux CE 2.12.43 (Orel). Официальная документация по ОС Astra Linux: https://wiki.astralinux.ru.

Также предполагается, что на сервере уже установлено следующее системное ПО:

- русская локализация;

Проверка локализации:

```
svody@dev-svody-web:~$ locale
LANG=ru_RU.UTF-8
LANGUAGE=
LC_CTYPE="ru_RU.UTF-8"
LC_NUMERIC="ru_RU.UTF-8"
LC_TIME="ru_RU.UTF-8"
LC_COLLATE="ru_RU.UTF-8"
LC_MONETARY="ru_RU.UTF-8"
LC_MESSAGES="ru_RU.UTF-8"
LC_PAPER="ru_RU.UTF-8"
LC_NAME="ru_RU.UTF-8"
LC_ADDRESS="ru_RU.UTF-8"
LC_TELEPHONE="ru_RU.UTF-8"
LC_MEASUREMENT="ru_RU.UTF-8"
LC_IDENTIFICATION="ru_RU.UTF-8"
LC_ALL=
```

Для установки русской локализации используйте команду:

```
localectl set-locale LANG=ru_RU.UTF-8
```

Далее перезаходим в ПП МЗ и проверяем через команду `locale`

- SSH-сервер с авторизацией по логину/паролю;
- OpenSSL версии 1.1.0.

4.1 Настройка репозиториев на web-сервере и сервере баз данных

Отредактируйте файл vi /etc/apt/sources.list.

Закомментируйте строки, уже имеющиеся по умолчанию в файле. Для этого добавьте знак # в начало строки. Это необходимо для того, чтобы ПП МЗ игнорировала данные записи. Например:

```
      #deb https://download.astralinux.ru/astra/stable/orel/repository/
orel main contrib non-free
      #deb http://mirror.yandex.ru/astra/stable/orel/repository/ orel
main contrib non-free
```

Ниже добавьте записи репозиториев, которые будут использованы при дальнейшей установке:

```
deb http://deb.debian.org/debian stretch main
deb-src http://deb.debian.org/debian stretch main
deb http://apt.postgresql.org/pub/repos/apt/ orel-pgdg main
```

Далее сохраните изменения в файле и запустите обновление:

```
sudo apt-get update
```

4.2 Установка Postgres на сервере баз данных

Выполните подготовительные команды:

```
wget --quiet -O -
https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add –
echo "deb http://apt.postgresql.org/pub/repos/apt/ `lsb_release -
cs`-pgdg main" |sudo tee /etc/apt/sources.list.d/pgdg.list
echo "deb http://apt.postgresql.org/pub/repos/apt/ stretch-pgdg
main" | sudo tee /etc/apt/sources.list.d/postgresql.list
sudo apt-get update
sudo apt install -y postgresql-11 postgresql-contrib-11 --allow-
unauthenticated
```

Для оптимизации работы сервера базы данных отредактируйте конфигурационный файл:

```
vi /etc/postgresql/11/main/postgresql.conf
```

Значения параметров необходимо определить самостоятельно путем анализа ваших характеристик сервера и изучения официальной документации https://postgrespro.ru/docs/postgresql/11.

Для упрощения анализа можно использовать готовые генераторы конфигураций. Например, https://pgtune.leopard.in.ua/#/

Примечание – При разделении сервера БД и сервера web-приложения необходимо открыть доступы в конфигурационном файле:

```
vi /etc/postgresql/11/main/pg_hba.conf
```

Согласно официальной документации Postgres

https://postgrespro.ru/docs/postgresql/11/auth-pg-hba-conf

Откройте порт:

```
sudo ufw allow 5432
```

Перезапустите службу:

```
sudo systemctl reload postgresql
sudo systemctl restart postgresql
```

4.3 Установка Redis на web-сервере

Установите сервер Redis:

```
sudo apt-get -y install redis-server
```

Отредактируйте файл `/etc/redis/redis.conf`, чтобы открыть к нему доступ с других серверов:

```
#bind 127.0.0.1 -::1
bind * -::*
```

Откройте порт:

```
sudo ufw allow 6379
```

Запустите службу:

```
sudo systemctl enable redis-server
sudo systemctl start redis-server
```

4.4 Установка Dotnet на web-сервере

Выполните подготовительные команды:

```
wget -O - https://packages.microsoft.com/keys/microsoft.asc | gpg
--dearmor > microsoft.asc.gpg
sudo mv microsoft.asc.gpg /etc/apt/trusted.gpg.d/
wget https://packages.microsoft.com/config/debian/9/prod.list
sudo mv prod.list /etc/apt/sources.list.d/microsoft-prod.list
sudo chown root:root /etc/apt/trusted.gpg.d/microsoft.asc.gpg
sudo chown root:root /etc/apt/sources.list.d/microsoft-prod.list
```

Установите SDK:

```
sudo apt-get -y install dotnet-sdk-6.0 --allow-unauthenticated
```

Установите runtime:

```
sudo apt-get –y install apt-transport-https --allow-
unauthenticated
sudo apt-get –y install dotnet-runtime-6.0 --allow-
unauthenticated
```

Проверить установленные версии Dotnet можно с помощью команд:

```
dotnet --list-sdks
dotnet --list-runtimes
```

Пример вывода установленного на машине Dotnet:

```
root@svody-astra-orel212:/home/astra# dotnet --list-sdks
6.0.302 [/usr/share/dotnet/sdk]
root@svody-astra-orel212:/home/astra# dotnet --list-runtimes
```

```
      Microsoft.AspNetCore.App 6.0.7
[/usr/share/dotnet/shared/Microsoft.AspNetCore.App]
      Microsoft.NETCore.App 6.0.7
[/usr/share/dotnet/shared/Microsoft.NETCore.App]
```

Также для эксплуатации в условиях высокой нагрузки рекомендуется добавить настройки в конфигурационный файл ядра. Для этого отредактируйте файл vi /etc/sysctl.conf и добавьте в него следующие параметры:

```
net.core.somaxconn=20000
net.core.netdev_max_backlog=65535
fs.file-max=1000000
fs.inotify.max_user_instances=1024
fs.inotify.max_user_watches=1048576
fs.inotify.max_queued_events=163840
```

После чего перечитайте файл конфигурации командой:

```
sysctl –p
```

Либо перезагрузите web-сервер.

4.5 Установка Nginx на web-сервере

Установите Nginx:

```
sudo apt install nginx --allow-unauthenticated
```

Проведите настройки http и https сервера согласно официальной документации справочного центра по Nginx: https://docs.nginx.com/nginx/admin-guide/.

Примечание – Для https сервера требуется SSL-сертификат, выданный официальным удостоверяющим центром. Не подходят самоподписанные и самозаверенные сертификаты.

Создайте конфигурационный файл vi /etc/nginx/conf.d/svody.conf со следующим содержанием:

```
location /svody {
client_max_body_size 500M;
proxy_pass http://127.0.0.1:5001/svody;
proxy_http_version 1.1;
proxy_set_header Upgrade $http_Upgrade;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header X-Forwarded-Proto $realscheme;
proxy_set_header Connection keep-alive;
proxy_set_header Connection "upgrade";
proxy_send_timeout 600s;
proxy_read_timeout 600s;
proxy_connect_timeout 600s;
proxy_buffer_size 64k;
```

```
proxy_buffers 4 64k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 1024k;
proxy_headers_hash_max_size 512;
proxy_headers_hash_bucket_size 128;
}
```

Для увеличения времени таумаута при работе ПП МЗ необходимо увеличить значения следующих параметров:

```
proxy_send_timeout 600s;
proxy_read_timeout 600s;
```

В зависимости от количества активных пользователей дополнительно настройте Nginx:

а) в файле nginx.conf (/etc/nginx) в секцию http добавьте параметр, увеличивающий максимально допустимый объем заголовков запросов large_client_header_buffers 4 16k;

б) при подключении на схеме авторизации через Keycloak обязательно добавьте следующие директивы: large_client_header_buffers 4 16k и proxy_set_header Connection "upgrade";

в) в файле nginx.conf (/etc/nginx) отредактируйте параметр worker_processes auto;

г) в файле nginx.conf (/etc/nginx) добавьте параметр worker_connections 41 (количество статичных ресурсов при загрузке рабочего стола ПП МЗ) * суммарное число пользователей всех приложений ПП МЗ, доступ к которым осуществляется через Nginx;

д) в файле nginx.conf (/etc/nginx) добавьте параметр worker_rlimit_nofile worker_connections * 2 согласно рекомендациям из документации к Nginx;

е) в файле nginx.conf (/etc/nginx) в секцию http добавьте параметр:

```
map $http_x_forwarded_proto $realscheme {
default $scheme;
https https;
http http;
}
```

Сохраните настройки и перезапустите службу:

```
systemctl reload nginx
systemctl restart nginx
```

4.6 Установка приложения на web-сервере

Создайте директорию:

```
mkdir /opt/svody
```

Скопируйте файлы web-приложения из архива дистрибутива в созданную директорию.

Создайте директорию для файлов API:

```
mkdir /opt/svody/AddInLib
```

Скопируйте файлы API из архива дистрибутива AddInLib.zip в созданную директорию.

Раздайте права для запуска:

```
chmod +x /opt/svody/updater/BARS.Svody.DbUpdater
chmod +x /opt/svody/BARS.Svody.Web.Host
```

Откройте порты:

```
sudo ufw allow 80
sudo ufw allow 5001
sudo ufw allow 6379
```

Настройте подключение к БД согласно п. 10.2.

Создайте БД согласно п. 8.1.

Например:

```
/opt/svody/updater/BARS.Svody.DbUpdater --createSchema -
sysUserName postgres -sysUserPassword postgres -sysDataBase postgres -
connSettingsPath /opt/svody/Приложение.барс
```

Установите лицензию согласно п. 8.3.

Создайте все табличные пространства согласно п. 8.2.

Например:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations /opt/svody/ -
connSettingsPath /opt/svody/Приложение.барс -simpleProgress true -mode
platform -updateArchiveDatabases false
```

Создайте сервис приложения:

```
vi /etc/systemd/system/svody.service
[Unit]
Description = Svody app: svody
[Service]
WorkingDirectory = /opt/svody
ExecStart = /opt/svody/BARS.Svody.Web.Host
Restart = always
RestartSec = 10
SyslogIdentifier = svody
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5001
Environment = ASPNETCORE_BASEPATH=/svody
```

```
Environment = TMPDIR=/var/tmp
User = root
[Install]
WantedBy = multi-user.target
```

Отредактируйте файл настроек Redis, заполнив соответствующие параметры своими:

```
vi /opt/svody/ redis.config
<configuration>
<redis>
    <host>ip-адрес_сервера_redis</host>
    <port>6379</port>
    <user>default</user>
    <password>"redispw"</password>
</redis>
</configuration>
```

Примечание – Внутри пароля недопустимы следующие символы ", &, ', <, >, #,$.

Подробнее о настройке файла описано в п. 10.4.

Отредактируйте файл настроек сервера форм, заполнив соответствующие параметры своими:

```
vi /opt/svody/forms.service.json
```

Подробнее о настройке файла описано в п. 10.5.

Запустите приложение:

```
systemctl daemon-reload
systemctl start svody
systemctl enable svody
```

4.7 Установка приложения на сервере форм

Примечание – В данной инструкции описана настройка сервера форм на отдельной от web-сервера машине. Однако, если количество пользователей и нагрузка небольшие, можно совместить сервер форм и web-сервер на одной машине.

Создайте директорию:

```
mkdir /opt/forms
```

Скопируйте файлы сервиса форм из архива дистрибутива в созданную директорию.

Создайте директорию для файлов API:

```
 mkdir /opt/forms/AddInLib
```

Скопируйте файлы API из архива дистрибутива AddInLib.zip в созданную директорию.

Раздайте права для запуска:

```
chmod +x /opt/forms/Svody.Forms.Host
```

Создайте сервис приложения:

```
vi /etc/systemd/system/forms.service

[Unit]
Description = Svody forms service: svody
[Service]
User = root
WorkingDirectory = /opt/forms
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5003
Environment = ASPNETCORE_BASEPATH=/forms
Environment = TMPDIR=/var/tmp
Environment = SSL_CERT_DIR=/etc/ssl/certs/
Environment = LD_LIBRARY_PATH=/opt/cprocsp/cp-openssl-
1.1.0/lib/amd64/
ExecStart = /opt/forms/Svody.Forms.Host
SyslogIdentifier = svody-forms
Restart = always
RestartSec = 10
[Install]
WantedBy = multi-user.target
```

Скопируйте созданный и настроенный в предыдущем пункте файл `Приложение.барс` из каталога `/opt/svody` на web-сервере. Поместите данный файл в корень каталога `/opt/forms`.

Отредактируйте файл настроек AW, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/aw.json
{
  "aw": {
    "db": "default",
    "host": "ip-адрес_сервера_aw",
    "port": 9017,
    "user": "default",
    "password": "enter4z",
    "baseUrl": "URL-сервера_AW",
    "adminLogin": "tech_admin",
    "adminPassword": "123456"
  }
}
```

Подробнее о настройке файла описано в п. 10.10.

Отредактируйте файл настроек подключения к серверу БД, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/ postgres.json
```

```
{
  "postgres": {
    "dbName":"svody",
    "schemeName":"svody_forms_service",
    "host":"ip-адрес_сервера_БД",
    "port":5432,
    "login":"svody",
    "password":"123",
    "minPoolSize": 2,
    "maxPoolSize": 50,
    "connectionOpenTimeout": 60,
    "executeCommandTimeout": 60,
    "connectionIdleSeconds": 300,
    "connectionPruningSeconds": 50,
    "readBufferSize": 524288,
    "writeBufferSize": 524288
  }
}
```

Подробнее о настройке файла описано в п. 10.7.

Отредактируйте файл настроек Redis, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/ redis.json
```

```
{
  "redis" : {
    "host": "ip-адрес_сервера_redis",
    "port": 6379,
    "user": "default",
    "password": "redispw"
  }
}
```

Подробнее о настройке файла описано в п. 10.6.

Примечание – Конфигурационные файлы «metrics.json» и «formsBackups.json», находящиеся в подкаталоге Config, не требуют редактирования при стандартной установке. Однако подробности об их настройке при необходимости можно найти в п. 10.8 и 10.9.

Запустите приложение:

```
systemctl daemon-reload
systemctl start forms
```

4.8 Обновление приложения на web-сервере

Процедура обновления web-приложения аналогична процедуре развертывания web-приложения.

Перед обновлением web-приложения создайте резервную копию:

- папок «AddInLib», «wwwroot\apiJs», файлов новостей «wwwroot\actualNews.html», а после обновления скопируйте их в каталог с обновленным web-клиентом;
- всех файлов конфигурации («web.config», «svody.config», «redis.config», «forms.service.json»), а после обновления внесите индивидуальные настройки приложения согласно этим файлам в новые файлы конфигурации;
- файла конфигурации «Приложение.барс».

Выполните остановку пула приложений:

```
systemctl stop svody
```

Для обновления web-приложения повторно распакуйте новый архив «BARS.Svody.Linux-5.x.x.zip» в каталог приложения. При этом файлы («web.config», «svody.config», «redis.config», «forms.service.json» замените, а затем отредактируйте, согласно настройкам вашего приложения. Файл «Приложение.барс» оставляем без изменений, так как он содержит настройки подключения к БД.

Для обновления API создайте папку «AddInLib» в каталоге приложения. Например:

mkdir /opt/svody/AddInLib

После чего распакуйте в нее файлы API из одноименного архива.

Выполните миграции согласно п. 8.2 данной инструкции.

Пример команды:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations /opt/svody/ -
connSettingsPath /opt/svody/Приложение.барс -simpleProgress true -mode
platform -updateArchiveDatabases false
```

Выполните запуск пула приложений:

```
systemctl start svody
```

4.9 Обновление приложения на сервере форм

Процедура обновления приложения на сервере форм аналогична процедуре развертывания.

Перед обновлением сервиса форм создайте резервную копию:

- папок «AddInLib», файла «Приложение.барс». После обновления скопируйте файл «Приложение.барс» в каталог с обновленным приложением;
- всех файлов конфигурации, находящихся в папке «Config», а после обновления внесите индивидуальные настройки приложения согласно этим файлам в новые файлы конфигурации.

Выполните остановку пула приложений:

```
systemctl stop forms
```

Для обновления сервиса форм повторно распакуйте новый архив «Bars.Svody.Linux.Forms.Service-5.x.x.zip» в каталог приложения. При этом файлы, находящиеся в папке «Config», замените, а затем отредактируйте, согласно настройкам вашего приложения. Файл «Приложение.барс» оставьте без изменений, так как он содержит настройки подключения к БД.

Для обновления API создайте папку «AddInLib» в каталоге приложения. Например:

```
mkdir /opt/forms/AddInLib
```

После чего распакуйте в нее файлы API из одноименного архива.

Выполните запуск пула приложений:

```
systemctl start forms
```

4.10 Установка КриптоПРО на web-сервере

Перейдите на сайт ПО «КриптоПРО»: https://cryptopro.ru/user?destination=node%2F148#latest_csp50, выберите дистрибутив КриптоПро CSP 5.0 для UNIX.

Откроется список пакетов (Рисунок 5).

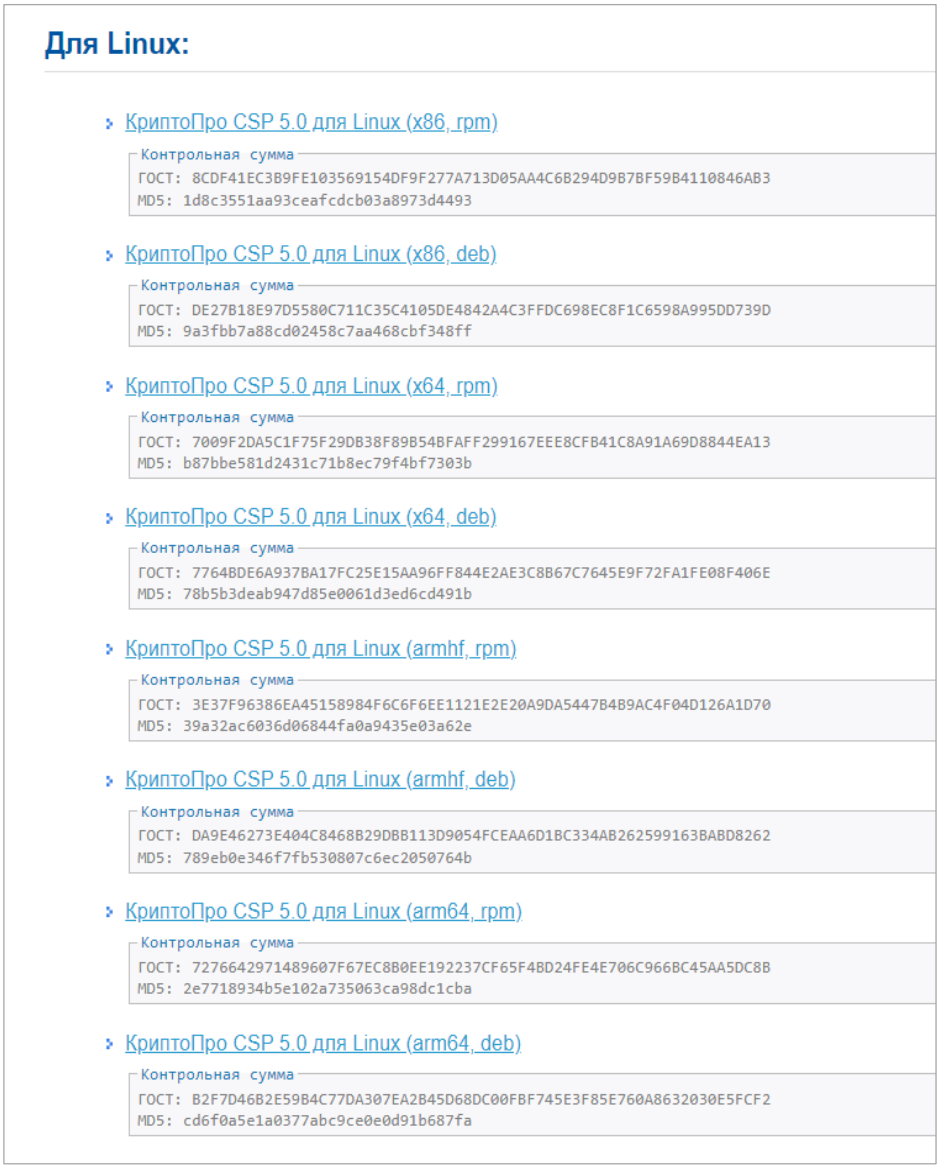


Рисунок 5 – Список пакетов

Выберите пакет КриптоПро CSP 5.0 для Linux (x64, deb) и загрузите его.

Также необходимы пакеты OpenSSL и PKCS11 – без них не будет работать подпись.

Распакуйте архив во временную директорию и перейдите в неё:

```
tar -zxf linux-amd64_deb.tgz -C /var/tmp/
cd /var/tmp/linux-amd64_deb
```

Установите в графическом режиме, запустив из директории распаковки архива:

```
sudo chmod a+x ./install_gui.sh
sudo ./install_gui.sh
```

В окне настроек кнопкой «Пробел» установите все «флажки».

Нужные пакеты OpenSSL и PKCS11 будут установлены.

Примечания

1 КриптоПро должна быть установлена как на web-сервере, так и на сервере форм.

2 Корневые и промежуточные сертификаты ЭП должны быть установлены на сервере форм.

4.11 Установка openssl-gost-engine

В состав дистрибутивов Astra Linux входит пакет библиотек для выполнения защитного преобразования по алгоритмам ГОСТ.

```
libgost-astra
```

Данный пакет обеспечивает включение в состав методов защитного преобразования, поддерживаемых пакетами openssl и openvpn, следующих алгоритмов:

- ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 – алгоритмы цифровой подписи. Также поддерживается обмен ключами, основанный на открытых ключах (детали см. в RFC 4357). Алгоритмы используют:
  - закрытые ключи 256 бит для ГОСТ 2001 и 256/512 бит для ГОСТ 2012;
  - открытые ключи 512 бит для ГОСТ 2001 и 512/1024 бит для ГОСТ 2012.
- ГОСТ Р 34.11-94 Алгоритм хеширования. Хэш 256 бит;
- ГОСТ Р 34.11-2012 Алгоритм хеширования. Хэш 256 и 512 бит;
- ГОСТ 28147-89 – Симметричное защитное преобразование с ключом 256 бит. Реализованы режимы CBC, CFB и CNT, поддерживается алгоритм «key meshing» (RFC 4357);
- ГОСТ 28147-89 в режиме выработки имитовставки. Базируется на алгоритме симметричного защитного преобразования. Имеет симметричный ключ 256 бит и разрядность вставки от 8 до 64 (по умолчанию 32) бит;
- ГОСТ Р 34.13–2015 – Симметричное защитное преобразование «Кузнечик» («Grasshopper»).

Для установки пакета можно использовать графический менеджер пакетов synaptic или выполнить установку из командной строки командой

```
apt -y install libgost-astra
```

Проверить список доступных алгоритмов можно командой:

```
openssl engine gost-astra –c
```

При установленном и включенном движке libgost-astra ответ команды будет выглядеть примерно так:

```
# openssl engine gost-astra -c
(gost-astra) Astra implementation of GOST engine
```

[gost89, gost89-cnt, gost89-cnt-12, gost89-cbc, grasshopper-ecb, grasshopper-cbc, grasshopper-cfb, grasshopper-ofb, grasshopper-ctr, md_gost94, gost-mac, md_gost12_256, md_gost12_512, gost-mac-12, gost2001, gost-mac, gost2012_256, gost2012_512, gost-mac-12]

4.12 Установка LibreOffice

Для того, чтобы была возможность выгружать печатные формы в форматах ods и odt необходимо установить на сервере последнюю версию LibreOffice

Примечание – Формат выгрузки задается в Дизайнере отчетных форм в разделе «Печатные формы» в поле «Формат выгрузки» напротив соответствующей печатной формы. Для выгрузки в формате ods и odt необходимо соответственно в этом поле выбрать значение «ods» или «odt».

Для Astra 2.12:

Установка из пакетов:

Wget https://download.documentfoundation.org/libreoffice/stable/7.6.0/deb/x86_64/LibreOffice_7.6.0_Linux_x86-64_deb.tar.gz

tar zxvf LibreOffice_7.6.0_Linux_x86-64_deb.tar.gz

cd LibreOffice_7.6.0.3_Linux_x86-64_deb/

cd DEBS/

sudo dpkg -i *.deb

libreoffice7.6 --version

Создаем символьную ссылку:

ln -s /usr/local/bin/libreoffice7.6 /usr/local/bin/libreoffice

libreoffice --version

Протестировано на версии LibreOffice 7.6.0.3

5 Настройка ПП МЗ версии 5.3.x на ОС AstraLinux Смоленск

Примечание – Официальная документация на операционную систему Astra Linux Special Edition: https://wiki.astralinux.ru/pages/viewpage.action?pageId=153486777.

Также предполагается, что на сервере уже установлено следующее системное ПО:

- русская локализация;

Проверка локализации:

```
svody@dev-svody-web:~$ locale
LANG=ru_RU.UTF-8
LANGUAGE=
LC_CTYPE="ru_RU.UTF-8"
LC_NUMERIC="ru_RU.UTF-8"
LC_TIME="ru_RU.UTF-8"
LC_COLLATE="ru_RU.UTF-8"
LC_MONETARY="ru_RU.UTF-8"
LC_MESSAGES="ru_RU.UTF-8"
LC_PAPER="ru_RU.UTF-8"
LC_NAME="ru_RU.UTF-8"
LC_ADDRESS="ru_RU.UTF-8"
LC_TELEPHONE="ru_RU.UTF-8"
LC_MEASUREMENT="ru_RU.UTF-8"
LC_IDENTIFICATION="ru_RU.UTF-8"
LC_ALL=
```

Для установки русской локализации используйте команду:

```
localectl set-locale LANG=ru_RU.UTF-8
```

Далее перезаходим в ПП МЗ и проверяем через команду `locale`

- SSH-сервер с авторизацией по логину/паролю;
- OpenSSL версии 1.1.0.

5.1 Установка PostgreSQL на сервере баз данных

Установку защищенной версии PostgreSQL 11 на специальной ОС Astra Linux необходимо проводить согласно официальной документации, доступной по ссылке ниже:

https://wiki.astralinux.ru/pages/viewpage.action?pageId=147162402

После проведения работ по пункту «установка пакетов» выполните команды:

```
usermod -a -G shadow postgres
setfacl -d -m u:postgres:r /etc/parsec/macdb
setfacl -R -m u:postgres:r /etc/parsec/macdb
setfacl -m u:postgres:rx /etc/parsec/macdb
setfacl -d -m u:postgres:r /etc/parsec/capdb
setfacl -R -m u:postgres:r /etc/parsec/capdb
setfacl -m u:postgres:rx /etc/parsec/capdb
```

Для оптимизации работы сервера базы данных отредактируйте конфигурационный файл:

```
vi /etc/postgresql/11/main/postgresql.conf
```

Значения параметров необходимо определить самостоятельно путем анализа ваших характеристик сервера и изучения официальной документации:

https://postgrespro.ru/docs/postgresql/11

Для упрощения анализа можно использовать готовые генераторы конфигураций. Например, https://pgtune.leopard.in.ua/#/.

Примечание – При разделении сервера БД и сервера web-приложения необходимо открыть доступы в конфигурационном файле:

```
vi /etc/postgresql/11/main/pg_hba.conf
```

Согласно официальной документации Postgres:

https://postgrespro.ru/docs/postgresql/11/auth-pg-hba-conf

Откройте порт:

```
sudo ufw allow 5432
```

Перезапустите службу:

```
sudo systemctl reload postgresql
sudo systemctl restart postgresql
```

5.2 Установка Redis на web-сервере

Установите сервер Redis:

```
sudo apt-get -y install redis-server
```

Отредактируйте файл `/etc/redis/redis.conf`, чтобы открыть к нему доступ с других серверов:

```
#bind 127.0.0.1 -::1
bind * -::*
```

Откройте порт:

```
sudo ufw allow 6379
```

Запустите службу:

```
sudo systemctl enable redis-server
sudo systemctl start redis-server
```

5.3 Установка Dotnet на web-сервере

Выполните подготовительные команды:

```
wget -O - https://packages.microsoft.com/keys/microsoft.asc | gpg
--dearmor > microsoft.asc.gpg
sudo mv microsoft.asc.gpg /etc/apt/trusted.gpg.d/
wget https://packages.microsoft.com/config/debian/9/prod.list
sudo mv prod.list /etc/apt/sources.list.d/microsoft-prod.list
sudo chown root:root /etc/apt/trusted.gpg.d/microsoft.asc.gpg
sudo chown root:root /etc/apt/sources.list.d/microsoft-prod.list
```

Установка SDK:

```
sudo apt-get install -y dotnet-sdk-6.0 --allow-unauthenticated
```

Установка runtime:

```
sudo apt-get install -y apt-transport-https --allow-
unauthenticated
sudo apt-get install -y dotnet-runtime-6.0 --allow-
unauthenticated
```

Проверить установленные версии Dotnet можно с помощью команд:

```
dotnet --list-sdks
dotnet --list-runtimes
```

Пример вывода установленного на машине Dotnet:

```
root@svody-astra:/home/astra# dotnet --list-sdks
6.0.302 [/usr/share/dotnet/sdk]
root@svody-astra:/home/astra# dotnet --list-runtimes
Microsoft.AspNetCore.App 6.0.7
[/usr/share/dotnet/shared/Microsoft.AspNetCore.App]
Microsoft.NETCore.App 6.0.7
[/usr/share/dotnet/shared/Microsoft.NETCore.App]
```

Также для эксплуатации в условиях высокой нагрузки рекомендуется добавить настройки в конфигурационный файл ядра. Для этого отредактируйте файл:

```
vi /etc/sysctl.conf
```

Добавьте в него следующие параметры:

```
net.core.somaxconn=20000
net.core.netdev_max_backlog=65535
fs.file-max=1000000
fs.inotify.max_user_instances=1024
fs.inotify.max_user_watches=1048576
fs.inotify.max_queued_events=163840
```

Далее перечитайте файл конфигурации командой:

```
sysctl –p\
```

Либо перезагрузите web-сервер.

5.4 Установка Nginx на web-сервере

Установите Nginx:

```
sudo apt install nginx --allow-unauthenticated
```

Проведите настройки http и https сервера согласно официальной документации справочного центра по Nginx:

https://docs.nginx.com/nginx/admin-guide/

Примечание – Для https сервера требуется SSL-сертификат, выданный официальным удостоверяющим центром. Не подходят самоподписанные и самозаверенные сертификаты.

Создайте конфигурационный файл:

```
vi /etc/nginx/conf.d/svody.conf
```

со следующим содержанием:

```
location /svody {
client_max_body_size 500M;
proxy_pass http://127.0.0.1:5001/svody;
proxy_http_version 1.1;
proxy_set_header Upgrade $http_Upgrade;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header X-Forwarded-Proto $realscheme;
proxy_set_header Connection keep-alive;
proxy_set_header Connection "upgrade";
proxy_send_timeout 600s;
proxy_read_timeout 600s;
proxy_connect_timeout 600s;
proxy_buffer_size 64k;
proxy_buffers 4 64k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 1024k;
proxy_headers_hash_max_size 512;
proxy_headers_hash_bucket_size 128;
}
```

В зависимости от количества активных пользователей дополнительно настройте Nginx:

а) в файле nginx.conf (/etc/nginx) в секцию http добавьте параметр, увеличивающий максимально допустимый объем заголовков запросов large_client_header_buffers 4 16k;

б) при подключении на схеме авторизации через Keycloak обязательно добавьте следующие директивы: large_client_header_buffers 4 16k и proxy_set_header Connection "upgrade";

в) в файле nginx.conf (/etc/nginx) отредактируйте параметр worker_processes auto;

г) в файле nginx.conf (/etc/nginx) добавьте параметр worker_connections 41 (количество статичных ресурсов при загрузке рабочего стола ПП МЗ) * суммарное число пользователей всех приложений ПП МЗ, доступ к которым осуществляется через Nginx;

д) в файле nginx.conf (/etc/nginx) добавьте параметр worker_rlimit_nofile worker_connections * 2 согласно рекомендациям из документации к Nginx;

е) в файле nginx.conf (/etc/nginx) в секцию http добавьте параметр:

```
map $http_x_forwarded_proto $realscheme {
default $scheme;
https https;
http http;
}
```

Сохраните настройки и перезапустите службу

```
systemctl reload nginx
systemctl restart nginx
```

5.5 Установка приложения на web-сервере

Создайте директорию:

```
mkdir /opt/svody
```

Скопируйте файлы web-приложения из архива дистрибутива в созданную директорию.

Создайте директорию для файлов API:

```
 mkdir /opt/svody/AddInLib
```

Скопируйте файлы API из архива дистрибутива AddInLib.zip в созданную директорию.

Раздайте права для запуска:

```
chmod +x /opt/svody/updater/BARS.Svody.DbUpdater
chmod +x /opt/svody/BARS.Svody.Web.Host
```

Откройте порты:

```
sudo ufw allow 80
sudo ufw allow 5001
sudo ufw allow 6379
```

Настройте подключение к БД согласно п. 10.2.

Создайте БД согласно п. 8.1.

Например:

```
/opt/svody/updater/BARS.Svody.DbUpdater --createSchema -
sysUserName postgres -sysUserPassword postgres -sysDataBase postgres -
connSettingsPath /opt/svody/Приложение.барс
```

Установите лицензию согласно п. 8.3.

Создайте все табличные пространства согласно п. 8.2.

Например:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations /opt/svody/ -
connSettingsPath /opt/svody/Приложение.барс -simpleProgress true -mode
platform -updateArchiveDatabases false
```

Создайте сервис приложения:

```
vi /etc/systemd/system/svody.service
[Unit]
Description = Svody app: svody
[Service]
WorkingDirectory = /opt/svody
ExecStart = /opt/svody/BARS.Svody.Web.Host
Restart = always
RestartSec = 10
SyslogIdentifier = svody
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5001
Environment = ASPNETCORE_BASEPATH=/svody
Environment = TMPDIR=/var/tmp
User = root
[Install]
WantedBy = multi-user.target
```

Отредактируйте файл настроек Redis, заполнив соответствующие параметры своими:

```
vi /opt/svody/ redis.config
<configuration>
<redis>
    <host> ip-адрес_сервера_redis</host>
    <port>6379</port>
    <user>default</user>
    <password>"redispw"</password>
</redis>
</configuration>
```

Примечание – Внутри пароля недопустимы следующие символы ", &, ', <, >, #,$.

Подробнее о настройке файла описано в п. 10.4.

Отредактируйте файл настроек сервера форм, заполнив соответствующие параметры своими:

```
vi /opt/svody/forms.service.json
{
  "FormEnginesConfig" : {
    "Urls":["http:// ip-адрес_сервера_форм:5003"],
    "HealthCheckIntervalInSeconds":60
  }
}
```

Если требуется настроить несколько сервисов форм, то файл forms.service.json будет выглядеть следующим образом:

```
vi /opt/svody/forms.service.json
{
  "FormEnginesConfig" : {
    "Urls":["http:// ip-адрес_сервера_форм 1:5003", "http:// ip-адрес_сервера_форм 2:5003", "http:// ip-адрес_сервера_форм 3:5003"],
    "HealthCheckIntervalInSeconds":60
  }
}
```

Подробнее о настройке файла описано в п. 10.5.

Запустите приложение:

```
systemctl daemon-reload
systemctl start svody
systemctl enable svody
```

5.6 Установка приложения на сервере форм

Примечание – В данной инструкции описана настройка сервера форм на отдельной от web-сервера машине. Однако, если количество пользователей и нагрузка небольшие, можно совместить сервер форм и web-сервер на одной машине.

Создайте директорию:

```
mkdir /opt/forms
```

Скопируйте файлы сервиса форм из архива дистрибутива в созданную директорию.

Создайте директорию для файлов API:

```
mkdir /opt/forms/AddInLib
```

Скопируйте файлы API из архива дистрибутива AddInLib.zip в созданную директорию.

Раздайте права для запуска:

```
chmod +x /opt/forms/Svody.Forms.Host
```

Создайте сервис приложения:

```
vi /etc/systemd/system/forms.service

[Unit]
Description = Svody forms service: svody
[Service]
User = root
WorkingDirectory = /opt/forms
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5003
Environment = ASPNETCORE_BASEPATH=/forms
Environment = TMPDIR=/var/tmp
Environment = SSL_CERT_DIR=/etc/ssl/certs/
Environment = LD_LIBRARY_PATH=/opt/cprocsp/cp-openssl-
1.1.0/lib/amd64/
ExecStart = /opt/forms/Svody.Forms.Host
SyslogIdentifier = svody-forms
Restart = always
RestartSec = 10
[Install]
WantedBy = multi-user.target
```

Скопируйте созданный и настроенный в предыдущем пункте файл `Приложение.барс` из каталога `/opt/svody` на web-сервере. Поместите данный файл в корень каталога `/opt/forms`.

Отредактируйте файл настроек AW, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/aw.json
{
  "aw": {
    "db": "default",
    "host": "ip-адрес_сервера_aw",
    "port": 9017,
    "user": "default",
    "password": "enter4z",
    "baseUrl": "URL-сервера_AW",
    "adminLogin": "tech_admin",
    "adminPassword": "123456"
  }
}
```

Подробнее о настройке файла описано в п. 10.10.

Отредактируйте файл настроек подключения к серверу БД, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/ postgres.json

{
  "postgres": {
```

```
    "dbName":"svody",
    "schemeName":"svody_forms_service",
    "host":"ip-адрес_сервера_БД",
    "port":5432,
    "login":"svody",
    "password":"123",
    "minPoolSize": 2,
    "maxPoolSize": 50,
    "connectionOpenTimeout": 60,
    "executeCommandTimeout": 60,
    "connectionIdleSeconds": 300,
    "connectionPruningSeconds": 50,
    "readBufferSize": 524288,
    "writeBufferSize": 524288
  }
}
```

Подробнее о настройке файла описано в п. 10.7.

Отредактируйте файл настроек Redis, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/ redis.json

{
  "redis" : {
    "host": "ip-адрес_сервера_redis",
    "port": 6379,
    "user": "default",
    "password": "redispw"
  }
}
```

Подробнее о настройке файла описано в п. 10.6.

Примечание – Конфигурационные файлы «metrics.json» и «formsBackups.json», находящиеся в подкаталоге Config, не требуют редактирования при стандартной установке. Однако подробности об их настройке при необходимости можно найти в п.10.8 и 10.9.

Запустите приложение:

```
systemctl daemon-reload
systemctl start forms
```

5.7 Обновление приложения на web-сервере

Процедура обновления web-приложения аналогична процедуре развертывания web-приложения.

Перед обновлением web-приложения создайте резервную копию:

- папок «AddInLib», «wwwroot\apiJs», файлов новостей «wwwroot\actualNews.html», а после обновления скопируйте их в каталог с обновленным web-клиентом;
- всех файлов конфигурации («web.config», «svody.config», «redis.config», «forms.service.json»), а после обновления внесите индивидуальные настройки приложения согласно этим файлам в новые файлы конфигурации;
- файла конфигурации «Приложение.барс».

Выполните остановку пула приложений:

```
systemctl stop svody
```

Для обновления web-приложения повторно распакуйте новый архив «BARS.Svody.Linux-5.x.x.zip» в каталог приложения. При этом файлы «web.config», «svody.config», «redis.config», «forms.service.json» замените, а затем отредактируйте согласно настройкам вашего приложения. Файл «Приложение.барс» оставьте без изменений, так как он содержит настройки подключения к БД.

Для обновления API создайте папку «AddInLib» в каталоге приложения. Например:

```
mkdir /opt/svody/AddInLib
```

После чего распакуйте в нее файлы API из одноименного архива.

Выполните миграции согласно п. 8.2 данной инструкции.

Пример команды:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations /opt/svody/ -
connSettingsPath /opt/svody/Приложение.барс -simpleProgress true -mode
platform -updateArchiveDatabases false
```

Выполните запуск пула приложений:

```
systemctl start svody
```

5.8 Обновление приложения на сервере форм

Процедура обновления приложения на сервере форм аналогична процедуре развертывания.

Перед обновлением сервиса форм создайте резервную копию:

- папок «AddInLib», файла «Приложение.барс». После обновления скопируйте файл «Приложение.барс» в каталог с обновленным приложением;
- всех файлов конфигурации, находящихся в папке «Config», а после обновления внесите индивидуальные настройки приложения согласно этим файлам в новые файлы конфигурации.

Выполните остановку пула приложений:

```
systemctl stop forms
```

Для обновления сервиса форм повторно распакуйте новый архив «Bars.Svody.Linux.Forms.Service-5.x.x.zip» в каталог приложения. При этом файлы, находящиеся в папке «Config», замените, а затем отредактируйте согласно настройкам вашего приложения. Файл «Приложение.барс» оставьте без изменений, так как он содержит настройки подключения к БД.

Для обновления API создайте папку «AddInLib» в каталоге приложения. Например:

```
mkdir /opt/forms/AddInLib
```

После чего распакуйте в нее файлы API из одноименного архива.

Выполните запуск пула приложений:

```
systemctl start forms
```

5.9 Установка КриптоПРО на web-сервере

Перейдите на сайт ПО «КриптоПРО»: https://cryptopro.ru/user?destination=node%2F148#latest_csp50, выберите дистрибутив КриптоПро CSP 5.0 для UNIX.

Откроется список пакетов (Рисунок 6).

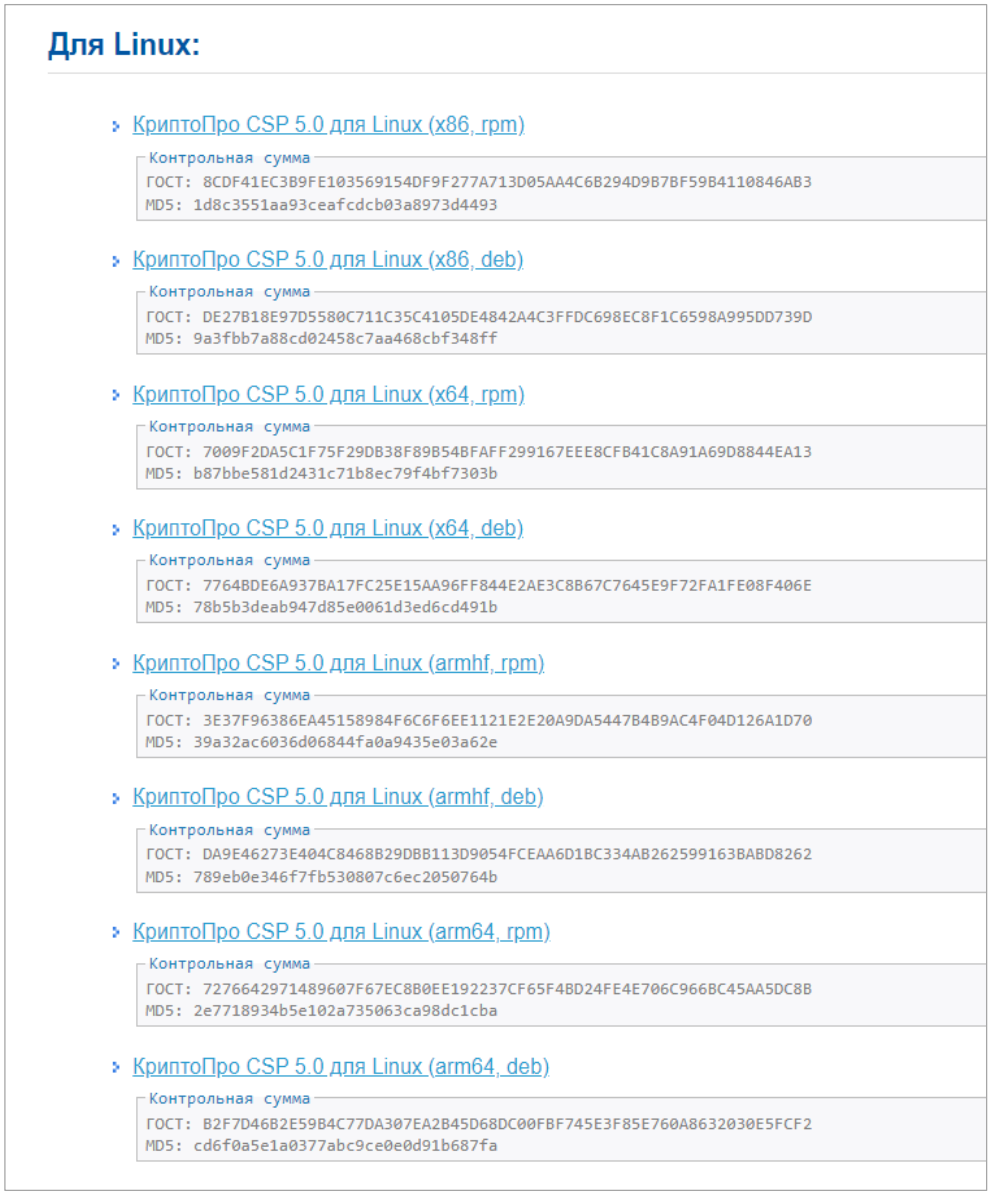


Рисунок 6 – Список пакетов

Выберите пакет КриптоПро CSP 5.0 для Linux (x64, deb) и загрузите его.

Также необходимы пакеты OpenSSL и PKCS11 – без них не будет работать подпись.

Распакуйте архив во временную директорию и перейдите в неё:

```
tar -zxf linux-amd64_deb.tgz -C /var/tmp/
cd /var/tmp/linux-amd64_deb
```

Установите в графическом режиме, запустив из директории распаковки архива:

```
sudo chmod a+x ./install_gui.sh
sudo ./install_gui.sh
```

В окне настроек кнопкой «Пробел» установите все «флажки».

Нужные пакеты OpenSSL и PKCS11 будут установлены.

Примечания

1 КриптоПро должна быть установлена как на web-сервере, так и на сервере форм.

2 Корневые и промежуточные сертификаты ЭП должны быть установлены на сервере форм.

5.10 Установка openssl-gost-engine

В состав дистрибутивов Astra Linux входит пакет библиотек для выполнения защитного преобразования по алгоритмам ГОСТ

```
libgost-astra
```

Данный пакет обеспечивает включение в состав методов защитного преобразования, поддерживаемых пакетами openssl и openvpn, следующих алгоритмов:

- ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 – алгоритмы цифровой подписи. Также поддерживается обмен ключами, основанный на открытых ключах (детали см. в RFC 4357). Алгоритмы используют:
  - закрытые ключи 256 бит для ГОСТ 2001, и 256/512 бит для ГОСТ 2012;
  - открытые ключи 512 бит для ГОСТ 2001 и 512/1024 бит для ГОСТ 2012.
- ГОСТ Р 34.11-94 Алгоритм хеширования. Хэш 256 бит;
- ГОСТ Р 34.11-2012 Алгоритм хеширования. Хэш 256 и 512 бит;
- ГОСТ 28147-89 – Симметричное защитное преобразование с ключом 256 бит. Реализованы режимы CBC, CFB и CNT, поддерживается алгоритм «key meshing» (RFC 4357);
- ГОСТ 28147-89 в режиме выработки имитовставки. Базируется на алгоритме симметричного защитного преобразования. Имеет симметричный ключ 256 бит и разрядность вставки от 8 до 64 (по умолчанию 32) бит;
- ГОСТ Р 34.13–2015 – Симметричное защитное преобразование «Кузнечик» («Grasshopper»).

Для установки пакета можно использовать графический менеджер пакетов synaptic или выполнить установку из командной строки командой:

```
apt -y install libgost-astra
```

Проверить список доступных алгоритмов можно командой:

```
openssl engine gost-astra –c
```

При установленном и включенном движке libgost-astra ответ команды будет выглядеть примерно так:

```
# openssl engine gost-astra -c
(gost-astra) Astra implementation of GOST engine
```

[gost89, gost89-cnt, gost89-cnt-12, gost89-cbc, grasshopper-ecb, grasshopper-cbc, grasshopper-cfb, grasshopper-ofb, grasshopper-ctr, md_gost94, gost-mac, md_gost12_256, md_gost12_512, gost-mac-12, gost2001, gost-mac, gost2012_256, gost2012_512, gost-mac-12]

5.11 Установка LibreOffice

Для того, чтобы была возможность выгружать печатные формы в форматах ods и odt необходимо установить на сервере последнюю версию LibreOffice.

Примечание – Формат выгрузки задается в Дизайнере отчетных форм в разделе «Печатные формы» в поле «Формат выгрузки» напротив соответствующей печатной формы. Для выгрузки в формате ods и odt необходимо соответственно в этом поле выбрать значение «ods» или «odt».

Для Astra 1.7:

Установка из пакетов:

Wget https://download.documentfoundation.org/libreoffice/stable/7.6.0/deb/x86_64/LibreOffice_7.6.0_Linux_x86-64_deb.tar.gz

tar zxvf LibreOffice_7.6.0_Linux_x86-64_deb.tar.gz

cd LibreOffice_7.6.0.3_Linux_x86-64_deb/

cd DEBS/

sudo dpkg -i *.deb

libreoffice7.6 --version

Создаем символьную ссылку:

ln -s /usr/local/bin/libreoffice7.6 /usr/local/bin/libreoffice

libreoffice --version

Протестировано на версии LibreOffice 7.6.0.3

6 Настройка ПП МЗ версии 5.3.x на RED OS

Предполагается, что на сервере уже установлено следующее системное ПО:

- русская локализация;

Проверка локализации:

```
svody@dev-svody-web:~$ locale
LANG=ru_RU.UTF-8
LANGUAGE=
LC_CTYPE="ru_RU.UTF-8"
LC_NUMERIC="ru_RU.UTF-8"
LC_TIME="ru_RU.UTF-8"
LC_COLLATE="ru_RU.UTF-8"
LC_MONETARY="ru_RU.UTF-8"
LC_MESSAGES="ru_RU.UTF-8"
LC_PAPER="ru_RU.UTF-8"
LC_NAME="ru_RU.UTF-8"
LC_ADDRESS="ru_RU.UTF-8"
LC_TELEPHONE="ru_RU.UTF-8"
LC_MEASUREMENT="ru_RU.UTF-8"
LC_IDENTIFICATION="ru_RU.UTF-8"
LC_ALL=
```

Для установки русской локализации используйте команду:

```
localectl set-locale LANG=ru_RU.UTF-8
```

Далее перезаходим в ПП МЗ и проверяем через команду `locale`

- SSH-сервер с авторизацией по логину/паролю;
- OpenSSL версии 1.1.0.

Если в процессе установки ОС был включен компонент selinix, необходимо его отключить.

Проверить статус selinux можно командой:

```
Sestatus
```

Отключить selinux можно, отредактировав конфигурационный файл:

```
vi /etc/selinux/config
```

Выставив параметр:

```
SELINUX=disabled
```

После этого необходимо перезагрузить машину для применения изменений.

6.1 Установка PostgreSQL на сервере баз данных

Установка и настройка PostgreSQL 11:

Действия выполняются с правами пользователя root.

Установка осуществляется командой:

```
dnf install postgresql11-server
dnf install  postgresql11-contrib
```

Настройка PostgreSQL:

```
postgresql-11-setup initdb
```

Для оптимизации работы сервера базы данных отредактируйте конфигурационный файл:

```
vi /etc/postgresql/11/main/postgresql.conf
```

Значения параметров необходимо определить самостоятельно путем анализа ваших характеристик сервера и изучения официальной документации:

https://postgrespro.ru/docs/postgresql/11

Для упрощения анализа можно использовать готовые генераторы конфигураций. Например, https://pgtune.leopard.in.ua/#/.

Примечание – При разделении сервера БД и сервера web-приложения необходимо открыть доступы в конфигурационном файле:

```
vi /etc/postgresql/11/main/pg_hba.conf
```

Согласно официальной документации Postgres:

https://postgrespro.ru/docs/postgresql/11/auth-pg-hba-conf

Запуск сервера PostgreSQL:

```
systemctl enable postgresql-11.service
systemctl start postgresql-11.service
systemctl status postgresql-11.service
```

6.2 Установка Redis на web-сервере

Установите сервер Redis:

```
sudo dnf install redis
```

Отредактируйте файл `/etc/redis/redis.conf`, чтобы открыть к нему доступ с других серверов:

```
#bind 127.0.0.1 -::1
bind * -::*
```

Запустите службу:

```
sudo systemctl enable redis-server
sudo systemctl start redis-server
```

6.3 Установка Dotnet на web-сервере

Установите Dotnet:

```
sudo dnf install dotnet-sdk-6.0
```

Проверить установленные версии Dotnet можно с помощью команд:

```
dotnet --list-sdks
dotnet --list-runtimes
```

Пример вывода, установленного на машине Dotnet:

```
root@svody:/home/astra# dotnet --list-sdks
6.0.302 [/usr/share/dotnet/sdk]
root@svody:/home/astra# dotnet --list-runtimes
Microsoft.AspNetCore.App 6.0.7
[/usr/share/dotnet/shared/Microsoft.AspNetCore.App]
Microsoft.NETCore.App 6.0.7
[/usr/share/dotnet/shared/Microsoft.NETCore.App]
```

Также для эксплуатации в условиях высокой нагрузки рекомендуется добавить настройки в конфигурационный файл ядра. Для этого отредактируйте файл:

```
vi /etc/sysctl.conf
```

И добавьте в него следующие параметры:

```
net.core.somaxconn=20000
net.core.netdev_max_backlog=65535
fs.file-max=1000000
fs.inotify.max_user_instances=1024
fs.inotify.max_user_watches=1048576
fs.inotify.max_queued_events=163840
```

После чего перечитайте файл конфигурации командой:

```
sysctl –p
```

Либо перезагрузите web-сервер.

6.4 Установка Nginx на web-сервере

Установите Nginx:

```
dnf install nginx
```

Проведите настройки http и https сервера согласно официальной документации справочного центра по Nginx:

https://docs.nginx.com/nginx/admin-guide/

Примечание – Для https сервера требуется SSL-сертификат, выданный официальным удостоверяющим центром. Не подходят самоподписанные и самозаверенные сертификаты.

Создайте конфигурационный файл:

```
vi /etc/nginx/conf.d/svody.conf
```

со следующим содержанием:

```
location /svody {
client_max_body_size 500M;
proxy_pass http://127.0.0.1:5001/svody;
proxy_http_version 1.1;
proxy_set_header Upgrade $http_Upgrade;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header X-Forwarded-Proto $realscheme;
proxy_set_header Connection keep-alive;
proxy_set_header Connection "upgrade";
proxy_send_timeout 600s;
proxy_read_timeout 600s;
proxy_connect_timeout 600s;
proxy_buffer_size 64k;
proxy_buffers 4 64k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 1024k;
proxy_headers_hash_max_size 512;
proxy_headers_hash_bucket_size 128;
}
```

В зависимости от количества активных пользователей дополнительно настройте Nginx:

а) в файле nginx.conf (/etc/nginx) в секцию http добавьте параметр, увеличивающий максимально допустимый объем заголовков запросов large_client_header_buffers 4 16k;

б) при подключении на схеме авторизации через Keycloak обязательно добавьте следующие директивы: large_client_header_buffers 4 16k и proxy_set_header Connection "upgrade";

в) в файле nginx.conf (/etc/nginx) отредактируйте параметр worker_processes auto;

г) в файле nginx.conf (/etc/nginx) добавьте параметр worker_connections 41 (количество статичных ресурсов при загрузке рабочего стола ПП МЗ) *

суммарное число пользователей всех приложений ПП М3, доступ к которым осуществляется через Nginx;

д) в файле nginx.conf (/etc/nginx) добавьте параметр worker_rlimit_nofile worker_connections * 2 согласно рекомендациям из документации к Nginx;

е) в файле nginx.conf (/etc/nginx) в секцию http добавьте параметр:

```
map $http_x_forwarded_proto $realscheme {
default $scheme;
https https;
http http;
}
```

Сохраните настройки и перезапустите службу:

```
systemctl reload nginx
systemctl restart nginx
```

6.5 Установка приложения на web-сервере

Создайте директорию:

```
mkdir /opt/svody
```

Скопируйте файлы web-приложения из архива дистрибутива в созданную директорию.

Создайте директорию для файлов API:

```
 mkdir /opt/svody/AddInLib
```

Скопируйте файлы API из архива дистрибутива AddInLib.zip в созданную директорию.

Раздайте права для запуска:

```
chmod +x /opt/svody/updater/BARS.Svody.DbUpdater
chmod +x /opt/svody/BARS.Svody.Web.Host
```

Настройте подключение к БД согласно п. 10.2.

Создайте БД согласно п. 8.1.

Например:

```
/opt/svody/updater/BARS.Svody.DbUpdater --createSchema -
sysUserName postgres -sysUserPassword postgres -sysDataBase postgres -
connSettingsPath /opt/svody/Приложение.барс
```

Установите лицензию согласно п. 8.3.

Создайте все табличные пространства согласно п. 8.2.

Например:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations /opt/svody/ -
connSettingsPath /opt/svody/Приложение.барс -simpleProgress true -mode
platform -updateArchiveDatabases false
```

Создайте сервис приложения:

```
vi /etc/systemd/system/svody.service
[Unit]
Description = Svody app: svody
[Service]
WorkingDirectory = /opt/svody
ExecStart = /opt/svody/BARS.Svody.Web.Host
Restart = always
RestartSec = 10
SyslogIdentifier = svody
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5001
Environment = ASPNETCORE_BASEPATH=/svody
Environment = TMPDIR=/var/tmp
User = root
[Install]
WantedBy = multi-user.target
```

Отредактируйте файл настроек Redis, заполнив соответствующие параметры своими:

```
vi /opt/svody/ redis.config
<configuration>
<redis>
    <host> ip-адрес_сервера_redis</host>
    <port>6379</port>
    <user>default</user>
    <password>"redispw"</password>
</redis>
</configuration>
```

Примечание – Внутри пароля недопустимы следующие символы ", &, ', <, >, #,$.

Подробнее о настройке файла описано в п. 10.4.

Отредактируйте файл настроек сервера форм, заполнив соответствующие параметры своими:

```
vi /opt/svody/forms.service.json
{
  "FormEnginesConfig" : {
    "Urls":["http:// ip-адрес_сервера_форм:5003"],
    "HealthCheckIntervalInSeconds":60
  }
}
```

Если требуется настроить несколько сервисов форм, то файл forms.service.json будет выглядеть следующим образом:

```
vi /opt/svody/forms.service.json
{
  "FormEnginesConfig" : {
    "Urls":["http:// ip-адрес_сервера_форм 1:5003", "http:// ip-адрес_сервера_форм 2:5003", "http:// ip-адрес_сервера_форм 3:5003"],
    "HealthCheckIntervalInSeconds":60
  }
}
```

Подробнее о настройке файла описано в п. 10.5.

Запустите приложение:

```
systemctl daemon-reload
systemctl start svody
systemctl enable svody
```

6.6 Установка приложения на сервере форм

Примечание – В данной инструкции описана настройка сервера форм на отдельной от web-сервера машине. Однако, если количество пользователей и нагрузка небольшие, можно совместить сервер форм и web-сервер на одной машине.

Создайте директорию:

```
mkdir /opt/forms
```

Скопируйте файлы сервиса форм из архива дистрибутива в созданную директорию.

Создайте директорию для файлов API:

```
 mkdir /opt/forms/AddInLib
```

Скопируйте файлы API из архива дистрибутива AddInLib.zip в созданную директорию.

Раздайте права для запуска:

```
chmod +x /opt/forms/Svody.Forms.Host
```

Создайте сервис приложения:

```
vi /etc/systemd/system/forms.service

[Unit]
Description = Svody forms service: svody
[Service]
User = root
WorkingDirectory = /opt/forms
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5003
Environment = ASPNETCORE_BASEPATH=/forms
Environment = TMPDIR=/var/tmp
```

```
Environment = SSL_CERT_DIR=/etc/ssl/certs/
Environment = LD_LIBRARY_PATH=/opt/cprocsp/cp-openssl-
1.1.0/lib/amd64/
ExecStart = /opt/forms/Svody.Forms.Host
SyslogIdentifier = svody-forms
Restart = always
RestartSec = 10
[Install]
WantedBy = multi-user.target
```

Скопируйте созданный и настроенный в предыдущем пункте файл `Приложение.барс` из каталога `/opt/svody` на web-сервере. Поместите данный файл в корень каталога `/opt/forms`.

Отредактируйте файл настроек AW, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/aw.json
{
  "aw": {
    "db": "default",
    "host": "ip-адрес_сервера_aw",
    "port": 9017,
    "user": "default",
    "password": "enter4z",
    "baseUrl": "URL-сервера_AW",
    "adminLogin": "tech_admin",
    "adminPassword": "123456"
  }
}
```

Подробнее о настройке файла описано в п. 10.10.

Отредактируйте файл настроек подключения к серверу БД, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/ postgres.json

{
  "postgres": {
    "dbName":"svody",
    "schemeName":"svody_forms_service",
    "host":"ip-адрес_сервера_БД",
    "port":5432,
    "login":"svody",
    "password":"123",
    "minPoolSize": 2,
    "maxPoolSize": 50,
    "connectionOpenTimeout": 60,
    "executeCommandTimeout": 60,
    "connectionIdleSeconds": 300,
    "connectionPruningSeconds": 50,
```

```
    "readBufferSize": 524288,
    "writeBufferSize": 524288
  }
}
```

Подробнее о настройке файла описано в п. 10.7.

Отредактируйте файл настроек Redis, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/ redis.json

{
  "redis" : {
    "host": "ip-адрес_сервера_redis",
    "port": 6379,
    "user": "default",
    "password": "redispw"
  }
}
```

Подробнее о настройке файла описано в п. 10.6.

Примечание – Конфигурационные файлы «metrics.json» и «formsBackups.json», находящиеся в подкаталоге Config, не требуют редактирования при стандартной установке. Однако подробности об их настройке при необходимости можно найти в п. 10.8 и 10.9.

Запустите приложение:

```
systemctl daemon-reload
systemctl start forms
```

6.7 Обновление приложения на web-сервере

Процедура обновления web-приложения аналогична процедуре развертывания web-приложения.

Перед обновлением web-приложения создайте резервную копию:

- папок «AddInLib», «wwwroot\apiJs», файлов новостей «wwwroot\actualNews.html», а после обновления скопируйте их в каталог с обновленным web-клиентом;
- всех файлов конфигурации («web.config», «svody.config», «redis.config», «forms.service.json»), а после обновления внесите индивидуальные настройки приложения согласно этим файлам в новые файлы конфигурации;
- файла конфигурации «Приложение.барс».

Выполните остановку пула приложений:

```
systemctl stop svody
```

Для обновления web-приложения повторно распакуйте новый архив «BARS.Svody.Linux-5.x.x.zip» в каталог приложения. При этом файлы «web.config», «svody.config», «redis.config», «forms.service.json» замените, а затем отредактируйте согласно настройкам вашего приложения. Файл «Приложение.барс» оставьте без изменений, так как он содержит настройки подключения к БД.

Для обновления API создайте папку «AddInLib» в каталоге приложения. Например:

```
mkdir /opt/svody/AddInLib
```

Распакуйте в нее файлы API из одноименного архива.

Выполните миграции согласно п. 8.2 данной инструкции.

Пример команды:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations /opt/svody/ -
connSettingsPath /opt/svody/Приложение.барс -simpleProgress true -mode
platform -updateArchiveDatabases false
```

Выполните запуск пула приложений:

```
systemctl start svody
```

6.8 Обновление приложения на сервере форм

Процедура обновления приложения на сервере форм аналогична процедуре развертывания.

Перед обновлением сервиса форм создайте резервную копию:

- папок «AddInLib», файла «Приложение.барс». После обновления скопируйте файл «Приложение.барс» в каталог с обновленным приложением;
- всех файлов конфигурации, находящихся в папке «Config», а после обновления внесите индивидуальные настройки приложения согласно этим файлам в новые файлы конфигурации.

Выполните остановку пула приложений:

```
systemctl stop forms
```

Для обновления сервиса форм повторно распакуйте новый архив «Bars.Svody.Linux.Forms.Service-5.x.x.zip» в каталог приложения. При этом файлы, находящиеся в папке «Config», замените, а затем отредактируйте согласно настройкам вашего приложения. Файл «Приложение.барс» оставьте без изменений, так как он содержит настройки подключения к БД.

Для обновления API создайте папку «AddInLib» в каталоге приложения. Например:

```
mkdir /opt/forms/AddInLib
```

Распакуйте в нее файлы API из одноименного архива.

Выполните запуск пула приложений:

```
systemctl start forms
```

6.9 Установка КриптоПРО на web-сервере

Скачайте архив (rpm-пакет) с сайта КриптоПро по ссылке:

https://www.cryptopro.ru/sites/default/files/private/csp/40/9963/linux-amd64.tgz

Распакуйте архив в папку (в примере /home/test/).

```
cd /home/test
tar -xvf linux-amd64.tgz
```

Перейдите в папку с КриптоПро:

```
cd /home/test/linux-amd64
```

Установите права на запуск:

```
chmod +x install_gui.sh
```

Выполните следующую команду (чтобы далее выполнять команды от пользователя root):

```
su root
```

Установите КриптоПро, выполнив команду:

```
./install_gui.sh
```

В открывшемся окне установки КриптоПро нажмите на кнопку «Next» для продолжения установки.

В следующем окне выберите пакеты для установки, указанные на скриншоте (Рисунок 7). «Флажки» устанавливаются кнопкой «Пробел».

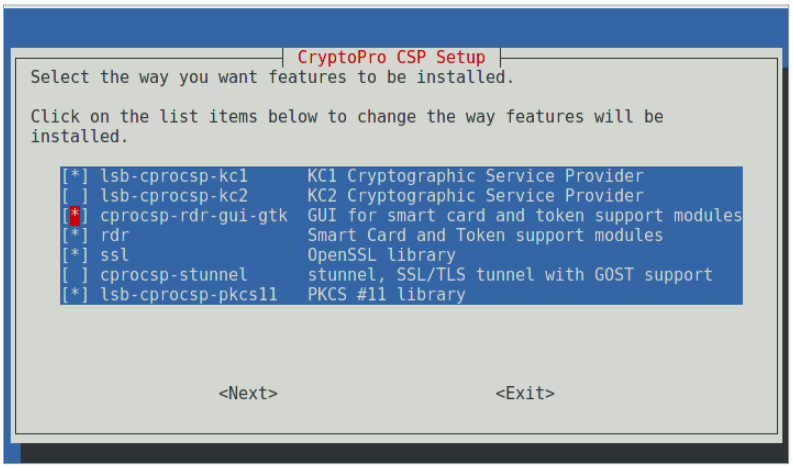


Рисунок 7 – Выбор пакетов для установки КриптоПРО

Нажмите кнопку «Next» для продолжения установки.

Далее нажмите кнопку «Install» для установки пакетов.

Затем установите дополнительные пакеты и драйверы.

Установка драйверов для токенов Rutoken S:

– для РЕД ОС 7.1 или 7.2:

```
yum install -y ifd-rutokens
```

– для РЕД ОС 7.3 и старше:

```
dnf install -y ifd-rutokens
```

Установка драйверов для токенов Jacarta:

Перейдите в папку:

```
cd /home/test/linux-amd64
```

– для РЕД ОС 7.1 или 7.2 выполните команду установки:

```
yum localinstall cprocsp-rdr-jacarta*.rpm
```

– для РЕД ОС 7.3 и старше перейдите в папку:

```
dnf install cprocsp-rdr-jacarta*.rpm
```

Примечания

1 КриптоПро должна быть установлена как на web-сервере, так и на сервере форм.

2 Корневые и промежуточные сертификаты ЭП должны быть установлены на сервере форм.

6.10 Установка openssl-gost-engine

В состав дистрибутива входит пакет библиотек, поддерживающих методы защитного преобразования по алгоритмам ГОСТ, openssl-gost-engine.

Пакет openssl-gost-engine включает в себя реализацию следующих алгоритмов ГОСТ:

- ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 – алгоритмы электронной цифровой подписи$
- ГОСТ Р 34.11-94 – алгоритм хэширования. 256-битное значение хэша;
- ГОСТ Р 34.11-2012 – алгоритм хэширования. 256- и 512-битные значения хэша;
- ГОСТ 28147-89 – симметричное шифрование с 256-битным ключом. Доступны режимы CBC, CFB и CNT. Для усложнения статистического анализа поддерживается «key meshing» (подробнее см. RFC 4357);
- ГОСТ 28147-89 в режиме выработки имитовставки (MAC). Основан на алгоритме хэширования с использованием алгоритмов симметричного шифрования. Он имеет 256-битный симметричный ключ и разрядность от 8 до 64 (по умолчанию 32) бит;
- ГОСТ Р 34.13–2015 – симметричное шифрование «Кузнечик» («Grasshopper»).

Для установки пакета openssl-gost-engine выполните команду:

```
sudo dnf install openssl-gost-engine
```

После установки openssl поддержку алгоритмов ГОСТ можно включить следующей командой:

```
openssl-switch-config <gost | default>
```

При указании аргумента gost поддержка алгоритмов ГОСТ включается, при указании аргумента default возвращаются настройки по умолчанию.

После проведения настройки проверьте, видит ли OpenSSL алгоритмы ГОСТ, командой:

```
openssl ciphers | tr ":" "\n" | grep GOST
GOST2012-GOST8912-GOST8912 GOST2001-GOST89-GOST89
```

6.11 Установка LibreOffice

Для того, чтобы была возможность выгружать печатные формы в форматах ods и odt необходимо установить на сервере последнюю версию LibreOffice

Примечание – Формат выгрузки задается в Дизайнере отчетных форм в разделе «Печатные формы» в поле «Формат выгрузки» напротив соответствующей печатной формы. Для выгрузки в формате ods и odt необходимо соответственно в этом поле выбрать значение «ods» или «odt».

Для RedOs:

Установка из стандартных репозитариев:

- `yum install libreoffice-core`
- `yum install libreoffice-writer`
- `yum install libreoffice-calc`

libreoffice --version

7 Настройка ПП МЗ версии 5.3.x на Альт 8 СП

Примечание – На данной ОС не поддерживается часть функционала web-приложения, а именно: перезапуск и обновление через web-интерфейс.

Также предполагается, что на сервере уже установлено следующее системное ПО:

- русская локализация;

Проверка локализации:

```
svody@dev-svody-web:~$ locale
LANG=ru_RU.UTF-8
LANGUAGE=
LC_CTYPE="ru_RU.UTF-8"
LC_NUMERIC="ru_RU.UTF-8"
LC_TIME="ru_RU.UTF-8"
LC_COLLATE="ru_RU.UTF-8"
LC_MONETARY="ru_RU.UTF-8"
LC_MESSAGES="ru_RU.UTF-8"
LC_PAPER="ru_RU.UTF-8"
LC_NAME="ru_RU.UTF-8"
LC_ADDRESS="ru_RU.UTF-8"
LC_TELEPHONE="ru_RU.UTF-8"
LC_MEASUREMENT="ru_RU.UTF-8"
LC_IDENTIFICATION="ru_RU.UTF-8"
LC_ALL=
```

Для установки русской локализации используйте команду:

```
localectl set-locale LANG=ru_RU.UTF-8
```

Далее перезаходим в ПП МЗ и проверяем через команду `locale`

- SSH-сервер с авторизацией по логину/паролю;
- OpenSSL версии 1.1.0.

7.1 Установка Postgres на сервере баз данных

Выполните подготовительные команды:

```
wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add -
echo "deb http://apt.postgresql.org/pub/repos/apt/ `lsb_release -cs`-pgdg main" |sudo tee /etc/apt/sources.list.d/pgdg.list
echo "deb http://apt.postgresql.org/pub/repos/apt/ stretch-pgdg main" | sudo tee /etc/apt/sources.list.d/postgresql.list
sudo apt-get update
sudo apt install -y postgresql-11 postgresql-contrib-11
```

Для оптимизации работы сервера базы данных отредактируйте конфигурационный файл:

```
vi /etc/postgresql/11/main/postgresql.conf
```

Значения параметров необходимо определить самостоятельно путем анализа ваших характеристик сервера и изучения официальной документации:

https://postgrespro.ru/docs/postgresql/11

Для упрощения анализа можно использовать готовые генераторы конфигураций. Например, https://pgtune.leopard.in.ua/#/.

Примечание – При разделении сервера БД и сервера web-приложения необходимо открыть доступы в конфигурационном файле:

```
vi /etc/postgresql/11/main/pg_hba.conf
```

Согласно официальной документации Postgres:

https://postgrespro.ru/docs/postgresql/11/auth-pg-hba-conf

Перезапустите службу:

```
sudo systemctl reload postgresql
sudo systemctl restart postgresql
```

7.2 Установка Redis на web-сервере

Установите сервер Redis:

```
sudo apt-get -y install redis
```

Отредактируйте файл `/etc/redis/redis.conf`, чтобы открыть к нему доступ с других серверов:

```
#bind 127.0.0.1 -::1
bind * -::*
```

Запустите службу:

```
sudo systemctl enable redis-server
sudo systemctl start redis-server
```

7.3 Установка Dotnet на web-сервере

Скачайте архив с пакетами SDK x64 по ссылке ниже:

https://dotnet.microsoft.com/download/dotnet/6.0.

При установке пакета SDK для .NET не нужно устанавливать соответствующую среду выполнения, т.к. она будет установлена вместе с SDK.

Затем используйте команду export, чтобы задать для переменной DOTNET_ROOT расположение скачанного архива:

```
DOTNET_FILE=имя_скачанного_файла.tar.gz
export DOTNET_ROOT=$(pwd)/.dotnet
```

Кроме того, после скачивания двоичного файла .NET можно выполнить следующие команды из каталога, в котором сохранен файл, для извлечения среды выполнения. После этого команды .NET CLI также станут доступны в терминале, и будут заданы нужные переменные среды:

```
mkdir -p "$DOTNET_ROOT" && tar zxf "$DOTNET_FILE" -C
"$DOTNET_ROOT"
export PATH=$PATH:$DOTNET_ROOT:$DOTNET_ROOT/tools
```

Такой подход позволяет устанавливать разные версии в отдельные расположения и выбирать, какие из них следует использовать для каждого приложения.

Если был использован предыдущий скрипт установки, набор переменных применяется только к текущему сеансу терминала. Добавьте их в профиль оболочки.

Оболочка Bash:

```
~/.bash_profile, ~/.bashrc
```

Задайте следующие две переменные среды в профиле оболочки:

– DOTNET_ROOT;

Эта переменная устанавливается в папку .NET, например $HOME/.dotnet:

```
export DOTNET_ROOT=$HOME/.dotnet
```

– PATH.

Эта переменная должна содержать папку DOTNET_ROOT и папку dotnet/tools пользователя:

```
export PATH=$PATH:$HOME/.dotnet:$HOME/.dotnet/tools
```

Проверить установленные версии Dotnet можно с помощью команд:

```
dotnet --list-sdks
dotnet --list-runtimes
```

Пример вывода, установленного на машине Dotnet:

```
root@svody:/home/svody# dotnet --list-sdks
6.0.302 [/usr/share/dotnet/sdk]
root@svody:/home/svody# dotnet --list-runtimes
Microsoft.AspNetCore.App 6.0.7
[/usr/share/dotnet/shared/Microsoft.AspNetCore.App]
Microsoft.NETCore.App 6.0.7
[/usr/share/dotnet/shared/Microsoft.NETCore.App]
```

Также для эксплуатации в условиях высокой нагрузки рекомендуется добавить настройки в конфигурационный файл ядра. Для этого отредактируйте файл:

```
vi /etc/sysctl.conf
```

И добавьте в него следующие параметры:

```
net.core.somaxconn=20000
net.core.netdev_max_backlog=65535
fs.file-max=1000000
fs.inotify.max_user_instances=1024
fs.inotify.max_user_watches=1048576
fs.inotify.max_queued_events=163840
```

После чего перечитайте файл конфигурации командой:

```
sysctl –p
```

Либо перезагрузите web-сервер.

7.4 Установка Nginx на web-сервере

Установите Nginx:

```
sudo apt install nginx
```

Провести настройки http и https сервера согласно официальной документации справочного центра по Nginx

https://docs.nginx.com/nginx/admin-guide/

Примечание – Для https сервера требуется SSL-сертификат, выданный официальным удостоверяющим центром. Не подходят самоподписанные и самозаверенные сертификаты.

Создайте конфигурационный файл:

```
vi /etc/nginx/conf.d/svody.conf
```

Со следующим содержанием:

```
location /svody {
client_max_body_size 500M;
proxy_pass http://127.0.0.1:5001/svody;
proxy_http_version 1.1;
proxy_set_header Upgrade $http_Upgrade;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header X-Forwarded-Proto $realscheme;
proxy_set_header Connection keep-alive;
proxy_set_header Connection "upgrade";
proxy_send_timeout 600s;
proxy_read_timeout 600s;
proxy_connect_timeout 600s;
```

```
proxy_buffer_size 64k;
proxy_buffers 4 64k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 1024k;
proxy_headers_hash_max_size 512;
proxy_headers_hash_bucket_size 128;
}
```

В зависимости от количества активных пользователей дополнительно настройте Nginx:

- в файле nginx.conf (/etc/nginx) в секцию http добавьте параметр, увеличивающий максимально допустимый объем заголовков запросов large_client_header_buffers 4 16k;2
- при подключении на схеме авторизации через Keycloak обязательно добавьте следующие директивы: large_client_header_buffers 4 16k и proxy_set_header Connection "upgrade";
- в файле nginx.conf (/etc/nginx) отредактируйте параметр worker_processes auto;
- в файле nginx.conf (/etc/nginx) добавьте параметр worker_connections 41 (количество статичных ресурсов при загрузке рабочего стола ПП МЗ) * суммарное число пользователей всех приложений ПП МЗ, доступ к которым осуществляется через Nginx;
- в файле nginx.conf (/etc/nginx) добавьте параметр worker_rlimit_nofile worker_connections * 2 согласно рекомендациям из документации к Nginx;
- в файле nginx.conf (/etc/nginx) в секцию http добавьте параметр:

```
map $http_x_forwarded_proto $realscheme {
default $scheme;
https https;
http http;
}
```

Сохраните настройки и перезапустите службу:

```
systemctl reload nginx
systemctl restart nginx
```

7.5 Установка приложения на web-сервере

Создайте директорию:

```
mkdir /opt/svody
```

Скопируйте файлы web-приложения из архива дистрибутива в созданную директорию.

Создайте директорию для файлов API:

```
mkdir /opt/svody/AddInLib
```

Скопируйте файлы API из архива дистрибутива AddInLib.zip в созданную директорию.

Раздайте права для запуска:

```
chmod +x /opt/svody/updater/BARS.Svody.DbUpdater
chmod +x /opt/svody/BARS.Svody.Web.Host
```

Настройте подключение к БД согласно п. 10.2.

Создайте БД согласно п. 8.1.

Например:

```
/opt/svody/updater/BARS.Svody.DbUpdater --createSchema -
sysUserName postgres -sysUserPassword postgres -sysDataBase postgres -
connSettingsPath /opt/svody/Приложение.барс
```

Установите лицензию согласно п. 8.3.

Создайте все табличные пространства согласно п. 8.2.

Например:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations /opt/svody/ -
connSettingsPath /opt/svody/Приложение.барс -simpleProgress true -mode
platform -updateArchiveDatabases false
```

Создайте сервис приложения:

```
vi /etc/systemd/system/svody.service
[Unit]
Description = Svody app: svody
[Service]
WorkingDirectory = /opt/svody
ExecStart = /opt/svody/BARS.Svody.Web.Host
Restart = always
RestartSec = 10
SyslogIdentifier = svody
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5001
Environment = ASPNETCORE_BASEPATH=/svody
Environment = TMPDIR=/var/tmp
User = root
[Install]
WantedBy = multi-user.target
```

Отредактируйте файл настроек Redis, заполнив соответствующие параметры своими:

```
vi /opt/svody/ redis.config
<configuration>
<redis>
```

```
    <host>ip-адрес_сервера_redis</host>
    <port>6379</port>
    <user>default</user>
    <password>"redispw"</password>
</redis>
</configuration>
```

Примечание – Внутри пароля недопустимы следующие символы ", &, ', <, >, #,$.

Подробнее о настройке файла описано в п. 10.4.

Отредактируйте файл настроек сервера форм, заполнив соответствующие параметры своими:

```
vi /opt/svody/forms.service.json
{
  "FormEnginesConfig" : {
    "Urls":["http://ip-адрес_сервера_форм:5003"],
    "HealthCheckIntervalInSeconds":60
  }
}
```

Если требуется настроить несколько сервисов форм, то файл forms.service.json будет выглядеть следующим образом:

```
vi /opt/svody/forms.service.json
{
  "FormEnginesConfig" : {
    "Urls":["http:// ip-адрес_сервера_форм 1:5003", "http:// ip-адрес_сервера_форм 2:5003", "http:// ip-адрес_сервера_форм 3:5003"],
    "HealthCheckIntervalInSeconds":60
  }
}
```

Подробнее о настройке файла описано в п. 10.5.

Запустите приложение:

```
systemctl daemon-reload
systemctl start svody
systemctl enable svodyy
```

7.6 Установка приложения на сервере форм

Примечание – В данной инструкции описана настройка сервера форм на отдельной от web-сервера машине. Однако, если количество пользователей мало и нагрузка небольшая, можно совместить сервер форм и web-сервер на одной машине.

Создайте директорию:

```
mkdir /opt/forms
```

Скопируйте файлы сервиса форм из архива дистрибутива в созданную директорию.

Создайте директорию для файлов API:

```
mkdir /opt/forms/AddInLib
```

Скопируйте файлы API из архива дистрибутива AddInLib.zip в созданную директорию.

Раздайте права для запуска:

```
chmod +x /opt/forms/Svody.Forms.Host
```

Создайте сервис приложения:

```
vi /etc/systemd/system/forms.service

[Unit]
Description = Svody forms service: svody
[Service]
User = root
WorkingDirectory = /opt/forms
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5003
Environment = ASPNETCORE_BASEPATH=/forms
Environment = SSL_CERT_DIR=/etc/ssl/certs/
Environment = LD_LIBRARY_PATH=/opt/cprocsp/cp-openssl-
1.1.0/lib/amd64/
ExecStart = /opt/forms/Svody.Forms.Host
SyslogIdentifier = svody-forms
Restart = always
RestartSec = 10
[Install]
WantedBy = multi-user.target
```

Скопируйте созданный и настроенный в предыдущем пункте файл `Приложение.барс` из каталога `/opt/svody` на web-сервере. Поместите данный файл в корень каталога `/opt/forms`.

Отредактируйте файл настроек AW, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/aw.json
{
  "aw": {
    "db": "default",
    "host": "ip-адрес_сервера_aw",
    "port": 9017,
    "user": "default",
    "password": "enter4z",
    "baseUrl": "URL-сервера_AW",
    "adminLogin": "tech_admin",
    "adminPassword": "123456"
  }
}
```

Подробнее о настройке файла описано в п. 10.10.

Отредактируйте файл настроек подключения к серверу БД, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/ postgres.json

{
  "postgres": {
    "dbName":"svody",
    "schemeName":"svody_forms_service",
    "host":"ip-адрес_сервера_БД",
    "port":5432,
    "login":"svody",
    "password":"123",
    "minPoolSize": 2,
    "maxPoolSize": 50,
    "connectionOpenTimeout": 60,
    "executeCommandTimeout": 60,
    "connectionIdleSeconds": 300,
    "connectionPruningSeconds": 50,
    "readBufferSize": 524288,
    "writeBufferSize": 524288
  }
}
```

Подробнее о настройке файла описано в п. 10.7.

Отредактируйте файл настроек Redis, заполнив соответствующие параметры своими:

```
vi /opt/forms/Config/ redis.json

{
  "redis" : {
    "host": "ip-адрес_сервера_redis",
    "port": 6379,
    "user": "default",
    "password": "redispw"
  }
}
```

Подробнее о настройке файла описано в п. 10.6.

Примечание – Конфигурационные файлы «metrics.json» и «formsBackups.json», находящиеся в подкаталоге Config, не требуют редактирования при стандартной установке. Однако подробности об их настройке при необходимости можно найти в п. 10.8 и 10.9.

Установите шрифты для формирования печатных форм:

```
sudo apt-get install -y fonts-ttf-ms
sudo apt-get install -y fonts-ttf-dejavu
```

Проверить, что шрифт установился:

```
fc-list | grep tahoma
```

Запустите приложение:

```
systemctl daemon-reload
systemctl start forms
```

7.7 Обновление приложения на web-сервере

Процедура обновления web-приложения аналогична процедуре развертывания web-приложения.

Перед обновлением web-приложения создайте резервную копию:

- папок «AddInLib», «wwwroot\apiJs», файлов новостей «wwwroot\actualNews.html», а после обновления скопируйте их в каталог с обновленным Web-клиентом;
- всех файлов конфигурации («web.config», «svody.config», «redis.config», «forms.service.json»), а после обновления внесите индивидуальные настройки приложения согласно этим файлам в новые файлы конфигурации;
- файла конфигурации «Приложение.барс».

Выполните остановку пула приложений:

```
systemctl stop svody
```

Для обновления web-приложения повторно распакуйте новый архив «BARS.Svody.Linux-5.x.x.zip» в каталог приложения. При этом файлы «web.config», «svody.config», «redis.config», «forms.service.json» замените, а затем отредактируйте согласно настройкам вашего приложения. Файл «Приложение.барс» оставьте без изменений, так как он содержит настройки подключения к БД.

Для обновления API создайте папку «AddInLib» в каталоге приложения. Например:

```
mkdir /opt/svody/AddInLib
```

После чего распакуйте в нее файлы API из одноименного архива.

Выполните миграции согласно п. 8.2 данной инструкции.

Пример команды:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations /opt/svody/ -connSettingsPath /opt/svody/Приложение.барс -simpleProgress true -mode platform -updateArchiveDatabases false
```

Выполните запуск пула приложений^

```
systemctl start svody
```

7.8 Обновление приложения на сервере форм

Процедура обновления приложения на сервере форм аналогична процедуре развертывания.

Перед обновлением web-приложения создайте резервную копию:

- папок «AddInLib», файла «Приложение.барс». После обновления скопируйте файл «Приложение.барс» в каталог с обновленным приложением;
- всех файлов конфигурации, находящихся в папке «Config», а после обновления внесите индивидуальные настройки приложения согласно этим файлам в новые файлы конфигурации.

Выполните остановку пула приложений:

```
systemctl stop forms
```

Для обновления сервиса форм повторно распакуйте новый архив «Bars.Svody.Linux.Forms.Service-5.x.x.zip» в каталог приложения. При этом файлы, находящиеся в папке «Config», замените, а затем отредактируйте согласно настройкам вашего приложения. Файл «Приложение.барс» оставьте без изменений, так как он содержит настройки подключения к БД.

Для обновления API создайте папку «AddInLib» в каталоге приложения. Например:

```
mkdir /opt/forms/AddInLib
```

После чего распакуйте в нее файлы API из одноименного архива.

Выполните запуск пула приложений:

```
systemctl start forms
```

7.9 Установка КриптоПРО на web-сервере

Перейдите на сайт ПО «КриптоПРО»: https://cryptopro.ru/user?destination=node%2F148#latest_csp50, выберите дистрибутив КриптоПро CSP 5.0 для UNIX.

Откроется список пакетов (Рисунок 8).

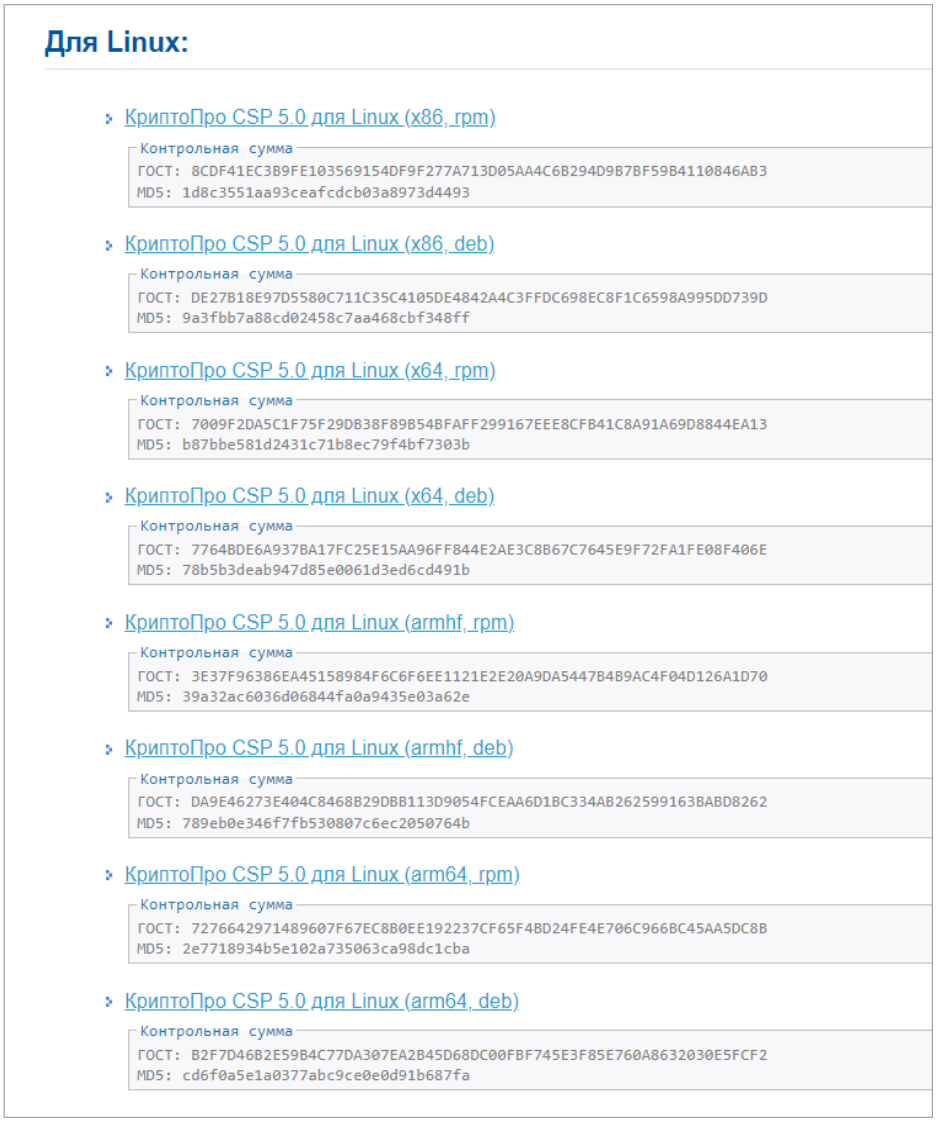


Рисунок 8 – Список пакетов

Выберите пакет КриптоПро CSP 5.0 для Linux (x64, deb) и загрузите его.

Также необходимы пакеты OpenSSL и PKCS11 – без них не будет работать подпись.

Распакуйте архив во временную директорию и перейдите в неё:

```
tar -zxf linux-amd64_deb.tgz -C /var/tmp/
cd /var/tmp/linux-amd64_deb
```

Установите в графическом режиме, запустив из директории распаковки архива:

```
sudo chmod a+x ./install_gui.sh
sudo ./install_gui.sh
```

В окне настроек кнопкой «Пробел» установите все «флажки».

Нужные пакеты OpenSSL и PKCS11 будут установлены.

Примечания

1 КриптоПро должна быть установлена как на web-сервере, так и на сервере форм.

2 Корневые и промежуточные сертификаты ЭП должны быть установлены на сервере форм.

7.10 Установка openssl-gost-engine

В состав дистрибутива входит пакет библиотек, поддерживающих методы защитного преобразования по алгоритмам ГОСТ, openssl-gost-engine.

Пакет openssl-gost-engine включает в себя реализацию следующих алгоритмов ГОСТ:

- ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 – алгоритмы электронной цифровой подписи;
- ГОСТ Р 34.11-94 – алгоритм хэширования. 256-битное значение хэша;
- ГОСТ Р 34.11-2012 – алгоритм хэширования. 256- и 512-битные значения хэша;
- ГОСТ 28147-89 – симметричное шифрование с 256-битным ключом. Доступны режимы CBC, CFB и CNT. Для усложнения статистического анализа поддерживается «key meshing» (подробнее см. RFC 4357);
- ГОСТ 28147-89 в режиме выработки имитовставки (MAC). Основан на алгоритме хэширования с использованием алгоритмов симметричного шифрования. Он имеет 256-битный симметричный ключ и разрядность от 8 до 64 (по умолчанию 32) бит;
- ГОСТ Р 34.13–2015 – симметричное шифрование «Кузнечик» («Grasshopper»).

Для установки пакета openssl-gost-engine выполните команду:

```
sudo apt-get -y install openssl-gost-engine
```

После установки openssl поддержку алгоритмов ГОСТ можно включить следующей командой:

```
sudo control openssl-gost enabled
```

После проведения настройки проверьте, видит ли OpenSSL алгоритмы ГОСТ, командой:

```
openssl ciphers | tr ":" "\n" | grep GOST
GOST2012-GOST8912-GOST8912 GOST2001-GOST89-GOST89
```

7.11 Установка LibreOffice

Для того, чтобы была возможность выгружать печатные формы в форматах ods и odt необходимо установить на сервере последнюю версию LibreOffice

Примечание – Формат выгрузки задается в Дизайнере отчетных форм в разделе «Печатные формы» в поле «Формат выгрузки» напротив соответствующей печатной формы. Для выгрузки в формате ods и odt необходимо соответственно в этом поле выбрать значение «ods» или «odt».

Для Альт 8 СП:

Установка из стандартных репозитариев:

apt-get install LibreOffice-still

libreoffice --version

Протестировано на версии LibreOffice 6.4.7.2 40(Build:2)

8 Инструкция по работе с DbUpdater-ом

С помощью DbUpdater можно выполнять следующие функции:

- создание новой схемы;
- обновление структуры ранее созданных схем на новые версии ПП М3;
- установка лицензии;
- конвертация БД с Oracle на PostgreSQL.

8.1 Создание новой схемы

Перед созданием схемы необходимо определить режим хранения персональных данных пользователей ПП М3. Существует два режима:

- вместе со всеми данными ПП М3;
- в отдельной базе данных.

В зависимости от выбранного режима перечень передаваемых в утилиту параметров меняется.

Для создания новой схемы запустите DBUpdater согласно инструкции ниже. Описание параметров запуска приведено ниже (Таблица 6).

Таблица 6 – Параметры запуска для создания схемы

Название параметра	Описание параметра	Пример использования
--createSchema	Обязательный параметр. Указывает, что консоль запущена в режиме создания схемы	--createSchema
-sysUserName	Логин от super пользователя	-sysUserName postgres
-sysUserPassword	Пароль от super пользователя	-sysUserPassword postgres
-sysDataBase	Главная база	-sysDataBase postgres
-dbDialect	Тип создаваемой СУБД	-dbDialect Npgsql
-dbIp	IP-адрес сервера БД, либо host	-dbIp 127.0.0.0
-dbPort	Порт БД	-dbPort 5432
-dbName	Наименование создаваемой БД	-dbName TestScheme
-dbScheme	Наименование создаваемой схемы	-dbScheme TestScheme
-dbPassword	Пароль пользователя БД	-dbPassword 123
-connSettingsPath	Путь до файла Приложение.барс.	-connSettingsPath "путьДоПапки\Приложение.барс"

Название параметра	Описание параметра	Пример использования
	Если путь содержит пробелы, значение параметра указывается в кавычках.	
--pd	Параметр, указывающий на то, что персональные данные будут храниться в отдельной БД	--pd
-pdUser	Имя пользователя и название БД, в которой будут храниться персональные данные	-pdUser test_pd
-pdPassword	Пароль пользователя-владельца БД с персональными данными	-pdPassword 123
-pdIp	IP-адрес сервера БД (или host) где будет создана БД, в которой будут храниться персональные данные	-pdIp 127.0.0.0
-pdPort	Порт БД, в которой будут храниться персональные данные	-pdPort 5433
-pdSysUserName	Логин от super пользователя в БД, в которой будут храниться персональные данные	-pdSysUserName postgres
-pdSysUserPassword	Пароль от super пользователя в БД, в которой будут храниться персональные данные	-pdSysUserPassword postgres
-pdSysDataBase	Главная база на сервере, где разворачивается база персональных данных. Обязателен при создании схемы на Postgres	-pdSysDataBase postgres

Примечания

1 Для запуска консоли необходимо передать значение параметра -connSettingsPath либо набор значений параметров -dbDialect -dbIp -dbName -dbScheme -dbPassword –dbPort.

2 Параметр -dbName и -dbScheme должны совпадать.

3 Схема и БД создаются всегда только с названиями в нижнем регистре, несмотря на формат их написания в параметрах запроса.

Пример для ОС Windows

– обычный режим создания:

```
BARS.Svody.DbUpdater.exe --createSchema -sysUserName postgres -sysUserPassword парольОтПользователяPostgres -sysDataBase postgres -connSettingsPath "путь\Приложение.барс"
BARS.Svody.DbUpdater.exe --createSchema -sysUserName postgres -sysUserPassword парольОтПользователяPostgres -sysDataBase postgres -dbDialect Npgsql -dbIp IPСервераБД -dbName имяБД -dbScheme имяСхемы -dbPassword парольОтСхемы -dbPort портБД
```

– режим отдельного хранения персональных данных:

```
BARS.Svody.DbUpdater.exe --createSchema -sysUserName postgres -sysUserPassword postgres -connSettingsPath "путь\Приложение.барс" --pd
```

```
-pdUser пользовательПД -pdPassword парольОтСхемыПД -pdIp IPСервераБДПД
-pdPort портБДПД -pdSysUserName postgres -pdSysUserPassword
парольОтПользователяPostgresПД -pdSysDataBase postgres
      BARS.Svody.DbUpdater.exe --createSchema -sysUserName postgres -
sysUserPassword парольОтПользователяPostgres -dbDialect Npgsql -dbIp
IPСервераБД -dbName имяБД -dbScheme имяСхемы -dbPassword парольОтСхемы
-dbPort портБД --pd -pdUser пользовательПД -pdPassword пользовательПД -
pdIp IPСервераБДПД -pdPort портБДПД -pdSysUserName postgres -
pdSysUserPassword парольОтПользователяPostgresПД -pdSysDataBase
postgres
```

Пример для ОС Linux

– обычный режим создания:

```
      /opt/svody/updater/BARS.Svody.DbUpdater --createSchema -
sysUserName postgres -sysUserPassword postgres -sysDataBase postgres -
connSettingsPath "/путь/Приложение.барс"
      /opt/svody/updater/BARS.Svody.DbUpdater --createSchema -
sysUserName postgres -sysUserPassword парольОтПользователяPostgres -
sysDataBase postgres -dbDialect Npgsql -dbIp IPСервераБД  -dbName имяБД
-dbScheme имяСхемы –dbPassword парольОтСхемы -dbPort портБД
```

– режим отдельного хранения персональных данных:

```
      /opt/svody/updater/BARS.Svody.DbUpdater --createSchema -
sysUserName postgres -sysUserPassword postgres -connSettingsPath
"путь\Приложение.барс" --pd -pdUser пользовательПД -pdPassword
парольОтСхемыПД -pdIp IPСервераБДПД -pdPort портБДПД -pdSysUserName
postgres -pdSysUserPassword парольОтПользователяPostgresПД -
pdSysDataBase postgres
      /opt/svody/updater/BARS.Svody.DbUpdater --createSchema -
sysUserName postgres -sysUserPassword парольОтПользователяPostgres -
dbDialect Npgsql -dbIp IPСервераБД -dbName имяБД -dbScheme имяСхемы -
dbPassword парольОтСхемы -dbPort портБД --pd -pdUser пользовательПД -
pdPassword пользовательПД -pdIp IPСервераБДПД -pdPort портБДПД -
pdSysUserName postgres -pdSysUserPassword
парольОтПользователяPostgresПД -pdSysDataBase postgres
```

8.2 Обновление структуры БД

С помощью обновления синхронизируется структура таблиц в БД с той, которая нужна для работы в приложении. При каждом обновлении web-приложения необходимо обновлять структуру БД.

Параметры запуска приведены в таблице ниже (Таблица 7).

Таблица 7 – Параметры запуска режима обновления

Название параметра	Описание параметра	Пример использования
-connSettingsPath	Путь до файла «Приложение.барс». Если путь содержит пробелы, значение параметра указывается в кавычках	-connSettingsPath "путьПриложение.барс"
-dbDialect	Тип обновляемой СУБД. Допустимые значения: Npgsql	-dbDialect Npgsql
-dbIp	IP-адрес сервера БД либо host	-dbIp 127.0.0.1
-dbPort	Порт БД	-dbPort 5432
-dbName	Наименование обновляемой БД	-dbName DB_NAME
-dbScheme	Наименование обновляемой схемы	-dbScheme SCHEMA_NAME
-dbPassword	Пароль пользователя БД	-dbPassword 123
-updateArchiveDatabases или --updateArchiveDatabases	«Флажок» обновления архивных БД, привязанных к указанным параметрам подключения. Если значение параметра не указано, по умолчанию архивные БД будут обновлены	-updateArchiveDatabases true --updateArchiveDatabases (аналог -updateArchiveDatabases true)
-migrations	Путь до папки с дистрибутивом web-приложения .dll файлы из дистрибутива будут использованы для формирования миграций. В случае если путь содержит пробелы, значение параметра указывается в кавычках. Обязательный параметр	-migrations "путь\Папка приложения"
-zip	Путь к zip-архиву с дистрибутивом обновления. Используется при обновлении API	-zip "путь\AddInLib.zip"
-simpleProgress или --simpleProgress	Формат оповещения о прогрессе обновления. В случае, если значение параметра false – консоль будет оповещать о прогрессе сериализованными моделями, иначе в текстовом формате. Допустимые значения: true, false Значение по умолчанию – true Необязательный параметр	-simpleProgress true или -simpleProgress false --simpleProgress (аналог -simpleProgress true)
-mode	Режимы обновления. Допустимые значения: api, platform Обязательный параметр	-mode api или -mode platform
--pd	Параметр указывающий на то, что персональные данные будут храниться в отдельной БД	--pd
-pdUser	Имя пользователя и название БД, в которой будут храниться персональные данные	-pdUser test_pd
-pdPassword	Пароль пользователя БД	-pdPassword 123

Название параметра	Описание параметра	Пример использования
-pdIp	IP-адрес сервера БД, либо host	-pdIp 127.0.0.1
-pdPort	Порт БД	-pdPort 5432
-pdSysUserName	Логин от super пользователя в БД в которой будут храниться персональные данные	-pdSysUserName postgres
-pdSysUserPassword	Пароль от super пользователя в БД в которой будут храниться персональные данные	-pdSysUserPassword postgres
-pdSysDataBase	Главная база на сервере где разворачивается база персональных данных. Обязателен при создании схемы на Postgres	-pdSysDataBase postgres

Режимы обновлений приведены в таблице ниже (Таблица 8).

Таблица 8 – Режимы обновлений

Режим обновления	Значение
platform	Обновление серверной части web-приложения
api	Обновление API web-приложения. Установленные API, которых нет в обновлении, не затираются

Примеры запуска обновления серверной части web-приложения с обычным режимом хранения персональных данных:

– Пример запуска для ОС Windows:

```
BARS.Svody.DbUpdater.exe -migrations "путьДоПапкиПриложения" -dbDialect Npgsql -dbIp IPСервераБД -dbName имяБД -dbScheme имяСхемы -dbPassword парольОтСхемы -dbPort портБД -simpleProgress true -mode режимОбновления -updateArchiveDatabases false
```

– Пример запуска для ОС Linux:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations "путьДоПапкиПриложения" -dbDialect Npgsql -dbIp IPСервераБД -dbName имяБД -dbScheme имяСхемы -dbPassword парольОтСхемы -dbPort портБД -simpleProgress true -mode режимОбновления -updateArchiveDatabases false
```

В API можно реализовать миграции структуры БД. Для запуска обновления необходим zip-архив с файлами API с расширениями .migrations.dll:

– пример запуска для ОС Windows:

```
BARS.Svody.DbUpdater.exe -zip "C:\svodyapp\web\svody\AddInLib.zip" -dbDialect Npgsql -dbIp IPСервераБД -dbName имяБД -dbScheme имяСхемы -dbPassword парольОтСхемы
```

```
-dbPort портБД -simpleProgress true -mode api -updateArchiveDatabases
false
```

– пример запуска для ОС Linux:

```
/opt/svody/updater/BARS.Svody.DbUpdater -zip
"/opt/tmp/AddInLib.zip" -dbDialect Npgsql -dbIp IPСервераБД -dbName
имяБД -dbScheme имяСхемы -dbPassword парольОтСхемы -dbPort портБД -
simpleProgress true -mode api -updateArchiveDatabases false
```

При обновлении схемы с ПД, к основным параметрам запуска, указанным выше, необходимо добавить параметры из раздела "Параметры ПД" тут - Параметры запуска, а также должны быть указаны параметры -sysUserName и –sysUserPassword.

Обновление в режиме отдельного хранения персональных данных:

```
/opt/svody/updater/BARS.Svody.DbUpdater -migrations "/opt/svody"
-dbDialect Npgsql -dbIp IPСервераБД -dbName имяБД –dbScheme имяСхемы -
dbPassword парольОтСхемы -dbPort портБД -simpleProgress true -mode
platform -updateArchiveDatabases false -sysUserName
ИмяСистемногоПользователя -sysUserPassword ПарольСистемногоПользователя
--pd –pdUser ИмяСхемы_pd -pdPassword парольОтСхемы_pd -pdIp
IPСервераБД_pd -pdPort портБД_pd -pdSysUserName
ИмяСистемногоПользователя_pd -pdSysUserPassword
ПарольСистемногоПользователя_pd -pdSysDataBase ИмяГлавноеБДНаСервере_pd
```

8.3 Установка лицензии

Параметры запуска приведены в таблице ниже (Таблица 9).

Таблица 9 – Параметры запуска

Название параметра	Описание параметра	Пример использования
-connSettingsPath	Путь до файла «Приложение.барс». Если путь содержит пробелы, значение параметра указывается в кавычках.	-connSettingsPath "путь\Приложение.барс"
-dbDialect	Тип обновляемой СУБД. Допустимые значения: Npgsql	-dbDialect Npgsql
-dbIp	IP-адрес сервера БД либо host	-dbIp 127.0.0.1
-dbPort	Порт БД	-dbPort 5432
-dbName	Наименование обновляемой БД	-dbName DB_NAME
-dbScheme	Наименование обновляемой схемы	-dbScheme SCHEME_NAME
-dbPassword	Пароль пользователя БД	-dbPassword 123

Название параметра	Описание параметра	Пример использования
-updateArchiveDatabases или --updateArchiveDatabases	«Флажок» обновления архивных БД, привязанных к указанным параметрам подключения. Если значение параметра не указано, по умолчанию архивные БД будут обновлены	-updateArchiveDatabases true – updateArchiveDatabases (аналог -updateArchiveDatabases true)
-lic	Путь к файлу лицензионного ключа ПП МЗ	-lic "путь\key.lic"
--force	Выполнять действия без подтверждения пользователя. Например, если при установке нового лицензионного ключа выясняется, что в БД ключ уже есть. Без этого параметра потребуется подтверждения от пользователя на удаление ключа в интерактивном режиме. С этим параметром старый ключ будет удален без подтверждения. Необязательный параметр. Если параметр не указан, по умолчанию программа потребует подтверждение от пользователя	--force

Последовательность действий для установки лицензии:

а) запустите утилиту в режиме установки лицензии с соответствующими заполненными параметрами

Примеры установки лицензии:

– пример запуска для ОС Windows:

```
BARS.Svody.DbUpdater.exe -connSettingsPath "путь\Приложение.барс" -lic "путь\лицензия.lic"
BARS.Svody.DbUpdater.exe -lic "путь\лицензия.lic" -dbDialect Npgsql -dbIp IPСервераБД -dbName имяБД -dbScheme имяСхемы -dbPassword парольОтСхемы -dbPort портБД -updateArchiveDatabases false --force
```

– пример запуска для ОС Linux:

```
/opt/svody/updater/BARS.Svody.DbUpdater -connSettingsPath "путь/Приложение.барс" -lic "путь\лицензия.lic"
/opt/svody/updater/BARS.Svody.DbUpdater -lic "путь\лицензия.lic" -dbDialect Npgsql -dbIp IPСервераБД -dbName имяБД -dbScheme имяСхемы -dbPassword парольОтСхемы -dbPort портБД -updateArchiveDatabases true --force
```

б) скопируйте ключ, который выдан ПП М3, и отдайте его курирующему сотруднику компании. Сотрудник в ответ предоставит вам ответный ключ;

в) вставьте ответный ключ в консоль.

Примеры успешной установки лицензии приведены на рисунках ниже (Рисунок 9, Рисунок 10).

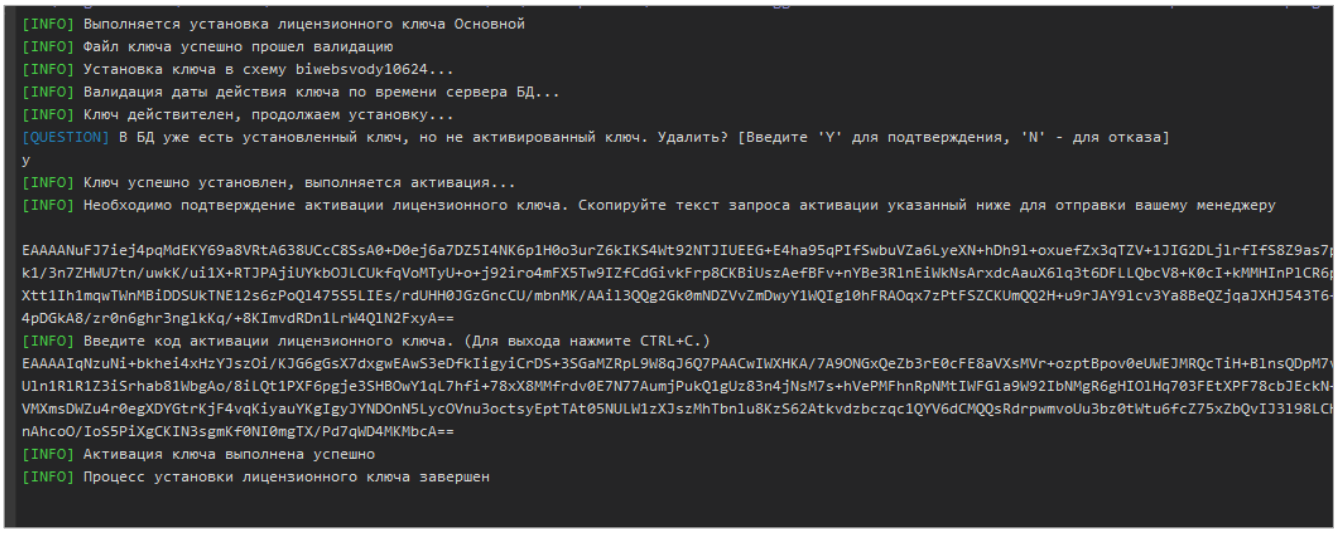


Рисунок 9 – Пример успешной установки лицензии

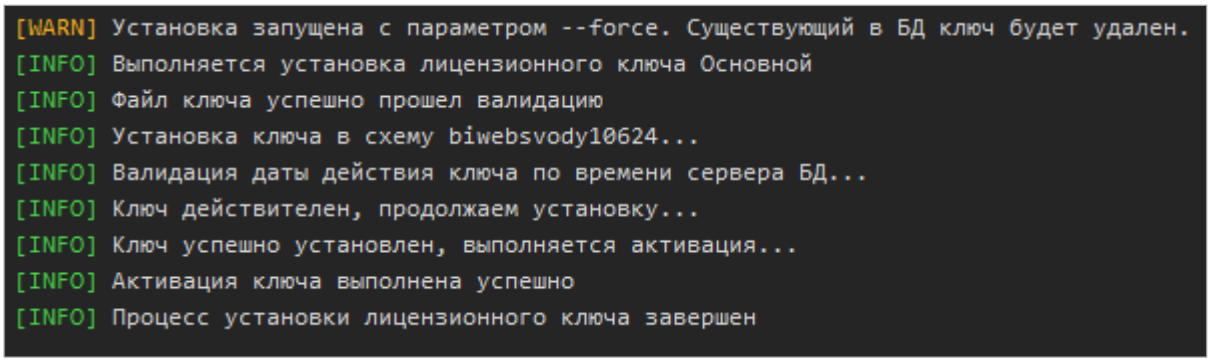


Рисунок 10 – Пример успешной установки лицензии

8.4 Конвертация Oracle на Postgres

Для ПП М3, которые существуют давно и изначально работали на СУБД Oracle, разработан функционал конвертации БД на СУБД Postgres.

Выполните настройки:

а) разверните новую схему на Postgres;

б) установите обновление той версии, которая установлена на текущей БД:

Примечания

1 Версии исходной БД на Oracle должна быть идентична версии новой схемы на Postgres.

2 Несмотря на то, что версии ПП М3 одинаковые, возможно, что в исходной БД будет больше таблиц, чем в новой БД. Возможные причины:

- долгое использование ПП М3: в БД остались старые, неактуальные таблицы;
- проектные реализации требовали создания новых таблиц в БД.

в) установите лицензионный ключ.

В процессе конвертации ПП М3 пропускает и не переносит данные по следующим таблицам:

- RUPD%;
- MLOG$_%;
- %$REF;
- SYS_EXPORT_SCHEMA%;
- OLAP%;
- QRTZ_%;
- SCHEMA%;
- BARS_MUTEX;
- ADDRESS;
- CLASSIFICATIONELEM;
- ENTEXATTRDESC;
- ENTEXATTRDESC$ARC;
- EXECUTION_TRIGGER;
- EXECUTION_TRIGGER$ARC;
- GRUPPAPRAVDOSTUPA;
- HRANIMAYAOLAPVYBORKA;
- JOB;
- JOB$ARC;
- NOTIFICATIONRULE;
- NOTIFICATIONRULE$ARC;
- NOTIFRULEGROUP;
- NOTIFRULEGROUP$ARC;
- NOTIFRULEUSER;
- NOTIFRULEUSER$ARC;
- NTFRULEGROUPROLE;
- NTFRULEGROUPROLE$ARC;
- NTFRULENTFRULEGROUP;

- NTFRULENTFRULEGROUP$ARC;
- OFFLINEKEYS;
- OFFLINEKEYS$ARC;
- OGRANICHENIEDOSTUPA;
- POLZOV_UVYAZKA;
- STORED_META_FIELD;
- SUMMARYCHECKMARK;
- SUMMARYCHECKMARK$ARC;
- TEMP_OLAP_TABLE;
- UNIVERSALNYISPRAVOCH;
- USER_REGISTRATION_PA;
- USER_REGISTRATION_PA$ARC;
- ZAPISKLADRA;
- ZAPISKLADRA$ARC;
- ZAPISSPRAVOCHNIKA;
- а также по таблицам, код которых начинается на OLAP, SCHEMA и BARS_MUTEX.

Запрос для получения всех таблиц, которых нет в новой БД:

```
      select a.table_name from all_tables a where a.owner =
'НазваниеСхемы'
      and a.table_name not like ('OLAP%')
      and a.table_name not like ('DIC_%')
      and a.table_name not like (Schema%')
      and a.table_name not like ('BARS_MUTEX%')
      and a.table_name not in ('ADDRESS',
                'CLASSIFICATIONELEM',
                 'ENTEXATTRDESC',
      'ENTEXATTRDESC$ARC',
      'EXECUTION_TRIGGER',
      'EXECUTION_TRIGGER$ARC',
      'GRUPPAPRAVDOSTUPA',
      'HRANIMAYAOLAPVYBORKA',
      'JOB',
      'JOB$ARC',
      'NOTIFICATIONRULE',
      'NOTIFICATIONRULE$ARC',
      'NOTIFRULEGROUP',
      'NOTIFRULEGROUP$ARC',
      'NOTIFRULEUSER',
      'NOTIFRULEUSER$ARC',
      'NTFRULEGROUPROLE',
      'NTFRULEGROUPROLE$ARC',
```

```
'NTFRULENTFRULEGROUP',
'NTFRULENTFRULEGROUP$ARC',
'OFFLINEKEYS',
'OFFLINEKEYS$ARC',
'OGRANICHENIEDOSTUPA',
'POLZOV_UVYAZKA',
'STORED_META_FIELD',
'SUMMARYCHECKMARK',
'SUMMARYCHECKMARK$ARC',
'TEMP_OLAP_TABLE',
'UNIVERSALNYISPRAVOCH',
'USER_REGISTRATION_PA',
'USER_REGISTRATION_PA$ARC',
'ZAPISKLADRA',
'ZAPISKLADRA$ARC',
'ZAPISSPRAVOCHNIKA' ,
ПереченьТаблицИзПредыдущегоПункта
);
```

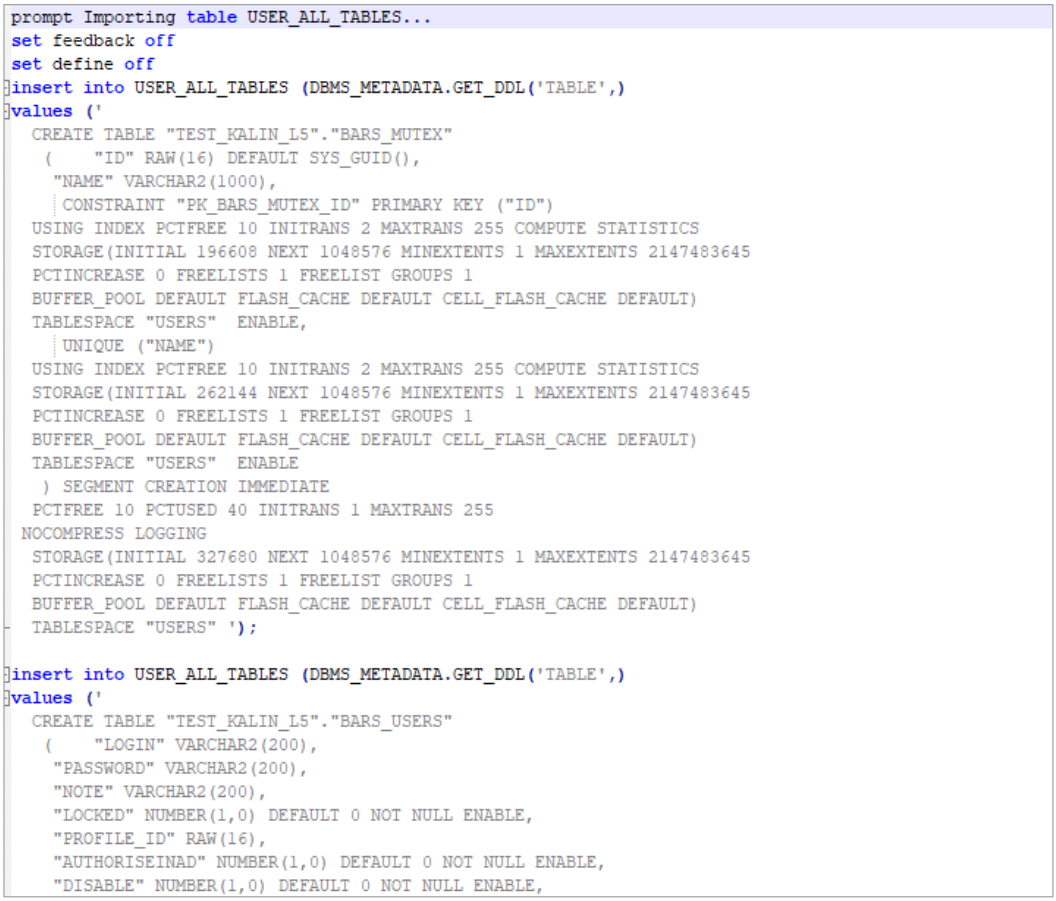
После выполнения запроса отобразится список таблиц, которые необходимо создать вручную на новой схеме Postgres.

г) создайте таблицы, полученные выше, в новой схеме Postgres:

– получите скрипты для создания таблиц на схеме Oracle;

– зайдите на схему пользователя, выполните скрипт:

```
SELECT DBMS_METADATA.GET_DDL('TABLE',u.table_name)
     FROM USER_ALL_TABLES u
     WHERE u.table_name IN ('ТАБЛИЦА1', 'ТАБЛИЦА2');
```



```
prompt Importing table USER_ALL_TABLES...
set feedback off
set define off
insert into USER_ALL_TABLES (DBMS_METADATA.GET_DDL('TABLE',)
values ('
   CREATE TABLE "TEST_KALIN_L5"."BARS_MUTEX"
    (    "ID" RAW(16) DEFAULT SYS_GUID(),
     "NAME" VARCHAR2(1000),
      CONSTRAINT "PK_BARS_MUTEX_ID" PRIMARY KEY ("ID")
   USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255 COMPUTE STATISTICS
   STORAGE(INITIAL 196608 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
   PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
   BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
   TABLESPACE "USERS"  ENABLE,
     UNIQUE ("NAME")
   USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255 COMPUTE STATISTICS
   STORAGE(INITIAL 262144 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
   PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
   BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
   TABLESPACE "USERS"  ENABLE
    ) SEGMENT CREATION IMMEDIATE
   PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255
  NOCOMPRESS LOGGING
   STORAGE(INITIAL 327680 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
   PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
   BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
   TABLESPACE "USERS" ');

insert into USER_ALL_TABLES (DBMS_METADATA.GET_DDL('TABLE',)
values ('
   CREATE TABLE "TEST_KALIN_L5"."BARS_USERS"
    (    "LOGIN" VARCHAR2(200),
     "PASSWORD" VARCHAR2(200),
     "NOTE" VARCHAR2(200),
     "LOCKED" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
     "PROFILE_ID" RAW(16),
     "AUTHORISEINAD" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
     "DISABLE" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
```

Рисунок 11 – Пример полученного скрипта

Необходимы только create-скрипты с перечнем полей.

– перепишите полученные скрипты под Postgres:

Например, из скрипта:

```
CREATE TABLE "НазваниеСхемы"."BARS_USERS"
   (     "LOGIN" VARCHAR2(200),
    "PASSWORD" VARCHAR2(200),
    "NOTE" VARCHAR2(200),
    "LOCKED" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
    "PROFILE_ID" RAW(16),
    "AUTHORISEINAD" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
    "DISABLE" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
    "CHANGEPASSWORD" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
    "ID" RAW(16),
    "NAME" VARCHAR2(600),
    "REPLICA" VARCHAR2(80),
    "DATECREATE" DATE NOT NULL ENABLE,
    "DATEEDIT" DATE NOT NULL ENABLE,
    "USERCREATE" VARCHAR2(80),
    "USEREDIT" VARCHAR2(80),
    "IPADDREDIT" VARCHAR2(80),
    "OBJECTVERSION" NUMBER(8,0) NOT NULL ENABLE,
    "PASSWORD_CHANGE_DATE" DATE,
    "EMAIL" VARCHAR2(2000),
```

```
          "LOCKTYPE" NUMBER(3,0),
           CONSTRAINT "PK_BARS_USERS" PRIMARY KEY ("ID") DEFERRABLE
INITIALLY DEFERRED
        USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255 COMPUTE
STATISTICS
        STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS
2147483645
        PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
        BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE
DEFAULT)
        TABLESPACE "USERS"  ENABLE,
      CONSTRAINT "FK_BARS_USERS_$$B128" FOREIGN KEY ("PROFILE_ID")
      REFERENCES "НазваниеСхемы"."BARS_PROFILE" ("ID") DEFERRABLE
INITIALLY DEFERRED ENABLE
         ) SEGMENT CREATION IMMEDIATE
        PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255
       NOCOMPRESS LOGGING
        STORAGE(INITIAL 196608 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS
2147483645
        PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
        BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE
DEFAULT)
        TABLESPACE "USERS" ');
```

Получается скрипт для Oracle:

```
CREATE TABLE "НазваниеСхемы"."BARS_USERS"
   (     "LOGIN" VARCHAR2(200),
    "PASSWORD" VARCHAR2(200),
    "NOTE" VARCHAR2(200),
    "LOCKED" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
    "PROFILE_ID" RAW(16),
    "AUTHORISEINAD" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
    "DISABLE" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
    "CHANGEPASSWORD" NUMBER(1,0) DEFAULT 0 NOT NULL ENABLE,
    "ID" RAW(16),
    "NAME" VARCHAR2(600),
    "REPLICA" VARCHAR2(80),
    "DATECREATE" DATE NOT NULL ENABLE,
    "DATEEDIT" DATE NOT NULL ENABLE,
    "USERCREATE" VARCHAR2(80),
    "USEREDIT" VARCHAR2(80),
    "IPADDREDIT" VARCHAR2(80),
    "OBJECTVERSION" NUMBER(8,0) NOT NULL ENABLE,
    "PASSWORD_CHANGE_DATE" DATE,
    "EMAIL" VARCHAR2(2000),
    "LOCKTYPE" NUMBER(3,0),
);
```

Конвертируйте его в вид для Postgres:

```
CREATE TABLE BARS_USERS
   (     LOGIN VARCHAR(200),
         PASSWORD VARCHAR(200),
```

```
            NOTE VARCHAR(200),
            LOCKED numeric(1,0),
            PROFILE_ID uuid,
            AUTHORISEINAD numeric(1,0),
            DISABLE numeric(1,0) ,
            CHANGEPASSWORD numeric(1,0),
            ID uuid,
            NAME VARCHAR(600),
            REPLICA VARCHAR(80),
            DATECREATE DATE NOT NULL ,
            DATEEDIT DATE NOT NULL ,
            USERCREATE VARCHAR(80),
            USEREDIT VARCHAR(80),
            IPADDREDIT VARCHAR(80),
            OBJECTVERSION numeric(8,0) NOT NULL ,
            PASSWORD_CHANGE_DATE DATE,
            EMAIL VARCHAR(2000),
            LOCKTYPE numeric(3,0)
);
```

Замените типы по правилам:

- varchar2 => varchar;
- number => numeric;
- raw(16) => uuid.

Таким образом создайте каждую недостающую таблицу.

д) запустите скрипт конвертации:

- пример для ОС Windows:

```
BARS.Svody.DbUpdater.exe --convert -fromDbDialect Oracle -
fromDbIp IPСервераБДИсточник -fromDbName имяБДИсточник -fromDbScheme
имяСхемыИсточник -fromDbPassword парольСхемыИсточник -fromDbPort
портБДИсточник -toDbDialect Npgsql -toDbIp IPСервераБДПриемник -
toDbName имяБДПриемник -toDbScheme имяСхемыПриемник -toDbPassword
парольСхемыПриемник -toDbPort портБДПриемник
```

- пример для ОС Linux:

```
/opt/svody/updater/BARS.Svody.DbUpdater --convert -fromDbDialect
Oracle -fromDbIp IPСервераБДИсточник -fromDbName имяБДИсточник -
fromDbScheme имяСхемыИсточник -fromDbPassword парольСхемыИсточник -
fromDbPort портБДИсточник -toDbDialect Npgsql -toDbIp
IPСервераБДПриемник -toDbName имяБДПриемник -toDbScheme
имяСхемыПриемник -toDbPassword парольСхемыПриемник -toDbPort
портБДПриемник
```

е) при необходимости настройте во вручную созданных таблицах ограничения.

9 Работа со схемой БД

9.1 Создание резервных копий схем БД для PostgreSQL

Автоматическое создание резервных копий схем БД осуществляется с помощью утилиты «pg_dump». Восстановление БД PostgreSQL осуществляется с помощью утилиты «pg_restore» из файла архива, созданного командой «pg_dump».

Для выполнения резервного копирования:

- создайте каталог, в котором будут храниться файлы архивов схемы;
- создайте исполняемый файл с расширением .cmd или .bat, который содержит название конфигурационных файлов, подлежащих резервированию;
- создайте конфигурационный файл с расширением .bat, в котором укажите конфигурацию резервируемого файла, например:

```
For /f "tokens=1,2,3,4,5 delims=/. " %%a in ('date/T') do set
nowdate=%%a-%%b-%%c
SET PGBIN=C:\Program Files\PostgreSQL\11\bin
 SET PGDATABASE=имяБазыДанных
 SET PGHOST=IPАдресСервераБазыДанных
 SET PGPORT=ПортСервераБазыДанных
 SET PGUSER=ИмяПользователяСполнымиПравами
 SET PGPASSWORD=ПарольОтПользователя
 cd /d C:\Program Files\PostgreSQL\11\bin
 pg_dump.exe --host localhost --port 5432 --username "postgres" -
-role "postgres" --no-password --format custom --blobs --verbose --file
"C:\AUTODUMPS\Manual\%nowdate%-ИмяБазыДанных.backup" "ИмяБазыДанных"
forfiles /P E:\AUTODUMPS\Postgres\TEST\ /M *.backup /D -3 -S /C
"cmd /C del @file /q"
```

- для периодического вызова утилиты создайте новое задание с помощью планировщика задач.

9.2 Работа с планировщиком задач

9.2.1 Работа с планировщиком задач на ОС Linux

Для автоматизации системных задач, или более известный как jobs под Linux, можно использовать утилиту под названием Cron. С помощью Cron можно запускать скрипты автоматически в течение определенного периода времени, создавать или других важных файлов, мониторинг служб, запущенных на вашем сервере и многое другое.

Если у вас не установлен Cron, установите его с помощью команд:

```
apt-get update
apt-get install cron
```

Чтобы проверить, работает ли сервис cron, используйте следующую команду:

```
sudo systemctl status cron
```

Чтобы настроить cron на рабочем месте, измените файл /etc/crontab. Обратите внимание, что он может быть изменен только суперпользователем. Для проверки текущей конфигурации, используйте следующую команду:

```
sudo cat /etc/crontab
```

- crontab -u %username% – определяет пользователя, чьи задачи будут просматриваться/редактироваться, отсутствие данного параметра устанавливает текущего пользователя;
- crontab -l – показывает список текущих задач;
- crontab -e – запускает редактор планировщика задач;
- crontab -r – удаляет все текущие задачи.

Файл crontab уже содержит пояснения о том, как определить свои собственные рабочие файлы. Синтаксис выглядит следующим образом:

```
minute hour day month day_of_week username command
```

Звездочка (*) в crontab может быть использована для определения всех допустимых значений.

Например, 0 4 * * * — запускать команду каждый день в 4:00.

После внесения изменений перезапустите службу cron с помощью команды ниже:

```
sudo systemctl restart cron
```

Команда для снятия бэкапа базы данных выглядит так:

```
pg_dump -h адрес_сервера -p порт -U пользователь -d база -Fc -v -f /путьДоФайла/ИмяФайла.backup
```

Заполните соответствующие пункты вашими значениями.

Для восстановления из бэкапа:

```
pg_restore -h адрес_сервера -p порт -U пользователь -d база -Fc -v /путьДоФайла/ИмяФайла.backup
```

Сохраните команду в файл скрипта.

Пример:

- создайте новый файл скрипта с названием backup.sh и сохраните по пути /home/scripts/;

– отредактируйте его, добавив туда выполнение команды бэкапа:

```
#!/bin/bash
pg_dump -h адрес_сервера -p порт -U пользователь -d база -Fc -v -
f /путьДоФайла/ИмяФайла.backup
```

– сохраните изменения в файле;

– добавьте в Crontab выполнение этого скрипта в 4 ночи каждый день, будет иметь вид:

```
crontab -e
```

– откроется редактор. В нём добавьте строчку:

```
0 4 * * *  root /home/scripts/backup.sh
```

Также в редакторе будет краткая справка по синтаксису (Рисунок 12).

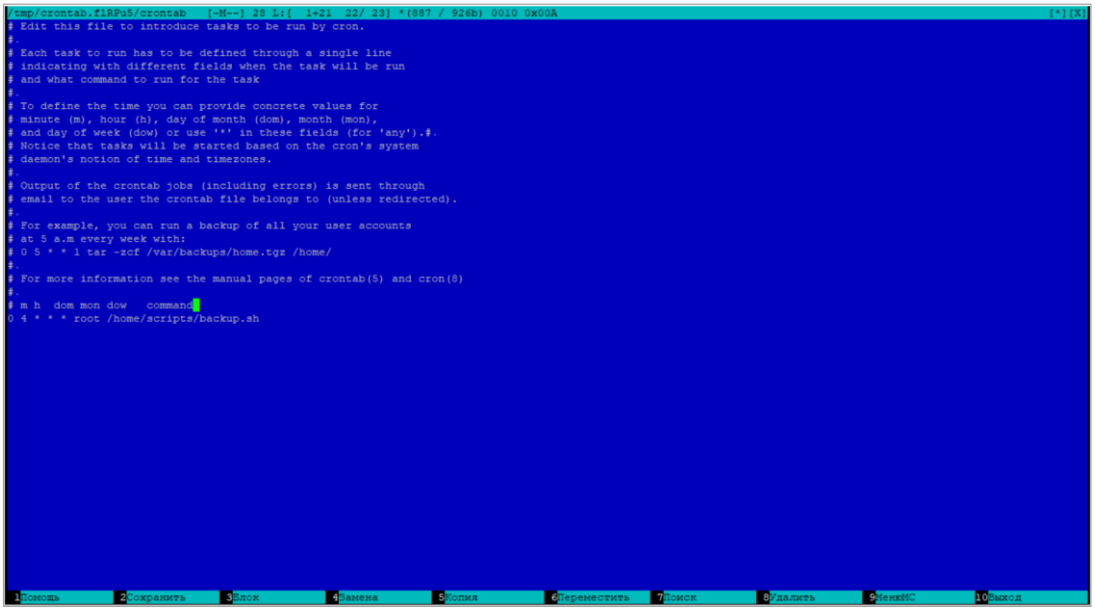


Рисунок 12 – Краткая справка по синтаксису

Если всё добавлено верно, создастся новое задание. В противном случае выйдет ошибка с предложением изменить или отменить действие. Например, такая:

```
new crontab file is missing newline before EOF, can't install.
Do you want to retry the same edit? (y/n)
```

Для получения дополнительной информации можете проверить страницу man:

```
man cron
```

а также:

```
man crontab
```

9.3 Снятие дампов для схем с данными отчетной формы больше 512 МБ

При снятии дампа может возникнуть ошибка «Invalid memory alloc request size». Данная ошибка возникает только при наличии файлов в БД размером больше 512 МБ. Чтобы обойти данную ошибку, была создана утилита для снятия дампов. При необходимости запрашивайте ее у менеджера компании.

Примечание – Используйте утилиту только в случае необходимости.

Утилита позволяет переместить файлы, у которых размер превышает допустимую для PostgreSQL норму, из таблиц ПП МЗ в системную таблицу PostgreSQL pg_largeobject. После работы утилиты в режиме -mode export необходимо снять дамп, развернуть дамп по месту назначения, запустить утилиту в режиме -mode import (утилита переместит файлы из таблицы pg_largeobject в родные таблицы).

У утилиты есть два режима:

- -mode export. В данном случае утилита создаст аналоги больших файлов в pg_largeobject и переведет ячейки больших файлов в null;
- -mode import. В данном случае утилита переместит проблемные файлы из pg_largeobject обратно в очищенные ячейки.

Запуск утилиты осуществляется через командную строку с заданием аргументов.

Таблица 10 – Аргументы для утилиты для снятия дампа

Аргумент	Описание	Пример значений
-mode export	Режим работы: - export для перемещения файлов из родных таблиц в системную таблицу PostgreSQL pg_largeobject перед снятием дампа - import для перемещения файлов из pg_largeobject в родную таблицу после снятия/накатки дампа	-mode export -mode import
-h	IP-адрес сервера БД	-h 127.0.0.1
-p	Порт	-p 5432
-un	Логин для доступа к БД postgres	-un postgres
-pw	Пароль для доступа к БД postgres	-pw postgres
-db	Название БД, в которой расположена схема для снятия дампа	-db dbfordump
-sc	Название схемы для снятия дампа	-sc scfordumpdb

Пример запуска через командную строку до снятия дампа для переноса файлов из таблиц в pg_largeobject:

– для ОС Windows:

```
ExpImpLargeFilesWhileDump.exe -mode export -h 127.0.0.1 -p 5432 -un postgres -pw postgres -db dbfordump -sc scfordumpdb
```

– для ОС Linux:

```
ExpImpLargeFilesWhileDump -mode export -h 127.0.0.1 -p 5432 -un postgres -pw postgres -db dbfordump -sc scfordumpdb
```

Пример запуска через командную строку после раскатки дампа для переноса файлов из pg_largeobject в исходные таблицы:

– для ОС Windows:

```
ExpImpLargeFilesWhileDump.exe -mode import -h 127.0.0.1 -p 5432 -un postgres -pw postgres -db dbrestoredump -sc scfordumpdb
```

– для ОС Linux:

```
ExpImpLargeFilesWhileDump -mode import -h 127.0.0.1 -p 5432 -un postgres -pw postgres -db dbrestoredump -sc scfordumpdb
```

Пример полного процесса снятия дампа:

– запуск утилиты в режиме -mode export;

– снятие дампа стандартным способом;

– развертывание дампа стандартным способом;

– запуск утилиты в режиме -mode import на сервере БД развернутого дампа (для перемещения файлов в очищенные ячейки);

– запуск утилиты в режиме -mode import на сервере БД снятого дампа (для возврата файлов в очищенные ячейки).

10 Описание конфигурационных файлов и файлов логирования приложения ПП МЗ

10.1 Описание конфигурационного файла svody.config

Основным конфигурационным файлом ПП МЗ является svody.config. В примере представлен текст настроек по умолчанию с комментариями-пояснениями.

Пример:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <Bars.RIA>
    <Elements>
      <!--
          В случае переопределения стартовой на проекте путь
будет AddInLib/Views/Templates/{IndexTemplateName}/Index.cshtml
          default - шаблон по умолчанию
      -->
      <IndexTemplateName>default</IndexTemplateName>
      <!--Наименования скрываемых родительских пунктов меню
рабочего стола через запятую-->
      <HiddenParentMenuItems></HiddenParentMenuItems>
      <!--Наименования скрываемых пунктов меню рабочего стола
через запятую-->
      <HiddenMenuItems>Поиск отчетных форм</HiddenMenuItems>
      <!-- Заголовок страницы браузера -->
      <ProjectTitle>Своды</ProjectTitle>
      <!-- Локализация по умолчанию -->
      <DefaultLocale>ru</DefaultLocale>
      <!-- Url по которому будет выполнен переход при клике на
логотип -->

<LogoClickRedirectUrl>https://bars.group/technology/svody/</LogoClickRe
directUrl>
      <!-- Интервал запуска задачи автоматического сброса паролей
в секундах-->

<ForceChangePasswordJobInterval>86400</ForceChangePasswordJobInterval>
      <AjaxTimeout>1200000</AjaxTimeout>
      <!-- Настройка использования хэш-функций, определенных в
ГОСТ Р 34.11-2012 -->
      <UseGostHash>false</UseGostHash>
    </Elements>
  </Bars.RIA>

  <Bars.Authorization>
    <Entries Name="Svody" Enabled="true" ButtonName="Войти в
систему" SortOrder="1" AuthorizationType="Default"
LoginToAnalytics="false"/>
```

```
          <Entries Name="Keycloak" Enabled="false" ButtonName="Войти
через Keycloak" SortOrder="2" AuthorizationType="OpenId">
            <OpenIdConnectProviderConfig>
              <ReverseProxyUrl><!-- URL, на который будет перенаправлен
пользователь после успешной авторизации на стороне OpenId. Необходимо
указывать внешний URL приложения, по которому приходят пользователь
(это может быть URL прокси-сервера, на котором установлен https-
сертификат) --></ReverseProxyUrl>
              <Issuer><!-- значение issuer --></Issuer>
              <AuthorizationEndpoint><!-- значение
authorization_endpoint--></AuthorizationEndpoint>
              <TokenEndpoint><!-- значение token_endpoint--
></TokenEndpoint>
              <UserInfoEndpoint><!-- значение userinfo_endpoint--
></UserInfoEndpoint>
              <SignOutEndpoint><!-- значение end_session_endpoint--
></SignOutEndpoint>
              <ClientId><!-- значение Идентификатора системы (вкладка
настройки) --></ClientId>
              <ClientSecret><!-- значение "Секретный ключ" системы
(вкладка полномочия) --></ClientSecret>
              <Authority><!-- корневой URL Keycloak -->/</Authority>
              <RealmsName><!-- Имя домена SSO провайдера, в котором был
создан клиент--></RealmsName>
              <ProviderId>0</ProviderId><!-- ИД SSO провайдера
(BARS.AM, KeyCloak), настроенного а AW на подключение к тому же клиенту
-->
              <ProviderPublicKey><!-- Публичный ключ домена Keycloak --
></ProviderPublicKey>
            </OpenIdConnectProviderConfig>
          </Entries>
          <Entries Name="SvodyKerberos" Enabled="false"
ButtonName="Войти в систему через домен" SortOrder="3"
AuthorizationType="Kerberos">
            <KerberosAuthenticationConfig>
              <Login><!-- Логин пользователя с правами доступа на
чтение к каталогу пользователей домена через LDAP --></Login>
              <Password><!-- Пароль пользователя с правами доступа на
чтение к каталогу пользователей домена через LDAP --></Password>
              <CCacheDirectoryPath><!--Папка, в которую будут
сохраняться kerberos-билеты, полученные при авторизации через kerberos
в LDAP--></CCacheDirectoryPath>
              <Realm><!--Имя домена--></Realm>
              <DomainControllerName><!--DNS-имя сервера, который
является контроллером домена--></DomainControllerName>
              <UsersOu><!--Узел дерева каталога OpenLDAP, под которым
добавлены все пользователи. При авторизации выполняется поиск данных о
пользователе под этим узлом (по умолчанию указать users) --></UsersOu>
              <GroupsFilterAttribute><!-- Атрибут группы, по которому
будем искать в LDAP группы пользователей домена, в которые
администратор включил пользователя (по умолчанию указать memberUid) --
></GroupsFilterAttribute>
```

```
            <KeyTabPath><!-- Путь до keytab-файла, в который
выгружены ключи доменных сервисов HTTP, ldap /etc/krb5.keytab--
></KeyTabPath>
          </KerberosAuthenticationConfig>
        </Entries>
      </Bars.Authorization>

      <Bars.TwoFactorAuthentication>
        <!-- Настройка управлением максимального времени, в течении
которого, можно запросить одноразовый пароль повторно.-->
        <!-- Время устанавливается в секундах. Минимальное значение
60 (1минута). Максимальное значение 900(15минут).-->
        <!-- Если значение указано не верно, то применяется значение
по умолчанию равное 120 -->
        <PasswordLifeTime>120</PasswordLifeTime>
      </Bars.TwoFactorAuthentication>

      <Bars.MessengerService>
        <Elements>
          <!-- Адрес сервера, где развернут сервис отправки сообщений
(без знака "/" в конце адреса, например "http://192.168.12.12") -->
          <URL></URL>
          <!-- Период вызова сервиса для отправки сообщений (в
секундах) -->
          <Period>10</Period>
        </Elements>
      </Bars.MessengerService>

      <!-- Настройки ReminderWorker -->
      <Bars.RemindNotificator>
        <enabled>false</enabled>
        <ReminderWorkerJobInterval>43200</ReminderWorkerJobInterval>

<ReminderCalculatorChangesAnalyzerJobInterval>3600</ReminderCalculatorC
hangesAnalyzerJobInterval>
      </Bars.RemindNotificator>

      <!-- Настройки менеджера фоновых процессов -->
      <Bars.ProcessManager Culture="ru-RU"
ThreadCount="5"></Bars.ProcessManager>

      <Bars.ControlConfigurationPanel>
          <!-- Логин -->
          <Login>root</Login>
          <!-- Пароль -->
          <Password>Je6teGLoc+rrPkr5VpYYow==</Password>
      </Bars.ControlConfigurationPanel>

      <ext.direct>
        <Name>Svody.RemotingAPI</Name>
        <Assembly>BARS.Svody.Web.Host, Bars.Svody.Web.Host,
ApiWrappers</Assembly>
        <DateFormat>ISO</DateFormat>
```

```
          <Debug>true</Debug>
          <MaxRetries>0</MaxRetries>
        </ext.direct>

        <sessionState>
          <Mode>InProc</Mode>
          <TimeoutInMinutes>5</TimeoutInMinutes>
        </sessionState>

        <Bars.NewsService NotificationDurationInMinutes="2880"/>
        <Bars.SoapServices>
          <!-- Пример добавленного сервиса
           <Entries Name="SampleService"
Type="Api.LegacyWcf.SampleService, Api.LegacyWcf"
Endpoint="/SampleService.asmx"/>

           Name - Название сервиса
           Type - Полное название типа по которому генерируется WDSL-
описание сервиса и которому будут переданы запросы
           Endpoint - Конечная точка маршрута сервиса
          -->
        </Bars.SoapServices>

        <!-- Настройки безопасности, определяющие параметры защиты от
CSRF-атаки на приложение

          AllowedDomainsForShowInFrame - указывается значение http-
заголовка, который позволяет добавлять в исключения домены, на которых
возможно открытие UI платформы в IFRAME.
            например http://your.site https://my.site.
            Значение по умолчанию - пустая строка

          SameSiteCookiePolicy - указывается политика, применяемая к
сессионной cookie, выдаваемой сервером каждому пользователю, который
смог успешно авторизоваться в системе.
            Подробнее о значениях - https://developer.mozilla.org/en-
US/docs/Web/HTTP/Headers/Set-Cookie/SameSite,
https://docs.microsoft.com/ru-
ru/dotnet/api/microsoft.aspnetcore.http.samesitemode?view=aspnetcore-
3.1
            Значение по умолчанию - Lax. Для кроссавторизации
необходимо указать значение Unspecified
        -->
        <CsrfSecurity>
          <AllowedDomainsForShowInFrame></AllowedDomainsForShowInFrame>
          <SameSiteCookiePolicy>Lax</SameSiteCookiePolicy>
        </CsrfSecurity>

        <!-- Настройка глобализации реквестов приложения -->
        <globalization>
          <Culture>ru-RU</Culture>
          <UiCulture>ru-RU</UiCulture>
        </globalization>
```

```
        <!-- Настройка КриптоПро-->
        <Bars.Signature>
          <!-- Пример пути до КриптоПро для сервера на Linux :
/opt/cprocsp/bin/amd64 -->
          <CryptoProPath></CryptoProPath>
        </Bars.Signature>

        <Bars.Themes DefaultThemeName = "svody">
          <Themes Name="svody" DisplayName="Светлая"
PreviewImageCls="svody-theme-preview"/>
          <Themes Name="svody-dark" DisplayName="Тёмная"
PreviewImageCls="svody-dark-theme-preview"/>
        </Bars.Themes>

        <Svody.Designer>
          <!--
            Name - наименование подключения (значение обязательное,
уникальное)
            Url - ссылка на приложение дизайнер
            SortOrder - порядок обращения по ссылкам, чем меньше
SortOrder - тем раньше при установке соединения с дизайнером будет
использована ссылка

            Пример:
            <Entry Name="primary" Url="https://192.168.0.2/designer"
SortOrder="0"/>
            <Entry Name="secondary"
Url="https://domain.name.ru/designer" SortOrder="1"/>

            При такой настройке сначала произойдет попытка авторизации
по ссылке https://192.168.0.2/designer, в случае неудачи - произойдет
попытка авторизации по ссылке https://domain.name.ru/designer.
            Количество ссылок не ограничено.
          -->
          <Entry Name="primary" Url="" SortOrder="0"/>
        </Svody.Designer>

        <Svody.Aw>
          <Db><!-- БД Clickhouse AW --></Db>
          <Host><!-- IP БД Clickhouse AW --></Host>
          <Port>9017</Port><!-- TCP Порт Clickhouse AW -->
          <User><!-- Пользователь БД Clickhouse AW --></User>
          <Password><!-- Пароль пользователя БД Clickhouse AW --
></Password>
          <BaseUrl><!-- URl приложения AW. Указывается без "/" в конце
--></BaseUrl>
          <AdminLogin><!--Логин админа AW--></AdminLogin>
          <AdminPassword><!--Пароль админа AW--></AdminPassword>
        </Svody.Aw>

      <Svody.Analytics>
          <!-- Отображать кнопку Аналитика -->
```

```
        <Visible>true</Visible><!-- Отображать кнопку Аналитика -->
        <!-- true - открыть в новой вкладке приложения, false -
открыть в новом окне браузера-->
        <InFrame>true</InFrame><!-- true - открыть в новой вкладке
сводов, false - открыть в новом окне браузера-->
        <!-- URl приложения AW. Указывается без "/" в конце -->
        <Url></Url>
      </Svody.Analytics>

      <Svody.DataProtection>
        <!-- Срок жизни ключа, указывается в днях -->
        <KeyLifeTime>90</KeyLifeTime>
      </Svody.DataProtection>
    </configuration>
```

Файл «svody.config» содержит параметры различных настроек приложения и по умолчанию содержит следующие секции:

- Bars.RIA – общие настройки приложения. Содержит параметры, описанные в таблице ниже (Таблица 11);

Таблица 11 – Параметры секции Bars.RIA

Название параметра	Описание параметра
IndexTemplateName	Название папки индексной страницы группы тем оформления относительно пути Views/Templates. Доступный шаблон – «default»
HiddenParentMenuItems	Наименования скрываемых родительских и дочерних пунктов меню рабочего стола («Профиль», «Учреждение», «Мои хранимые блокировки», «Мои фоновые процессы», «Центр сообщений», а также «Отчетные формы», «Аналитические выборки», «Администрирование», «Помощь», «Новости проекта»). Вводить необходимо через запятую
HiddenMenuItems	Наименования скрываемых пунктов меню рабочего стола. Вводить необходимо через запятую
ProjectTitle	1.Заголовок страницы web-браузера, на которой открывается приложение ПП МЗ. 2.Наименование ПП МЗ в темах сообщений ,отправляемых пользователям и экспертам
DefaultLocale	Локализация по умолчанию
LogoClickRedirectUrl	URL, по которому будет выполнен переход при нажатии на логотип
ForceChangePasswordJobInterval	Интервал запуска задачи автоматического сброса паролей в секундах
AjaxTimeout	Количество миллисекунд, которое дается на выполнение запроса от клиента к серверу. По умолчанию 1200000
UseGostHash	Настройка использования хэш-функций, определенных в ГОСТ Р 34.11-2012

Примечание – При включенном параметре UseGostHash требуется дополнительно настроить сертифицированный пакет openssl-gost-engine, который включает в себя реализацию алгоритмов ГОСТ. Поддержка алгоритмов ГОСТ должна производиться всеми вычислительными машинами, не только на сервере приложения ПП М3, но и сервер с сервисом форм и Дизайнером. Установка и настройка ГОСТ OpenSSL описана на сайтах: https://redos.red-soft.ru/base/manual/safe-redos/gost-in-openssl/, https://www.altlinux.org/ГОСТ_в_OpenSSL.

- Bars.Authorization – секция, отвечающая за настройки авторизации. Содержит параметры, описанные в таблице ниже (Таблица 12);

Таблица 12 – Параметры секции Bars.Authorization

Название параметра	Описание параметра
Name	Наименование блока для авторизации
Enabled	Принимает два значения: true и false. При значении true на экране авторизации отобразится новая кнопка, при значении false блок не учитывается
ButtonName	Текст внутри кнопки
SortOrder	Порядок сортировки кнопок, принимает числовые значения, так при наличии нескольких способов авторизации можно поменять порядок кнопок
AuthorizationType	Принимает Default для авторизации по умолчанию, OIDC для авторизации через SSO и Kerberos для авторизации через домен LDAP
LoginToAnalytics	Принимает два значения: true и false. При значении true появляется возможность через страндартный вариант авторизации входить в AW
ReverseProxyUrl	Необходимо указать ссылку на приложение
Issuer	Значение issuer из настроек endpoint SSO (из пункта о) в п. 14.1.1 для BarsAM и из пункта в) в п. 14.1.2 для Keycloak)
AuthorizationEndpoint	Значение authorization_endpoint из настроек endpoint SSO (из пункта о) в п. 14.1.1 для BarsAM и из пункта в) в п. 14.1.2 для Keycloak)
TokenEndpoint	Значение token_endpoint из настроек endpoint SSO (из пункта о) в п. 14.1.1 для BarsAM и из пункта в) в п. 14.1.2 для Keycloak)
UserInfoEndpoint	Значение userinfo_endpoint из настроек endpoint SSO (из пункта о) в п. 14.1.1 для BarsAM и из пункта в) в п. 14.1.2 для Keycloak)
SignOutEndpoint	Значение end_session_endpoint из настроек endpoint (из пункта о) в п. 14.1.1 для BarsAM и из пункта в) в п. 14.1.2 для Keycloak)
ClientId	Значение уникального идентификатора ПП М3 (из пункта о) в п. 14.1.1 для BarsAM и из пункта в) в п. 14.1.2 для Keycloak)
ClientSecret	Значение секретного ключа ПП М3 (из пункта н) в п. 14.1.1 для BarsAM и из пункта м) в п. 14.1.2 для Keycloak)
Authority	Ссылка на SSO

Название параметра	Описание параметра
RealmsName	Имя домена из настроек домена, например, master (только для Keycloak из пункта г) в п. 14.1.2, необходимо для возможности массового экспорта пользователей из ПП М3 в Keycloak, можно оставить пустым при необходимости)
ProviderId	Необходимо для работы аналитических выборок, в случае, если аналитические выборки не используются, необходимо удалить или заключить в комментарий
ProviderPublicKey	Публичный ключ домена (из пункта о) п. 14.1.1 для BarsAM и из пункта н) в п. 14.1.2 для Keycloak)
Login	Логин пользователя с правами доступа на чтение к каталогу пользователей домена через LDAP
Password	Пароль пользователя с правами доступа на чтение к каталогу пользователей домена через LDAP
CCacheDirectoryPath	Папка, в которую будут сохраняться kerberos-билеты, полученные при авторизации через kerberos в LDAP
Realm	Имя домена
DomainControllerName	DNS-имя сервера, который является контроллером домена
UsersOu	Узел дерева каталога OpenLDAP, под которым добавлены все пользователи. При авторизации выполняется поиск данных о пользователе под этим узлом (по умолчанию указать users)
GroupsFilterAttribute	Атрибут группы, по которому будем искать в LDAP группы пользователей домена, в которые администратор включил пользователя (по умолчанию указать memberUid)
KeyTabPath	Путь до keytab-файла, в который выгружены ключи доменных сервисов HTTP, ldap /etc/krb5.keytab

- Bars.TwoFactorAuthentication – настройка управлением максимального времени, в течение которого можно запросить одноразовый пароль повторно. Время устанавливается в секундах. Минимальное значение 60 (1 минута). Максимальное значение 900 (15 минут). Если значение указано неверно, то в атрибуте PasswordLifeTime применяется значение по умолчанию, равное 120;
- Bars.MessengerService – секция отвечает за настройки сервиса отправки сообщений. Содержит параметры, описанные в таблице ниже (Таблица 13);

Таблица 13 – Параметры секции Bars.MessengerService

Название параметра	Описание параметра
Period	Период вызова сервиса для отправки сообщений (в секундах)
URL	Адрес сервера, где развернут сервис отправки сообщений (без символа «/» в конце адреса, например, «http://192.168.12.12»)

- Bars.RemindNotificator – отвечает за настройки уведомлений. Содержит параметры, описанные в таблице ниже (Таблица 14);

Таблица 14 – Параметры секции Bars.RemindNotificator

Название параметра	Описание параметра
enabled	«Флажок» включения/отключения сервиса расчета сроков сдачи отчетности и рассылки уведомлений
ReminderWorkerJobInterval	Интервал запуска задачи расчета и рассылки уведомлений
ReminderCalculatorChangedAnalyzerJobInterval	Интервал запуска задачи обновление кэша калькуляторов строк расчета

- DictionaryCache – настройки кэширования справочников. Возможные значения:
  - Memory (значение по умолчанию) – кэширование в оперативной памяти;
  - Sqlite – кэширование на диске в БД sqlite.
- Bars.ProcessManager – настройки менеджера фоновых процессов (Таблица 15);

Таблица 15 – Параметры секции Bars.ProcessManager

Название параметра	Описание параметра
Culture	Локализация (язык)
ThreadCount	Количество одновременно выполняемых фоновых процессов

- Bars.ControlConfigurationPanel – настройки входа в панель конфигурации приложения. Содержит параметры, описанные в таблице ниже (Таблица 16);

Таблица 16 – Параметры секции Bars.ControlConfigurationPanel

Название параметра	Описание параметра
Login	Логин пользователя для входа в панель конфигурации приложения
Password	Хэш пароля пользователя для входа в панель конфигурации приложения. Хэш вычисляется по специальному алгоритму

- ext.direct – настройка работы Ext.Direct. В атрибуте Assembly указываются наименования сборок для контроллеров, из которых необходимо сформировать обертки на javascript. Наименования вводятся через запятую;
- sessionState – секция для настройки сессии. В параметре TimeoutInMinutes указывается время жизни сессии (в состоянии неактивности) на web-сервере в минутах (Таблица 17);

Таблица 17 – Параметры секции sessionState

Название параметра	Описание параметра
Mode	Параметр настройки состояния сеанса Mode позволяет указать, какой поставщик состояния сеанса должен использоваться для хранения данных состояния сеанса между запросами. ("Off|InProc|StateServer|SQLServer|Custom") Подробнее о значениях: https://professorweb.ru/my/ASP_NET/base/level5/5_4.php
Type	Текущее количество минут, которое должно пройти, прежде чем текущий сеанс будет завершен при условии отсутствия запросов от клиента. Это значение может изменяться программно, что дает возможность при необходимости продлевать срок жизни коллекции сеанса для более важных операций

- Bars.NewsService – настройка оповещений об обновлении раздела «Новости проекта». В параметре секции NotificationDurationInMinutes задается время действия оповещения в минутах , по умолчанию равное 2880;
- Bars.SoapServices – регистрация SOAP-сервисов из прикладных API в качестве endpoint-ов ПП М3. Секция содержит параметры, описанные в таблице ниже (Таблица 18);

Таблица 18 – Параметры секции Bars.SoapServices

Название параметра	Описание параметра
Name	Наименование сервиса
Type	Полное название типа, по которому генерируется WDSL-описание сервиса и которому будут переданы запросы
Endpoint	Конечная точка маршрута сервиса

- CsrfSecurity – содержит параметры, описанные в таблице ниже (Таблица 19);

Таблица 19 – Параметры секции CsrfSecurity

Название параметра	Описание параметра
AllowedDomainsForShowInFrame	Указывается значение http-заголовка, который позволяет добавлять в исключения домены, на которых возможно открытие UI ПП М3 в IFRAME. Например, http://your.site https://my.site. Значение по умолчанию – пустая строка
SameSiteCookiePolicy	Указывается политика, применяемая к сессионной cookie, выдаваемой сервером каждому пользователю, который смог успешно авторизоваться в ПП М3.

Название параметра	Описание параметра
	Подробнее о значениях – https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite, https://docs.microsoft.com/ru-ru/dotnet/api/microsoft.aspnetcore.http.samesitemode?view=aspnetcore-3.1. Значение по умолчанию – Lax. Для кроссавторизации необходимо указать значение «Unspecified»

- globalization – секция для настройки глобализации реквестов приложения (Таблица 20);

Таблица 20 – Параметры секции globalization

Название параметра	Описание параметра
Culture	Настройка глобализации реквестов приложения. По умолчанию ru-RU у обоих атрибутов
UiCulture	

- Bars.Signature – секция для настройки пути до КриптоПро. В атрибуте CryptoProPath указывается путь до КриптоПро на сервере приложения. Если данная настройка пустая, то будут использоваться значения по умолчанию. Путь для Linux: /opt/cprocsp/bin/amd64;
- Bars.Themes – секция для настройки доступных пользователям тем оформления приложения. В атрибуте DefaultThemeName указывается используемая по умолчанию тема. Она используется в следующих случаях:
  - если пользователь не выбирал тему из списка;
  - если выбранная тема перестала быть валидной;
  - если выбранная тема не валидная;
  - если отключена настройка «Отслеживать и сохранять настройки пользователей».
- Svody.Designer – секция для настройки параметров подключения к дизайнеру отчетных форм. В параметре URL указывается ссылка на приложение web-дизайнера, по которой будет осуществлен переход при нажатии на соответствующую кнопку в «Дизайнер» в главном меню ПП МЗ;
- Svody.Aw – секция для настройки параметров подключение AW. Содержит параметры, описанные в таблице ниже (Таблица 21);

Таблица 21 – Параметры секции Svody.Aw

Название параметра	Описание параметра
Db	БД Clickhouse AW
Host	IP БД Clickhouse AW
Port	TCP Порт Clickhouse AW
User	Пользователь БД Clickhouse AW
Password	Пароль пользователя БД Clickhouse AW
BaseUrl	URL приложения AW. Указывается без символа «/» в конце
AdminLogin	Логин админа AW
AdminPassword	Пароль админа AW

– Svody.Analytics – секция для настройки кросс-авторизации с AW. Содержит параметры, описанные в таблице ниже (Таблица 22);

Таблица 22 – Параметры секции Svody.Analytics

Название параметра	Описание параметра
Visible	Отображение/скрытие кнопки «Аналитика» - по умолчанию кнопка скрыта, установлено значение «false»
InFrame	Открытие страницы во вкладке внутри ПП М3 («true») или в отдельной вкладке web-браузера («false»)
Url	URL адрес, по которому будет происходить переход по кнопке «Аналитика»

– Svody.DataProtection - срок жизни ключа для авторизации запросов между приложением и сервисом форм, указывается в днях.

Для применения изменений перезапустите приложение.

10.2 Описание конфигурационного файла Приложение.барс

Для подключения приложения к базе данных используется файл Приложение.барс, который расположен в корне приложения. Параметры подключения указаны в таблице ниже (Таблица 23).

Таблица 23 – Параметры подключения

Параметр	Описание
DbDialect	Вид СУБД, к которой выполняется подключение.

Параметр	Описание
	Доступное значение – Npgsql
ИмяПользователя	Имя пользователя БД
Пароль	Пароль пользователя БД
Порт	Порт
Сервер	IP-адрес сервера БД
БД	Наименование базы данных, к которой выполняется подключение
НазваниеСхемы	Наименование схемы в базе данных
EnablePooling	Использовать пулинг соединений БД Возможные значения: True, False В случае если параметр отсутствует, используется значение по умолчанию, т.е. True
UseArchiveDatabases	Возможные значения: True, False В случае если параметр отсутствует, используется значение по умолчанию, т.е. True При значении True приложение использует для своей работы все доступные архивные БД
CommandTimeout	Указывает время таймаутов запроса к БД (в секундах). Если параметр не указан, по умолчанию берется 600с. Если указан 0 - таймаут запроса неограничен.

Примечание – Параметры «ИмяПользователя», «НазваниеСхемы» и «БД» должны совпадать.

Помимо стандартных параметров, можно также использовать дополнительные параметры:

```
<parameter keyword="MinPoolSize" value="1" />
<parameter keyword="MaxPoolSize" value="500" />
<parameter keyword="Timeout" value="120" />
```

Пример:

```
<Барс>
  <Подключение>
    <DbDialect>Npgsql</DbDialect>
    <ИмяПользователя>userName</ИмяПользователя>
    <Пароль>123</Пароль>
    <Порт>5432</Порт>
    <Сервер>127.0.0.1</Сервер>
    <БД>dbName</БД>
    <НазваниеСхемы>userName</НазваниеСхемы>
    <EnablePooling>False</EnablePooling>
    <parameter keyword="MinPoolSize" value="1" />
    <parameter keyword="MaxPoolSize" value="500" />
```

```
  </Подключение>
</Барс>
```

10.3 Описание конфигурационного файла userActivityMonitor.config

ПП М3 позволяет включить логирование запросов на web-сервер и sql-скриптов, которые обращаются к базе данных. Настройка логирования происходит в файле userActivityMonitor.config. Логи записываются в файл userActionsMonitor.log, который находится по пути:

\websvody\src\BARS.Svody.Web.Host\bin\NetCoreDebug\netcoreapp3.1\.logs.

Пример конфигурационного файла по умолчанию:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <configSections>
        <section name="Bars.UserActivityMonitor"
type="BARS.Svody.UserActivityMonitor.Contract.ConfigSection,
BARS.Svody.UserActivityMonitor.Contract" />
    </configSections>
    <Bars.UserActivityMonitor Enabled="false"
UseDefaultConnection="false">
        <ConnectionConfig DbType="Npgsql" Server="" Port="5432"
DbName="" Schema="" Password="" />
        <BuffersConfig Web="100" Sql="1000" />
        <ExcludedSqls name="0" Value="INSERT INTO
USER_ACTION_WEB_CONTROLLER" />
        <ExcludedSqls name="1" Value="INSERT INTO
USER_ACTION_SQL" />
        <ExcludedControllers name="0" ControllerName = "Login"
ActionName="*" />
    </Bars.UserActivityMonitor>
</configuration>
```

Секция <Bars.UserActivityMonitor/> содержит следующие атрибуты (Таблица 24):

Таблица 24 – Атрибуты секции <Bars.UserActivityMonitor/>

Атрибут	Описание
Enabled	Значения: false – мониторинг действий пользователя выключен, true – включен
UseDefaultConnection	Значения: true – использовать для логирования БД подключение к которой указано в Приложение.барс, false – использовать другую

Примечание – Параметры подключения указываются в секции ConnectionConfig.

Секция <ConnectionConfig/> – секция для настроек параметров подключения к БД, в которую будет вестись логирование. Атрибуты описаны в таблице (Таблица 25):

Таблица 25 – Атрибуты секции <ConnectionConfig/>

Атрибут	Описание
Атрибут	Описание
DbType	Тип СУБД. Доступное значение – PostgreSQL
Server	Хост сервера БД (домен или IP-адрес)
Port	Порт БД
DbName	Наименование БД
Schema	Наименование схемы в БД (должно быть равно имени пользователя)
Password	Пароль пользователя БД

Секция <BuffersConfig/> – секция для настроек количества логируемых запросов. Приложение накапливает указанное количество действий для записи и затем выполняет массовую вставку в БД. Атрибуты описаны в таблице (Таблица 26):

Таблица 26 – Атрибуты секции <BuffersConfig/>

Атрибут	Описание
Web	Количество web-запросов к web-серверу, которые необходимо накопить для записи в БД
Sql	Количество sql-запросов к БД, которые необходимо накопить для записи в БД

Секция <ExcludedSqls/> – секция для исключения логирования некоторых SQL-запросов (по умолчанию исключены запросы самого логирования). Атрибуты описаны в таблице (Таблица 27):

Таблица 27 – Атрибуты секции <ExcludedSqls/>

Атрибут	Описание
name	Наименование исключения, должно быть уникальным на все секции ExcludedSqls
Value	Подстрока SQL-запроса. Все запросы, содержащие указанное значение, будут исключены из логирования. Также может содержать значение "*" – это означает, что необходимо исключить все SQL-запросы из логирования

Секция <ExcludedControllers/> – секция для исключения логирования некоторых web-запросов (по умолчанию исключены все запросы на контроллер Login, т.е. запрос авторизации и логаута). Атрибуты описаны в таблице (Таблица 28):

Таблица 28 – Атрибуты секции <ExcludedControllers/>

Атрибут	Описание
name	Наименование исключения, должно быть уникальным на все секции ExcludedControllers
ControllerName	Наименование контроллера, экшены которого должны быть исключены из логирования. Так же может содержать значение "*", что означает, что необходимо исключить все контроллеры из логирования.
ActionName	Наименование экшена контроллера, который должен быть исключен из логирования. Так же может содержать значение "*" – это означает, что необходимо исключить все экшены контроллера из логирования.

Для применения изменений перезапустите приложение.

10.4 Описание конфигурационного файла redis.config

Таблица 29 – Описание конфигурационного файла redis.config

Атрибут	Описание значения
host	IP-адрес сервера, на котором развернут Redis
port	Порт
user	Имя пользователя Redis
password	Пароль пользователя Redis
connectRetry	Количества попыток подключения
connectTimeout	Время ожидания подключения

Пример конфигурационного файла redis.config:

```
<configuration>
<redis>
    <host>172.21.21.31</host>
    <port>6379</port>
    <user>default</user>
    <password>redispw</password>
    <connectRetry>3</connectRetry>
    <connectTimeout>5000</connectTimeout>
```

```
</redis>
</configuration>
```

10.5 Описание конфигурационного файла forms.service.json

Таблица 30 – Описание конфигурационного файла forms.service.json

Атрибут	Описание значения
FormEnginesConfig	Название секции, по которому web-приложение забирает параметры подключения к приложению сервиса
Engines	Список приложений сервиса, которые будут использованы web-приложением для работы пользователей с формами
Url	Url сервиса для обработки отчетных форм
FormsAvailable	true/false, указывает на возможность использования сервиса для работ с формами
AnalyticsAvailable	true/false, указывает на возможность использования сервиса для работ с выборками
HealthCheckIntervalInSeconds	Интервал в секундах. Определяет периодичность проверки доступности всех сервисов, указанных в url и количества открытых форм на каждом из них

Пример конфигурационного файла forms.service.json:

```
{
  "FormEnginesConfig" : {
    "Engines": [
      {
        "Url": "http://localhost:5050",
        "FormsAvailable": true,
        "AnalyticsAvailable": true
      },
      {
        "Url": "http://localhost:5051",
        "FormsAvailable": true,
        "AnalyticsAvailable": false
      },
      {
        "Url": "http://localhost:5052",
        "FormsAvailable": false,
        "AnalyticsAvailable": true
      }
    ],
    "HealthCheckIntervalInSeconds": 60
  }
}
```

10.6 Описание конфигурационного файла redis.json

Таблица 31 – Описание конфигурационного файла redis.json

Атрибут	Описание значения
host	IP-адрес сервера, на котором развернут Redis
port	Порт
user	Имя пользователя
password	Пароль пользователя

Примечание – В пароле недопустимы символы ", &, ', <, >, #,$.

Пример конфигурационного файла redis.json:

```
{
  "redis" : {
    "host": "172.21.21.31",
    "port": 6379,
    "user": "default",
    "password": "redispw"
  }
}
```

10.7 Описание конфигурационного файла postgres.json

Таблица 32 – Описание конфигурационного файла postgres.json

Атрибут	Описание значения
dbName	Имя БД
schemeName	Название схемы
formMetaSchemeName	Имя схемы postgres, в которой сервис форм найдет таблицы метаданных, необходимых для формирования представлений данных ОФ
showcaseDbUser	Имя пользователя postgres, для которого будут назначены права на select из представлений данных ОФ
host	IP-адрес сервера БД
port	Порт
login	Логин для авторизации в БД
password	Пароль
minPoolSize	Минимальный размер пула подключений
maxPoolSize	Максимальный размер пула подключений

Атрибут	Описание значения
connectionOpenTimeout	Время (в секундах) ожидания при попытке установить подключение, по истечении которого попытка подключения завершается и создается ошибка
executeCommandTimeout	Время (в секундах) ожидания выполнения команды, по истечении которого попытка выполнения команды завершается и создается ошибка
connectionIdleSeconds	Время (в секундах) ожидания простоя подключения
connectionPruningSeconds	Время (в секундах) ожидания перед попыткой удалить бездействующие соединения, срок действия которых истек
readBufferSize	Размер внутреннего буфера, который npgsql использует при чтении
writeBufferSize	Размер внутреннего буфера, который npgsql использует при записи

Пример конфигурационного файла postgres.json:

```
{
  "postgres": {
    "dbName":"test",
    "schemeName":"test_forms",
    "formMetaSchemeName": "test_forms",
    "host":"172.21.21.20",
    "port":5432,
    "showcaseDbUser": "user",
    "login":"test",
    "password":"123",
    "minPoolSize": 2,
    "maxPoolSize":50,
    "connectionOpenTimeout": 60,
    "executeCommandTimeout": 60,
    "connectionIdleSeconds": 300,
    "connectionPruningSeconds": 50,
    "readBufferSize": 524288,
    "writeBufferSize": 524288
  }
}
```

10.8 Описание конфигурационного файла metrics.json

Таблица 33 – Описание конфигурационного файла metrics.json

Атрибут	Описание значения
enabled	Флаг включения/выключения сервиса мониторинга (true - включен, false - выключен), позволяет включить/отключить сбор метрик во время работы приложения
port	Номер локального порта на сервере, где развернуто приложение, на котором будет доступна конечная точка с данными метрик в формате prometeus по url вида http://localhost:{port}/metrics

Пример конфигурационного файла metrics.json:

```
{
  "metrics": {
    "enabled": false,
    "port": 0
  }
}
```

10.9 Описание конфигурационного файла formsBackups.json

Таблица 34 – Описание конфигурационного файла formsBackups.json

Атрибут	Описание значения
maxFormBackupsCount	Максимальное количество резервных копий формы
maxFormAutoSaveCount	Максимальное количество автосохранений формы

Пример конфигурационного файла formsBackups.json:

```
{
  "formBackups": {
    "maxFormBackupsCount": 3,
    "maxFormAutoSaveCount": 3
  }
}
```

10.10 Описание конфигурационного файла aw.json

Таблица 35 – Описание конфигурационного файла aw.json

Атрибут	Описание значения
db	Название БД clickhouse AW
host	IP-адрес сервера clickhouse AW
port	Порт clickhouse
user	Имя пользователя clickhouse
password	Пароль пользователя clickhouse
baseUrl	url-ссылка на AW
adminLogin	Логин администратора AW
adminPassword	Пароль администратора AW

Пример конфигурационного файла aw.json:

```
{
  "aw": {
    "db": "default",
    "host": "172.21.21.33",
    "port": "9017",
    "user": "default",
    "password": "enter4z",
    "baseUrl": "https://aw.regname.ru",
    "adminLogin": "admin",
    "adminPassword": "123456"
  }
}
```

10.11 Описание файлов логирования

Файлы сохраняются в папку .logs, которая находится в корневой папке приложения, сервиса форм или дизайнера отчетных форм.

При возникновении потребности анализа логов или возникновении ошибок в ПП МЗ необходимо учесть:

- при возникновении ошибок при работе с отчетной формой, логи необходимо в первую очередь смотреть в сервисе форм;
- при возникновении ошибок во время сборки аналитических выборок, логи необходимо в первую очередь смотреть в сервисе форм, далее логи приложения;
- в любых других случаях в приложении.

Примечани - всегда стоит выгружать логи и из приложения, и из сервиса форм в случае работы с данными отчетных форм.

В каталогах формата «гггг-мм-дд» сохраняются файлы (на каждую дату создается отдельный каталог):

- debug.log – содержит информацию про кэш справочников, создание экземпляров фоновых процессов;
- errors.log – в файле фиксируются все ошибки при работе с ПП МЗ, кроме ошибок фоновых процессов;
- info.log – содержит информацию о старте и завершении работы приложения, о блокировке неактивных пользователей, об удалении результатов фоновых процессов, о запуске и завершении некоторых фоновых процессов, а также об ошибках компиляции макросов форм;

- trace.log – содержит информацию о начале и завершении сессии пользователей в ПП МЗ; логи при обновлении через root, при запуске приложения, при переносе данных в архив, при хранении вложений на диске, при скачивании архива ГАР, при работе с аналитическими выборками AW;
- userActionsMonitor.log – логи действий пользователя. Для формирования этого файла требуется конфигурационный файл, описанный в п. 10.3;
- printFormModule.log – информация о формировании печатных форм, в т.ч. об ошибках;
- formDataImportModule.log – информация об импорте отчетных форм;
- formDataExportModule.log – информация об экспорте отчетных форм;
- deadlineDateReminderModuleLogger.log – информация об ошибках в работе компонента «Напоминания о сроках сдачи»;
- checkModule.log – информация о формировании увязок в отчетных формах, в т.ч. об ошибках;
- summaryHandlerModule.log – информация об ошибках при сборе сводных в отчетных формах;
- formStatusModel.log – информация об ошибках при смене состояний отчетных форм;
- signatureModule.log – информация об ошибках при подписании отчетных форм;
- AW.log - в файле фиксируются все ошибки при авторизации в AW, при формировании аналитических выборок;
- authorization.log – информация об ошибках авторизации операторов в ПП МЗ;
- inactiveOperatorsBlocking.log – информация об операторах, которые были заблокированы вследствие их неактивности;
- blockingUserWithIrrelevantDate.log – информация об операторах, которые были заблокированы по окончании срока действия учетной записи или которые были разблокированы при наступлении срока действия учетной записи. Здесь также содержится информация об операторах, у которых были удалены временные роли вследствие окончания срока действия этой роли;

Отдельно в папке Quartz хранятся логи фоновых процессов. На каждую дату формируется отдельный файл, наименование которого имеет формат «гггг-мм-дд».

Для формирования логов используется файл NLog.config, который лежит в корне приложения.

NLog.config содержит следующие секции variable, targets и rules.

Секция <variable> определяет переменную конфигурации с заданным именем. Значение этой переменной - это шаблон, который определяет, как должны выглядеть записи в журнале.

Пример определения переменной "layout" в NLog.config .

```
<variable name="layout"
value="${longdate}|${level:uppercase=true}|${logger}|${message}
${exception:format=tostring,stacktrace:separator=*}" />
```

В значение переменной layout определяет следующий шаблон записи:

Атрибут	Описание значения
${longdate}	Дата и время записи
${level:uppercase=true}	Уровень логирования в верхнем регистре
${logger}	Имя логера
${message}	Сообщение об ошибке
${exception:format=tostring}	Исключение
${stacktrace:separator=}	Стек вызовов с разделителем

Секция <targets> является контейнером для элементов <target>. Он определяет различные места, в которые может быть записана информация о логе.

Пример секции <targets> в NLog.config.

Секция <targets>

```
<targets>
  <target name="trace-logfile" xsi:type="File"
fileName="${basedir}/.logs/${shortdate}/trace.log" encoding="utf-8"
layout="${layout}" />
  ...
  <target name="main-module" xsi:type="File"
fileName="${basedir}/.logs/${shortdate}/mainData.log" encoding="utf-8"
layout="${layout}" />
</targets>
```

Данная секция <targets> содержит несколько целей <target>. Например последняя секция <target> определяет цель для журналирования под названием "main-module", у которой тип файла определяется как "File". В атрибуте fileName указан путь до расположения файла лога. Этот путь состоит из следующих атрибутов:

Атрибут	Описание значения
${basedir}/	Текущая директория
.logs/	Папка .logs
${shortdate}/	Папка с наименованием текущей короткой даты
mainData.log	Имя файла лога

Кодировка файла установлена в "utf-8". В атрибут layout передана переменная "layout", которая была определена выше в секции <variable> и определяет формат записей в журнале.

Секция <rules> является контейнер для правил логирования.

Пример секции <rules> в NLog.config

```
<rules>
    <logger name="WebUpdater" writeTo="web-updater" final="true"
>
      <filters defaultAction="Log">
        <when condition="level != LogLevel.Trace" action="Ignore"
/>
      </filters>
    </logger>
    ...
    <logger name="MainLogger" writeTo="main-module" final="true">
      <filters defaultAction="Log">
        <when condition="level < LogLevel.Error" action="Ignore"
/>
      </filters>
    </logger>

    <logger name="*" level="Trace" writeTo="trace-logfile" />
    <logger name="*" level="Debug" writeTo="debug-logfile" />
    <logger name="*" level="Info" writeTo="info-logfile"  />
    <logger name="*" level="Warn" writeTo="warn-logfile"  />
    <logger name="*" level="Error" writeTo="error-logfile" />
    <logger name="*" level="Fatal" writeTo="fatal-logfile" />
```

```
</rules>
```

Данная секция <rules> содержит несколько секцией <logger>. Например, есть секция, которая определяет логгер с именем "MainLogger". Этот логгер будет писать сообщения в target с именем "main-module", который определен выше в секции <targets>. Значение "final" равное "true", означает, что сообщения, записанные в этот логгер, не будут перенаправляться на другие target'ы. Для данного логгера задан фильтр с условием и если это условие истинно, то результатом работы фильтра будет значение, указанное в атрибуте action, в данном случае все записи MainLogger уровня ниже, чем Error не будут записаны.

В самом конце секции <rules> определены логгеры, которые записывают сообщения в файлы в зависимости от уровня. Символ "*" означает произвольную последовательность символов. Например, логи уровня "Info" будут записываться в target с именем "info-logfile", который определен выше в секции <targets> и пишет логи в файл info.log

11 Настройка сервиса пересылки сообщений

В ПП МЗ реализован сервис пересылки сообщений (пользовательских и сгенерированных ПП МЗ) на электронную почту, указанную в карточках операторов. Сервис разворачивается как самостоятельное web-приложение. Исходный код сервиса является частью ПП МЗ.

Сервис содержит несколько конфигурационных файлов, которые необходимо поправить после его разворачивания:

- connection.config. Конфигурационный файл предназначен для указания подключения к БД приложения ПП МЗ. Сервис напрямую из БД получает сообщения для отправки на почту пользователей.

Пример с расшифровкой значения секций:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <!-- dbDialect - тип СУБД, значение: Npgsql-->
    <!-- userName - имя пользователя БД-->
    <!-- password - пароль пользователя БД-->
    <!-- host - ip-адрес сервера БД-->
    <!-- port - порт сервера БД-->
    <!-- dbName - наименование БД-->
    <Connection>
        <DbDialect>Npgsql</DbDialect>
        <UserName>имяСхемы</UserName>
        <Password>парольОтСхемы</Password>
        <Host>IPСервераБД</Host>
        <Port>портБД</Port>
        <DbName>имяБД</DbName>
    </Connection>
</configuration>
```

- messengerService.config. Конфигурационный файл предназначен для указания настроек к серверу почтовой рассылки. ПП МЗ поддерживает работу с двумя типами - ews и smtp.

Пример:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <!-- Способ работы с сообщениями. Возможные значения: ews,
smtp -->
    <MailServiceType>типСервиса</MailServiceType>

    <Ews>
        <MailFrom>out@svody.local</MailFrom>
        <User>7880</User>
        <Password>N0725369</Password>
```

```
            <Url>https://emailserver.ru/EWS/Exchange.asmx</Url>
            <Timeout>10000</Timeout>
            <ExchangeVersion>Exchange2010</ExchangeVersion>
        <SendHtml>false</SendHtml>
        </Ews>

        <Smtp>
            <MailFrom>out@svody.local</MailFrom>
            <Host>localhost</Host>
            <Port>25</Port>
            <Timeout>10000</Timeout>
            <SslEnabled>false</SslEnabled>
            <LoginFrom>out@svody.local</LoginFrom>
            <PasswordFrom>123</PasswordFrom>
            <DelSendedMessage>true</DelSendedMessage>
            <WithAttachments>true</WithAttachments>
        <SendHtml>false</SendHtml>
        </Smtp>
    </configuration>
```

В таблице ниже представлены дополнительные параметры по отправке сообщений (Таблица 36).

Таблица 36 – Параметры отправки сообщений

Параметр	Описание	Возможные значения
DelSendedMessage	Необходимость удаления сообщения из ПП МЗ после отправки их на электронную почту	true/false
WithAttachments	Необходимость отправки вложений на электронную почту. Ограничения: к отправке доступны файлы форматов .doc, .docx, .pdf, .zip не больше 3 МБ	true/false
SendHtml	Необходимость отправки сообщения с тем же форматированием, что было задано в ПП МЗ	true/false

Для просмотра версии MessengerService перейдите на страницу сервиса, указав endpoint – «/version», возвращающий номер версии сборки (Рисунок 13).

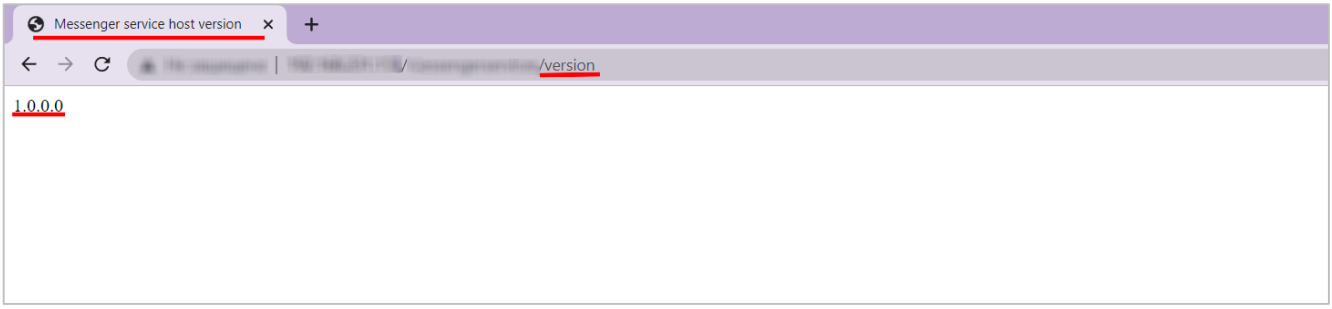


Рисунок 13 – Вывод на странице MessengerService номера сборки

11.1 Настройка сервиса пересылки сообщений на Linux-сервере

Порядок разворачивания экземпляра web-приложения сервиса на Linux-сервере:

Примечание – Ниже описывается первоначальная настройка только что установленной ОС Linux. Для работы сервиса под Linux может использоваться любой web-сервер, в котором есть режим ReverseProxy. Для удобства все команды выполняются от пользователя root.

- установите .NET 6.0 на Linux, перейдя по ссылке https://docs.microsoft.com/ru-ru/dotnet/core/install/linux. Выберите необходимый дистрибутив в списке, соответствующий вашей ОС. Выполните действия по установке, указанные в открывшейся инструкции;
- создайте папку под приложение:

```
mkdir /var/www/messengerservice
```

- скопируйте приложение в папку /var/www/messengerservice;
- добавьте пользователя: useradd messengerservice;
- добавьте пользователю права на папку:

```
chown -R messengerservice.
/var/www/messengerservice;
```

- создайте сервис:

```
cat > /etc/systemd/system/messengerService.service <<EOF
#/etc/systemd/system/messengerService.service
[Unit]
Description = Bars messengerService
[Service]
WorkingDirectory = /var/www/messengerservice
ExecStart = /usr/bin/dotnet
/var/www/messengerservice/BARS.MessengerService.Host.dll
Restart = always
RestartSec = 10
SyslogIdentifier = bars_messengerService
User = messengerservice
```

```
Environment = ASPNETCORE_ENVIRONMENT=Production
ASPNETCORE_URLS=http://127.0.0.1:5000
ASPNETCORE_BASEPATH=/messengerservice
[Install]
WantedBy = multi-user.target
EOF
```

– измените параметры подключения к базе в конфигурационном файле /var/www/messengerservice/connection.config;

– измените настройки отправки сообщений в конфигурационном файле /var/www/messengerservice/messengerService.config;

– запустите сервис и добавьте его в автозагрузку:

```
systemctl daemon-reload
systemctl start messengerService
systemctl enable messengerService
```

Проверить статус можно командой

```
systemctl status messengerService
```

При правильных настройках вывод команды `netstat -tuwpln | grep dotnet` будет выглядеть, как на рисунке ниже (Рисунок 14):

```
[root@forwork messengerservice]# netstat -tuwpln | grep dotnet
tcp        0      0 127.0.0.1:5000          0.0.0.0:*               LISTEN      8506/dotnet
```

Рисунок 14 – Вывод команды

– в качестве ReverseProxy используйте Nginx;

– в каталоге /etc/nginx/default.d/ создайте конфигурационный файл для сервиса messengerService.conf со следующим содержанием:

```
location /messengerservice {
 proxy_pass http://127.0.0.1:5000/messengerservice;
 proxy_http_version 1.1;
 proxy_set_header Upgrade $http_Upgrade;
 proxy_set_header Host $Host;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 proxy_set_header X-Forwarded-Proto $scheme;
 proxy_cache_bypass $http_upgrade;
}
```

– перезагрузите конфигурацию Nginx, чтобы применить изменения:

```
nginx -s reload;
```

12 Настройка дизайнера отчетных форм

Дизайнер отчетных форм предназначен для создания и актуализации отчетных форм, используемых в ПП МЗ.

Чтобы дизайнер отчетных форм работал корректно, после разворота приложения на web-сервере выполните уникальные настройки для ПП МЗ.

а) в приложении ПП МЗ в файле «svody.config» в секции <Svody.Designer> укажите URL приложения «Дизайнер»;

```
<Svody.Designer>
    <!--
      Name - наименование подключения (значение обязательное, уникальное)
      Url - ссылка на приложение дизайнер
      SortOrder - порядок обращения по ссылкам, чем меньше SortOrder - тем раньше при установке соединения с дизайнером будет использована ссылка
      Пример:
      <Entry Name="primary" Url="https://192.168.0.2/designer" SortOrder="0"/>
      <Entry Name="secondary" Url="https://domain.name.ru/designer" SortOrder="1"/>
      При такой настройке сначала произойдет попытка авторизации по ссылке https://192.168.0.2/designer, в случае неудачи - произойдет попытка авторизации по ссылке https://domain.name.ru/designer.
      Количество ссылок не ограничено.
    -->
    <Entry Name="primary" Url="" SortOrder="0"/>
</Svody.Designer>
```

В параметре URL указывается ссылка на Дизайнер отчетных форм, по которой он будет открываться у конечного пользователя. Можно указать несколько ссылок, тогда попытка перехода будет осуществляться по всем ссылкам по очереди в порядке приоритетности, пока ПП МЗ не сможет подключиться.

б) скопируйте файл «Приложение.барс» из приложения ПП МЗ, чтобы оба приложения подключались на одни и те же сервер и схему.

Примечание – Лицензия на ПП МЗ должна стоять с доступом к Дизайнеру отчетных форм.

12.1 Настройка дизайнера отчетных форм на сервере Linux

Порядок разворачивания дизайнера отчетных форм на Linux:

– распакуйте архив с дистрибутивом приложения «Дизайнер» любой удобной утилитой;

Пример для архива, сохраненного в каталоге home:

```
tar -xvf designer.tar.gz
```

- создайте каталог, из которого будет работать приложение «Дизайнер»;

Пример каталога:

```
mkdir /opt/designer
```

- переместите все распакованные файлы в созданный каталог;
- скопируйте файл «Приложение.барс» из каталога приложения ПП МЗ, либо заполните его точно так же, как он заполнен в приложении ПП МЗ;

Пример – Если папка приложения ПП МЗ находится по адресу /opt/svody, а приложение «Дизайнер» по адресу /opt/designer, то:

cp /opt/svody/Приложение.барс /opt/designer/

cat /opt/designer/Приложение.барс

- создайте сервис:

```
vi /etc/systemd/system/designer.service
```

- заполните файл как указано ниже, заменив «ПОРТ» на свободный, который будет в дальнейшем использоваться для приложения «Дизайнер»:

```
[Unit]
Description = Svody designer app: designer
[Service]
User = root
WorkingDirectory = /opt/designer
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:ПОРТ
Environment = ASPNETCORE_BASEPATH=/designer
Environment = TMPDIR=/var/tmp
Environment = SSL_CERT_DIR=/etc/ssl/certs/
Environment = LD_LIBRARY_PATH=/opt/cprocsp/cp-openssl-
1.1.0/lib/amd64/
ExecStart = /usr/bin/dotnet
/opt/designer/Svody.Designer.Web.Host.dll
SyslogIdentifier = svody-designer
Restart = always
RestartSec = 10
[Install]
WantedBy = multi-user.target
```

- измените не только порт, но и параметры, перечисленные ниже:
  - User = root – user, от которого будет работать приложение;
  - WorkingDirectory = /opt/designer – директория приложения, куда поместили файлы приложения;

- Environment = ASPNETCORE_URLS=http://0.0.0.0:5002 – порт, который указан выше;
- Environment = ASPNETCORE_BASEPATH=/designer – путь до приложения, но уже короткий;
- ExecStart = /usr/bin/dotnet /opt/designer/Svody.Designer.Web.Host.dll – путь до dll приложения;
- SyslogIdentifier = svody-designer – то, как будет указываться приложение в логах.

Пример:

```
[Unit]
Description = Svody designer app: designer
[Service]
User = root
WorkingDirectory = /opt/designer
Environment = ASPNETCORE_ENVIRONMENT=Production
Environment = ASPNETCORE_URLS=http://0.0.0.0:5002
Environment = ASPNETCORE_BASEPATH=/designer
Environment = TMPDIR=/var/tmp
Environment = SSL_CERT_DIR=/etc/ssl/certs/
Environment = LD_LIBRARY_PATH=/opt/cprocsp/cp-openssl-
1.1.0/lib/amd64/
Environment=ASPNETCORE_USE_XFORWARDEDFOR=true
ExecStart = /opt/designer/Svody.Designer.Web.Host
SyslogIdentifier = svody-designer
Restart = always
RestartSec = 10
[Install]
WantedBy = multi-user.target
```

- после редактирования файла выполните:

```
systemctl daemon-reload
```

- создайте файл конфигурации для приложения «Дизайнер»;

Пример файла конфигурации для приложения «Дизайнер» – nginx:

```
vi /etc/nginx/conf.d/designer.conf
```

Примечание – Если папка nginx отличается, или их несколько, можно завести в папке /etc/nginx/default.d/.

- заполните файл как указано ниже, заменив «ПОРТ» на порт, который был указан выше при создании сервиса:

```
location /designer {
    client_max_body_size  500M;
    proxy_pass   http://0.0.0.0:ПОРТ/designer;
    proxy_http_version   1.1;
```

```
          proxy_set_header    Upgrade $http_Upgrade;
          proxy_set_header    Host $Host;
          proxy_set_header    X-Forwarded-For
$proxy_add_x_forwarded_for;
          proxy_set_header    X-Forwarded-Proto $scheme;
          proxy_cache_bypass   $http_upgrade;
          proxy_send_timeout   600s;
          proxy_read_timeout   600s;
       }
```

– предоставьте права на выполнение файлу:

```
chmod +x /opt/designer/Svody.Designer.Web.Host
chmod +x /opt/designer/Svody.Designer.Web.Host.dll
```

Примечание – Помимо выдачи прав пользователю root на папку и файлы указанных выше, требуется еще выдача прав соответствующему пользователю, от которого запускается приложение Дизайнера.

– запустите сервис:

```
systemctl start designer.service
```

– перечитайте конфиг nginx, чтобы применились добавленные настройки:

```
systemctl reload nginx
```

– проверьте работоспособность приложения:

```
systemctl status designer.service
```

В случае правильной настройки у пользователей приложения ПП МЗ, имеющих права «Администратор», будет доступ к приложению «Дизайнер».

13 Настройка Keycloak

Для разворачивания и русификации Keycloak предварительно установите java (версию java-8-openjdk-amd64) и postgres. В postgres создайте базу Keycloak под пользователем «postgres».

Загрузите Keycloak 17.0.1 с официального сайта либо воспользуйтесь запрошенным дистрибутивом.

Распакуйте в /opt/keycloak и выдайте права на sh-скрипты директории /opt/keycloak/bin.

Создайте директорию для модуля драйвера postgres: /opt/keycloak/modules/system/layers/keycloak/org/postgresql/main/.

Загрузите в директорию postgresql-вашаВерсия.jar (передается вместе с дистрибутивом) и создайте там конфигурационный файл module.xml со следующим содержанием:

```
<?xml version="1.0" ?>
<module xmlns="urn:jboss:module:1.3" name="org.postgresql">
    <resources>
        <resource-root path="postgresql-вашаВерсия.jar"/>
    </resources>
    <dependencies>
        <module name="javax.api"/>
        <module name="javax.transaction.api"/>
    </dependencies>
</module>
```

Создайте файл сервиса /etc/systemd/system/keycloak.service со следующим содержанием:

```
[Unit]
Description=Jboss Application Server
After=network.target

[Service]
Type=idle
User=root
Group=root
ExecStart=/opt/keycloak/bin/standalone.sh -b 0.0.0.0
TimeoutStartSec=600
TimeoutStopSec=600

[Install]
WantedBy=multi-user.target
```

Далее измените конфигурационный файл самого Keycloak по пути /opt/keycloak/standalone/configuration/standalone.xml, а именно следующие секции datasources:

```
                <datasources>
                    <datasource jndi-
name="java:jboss/datasources/ExampleDS" pool-name="ExampleDS"
enabled="true" use-java-context="true" statistics-
enabled="${wildfly.datasources.statistics-enabled:${wildfly.statistics-
enabled:false}}">
                            <connection-
url>jdbc:h2:mem:test;DB_CLOSE_DELAY=-
1;DB_CLOSE_ON_EXIT=FALSE</connection-url>
                            <driver>h2</driver>
                            <security>
                                <user-name>sa</user-name>
                                <password>sa</password>
                            </security>
                        </datasource>
                        <datasource  jndi-
name="java:jboss/datasources/KeycloakDS"  pool-name="KeycloakDS"
enabled="true"  use-java-context="true">
                           <connection-
url>jdbc:postgresql://localhost:5432/keycloak</connection-url>
                            <driver>postgresql</driver>
                               <pool>
                                    <max-pool-size>20</max-pool-size>
                               </pool>
                                    <security>
                                       <user-name>postgres</user-
name>

<password>парольОтPostgres</password>
                                    </security>
                           </datasource>
                       <drivers>
                            <driver  name="postgresql"
module="org.postgresql">
                                    <xa-datasource-
class>org.postgresql.xa.PGXADataSource</xa-datasource-class>
                            <driver name="h2" module="com.h2database.h2">
                                    <xa-datasource-
class>org.h2.jdbcx.JdbcDataSource</xa-datasource-class>
                            </driver>
                       </drivers>
                </datasources>
```

Настройки интерфейса для внешнего доступа:

```
<interfaces>
<interface  name="management">
<inet-address value="0.0.0.0"/>
</interface>
```

```
<interface  name="public">
<inet-address value="0.0.0.0"/>
</interface>
</interfaces>
```

Добавьте пользователя скриптом:

```
/opt/keycloak/bin/add-user-keycloak.sh -u имя -p пароль
```

Запустите сервис:

```
systemctl start keycloak
```

14 Настройка авторизации

ПП МЗ поддерживает несколько видов авторизации:

- стандартная авторизация по паре логин / пароль;
- авторизация по протоколу OpenID;
- авторизация по протоколу LDAP для ОС Astra Linux Special Edition (Смоленск).

Способ авторизации настраивается в конфигурационном файле svody.config в секции <Bars.Authorization>. Существует возможность комбинировать способы авторизации.

Примечания

1 Для работы Компонента анализа данных должна использоваться либо авторизация по протоколу OpenID, либо авторизация по протоколу LDAP.

2 Совместное использование авторизации по протоколу OpenID и авторизации по протоколу LDAP невозможно.

14.1 Настройка для работы с OpenID Connect

В ПП МЗ предусмотрена возможность авторизации по протоколу OpenID Connect (Далее OpenID), то есть входа через пару логин/пароль сторонней системы (далее – SSO). Выполните настройку как самой SSO, так и приложения ПП МЗ в svody.config. После успешной настройки на главной странице авторизации приложения ПП МЗ отобразится кнопка, позволяющая выполнить вход с парой логин/пароль другой системы. Реализована функциональность подключения нескольких способов авторизации, а также совмещение авторизации по умолчанию и авторизации по OpenID.

14.1.1 Настройка BarsUP.AM для работы по OpenID

Порядок настройки:

а) разверните и настройте BarsUP.AM (в соответствии с инструкцией, предоставленной вместе с дистрибутивами продукта);

б) настройте сетевую связность между приложением BarsUP.AM и ПП МЗ;

в) авторизуйтесь под администратором в BarsUP.AM и перейдите в раздел «Системы» для регистрации ПП МЗ (Рисунок 15);

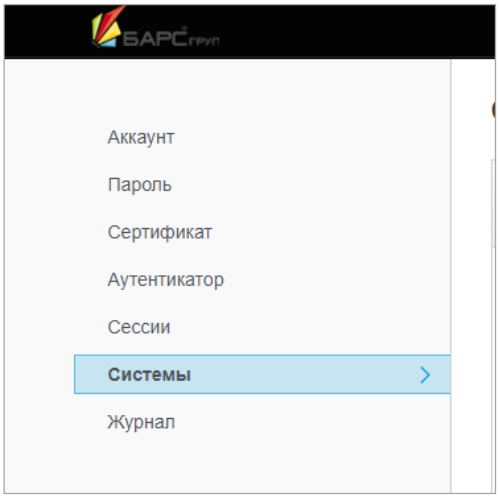


Рисунок 15 – BarsUP.AM. Раздел «Системы»

г) в разделе «Системы» найдите пункт «Административная консоль» и нажмите на него (Рисунок 16);

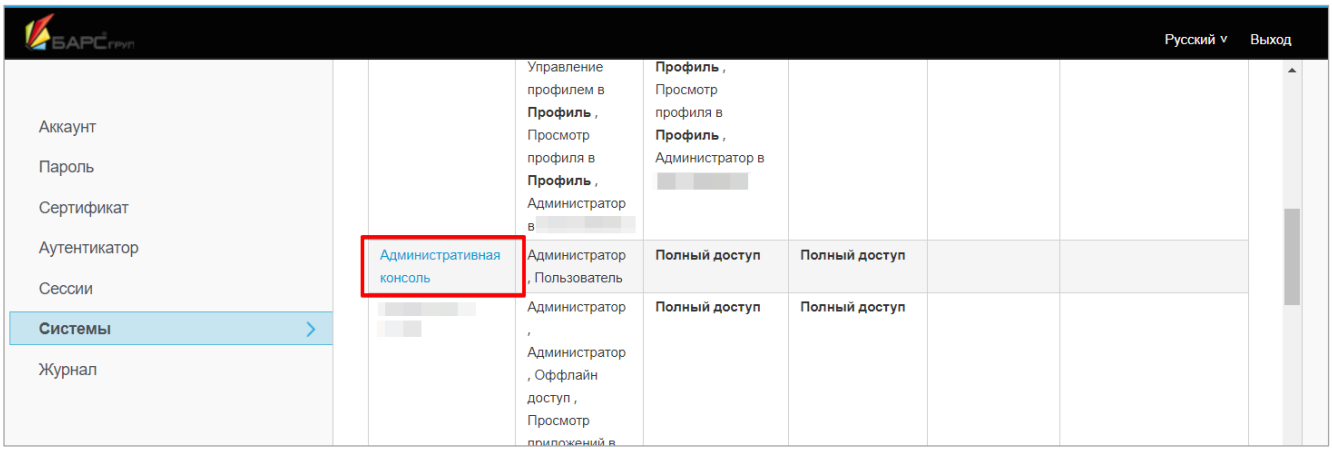


Рисунок 16 – BarsUP.AM. Раздел «Системы». Пункт «Административная консоль»

д) в административной консоли выберите пункт «Системы» в выпадающем списке слева (Рисунок 17);

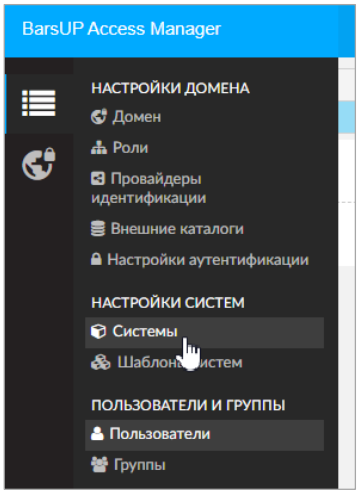


Рисунок 17 – BarsUP.AM. Административная консоль

е) в разделе «Системы» нажмите кнопку «Создать» (Рисунок 18);

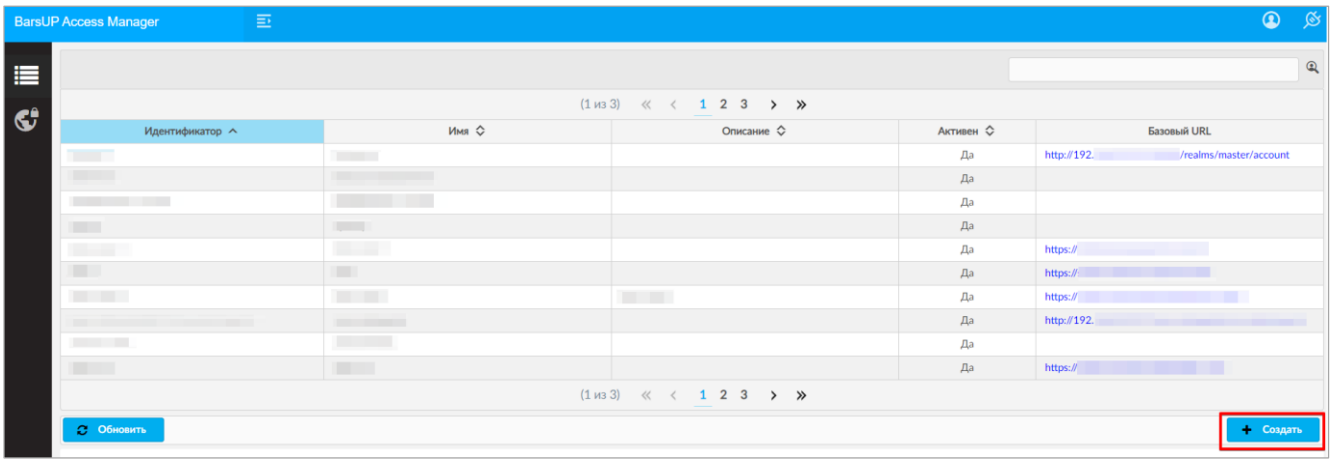


Рисунок 18 – BarsUP.AM. Раздел «Системы»

ж) в открывшемся окне «Создание информационной системы» укажите:

- уникальный идентификатор;
- имя (может совпадать с идентификатором);
- описание (необязательно);
- протокол «openid-connect»;
- корневой URL ПП МЗ.

з) нажмите кнопку «Создать» (Рисунок 19);

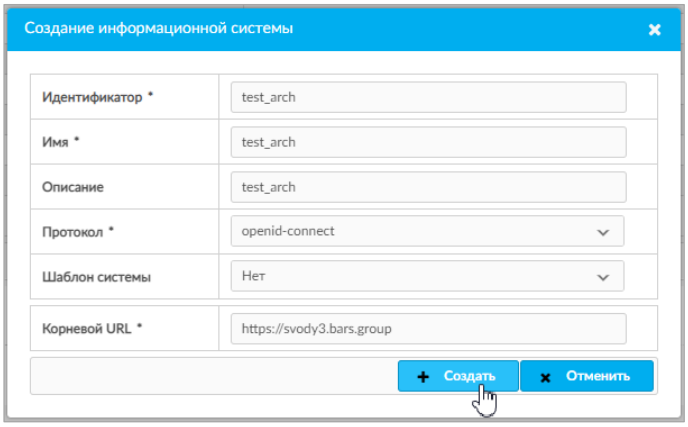


Рисунок 19 – BarsUP.AM. Окно «Создание информационной системы»

и) после создания информационной системы ее необходимо настроить. Для этого нажмите кнопку «Изменить» (Рисунок 20);

Рисунок 20 – BarsUP.AM. Пример создания информационной системы

к) установите в полях следующие значения (Рисунок 21):

- «Обязательность согласия» – «Да»;
- «Тип доступа» – «confidential»;
- «Разрешен Standard Flow» – «Да»;
- «Разрешен Direct Access Grants» – «Да»;
- «Тип аутентификатора» – Идентификатор клиента + секретный ключ;
- «Разрешенные URL для redirect» – (/*) – для тестирования; (/signin-oidc) – для продуктового приложения;
- «Базовый URL» – "/" + Корневой URL;
- «Web Origins» – корневой URL (URL, Разрешенные для CORS);

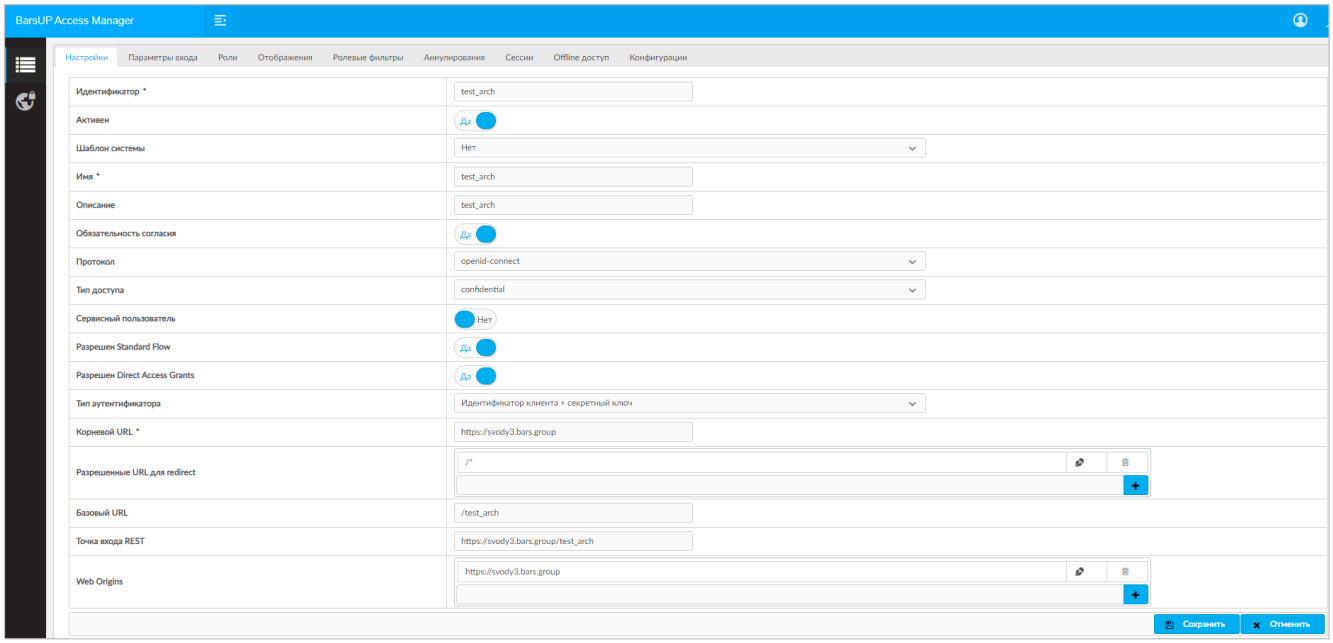


Рисунок 21 – BarsUP.AM. Пример настроенной информационной системы

л) нажмите кнопку «Сохранить» (см. Рисунок 21);

м) перейдите во вкладку «Отображения» (см. Рисунок 21) и добавьте следующие отображения: email (Рисунок 22, Рисунок 23), family name (Рисунок 24, Рисунок 25), full name (Рисунок 26, Рисунок 27), given name (Рисунок 28, Рисунок 29), middle name (Рисунок 30, Рисунок 31), username (Рисунок 32, Рисунок 33);

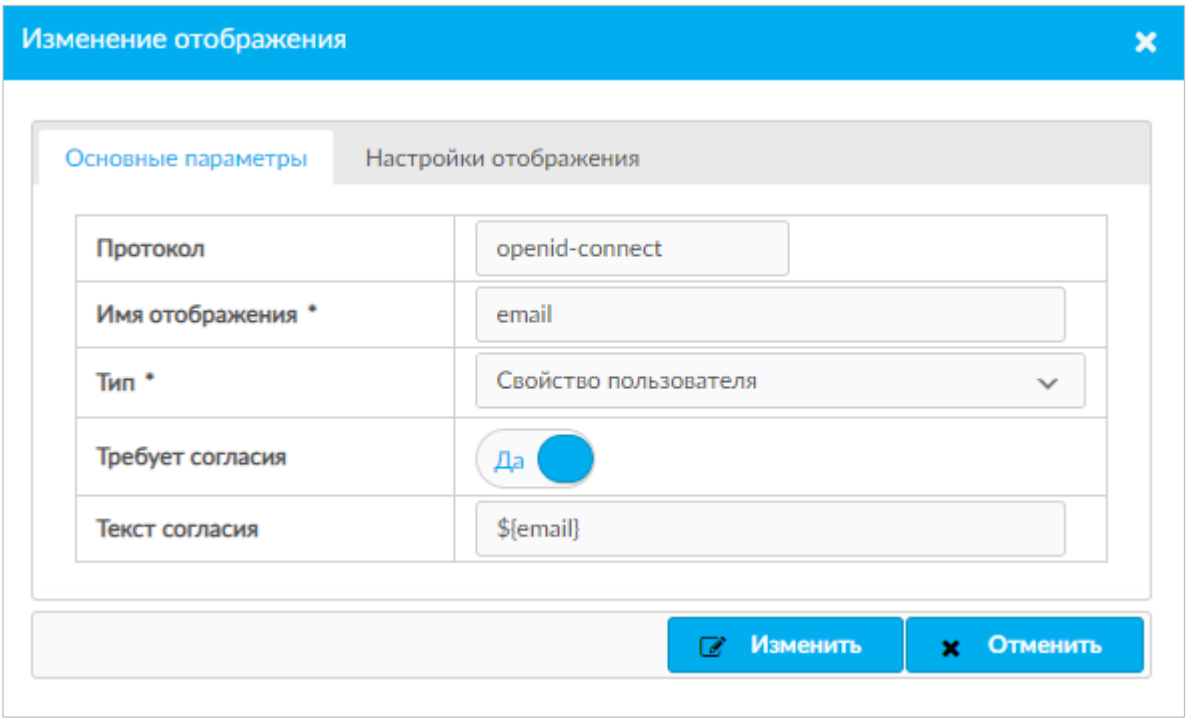


Рисунок 22 – BarsUP.AM. Основные параметры отображения email

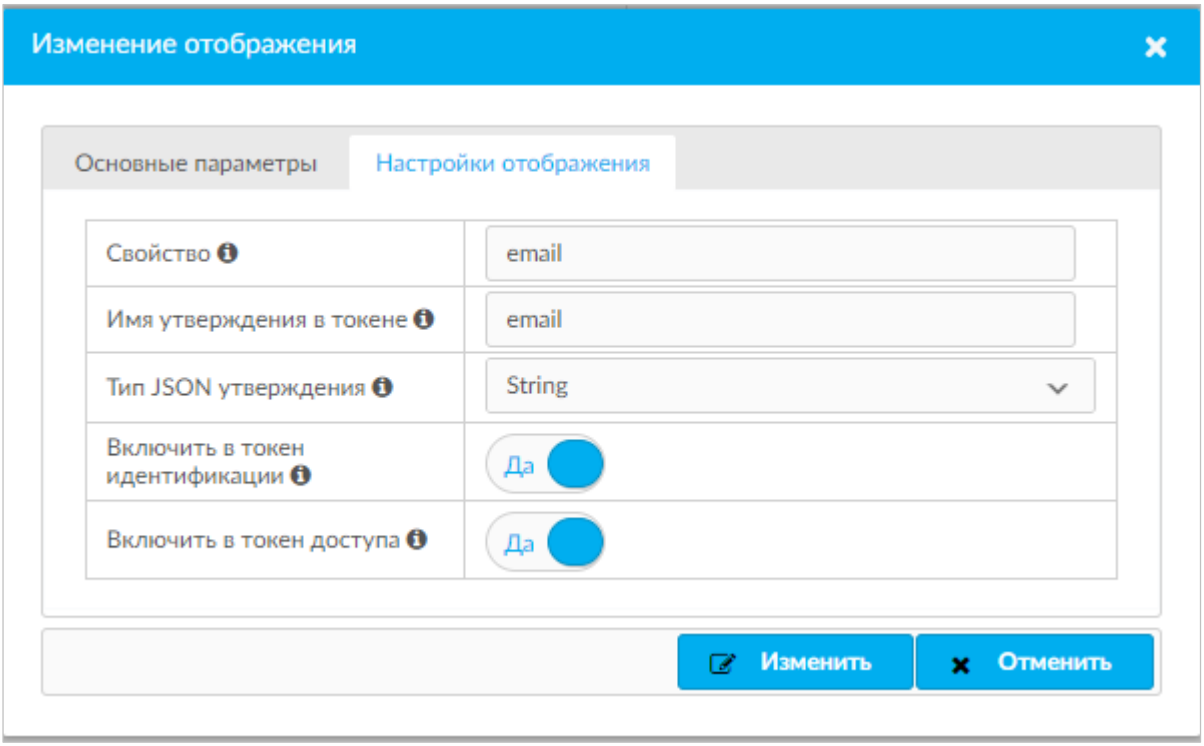


Рисунок 23 – BarsUP.AM. Настройки отображения email

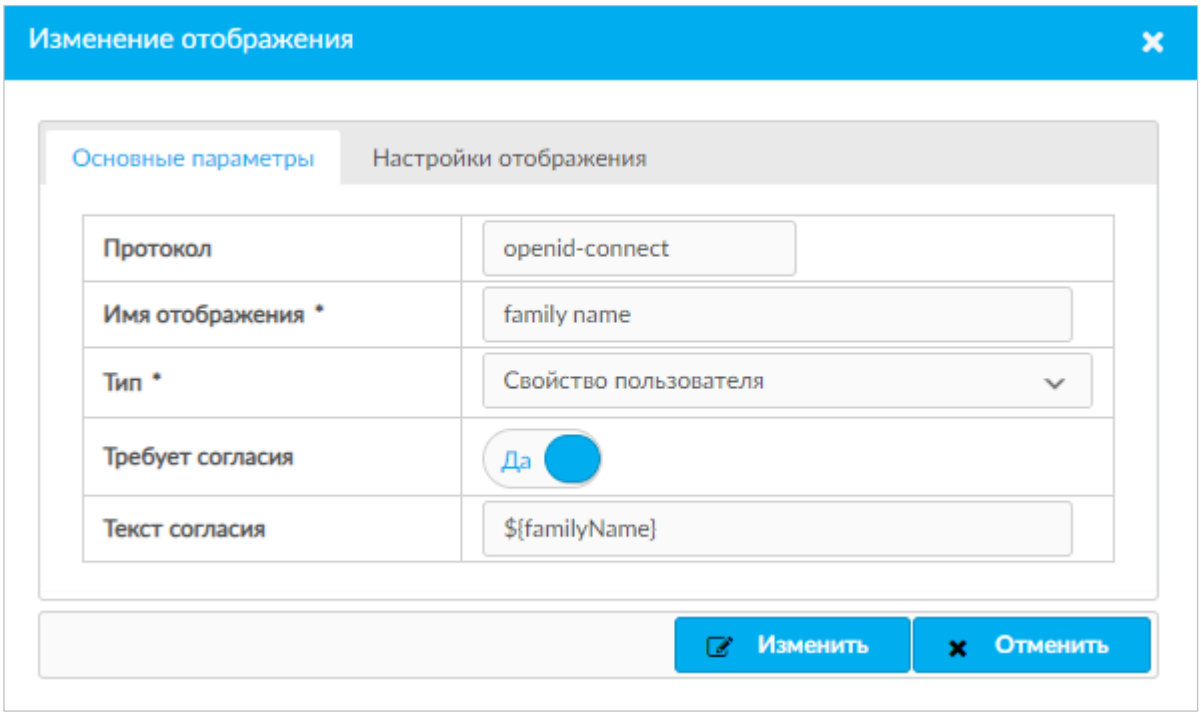


Рисунок 24 – BarsUP.AM. Основные параметры отображения family name

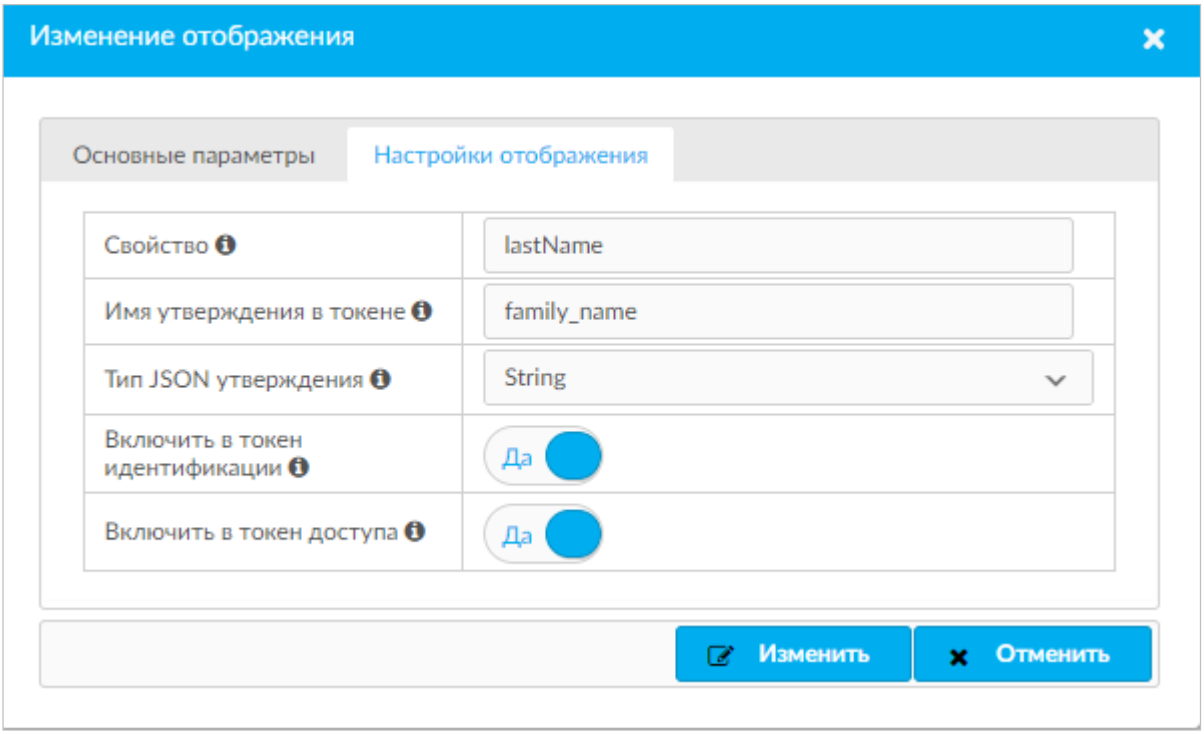


Рисунок 25 – BarsUP.AM. Настройки отображения family name

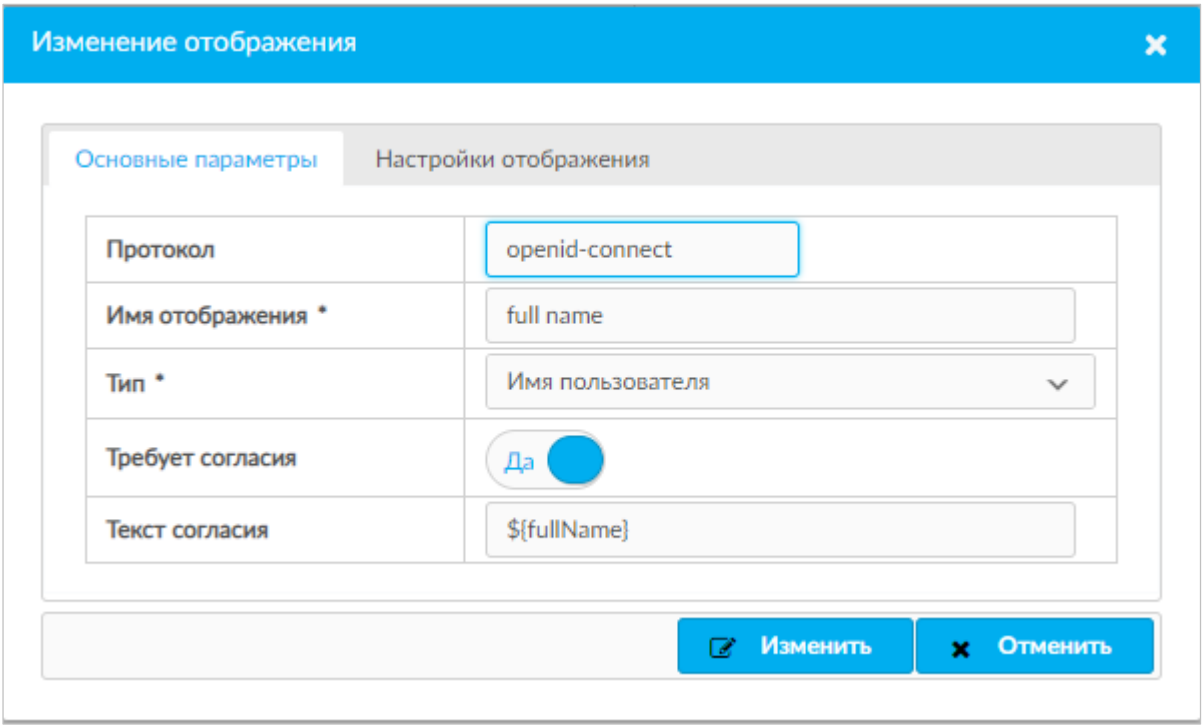


Рисунок 26 – BarsUP.AM. Основные параметры отображения full name

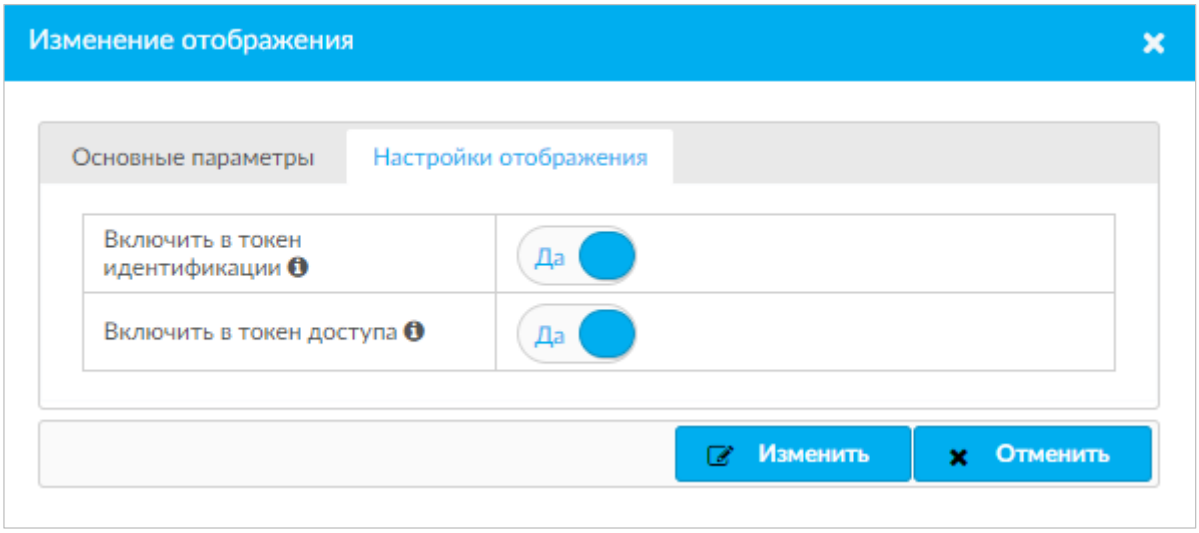


Рисунок 27 – BarsUP.AM. Настройки отображения full name

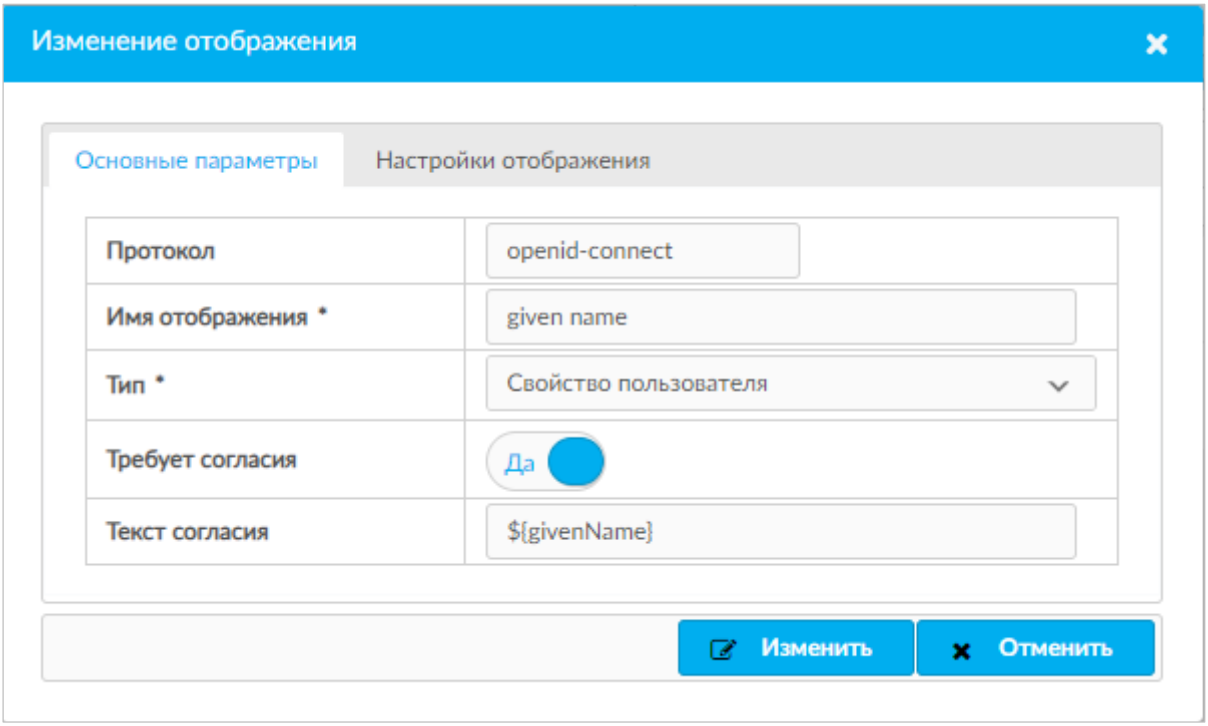


Рисунок 28 – BarsUP.AM. Основные параметры отображения given name

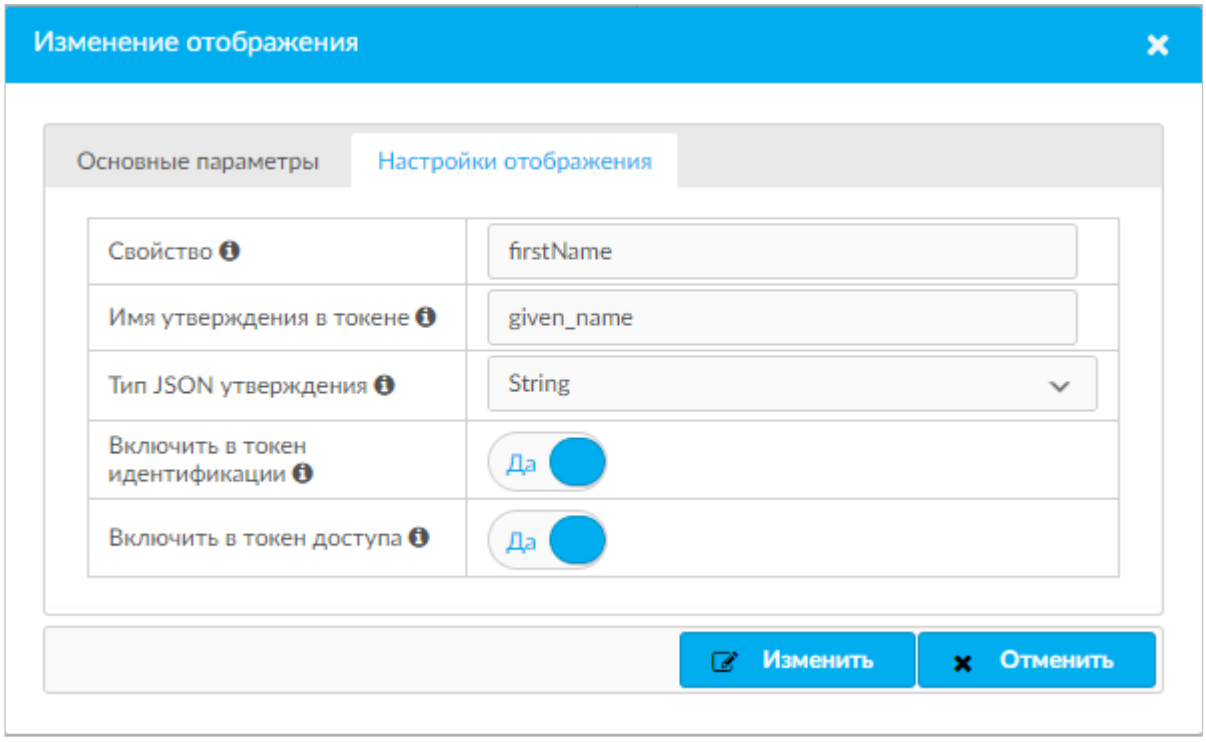


Рисунок 29 – BarsUP.AM. Настройки отображения given name

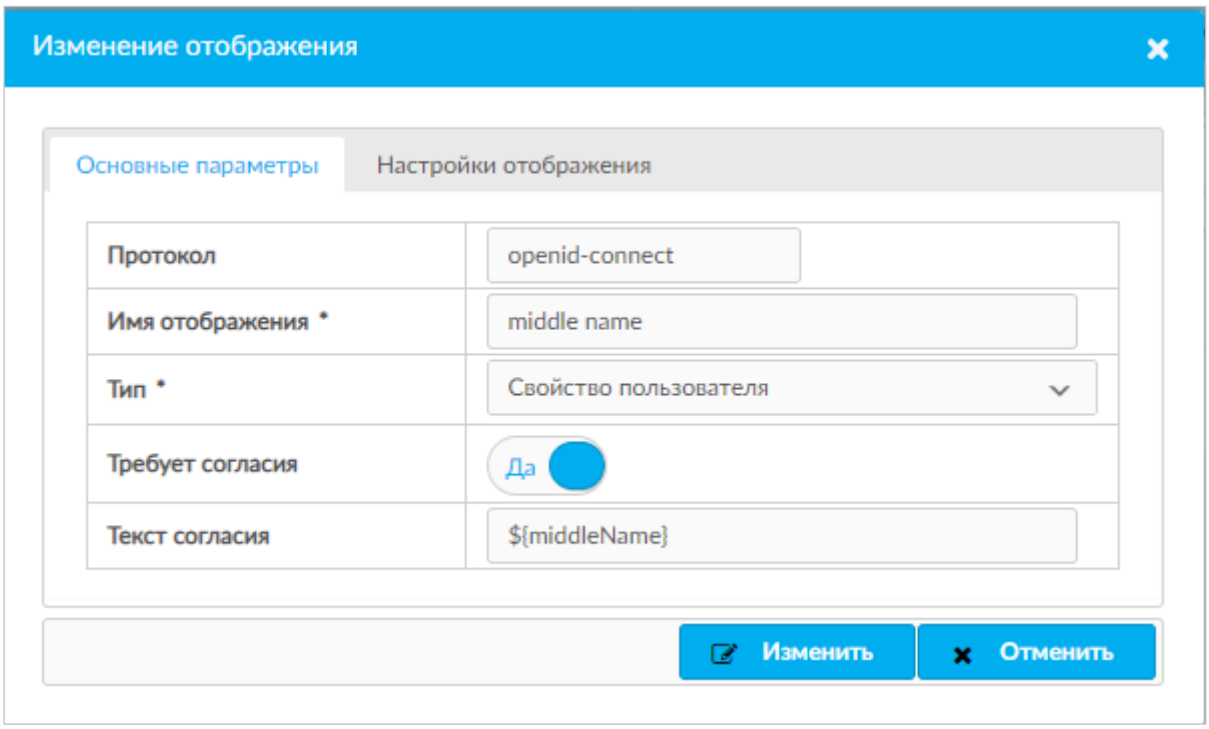


Рисунок 30 – BarsUP.AM. Основные параметры отображения middle name

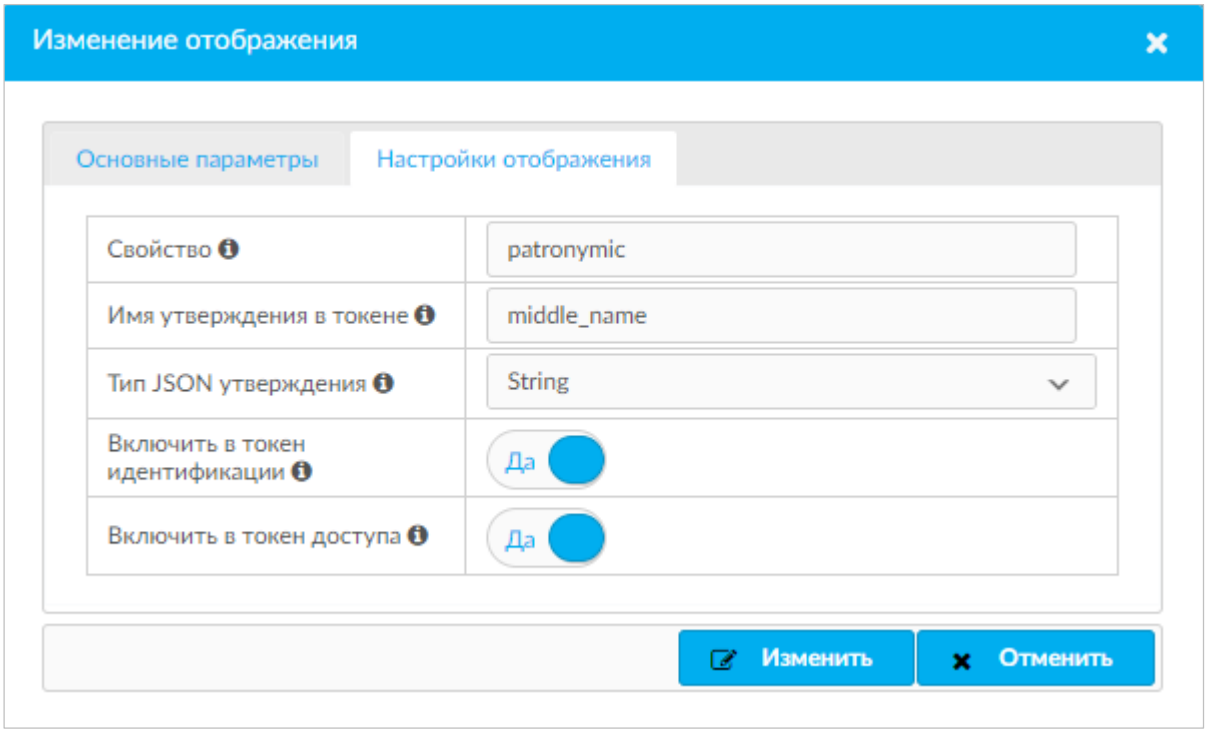


Рисунок 31 – BarsUP.AM. Настройки отображения middle name

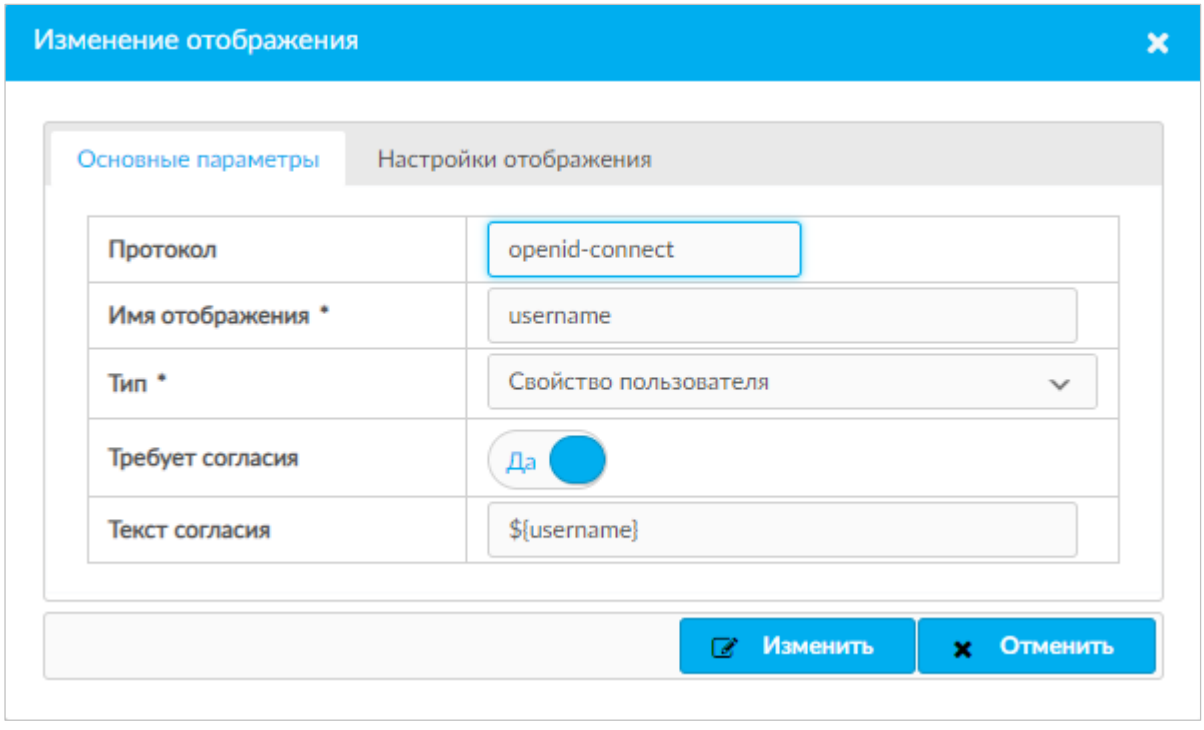


Рисунок 32 – BarsUP.AM. Основные параметры отображения username

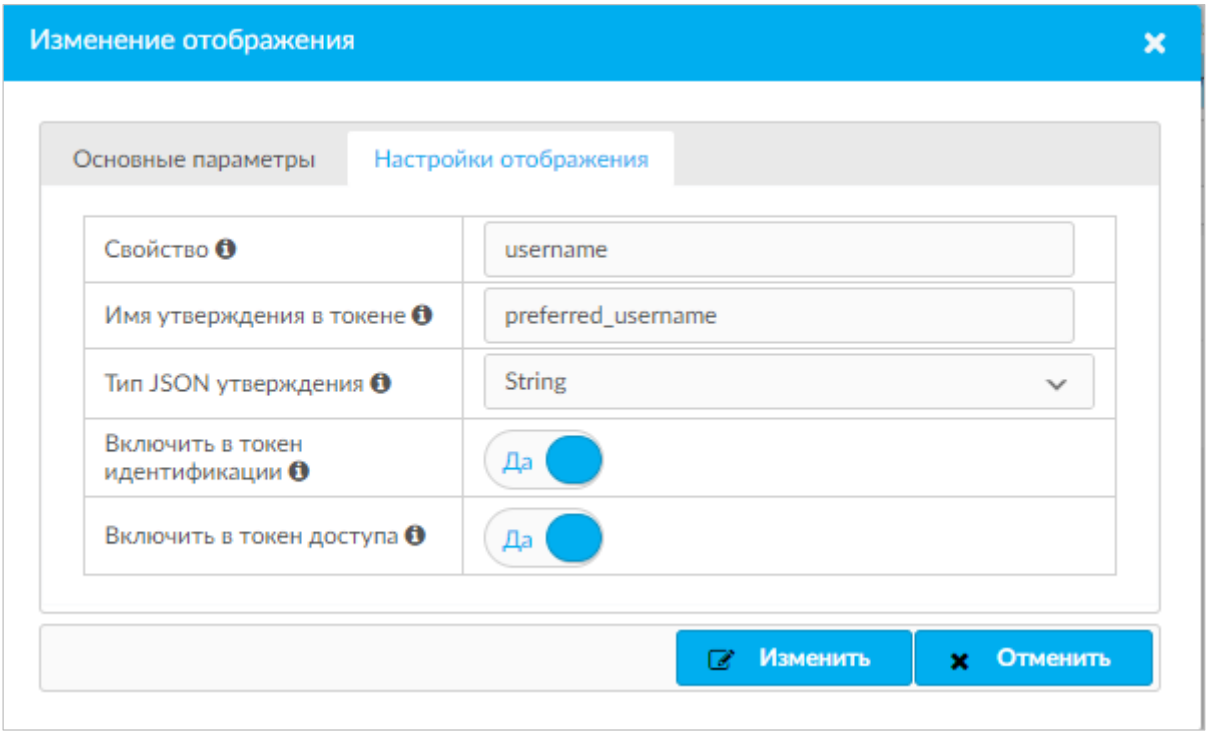


Рисунок 33 – BarsUP.AM. Настройки отображения username

н) из вкладки «Полномочия» скопируйте секретный ключ системы;

о) перейдите в настройки домена BarsUP.AM (Рисунок 34);

п) перейдите на вкладку «Ключи». Скопируйте публичный ключ домена (Рисунок 35);

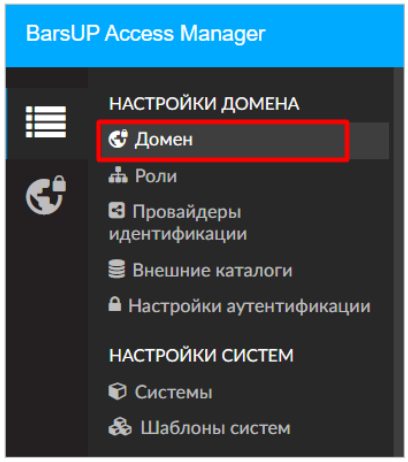


Рисунок 34 – BarsUP.AM. Настройки домена

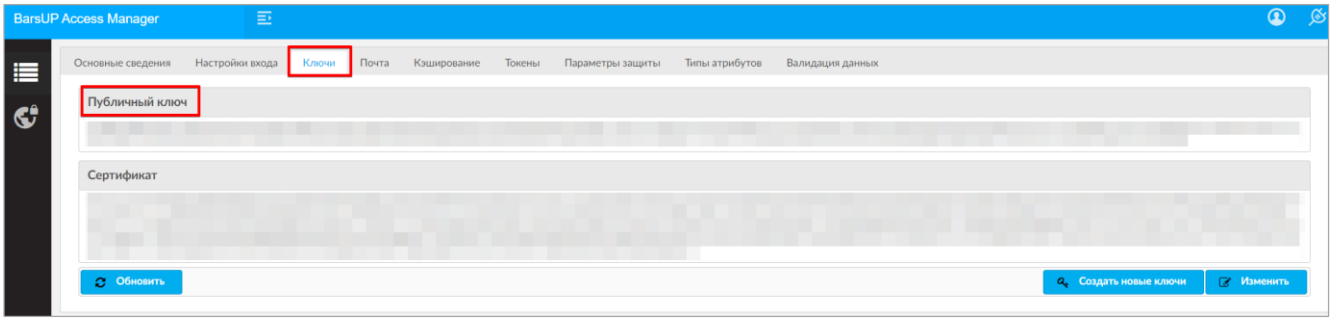


Рисунок 35 – BarsUP.AM. Настройки домена. Вкладка «Ключи»

р) перейдите по адресу http:///{ip/домен Bars.AM}/realms/master/.well-known/openid-configuration и скопируйте значения параметров (заключены в кавычках): issuer, authorization_endpoint, token_endpoint, userinfo_endpoint, end_session_endpoint.

14.1.2 Настройка Keycloak для работы по OpenID

Порядок настройки:

а) разверните и настройте Keycloak согласно инструкции (https://www.keycloak.org/guides#server) либо согласно инструкции из данного руководства;

б) настройте сетевую связность между приложением Keycloak и ПП М3;

в) авторизуйтесь под администратором в Keycloak и перейдите в раздел «Системы»;

г) создайте домен. Откройте выпадающее меню в административной консоли, нажмите кнопку «Добавить realm» (Рисунок 36). Откроется форма создания домена, в которой введите желаемое имя и подтвердите создание нажатием на кнопку «Создать» (Рисунок 37);

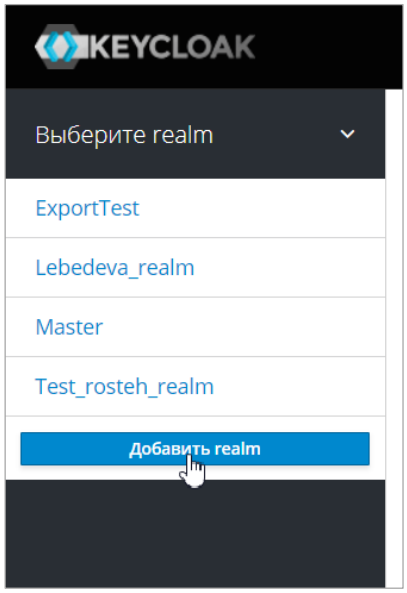


Рисунок 36 – Keycloak. Создание домена

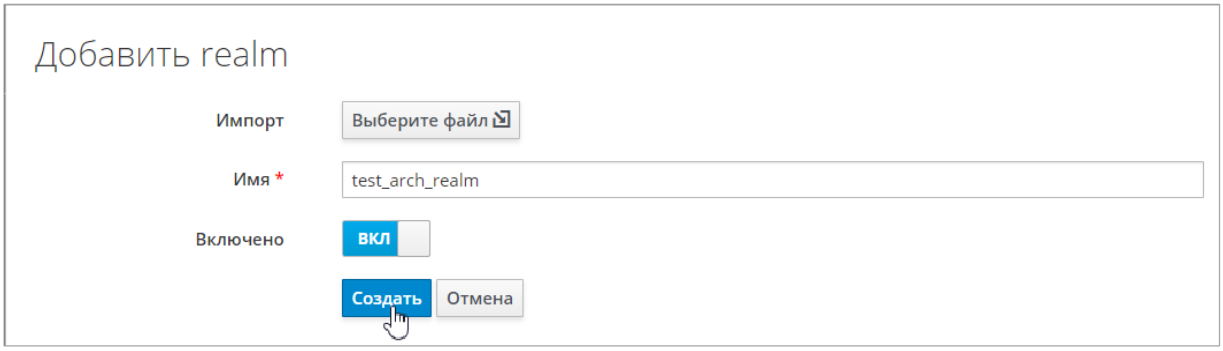


Рисунок 37 – Keycloak. Создание домена

д) для русификации Keycloak перейдите в раздел «Realm settings» во вкладку «Themes» и в графе «Default locale» выберите «ru»;

е) перейдите в раздел «Клиенты» в левом меню для регистрации ПП МЗ (Рисунок 38);

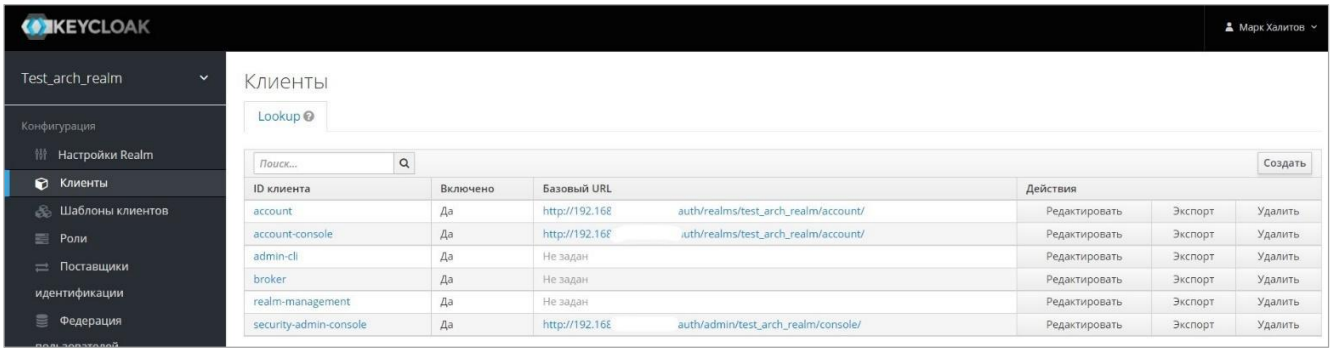


Рисунок 38 – Keycloak. Раздел «Клиенты»

ж) нажмите на кнопку «Создать»;

з) в окне «Добавить клиента»:

– введите ID клиента;
– выберите протокол клиента «opened-connect»;
– введите корневой URL ПП М3 и нажмите на кнопку «Сохранить» (Рисунок 39).

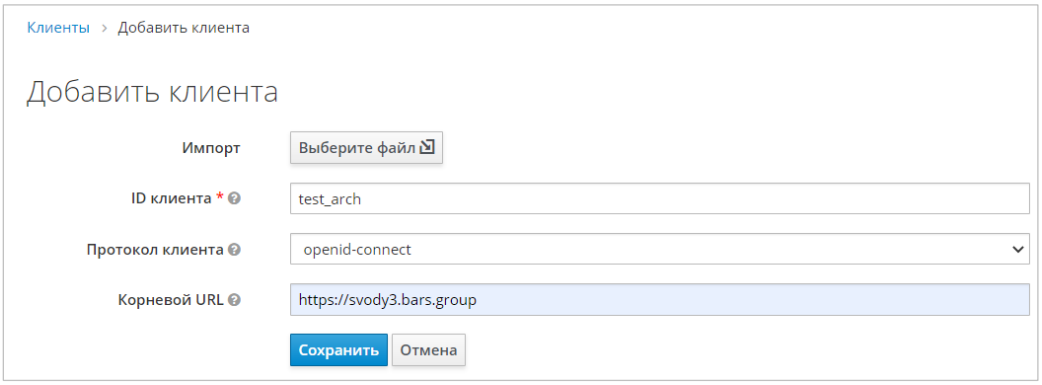


Рисунок 39 – Keycloak. Создание клиента

и) в окне редактирования клиента на вкладке «Настройки» введите:
– «Имя» (может совпадать с идентификатором) и описание (необязательно);
– «Включено» - «Да»;
– «Always Display in Console» - «Да»;
– «Необходимо согласие» – «Да»;
– «Standard Flow включен» – «Да»;
– «Разрешен Direct Access Grants» – «Да»;
– «Service Accounts включен» - «Да»;
– «Service Accounts включен» - «Да»;
– «Корневой URL» – корневой URL приложения без /;
– «Валидация URI перенаправления» – (/*) – для тестирования; (/signin-oidc) – для продуктового приложения;
– «Базовый URL» – "/" + название приложения после доменого имени;
– Web истоичники –"*";
– для остальных полей оставить значения по умолчанию.

к) в окне редактирования клиента на вкладке «Учетные данные» введите:
– «Проверка подлинности клиента» – "Client Id and Secret".

л) в окне редактирования клиента на вкладке «Сопоставления» добавьте следующие отображения по кнопке «Добавить встроенные»: email, family name, full name, given name, middle name, username (Рисунок 40);

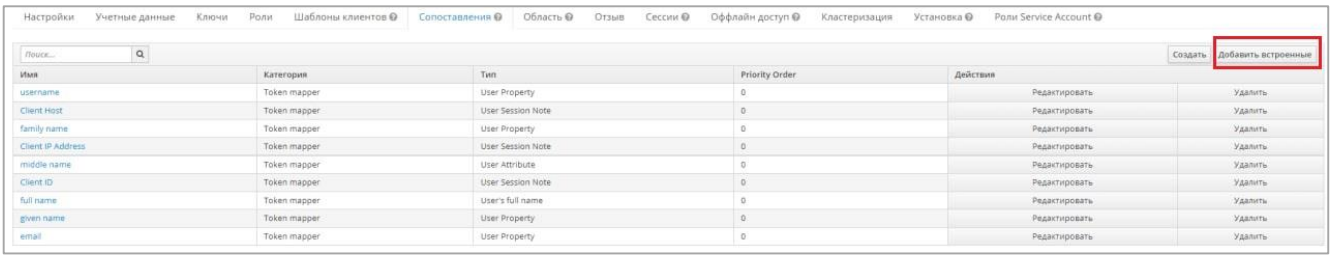


Рисунок 40 – Keycloak. Добавление отображений клиента

Примечание – Отображения Client ID, Client IP Address и Client Host добавляются по умолчанию, и их нельзя удалять. Удаление приведет к невозможности работы пользователей с AW.

м) из вкладки «Учетные данные» скопируйте секретный ключ;

н) перейдите в настройки домена Keycloak http://{ip/домен Keykloak}/auth/admin/master/console/#/realms, выбрать нужный домен (по умолчанию master). Слева выберите пункт «Realm Settings». Перейдите на вкладку «Keys». Скопируйте публичный ключ (Algorithm="RS256", Type="RSA", Use="SIG"). Нажмите на кнопку «Публичный ключ». Скопируйте ключ;

о) перейдите на вкладку «Главная» раздела «Настройки Realm», нажмите «OpenId Endpoint Configuration» и скопируйте значения параметров (заключены в кавычки): issuer, authorization_endpoint, token_endpoint, userinfo_endpoint, end_session_endpoint.

14.1.2.1 Настройка Keycloak для работы массового экспорта операторов

Для работы «Экспорта в Keycloak» произведите предварительные настройки в Keycloak:

– включите настройку «Service Accounts включен» в настройках конкретного клиента в Keycloak и сохраните изменения (Рисунок 41);

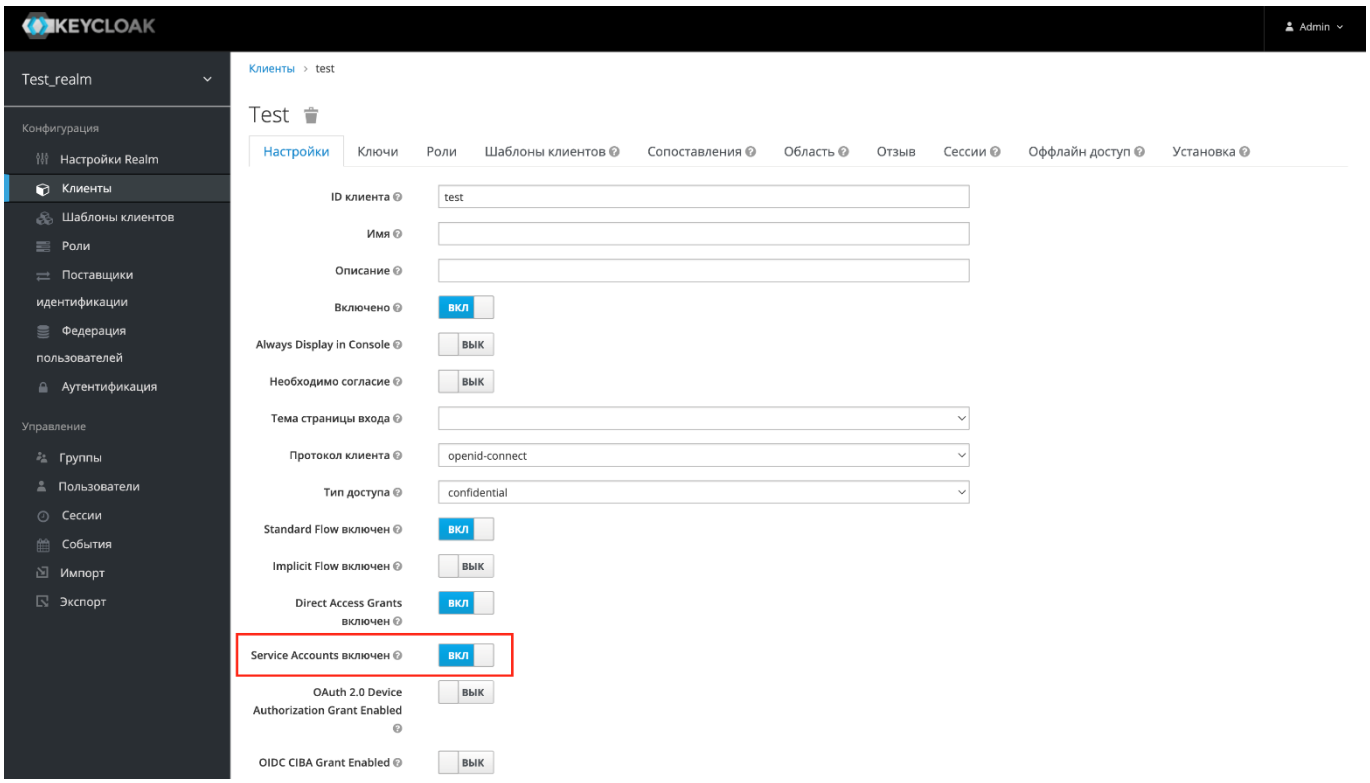


Рисунок 41 – Keycloak. Раздел «Клиенты»

– откройте настройки клиента. Появится новая вкладка «Роли Service Account» (Рисунок 42);

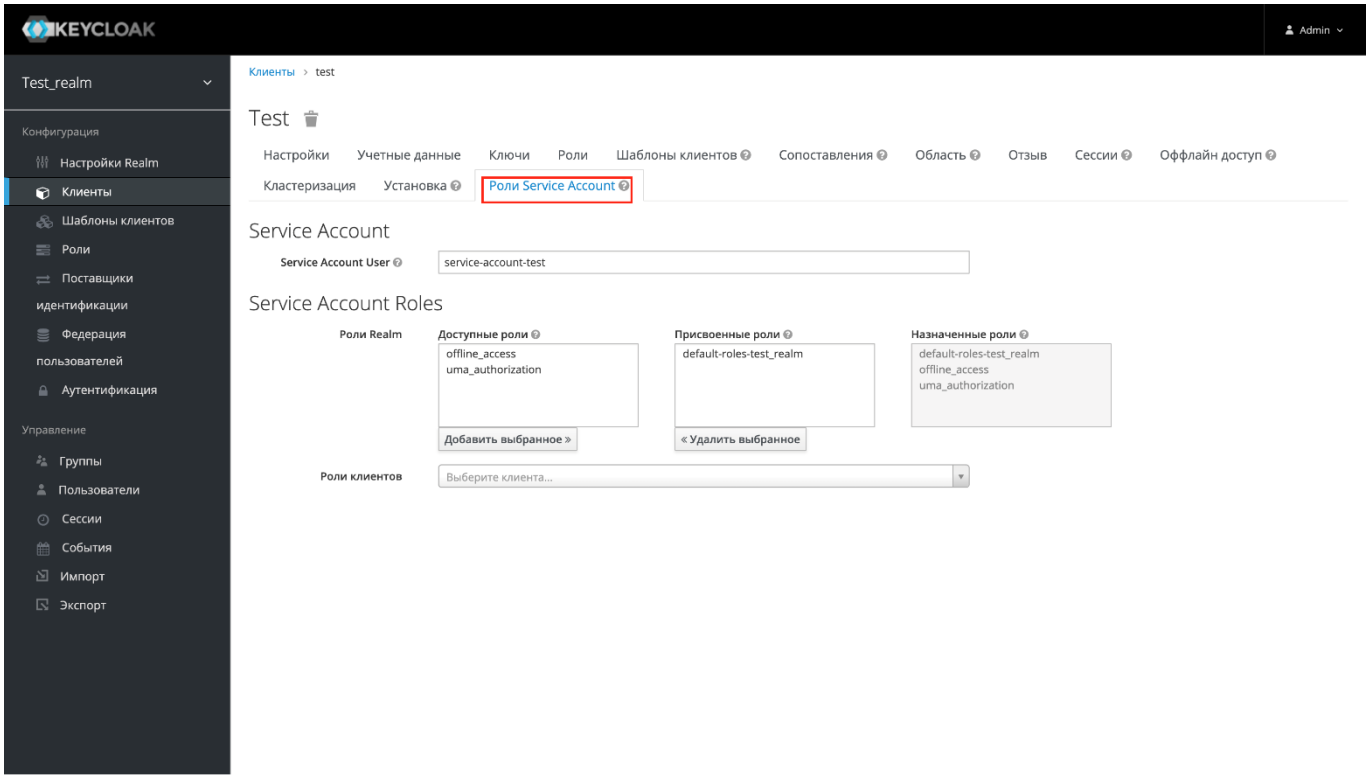


Рисунок 42 – Keycloak. Вкладка «Роли Service Account» раздела «Клиенты»

– перейдите в эту вкладку и назначьте права домена (Роли Realm) (Рисунок 43). Наименование роли строится как default-roles-НазваниеРеалма;

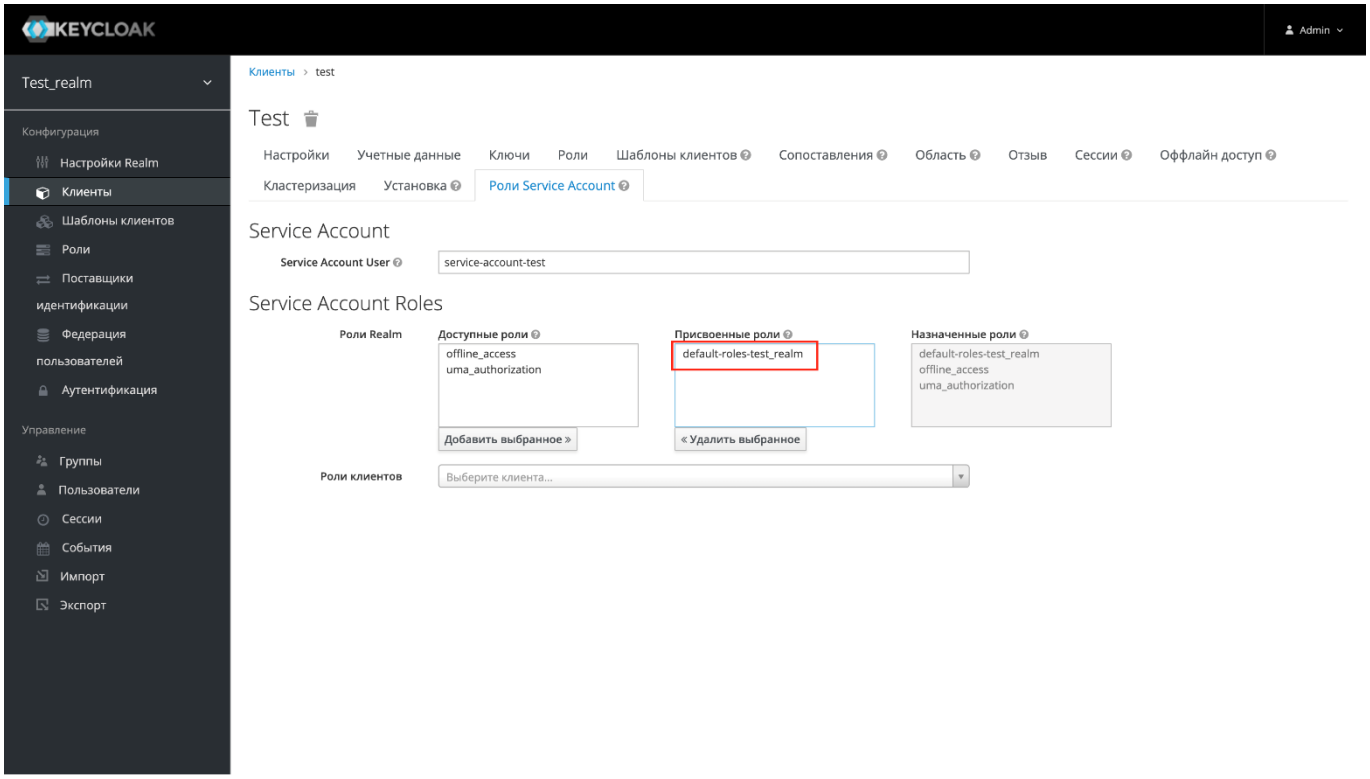


Рисунок 43 – Keycloak. Вкладка «Service Account Roles» раздела «Клиенты». Назначение прав домена

– назначьте права Client. Права Client зависят от того, где был создан клиент: на домене master или на другом домене. Если был создан на другом домене, в Combobox выберите значение «realm-management» и выберите роль «manage-users» (Рисунок 44);

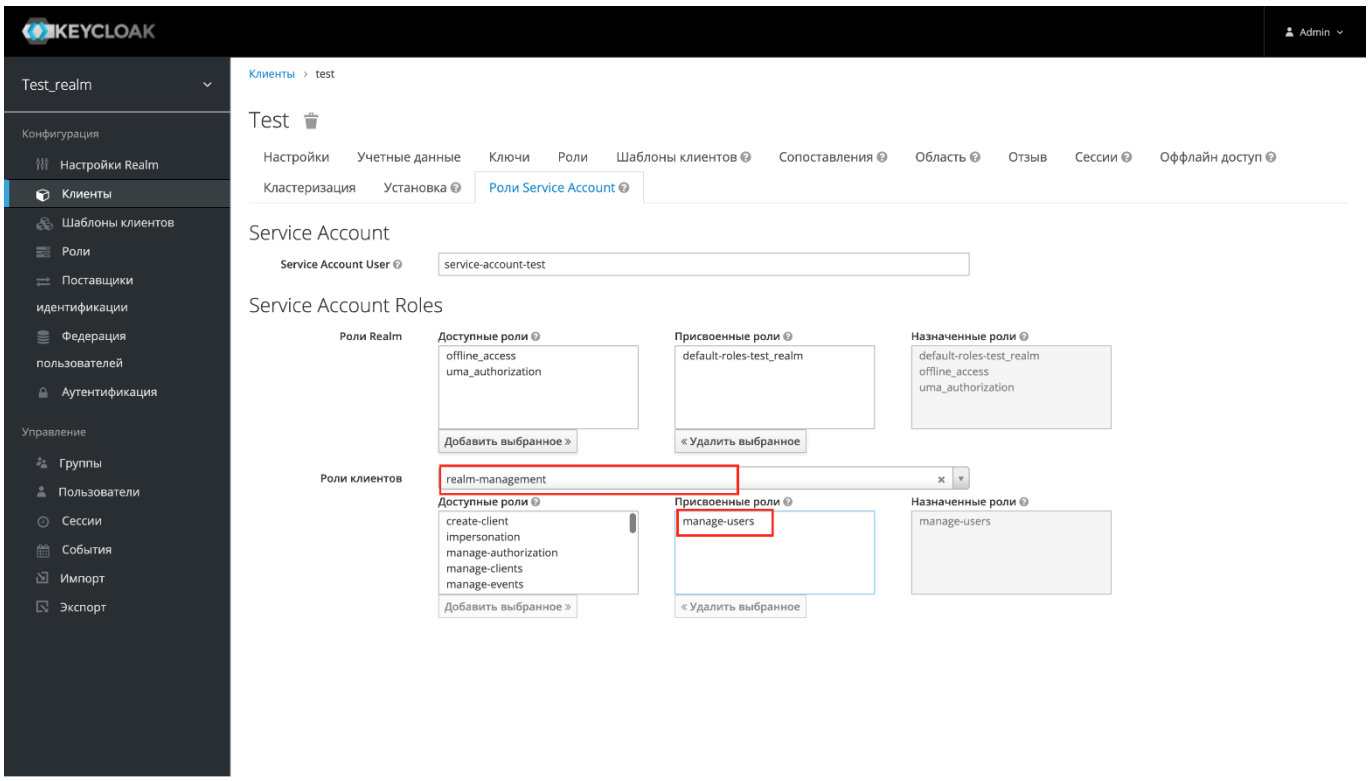


Рисунок 44 – Keycloak. Вкладка Service Account Roles раздела «Клиенты». Назначение прав Client

– измените параметр «RealmsName» блока <Entries> секции Bars.Authorization> файла svody.config. Пример: `<RealmsName>master</RealmsName>`.

14.1.3 Настройка ПП МЗ

Настройка авторизации по протоколу OpenID Connect описывается в новой секции <Bars.Authorization> файла svody.config. Для настройки необходимо использовать значения, полученные при настройке SSO (см. п. 14.1.1 для BarsAM и п. 14.1.2 для Keycloak).

В приложении ПП МЗ в файле «svody.config» в секции <Bars.Authorization> внесите соответствующие изменения согласно скопированным ранее параметрам и в соответствии со вторым примером.

Пример секции:

```
<Bars.Authorization>
  <Entries Name="Svody" Enabled="true" ButtonName="Войти в систему" SortOrder="1" AuthorizationType="Default" />

  <Entries Name="Keycloak" Enabled="false" ButtonName="Войти через Keycloak" SortOrder="2" AuthorizationType="OpenId">
    <OpenIdConnectProviderConfig>
```

```
            <ReverseProxyUrl><!-- URL, на который будет перенаправлен
пользователь после успешной авторизации на стороне OpenId. Необходимо
указывать внешний URL приложения, по которому приходят пользователь
(это может быть URL прокси-сервера, на котором установлен https-
сертификат) --></ReverseProxyUrl>
            <Issuer><!-- значение issuer --></Issuer>
            <AuthorizationEndpoint><!-- значение
authorization_endpoint--></AuthorizationEndpoint>
            <TokenEndpoint><!-- значение token_endpoint--
></TokenEndpoint>
            <UserInfoEndpoint><!-- значение userinfo_endpoint--
></UserInfoEndpoint>
            <SignOutEndpoint><!-- значение end_session_endpoint--
></SignOutEndpoint>
            <ClientId><!-- значение Идентификатора системы (вкладка
настройки) --></ClientId>
            <ClientSecret><!-- значение "Секретный ключ" системы
(вкладка полномочия) --></ClientSecret>
            <Authority><!-- корневой URL Keycloak -->/</Authority>
            <RealmsName><!-- Имя домена SSO провайдера, в котором был
создан клиент--></RealmsName>
            <ProviderId><!-- ИД SSO провайдера (BARS.AM, KeyCloak),
настроенного а AW на подключение к тому же клиенту --></ProviderId>
            <ProviderPublicKey><!-- Публичный ключ домена Keycloak --
></ProviderPublicKey>
          </OpenIdConnectProviderConfig>
        </Entries>
      </Bars.Authorization>
```

Каждый блок «Entries» отвечает за свой способ авторизации с настройками внутри, первый блок отвечает за авторизацию по умолчанию. Ниже приведена таблица с описанием параметров (Таблица 37).

Таблица 37 – Параметры блока <Entries>

Название параметра	Описание параметра	Пример использования
Name	Наименование блока, для авторизации	Name="Svody" Name="Keycloak"
Enabled	Принимает два значения true и false, при значении true, на экране авторизации отобразится новая кнопка, при значении false, блок не учитывается	Enabled="true"
ButtonName	Текст внутри кнопки	ButtonName="Войти через Keycloak"
SortOrder	Порядок сортировки кнопок, принимает числовые значения, так при наличии нескольких способов авторизации можно поменять порядок кнопок	SortOrder="2"

Название параметра	Описание параметра	Пример использования
AuthorizationType	Принимает Default для авторизации по умолчанию и OpenID для авторизации через SSO	AuthorizationType="OpenId"
ReverseProxyUrl	Необходимо указать ссылку на приложение	<ReverseProxyUrl> https://svody.bars.group/svody-openid-dev</ReverseProxyUrl>
Issuer	Значение issuer из настроек endpoint SSO	<Issuer>http://192.168.0.0:0000 /realms/master</Issuer>
AuthorizationEndpoint	Значение authorization_endpoint из настроек endpoint SSO	<AuthorizationEndpoint> http://192.168.0.0:0000 /realms/master/protocol/openid-connect/auth</AuthorizationEndpoint>
TokenEndpoint	Значение token_endpoint из настроек endpoint SSO	<TokenEndpoint> http://192.168.0.0:0000 /realms/master/protocol/openid-connect/token</TokenEndpoint>
UserInfoEndpoint	Значение userinfo_endpoint из настроек endpoint SSO	<UserInfoEndpoint> http://192.168.0.0:0000 /realms/master/protocol/openid-connect/userinfo</UserInfoEndpoint>
SignOutEndpoint	Значение end_session_endpoint из настроек endpoint SSO	<SignOutEndpoint> http://192.168.0.0:0000/realms/master /protocol/openid-connect/logout</SignOutEndpoint>
ClientId	Значение уникального идентификатора системы	<ClientId>svody-openid-dev</ClientId>
ClientSecret	Значение секретного ключа системы	<ClientSecret>a72d6172-4c8b-4c63-ab94-2345f9370aad</ClientSecret>
Authority	Ссылка на SSO	<Authority> http://192.168.0.0:0000/</Authority>
RealmsName	Имя домена из настроек домена, например, master (только для Keycloak, необходимо для возможности массового экспорта пользователей из ПП МЗ в Keycloak, можно оставить пустым при необходимости)	<RealmsName>master </RealmsName>
ProviderId	Необходимо для работы аналитических выборок в случае, если аналитические выборки не используются, необходимо удалить или заключить в комментарий	<ProviderId>12</ProviderId>
ProviderPublicKey	Публичный ключ домена	<ProviderPublicKey> MIIBIjANBgkqhkiG9w0BAQEFAAO CAQ8AMIIBCgKCAQEAyJdXqJ8lU8ql TP0fuPukQzzZZTi2hD6jUQtKT1gxJg AE7s7Lgw4x2hMwK217Ho99GJPo9 Yeo1Yd6S7X8GCcmJzfdumXELUia VBzfohHDaiAfndzR3vuJRzy72/FN

Название параметра	Описание параметра	Пример использования
		fWOE7J3/cyM+MVrErEENj/giOnzw IDAQTG</ProviderPublicKey>

Пример настроенной секции:

```
      <Bars.Authorization>
          <Entries Name="Svody" Enabled="false" ButtonName="Войти в
систему" SortOrder="1" AuthorizationType="Default" />

      <Entries Name="Keycloak" Enabled="true" ButtonName="Войти через
Keycloak" SortOrder="2" AuthorizationType="OpenId">
            <OpenIdConnectProviderConfig>
              <ReverseProxyUrl>https://svody.bars.group/svody-openid-
dev</ReverseProxyUrl>
              <Issuer>http://192.168.0.0:0000/realms/master</Issuer>

<AuthorizationEndpoint>http://192.168.0.0:0000/realms/master/protocol/o
penid-connect/auth</AuthorizationEndpoint>

<TokenEndpoint>http://192.168.0.0:0000/realms/master/protocol/openid-
connect/token</TokenEndpoint>

<UserInfoEndpoint>http://192.168.0.0:0000/realms/master/protocol/openid
-connect/userinfo</UserInfoEndpoint>

<SignOutEndpoint>http://192.168.0.0:0000/realms/master/protocol/openid-
connect/logout</SignOutEndpoint>
              <ClientId>svody-openid-dev</ClientId>
              <ClientSecret>a72d6205-4c8b-4c63-ab94-
2345f9370aad</ClientSecret>
              <Authority>http://192.168.0.0:0000/</Authority>
              <RealmsName>master</RealmsName>
              <!--<ProviderId><!-- ИД SSO провайдера (BARS.AM,
KeyCloak), настроенного а AW на подключение к тому же клиенту --
></ProviderId>!-->
<ProviderPublicKey>MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyJdXqJ8l
U8qlTP0fuPukQzzZZTi2hD6jUQtKT1gxJgAE7s7Lgw4x2hMwK217Ho99GJPo9Yeo1Yd6S7X
8GCcmJzfdumXELUiaVBzfohHDai/gdRI3u6PsLwpEBaXOrddNy3s4XbdGs2R/FfAyeTbHFU
cR3L/4u42SBa2P+7tQZoT37CI48dhrQvwRGhvjDcPZfGuCbE6D9rAkgOizRofgZ4Kf55QLR
/cyM+MVrErEENj/giOnzwIDAQGR</ProviderPublicKey>
            </OpenIdConnectProviderConfig>
          </Entries>
        </Bars.Authorization>
```

Сохраните файл svody.config и перезапустите приложение.

Примечания

1. При настройке секции можно добавлять несколько блоков «Entries» подряд в зависимости от того, какое количество систем необходимо подключить (например, BarsAM и Keycloak одновременно).

2. Для авторизации через ЕСИА требуются настройки на стороне BarsUP.AM по протоколу OpenID Connect и регистрация ИС в ЕСИА (https://esia.pro/integraciya_esia_gos_org).

Если используется Nginx, необходимо внести изменения в конфигурационный файл Nginx приложения по пути «etc/nginx/conf.d». Изменения касаются параметров buffer.

Пример настроенного файла:

```
location /sss {
  limit_req zone=one burst=10;
        limit_conn two 10;
        client_max_body_size  500M;
  proxy_pass  http://127.0.0.1:5011/sss;
  proxy_http_version  1.1;
  proxy_set_header  Upgrade $http_Upgrade;
  proxy_set_header  Host $host;
  proxy_set_header  X-Real-IP $remote_addr;
  proxy_set_header  X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_set_header  X-Forwarded-Proto $realscheme;
  proxy_set_header  Connection keep-alive;
        proxy_set_header        Connection "upgrade";
  proxy_send_timeout  600s;
  proxy_read_timeout  600s;
  proxy_connect_timeout  600s;
        proxy_buffer_size       64k;
        proxy_buffers           4 64k;
        proxy_busy_buffers_size 64k;
        proxy_temp_file_write_size 1024k;
        proxy_headers_hash_max_size 512;
        proxy_headers_hash_bucket_size 128;
}
```

Выполните перезагрузку командой:

```
nginx -s reload
```

14.2 Настройка для работы с OpenLDAP

14.2.1 Настройка Kerberos

Примечание – Данный тип авторизации работает только на ОС Astra Linux Special Edition (Смоленск).

Для корректной работы авторизации через kerberos в ПП МЗ, необходимо в keytab-файл записать ключи доменных служб HTTP и LDAP. По умолчанию такой файл находится по пути /etc/krb5.keytab. Если планируется использовать этот файл, необходимо дать права на чтение этого файла пользователю, от имени которого будет запущено приложение ПП МЗ.

Чтобы добавить ключи служб в keytab-файл, выполните:

– получите права администратора домена от имени суперпользователя:

```
sudo kinit admin
```

- действуя от имени суперпользователя с правами администратора домена, получите и сохраните таблицу ключей служб HTTP и LDAP (путь файла /etc/svody.keytab можно выбирать любой, либо использовать файл по умолчанию):
  - для IPA:

```
sudo ipa-getkeytab -s ipa0.ipadomain0.ru -k /etc/svody.keytab -p
HTTP/hostname
sudo ipa-getkeytab -s ipa0.ipadomain0.ru -k /etc/svody.keytab -p
ldap/hostname
```

  - для ALD:

```
keytab="/etc/svody.keytab"
ald-client update-svc-keytab HTTP/hostname --ktfile="$keytab"
ald-client update-svc-keytab ldap/hostname --ktfile="$keytab"
```

- если ключи служб были сохранены в отдельном keytab-файле (не в том, который по пути /etc/krb5.keytab), дайте права на чтение этого файла пользователю, от имени которого будет запущено приложение ПП МЗ.

Далее в файле svody.config отредактируйте секцию <Bars.Authorization>, добавьте новую запись с типом авторизации "Kerberos":

```
<Entries Name="SvodyKerberos" Enabled="true" ButtonName="Войти
через домен" SortOrder="1" AuthorizationType="Kerberos">
  <KerberosAuthenticationConfig>
      <Login><!-- логин доменной учетной записи с правами поиска
в LDAP --></Login>
      <Password><!-- пароль доменной учетной записи с правами
поиска в LDAP --></Password>
      <Realm><!-- Realm контроллера домена --></Realm>
      <DomainControllerName><!-- Полное dns-имя контроллера
домена --></DomainControllerName>
      <UsersOu>users</UsersOu>
    <GroupsFilterAttribute><!-- LDAP-атрибут группы, по которому
будет выполнен поиск групп домена, в которые добавлен пользователь(по
умолчанию memberUid) --></GroupsFilterAttribute>
      <CCacheDirectoryPath>/tmp</CCacheDirectoryPath><!-- путь к
папке, куда будут сохраняться билеты kerberos -->
      <KeyTabPath>/etc/krb5.keytab</KeyTabPath><!-- путь до
файла keytab, в котором сохранены ключи доменных служб HTTP и ldap -->
   </KerberosAuthenticationConfig>
</Entries>
```

Примечание – Если в ПП МЗ настроена kerberos-авторизация, то вторым способом авторизации может быть только дефолтная (по логину и паролю).

14.2.2 Создание пользователей на ALD-сервере

Для корректной работы в ALD должен быть уже заведен системный пользователь, от имени которого будет происходить проверка учетных записей обычных пользователей.

У этого пользователя должны быть права на чтение всего LDAP-дерева.

У остальных пользователей доступа к LDAP-каталогу может не быть, но должны быть права входа и просмотра своего узла.

Для работы ПП МЗ важны отмеченные поля (Рисунок 45):

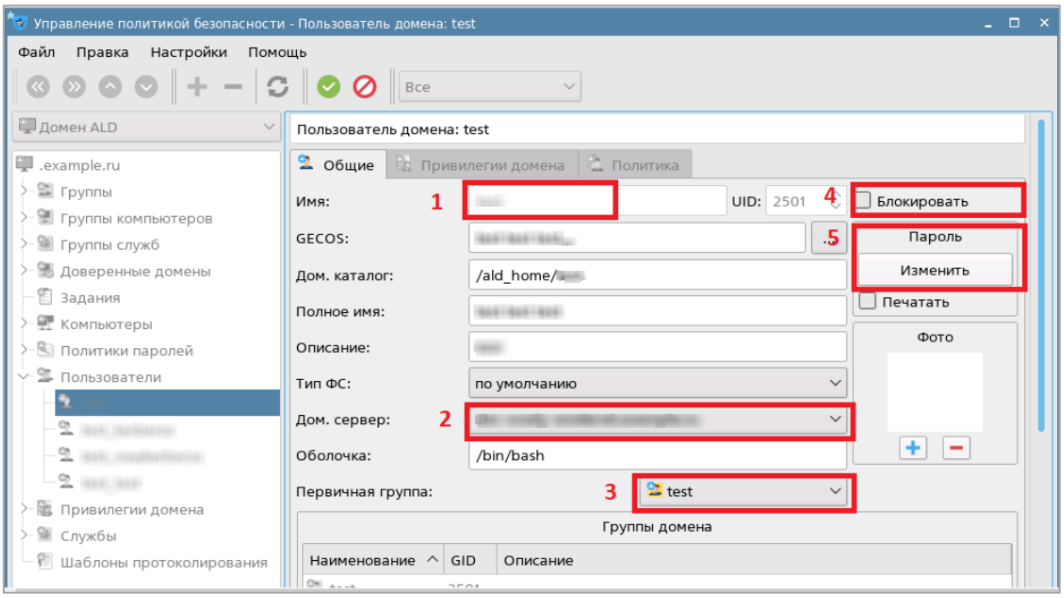


Рисунок 45 – Карточка системного пользователя

- Логин пользователя. Под этим логином пользователь авторизуется как в ОС, так и в ПП МЗ, связка пользователей тоже происходит по этому полю;
- Доменный сервер. Нужно, чтобы был тот же, что и в конфиге в поле <DomainControllerName>;
- Группа пользователя. Параметр, который указывает на блокировку пользователя. Если пользователь заблокирован, то он не сможет войти по доменной учетной записи. Но есть ограничения:
  - если подключена обычная авторизация, и пользователь не заблокирован в ПП МЗ (синхронизация параметра блокировки не происходит при авторизации), то под этой учетной записью можно будет зайти с помощью обычного окна авторизации;
  - если этот пользователь был создан в ПП МЗ автоматически при входе через kerberos, то пароль от ПП МЗ неизвестен, а если его сменить из ПП МЗ, тогда

не будет работать раздел выборок, т.к. пароль в ПП МЗ и AW не будет совпадать, и авторизация в AW не пройдет.

– Пароль пользователя.

Примечание – После создания пользователя на ALD-сервере, он не появится в ПП МЗ. Ему необходимо попытаться авторизоваться в ПП МЗ, а администратору после этого добавить его через функционал «Добавить из LDAP», который описан в документе «Руководство администратора».

15 Настройка для работы с аналитическими выборками

Данный раздел доступен в том случае, если в параметрах лицензионного ключа предусмотрено использование **Компонента анализа данных** программы ЭВМ БАРС.Мониторинг-Здравоохранение (далее – AW).

Для корректной работы AW необходимо, чтобы адрес состоял только из доменного имени.

Обновлять AW необходимо последовательно. Например, для обновления с 13 версии на 17, необходимо последовательно установить все промежуточные версии – 14, 15, 16.

15.1 Установка Docker

Установите Docker согласно инструкции:

https://docs.docker.com/engine/install/

Каждой версии ОС соответствует своя инструкция. Версия устанавливаемого Docker должна быть не ниже 20.10.9.

Также установите Docker Compose согласно инструкции и в соответствии с вашей версией ОС:

https://docs.docker.com/compose/install/

Проверить корректность установки можно с помощью команд:

```
docker --version
docker-compose –version
```

Пример:

```
root@dev-svody-web-ubuntu:/home/bars# docker --version
Docker version 20.10.21, build baeda1f
root@dev-svody-web-ubuntu:/home/bars# docker-compose --version
docker-compose version 1.29.2, build 5becea4c
```

Внесите изменения в файл «/etc/sysctl.conf», добавив туда строку:

```
vm.max_map_count=262144
```

Затем перезапустите службу командой:

```
sudo sysctl –p
```

15.2 Установка приложения

Создайте каталог, в котором будет в дальнейшем работать приложение:

```
mkdir /opt/aws
```

Разархивируйте полученный дистрибутив приложения. Например, «aw-bc-svody-версия_релиза.tar»:

```
cd /opt/aws
tar -xvf aw-bc-svody-версия_релиза.tar
rm -f aw-bc-svody-версия_релиза.tar
```

Создайте конфигурационный файл .env, скопировав его из файла .env.dist следующей командой:

```
cp /opt/aws/.env.dist /opt/aws/.env
```

Затем отредактируйте в этом файле .env следующие строки:

`BACKEND_URL=https://url/api` (подставляем свои значения url, соответствующие доменному адресу, на который выдана лицензия)

`FRONTEND_URL=https://url` (подставляем свои значения url, соответствующие доменному адресу, на который выдана лицензия)

Укажите параметры ClickHouse сервера:

```
AW_CLICKHOUSE_HTTP_PORT_EXPORTED=8123
AW_CLICKHOUSE_TCP_PORT_EXPORTED=9017
```

Примечания

1 Прочие параметры данного файла изменять без крайней необходимости не рекомендуется.

2 Если на сервере кроме AW уже установлены какие-либо другие приложения, которые используют http порт 80, существует возможность изменить порт web-приложения. Для этого в файле .env можно изменить значение параметра AW_FRONTEND_HTTP_PORT=80 на не занятый. Однако в целом не рекомендуется разворачивать AW совместно с иными, не связанными с AW напрямую, системами.

Создайте все необходимые каталоги, выполнив скрипт:

```
sh create_project_dirs.sh
```

Выполните загрузку образов из архива aw-docker-images.tar.xz с помощью команд:

```
cd /opt/aws
xzcat aw-docker-images.tar.xz | docker load
```

Дождитесь окончания процесса выполнения загрузки.

После чего последовательно выполните команды сборки и проведения миграций:

```
docker-compose up -d --build --force-recreate
docker-compose exec backend php yii migrate --interactive=0
docker-compose exec backend php yii run-code-migrations
docker-compose exec etl-api /app/manage migrate
```

По окончании процесса успешного выполнения команд установка считается выполненной.

После чего необходимо установить лицензию, используя Центр управления. Установка лицензии описана в п. 15.8.2.

15.2.1 Резервное копирование приложения

Перейдите в рабочую директорию приложения:

```
cd /opt/aws
```

Выполните остановку приложения:

```
docker-compose down
```

Создайте резервные копии файлов конфигурации:

```
tar -czf имя_резервной_копии_файлов_конфигурации.tar ./.env ./docker ./docker-compose.yml ./docker-compose.prod.yml ./*.sh
```

Создайте резервные копии файлов БД:

```
tar -czf имя_резервной_копии_БД ../db
```

Создайте резервные копии файлового хранилища:

```
tar -czf имя_резервной_копии_файлового_хранилища ../file_storage
```

По окончании процессов архивации, запустите приложение:

```
docker-compose up –d
```

Примечание – В качестве альтернативы после остановки приложения можно объединить раздельные команды в одну для создания единого архива:

```
tar -czf ../aw-backup-$(date +%Y-%m-%d).tar.gz ./.env ./docker ./docker-compose.yml ./docker-compose.prod.yml ./*.sh ../db ../file_storage
```

15.2.2 Обновление приложения

Убедитесь, что у вас существует актуальная копия приложения, созданная согласно п. 15.2.1. После этого можно приступать к обновлению.

Перейдите в каталог приложения:

```
cd /opt/aws
```

Завершите работу приложения:

```
docker-compose down
```

Перенесите полученный через менеджера проекта дистрибутив в каталог приложения. Например:

```
cp /tmp/aw-bc-svody-версия_релиза.tar /opt/aws/
```

После чего выполните команду распаковки архива с заменой файлов:

```
tar -xvf aw-bc-svody-версия_релиза.tar
```

После распаковки для экономии ресурсов архив можно удалить:

```
rm -f aw-bc-svody-версия_релиза.tar
```

Выполните загрузку образов из архива aw-docker-images.tar.xz с помощью команд:

```
cd /opt/aws
docker system prune
xzcat aw-docker-images.tar.xz | docker load
```

Дождитесь окончания процесса выполнения загрузки.

После чего последовательно выполните команды сборки и проведения миграций:

```
docker-compose up -d --build --force-recreate
docker-compose exec backend php yii migrate --interactive=0
docker-compose exec backend php yii run-code-migrations
```

По окончании процесса успешного выполнения команд, обновление считается выполненным.

15.3 Настройка AW

Если производится обновление с 13 версии на 17 и выше, то необходим лицензионный файл нового образца.

Для настройки AW необходимо:

- перейти в раздел «Общие настройки»;
- перейти в раздел «Группы пользователей», «Пользовательские» и добавить новую группу «Удаление объектов, созданных Сводами» с кодом aw_objects_delete (Рисунок 46).

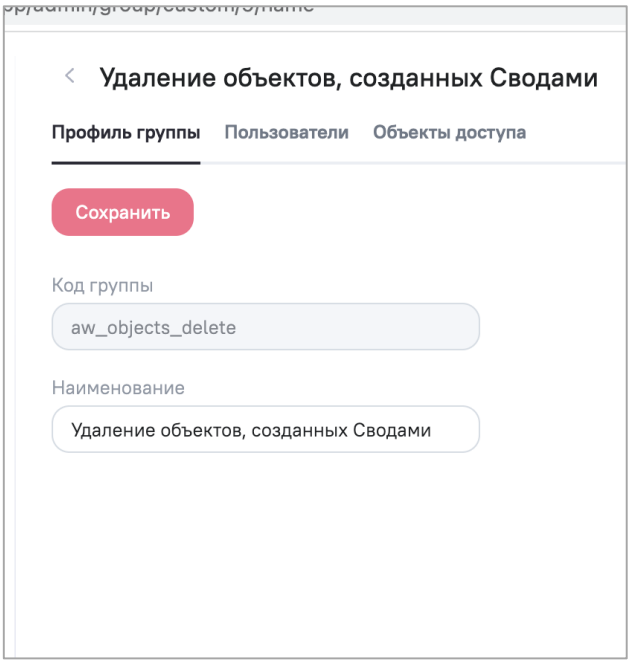


Рисунок 46 – Добавление пользовательской группы доступа

- перейти в раздел «Провайдеры» и нажать на кнопку «Добавить»;
- в открывшемся окне установить «флажок» в полях «Активный» и «Разрешить создание новых пользователей через внешнее управление»;
- ввести наименование провайдера;
- выбрать тип «OpenID Token»;
- ввести надпись кнопки сторонней аутентификации;
- выбрать базовые группы: «Просмотр виджетов», «Просмотр уведомлений», «Удаление объектов, созданных Сводами» (Рисунок 47);

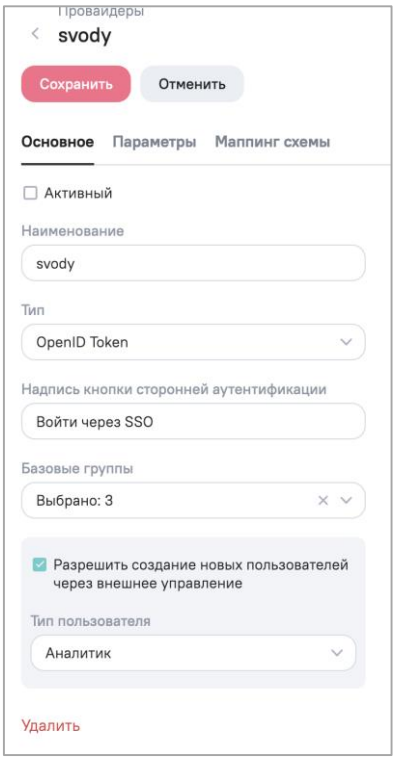


Рисунок 47 – AW. Создание провайдера

- задать тип пользователя по умолчанию «Аналитик»;
- перейти во вкладку «Параметры»;
- в поле «Идентификатор ИА» указать ID клиента, скопированный в п. 14.1.1 для BarsAM и п. 14.1.2 для Keycloak;
- в поле «Секретный ключ доступа» указать секретный ключ, скопированный в п. 14.1.1 для BarsAM и п. 14.1.2 для Keycloak;
- в поле «Внешний URL» вписать URL доступа до домена SSO, например, http://192.168.0.0:0000/auth/realms/test_arch_realm;
- перейти во вкладку «Маппинг схемы» и добавить к уже существующим значениям значения: preferred_username и email (Рисунок 48);

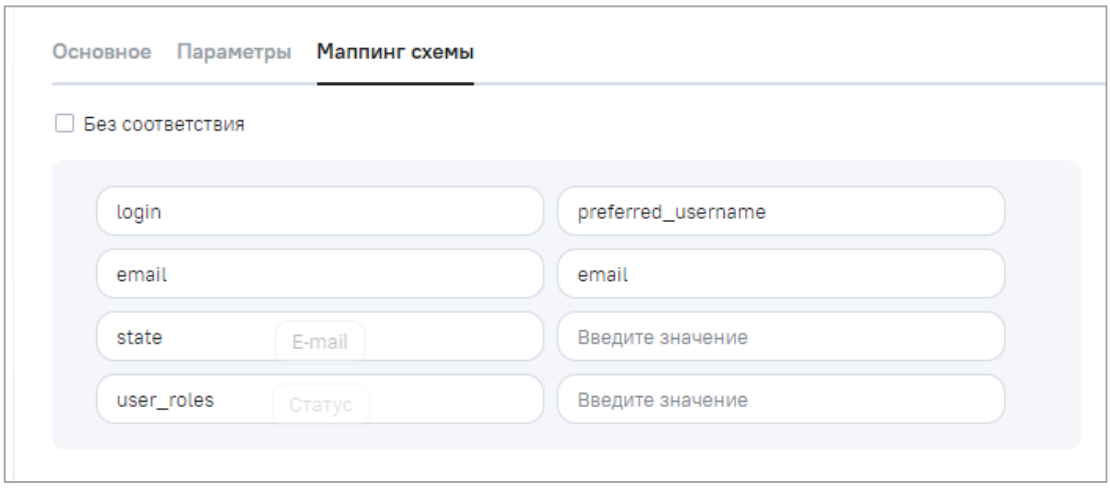


Рисунок 48 – Маппинг соответствия

– скопировать код провайдера из адресной строки, например, в адресе https://svody-aw.bars.group/app/admin/providers/update/13, это число будет 13.

15.4 Настройка svody.config и секции <Svody.Aw>

Для корректной работы аналитических выборок необходимо настроить секцию <Svody.Aw> и дополнить секцию <Bars.Authorization>:

– скопированный код провайдера необходимо ввести в тег <ProviderId> секции <Bars.Authorization>;

```
<ProviderId><!-- ИД SSO провайдера (BARS.AM, KeyCloak), настроенного а AW на подключение к тому же клиенту --></ProviderId>
```

– настроить секцию <Svody.Aw>, описания параметров описаны в таблице ниже (Таблица 38);

Таблица 38 – Параметры секции <Svody.Aw>

Название параметра	Описание параметра	Пример использования
<Db>	Наименование БД ClickHouse	<Db>default</Db>
<Host>	Адрес сервера БД ClickHouse	<Host>192.168.0.0</Host>
<Port>	Порт сервера БД ClickHouse	<Port>9017</Port>
<User>	Имя пользователя БД ClickHouse	<User>default</User>
<Password>	Пароль пользователя БД ClickHouse	<Password>enter4z </Password>
BaseUrl	Адрес Компонента анализа данных, в конце не должно быть слэша	<BaseUrl>https://svody-aw.bars.group</BaseUrl>

Название параметра	Описание параметра	Пример использования
AdminLogin	Пользователь приложения AW, который имеет право на создание новых пользователей Актуально только для авторизации через LDAP	<AdminLogin>admin </AdminLogin>
AdminPassword	Пароль от пользователя приложения AW, который имеет право на создание новых пользователей Актуально только для авторизации через LDAP	<AdminPassword>123456 </AdminPassword>

Пример секции:

```
<Svody.Aw>
    <Db><!-- БД Clickhouse AW --></Db>
    <Host><!-- IP БД Clickhouse AW --></Host>
    <Port><!-- TCP Порт Clickhouse AW --></Port>
    <User><!-- Пользователь БД Clickhouse AW --></User>
    <Password><!-- Пароль пользователя БД Clickhouse AW --
></Password>
    <BaseUrl><!-- URl приложения AW --></BaseUrl>
     <AdminLogin><!-- Пользователь приложения AW, который имеет
право на создание новых пользователей --></AdminLogin
    <AdminPassword><!-- Пароль от пользователя приложения AW,
который имеет право на создание новых пользователей --></AdminPassword>
  </Svody.Aw>
```

– перезапустить приложение.

15.5 Настройка svody.config и секции <Svody.Analytics>

Для настройки кросс-авторизации с AW необходимо настроить секцию <Svody.Analytics> и дополнить секцию <Bars.Authorization>:

– добавьте параметр «LoginToAnalytics» секцию <Entries> в секции <Bars.Authorization>. Данный тег принимает два значения: true и false. При значении true появляется возможность через страндартный вариант авторизации входить в AW;

```
<Bars.Authorization>
    <Entries Name="Svody" Enabled="true" ButtonName="Войти в
систему" SortOrder="1" AuthorizationType="Default"
LoginToAnalytics="false"/>
</Bars.Authorization>
```

– настройте секцию <Svody.Analytics>, описания параметров приведены в таблице ниже (Таблица 39);

Таблица 39 – Параметры секции <Svody.Analytics>

Название параметра	Описание параметра
Visible	Отображение/скрытие кнопки «Аналитика» - по умолчанию кнопка скрыта, установлено значение «false»
InFrame	Открытие страницы во вкладке внутри ПП МЗ («true») или в отдельной вкладке web-браузера («false»)
Url	URL адрес, по которому будет происходить переход по кнопке «Аналитика»

Пример секции:

```
<Svody.Analytics>
    <!-- Отображать кнопку Аналитика -->
    <Visible>true</Visible><!-- Отображать кнопку Аналитика -->
    <!-- true - открыть в новой вкладке приложения, false -
открыть в новом окне браузера-->
    <InFrame>true</InFrame><!-- true - открыть в новой вкладке
сводов, false - открыть в новом окне браузера-->
    <!-- URl приложения AW. Указывается без "/" в конце -->
    <Url></Url>
  </Svody.Analytics>
```

– перезапустите приложение.

15.6 Администрирование Компонента анализа данных

Если ранее у вас стоял Компонент анализа данных 13 версии, то после обновления на 18 версию и выше необходимо текущим пользователям присвоить роль «Аналитик» и активировать учетную запись вручную, при создании новых пользователей при соответствующей настройке провайдера роль будет присваиваться автоматически (п. 15.6.5). Установка лицензии и базовая настройка AW производится с учетной записи технического администратора AW (tech_admin).

Примечание – Данный способ входа в AW предназначен только для технического администратора AW. Описание входа в AW для пользователя приведено в Руководстве пользователя.

Для начала работы с AW:

– запустите web-браузер двойным нажатием левой кнопки мыши по его ярлыку на рабочем столе или нажмите на кнопку «Пуск» и в открывшемся меню выберите пункт, соответствующий используемому web-браузеру;
– в адресной строке введите адрес AW;

– в окне авторизации пользователя введите логин и пароль и нажмите на кнопку «Войти» (Рисунок 49).

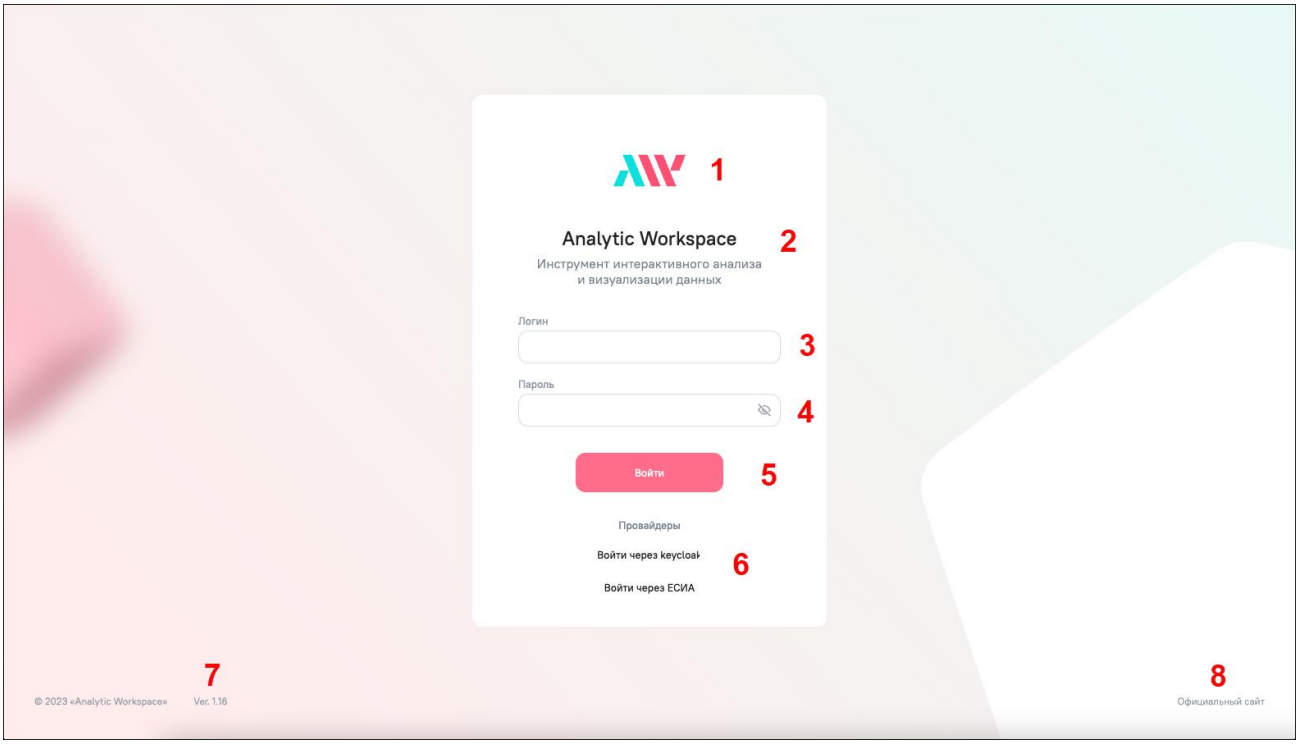


Рисунок 49 – Окно авторизации

Окно авторизации состоит из следующих элементов (Рисунок 49):

– логотип AW;
– наименование AW;
– поле для ввода логина;
– поле для ввода пароля;
– кнопка «Войти» для входа в AW;
– кнопки входа через внешние провайдеры. Кнопки отображаются, если внешние провайдеры настроены техническим администратором AW;
– номер версии AW.

Примечание – В целях защиты обратной связи при вводе аутентификационной информации в AW не отображаются вводимые символы в поле пароля.

При авторизации под учетной записью пользователя с открытой сессией откроется окно с предупреждением об ее активности с возможностью переноса сессии с одного устройства на другое (Рисунок 50). Для закрытия старой и открытия новой сессии нажмите на кнопку «Перенести сессию», для изменения учетной записи нажмите «Отмена» и в окне авторизации пользователя введите логин и пароль.

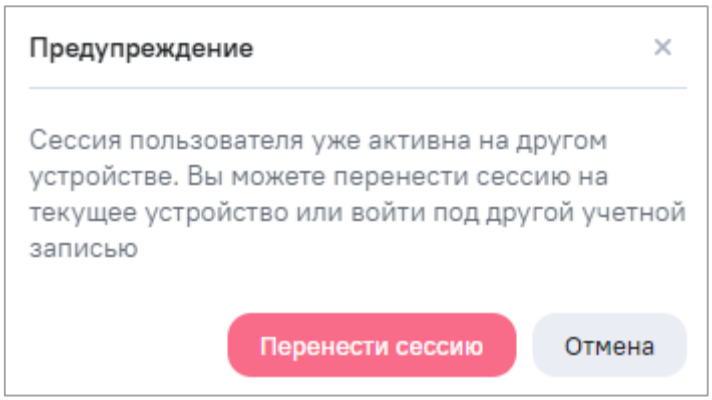


Рисунок 50 – Окно с предупреждением об активности сессии при входе в AW

Откроется окно AW (Рисунок 51). Слева отображается главное меню.

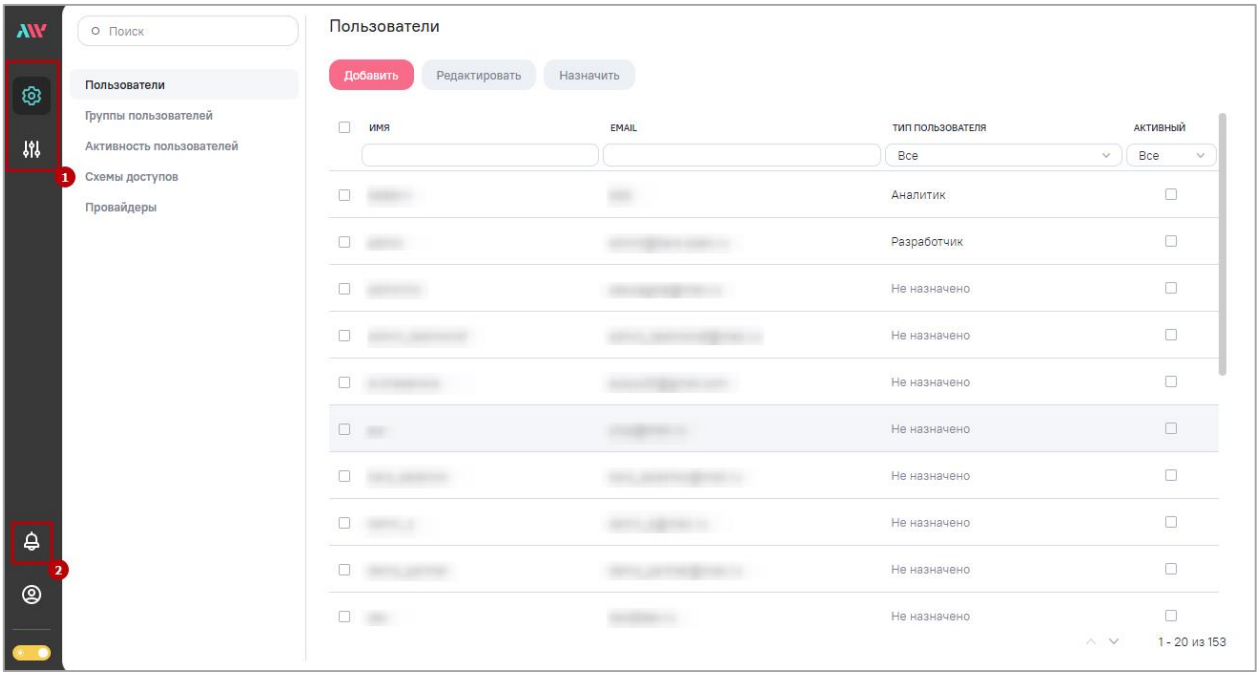


Рисунок 51 – Окно AW

Чтобы перейти в другие разделы AW, нажмите на соответствующую разделу кнопку (1, Рисунок 51). Откроется окно выбранного раздела, цвет фона окна в каждом разделе различается.

Чтобы посмотреть уведомления, нажмите на кнопку  (2, Рисунок 51). Откроется окно просмотра уведомления (Рисунок 52).

Примечание – Возле пиктограммы отображается число новых уведомлений (при их наличии).

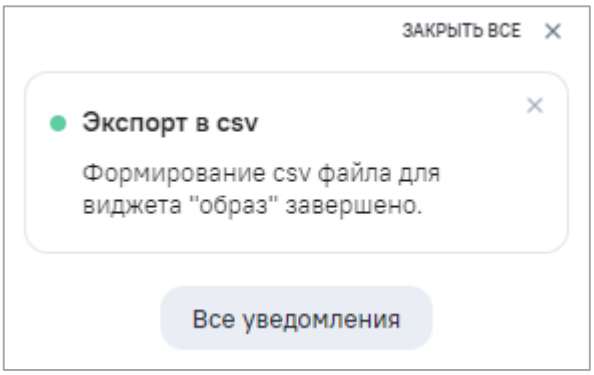


Рисунок 52 – Окно просмотра уведомления

После просмотра уведомления нажмите на кнопку «Закрыть все», чтобы закрыть окно, или на кнопку «Все уведомления», чтобы перейти в раздел «Центр уведомлений» (Рисунок 53).

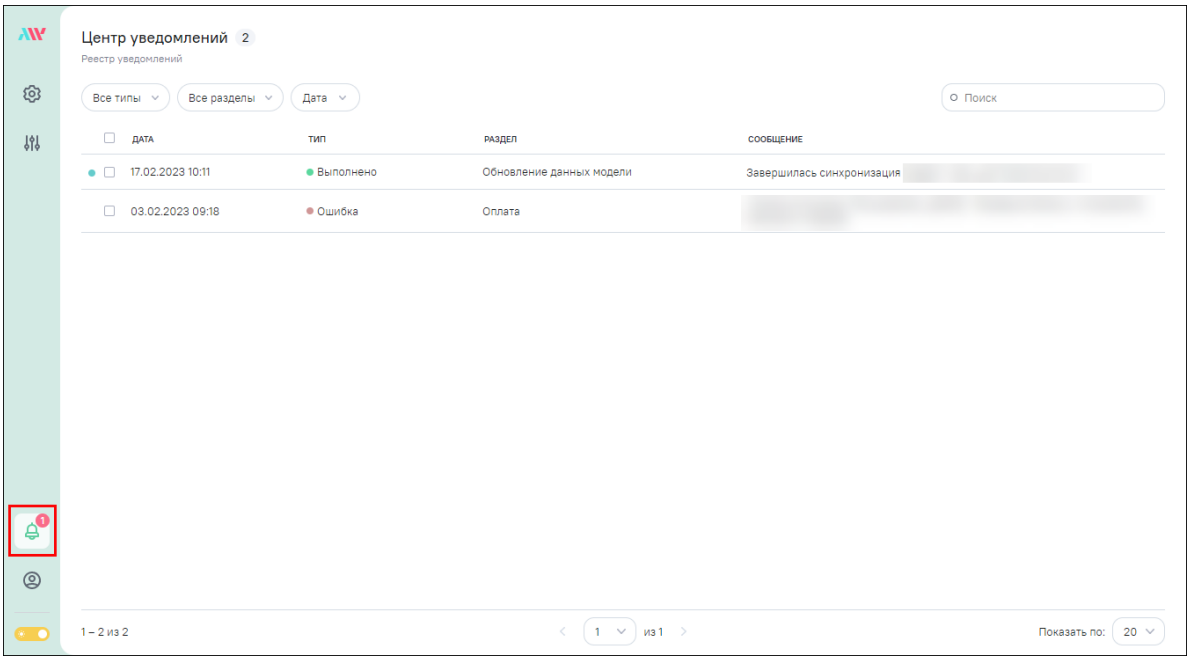


Рисунок 53 – Окно «Центр уведомлений»

Чтобы сменить тему AW, нажмите на кнопку  (Рисунок 54).

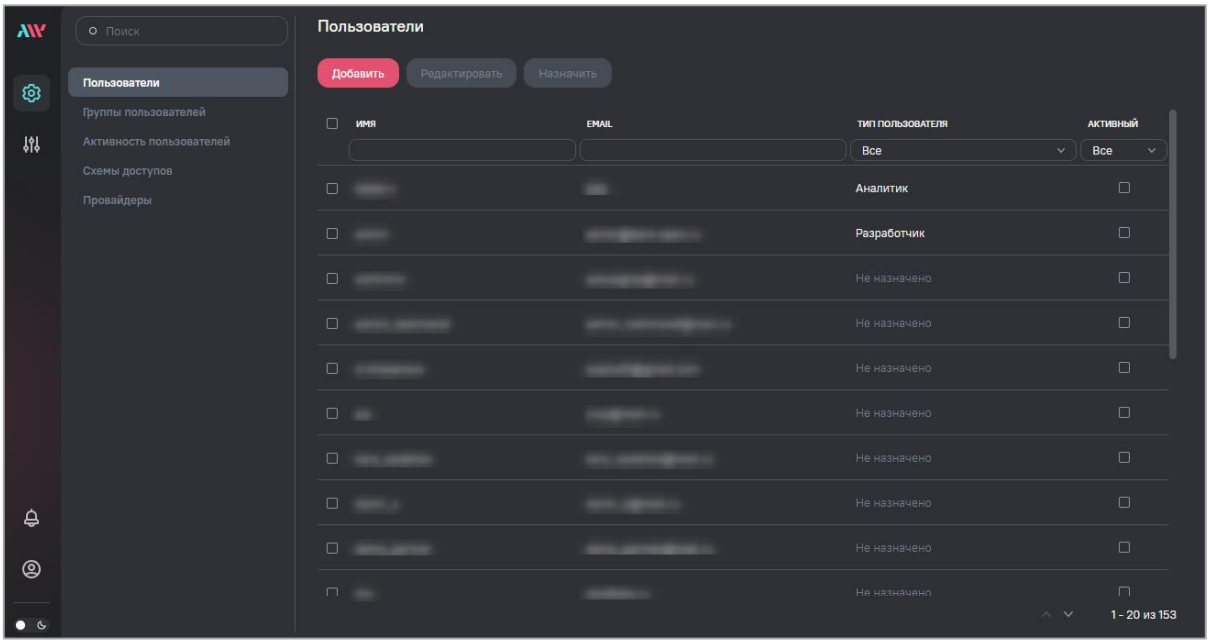


Рисунок 54 – Темная тема AW

В функции администратора AW входят задачи управления:

- пользователями (п. 15.6.1);
- группами пользователей (предназначены для массового присвоения пользователям стандартных наборов разрешений) (п. 15.6.2);
- активностью пользователей (п. 15.6.3);
- схемами доступов (п. 15.6.4);
- провайдерами (п. 15.6.5).

В AW действует разрешительная модель доступа пользователей к функциям и данным других пользователей. Доступ ко всему по умолчанию запрещен. Для созданных (своих объектов) пользователь получает доступ сразу (в рамках своих прав доступа к функциям). Пользователь может предоставить свои объекты в доступ другим пользователям и группам пользователей.

Пользовательский интерфейс блока администрирования построен в соответствии с указанным выше набором функций и имеет следующий вид (Рисунок 55):

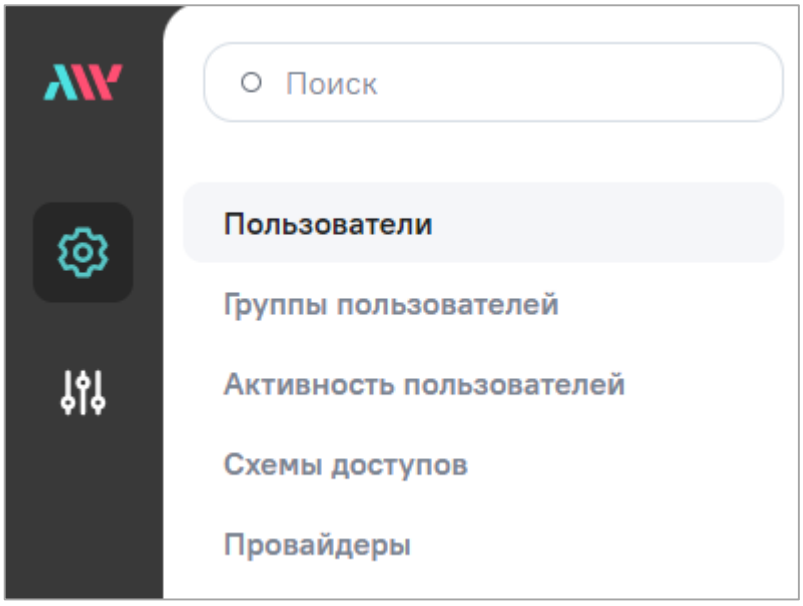


Рисунок 55 – Пользовательский интерфейс блока администрирования

15.6.1 Работа с пользователями Компонента анализа данных

Интерфейс управления пользователями (Рисунок 56) позволяет выполнять следующие действия:

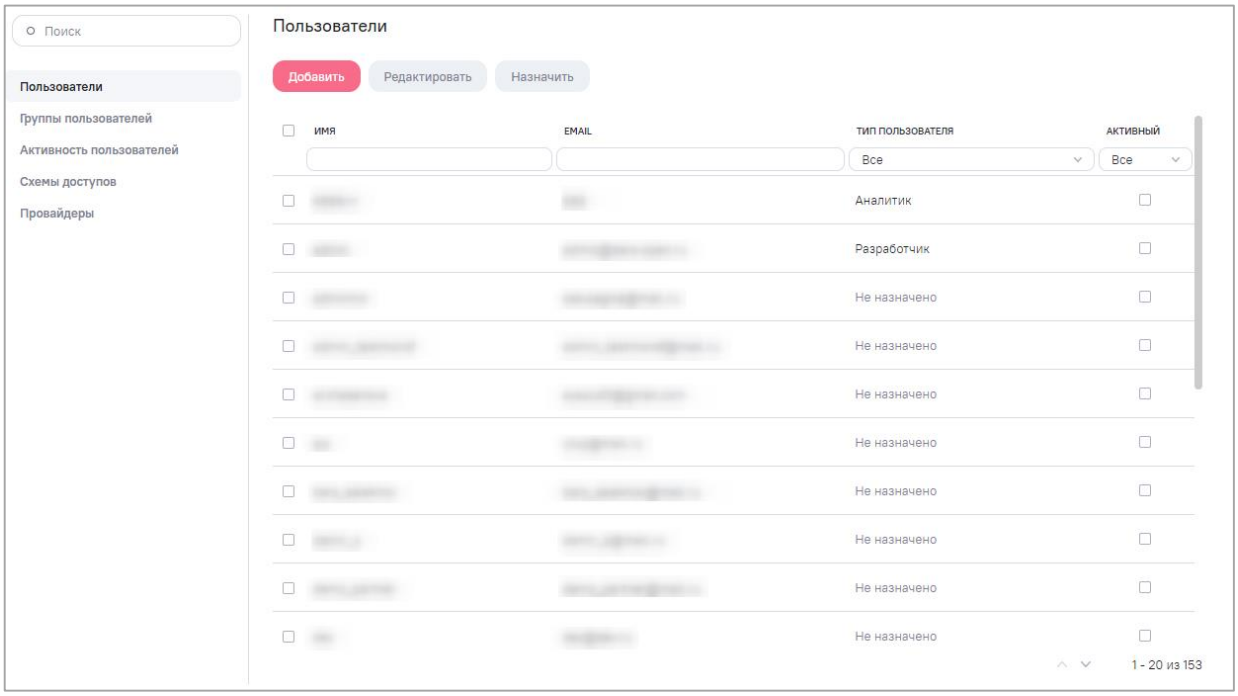


Рисунок 56 – Интерфейс управления пользователями

- создание учетных записей пользователей AW (15.6.1.1);
- редактирование учетных записей пользователей AW (15.6.1.2);

– назначение типа пользователей и изменение статуса активности учетных записей пользователей – установите «флажки» напротив необходимых записей и нажмите на кнопку «Назначить» на панели инструментов (Рисунок 56). Откроется окно для выбора типа пользователей и изменения статуса активности учетных записей пользователей (Рисунок 57). Установите «флажок» напротив типа и передвиньте переключатель в поле «Активный» (вправо (включен) – для предоставления доступа в AW, влево (выключен) – для блокировки доступа);

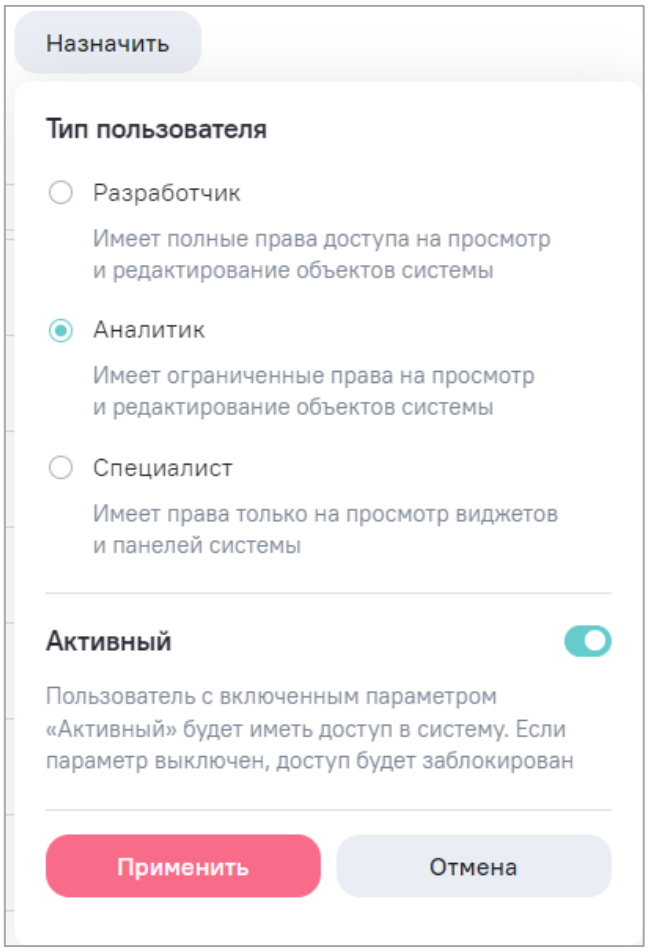


Рисунок 57 – Окно для выбора типа пользователей и изменения статуса активности учетных записей пользователей

Примечание – Доступно создание только пользователей с типом «Аналитик» в соответствии с доступными пользовательскими квотами лицензии.

– изменение типа пользователей (15.6.1.1);
– блокировка и активация учетных записей пользователей AW – в AW невозможно удалить пользователя. Пользователя можно только заблокировать (учетная запись пользователя станет неактивна). В AW можно блокировать ранее созданного (существующего) пользователя несколькими способами:

– в окне редактирования выбранной отдельной учетной записи пользователя – снимите «флажок» в поле «Активный» или нажмите на кнопку «Блокировать пользователя» (Рисунок 61). Откроется окно для подтверждения блокировки, в котором нажмите на кнопку «Блокировать» (Рисунок 58);

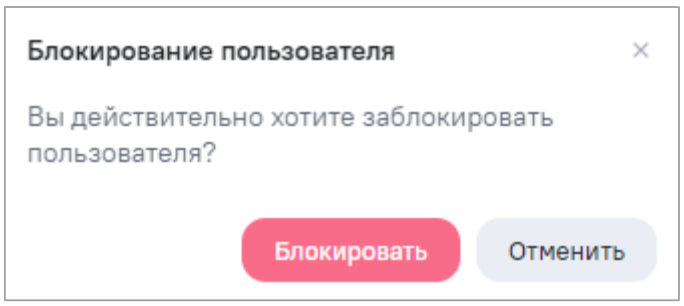


Рисунок 58 – Окно для подтверждения блокировки

– в интерфейсе просмотра списка пользователей – напротив необходимого пользователя снимите «флажок» в столбце «Активный» (Рисунок 59);

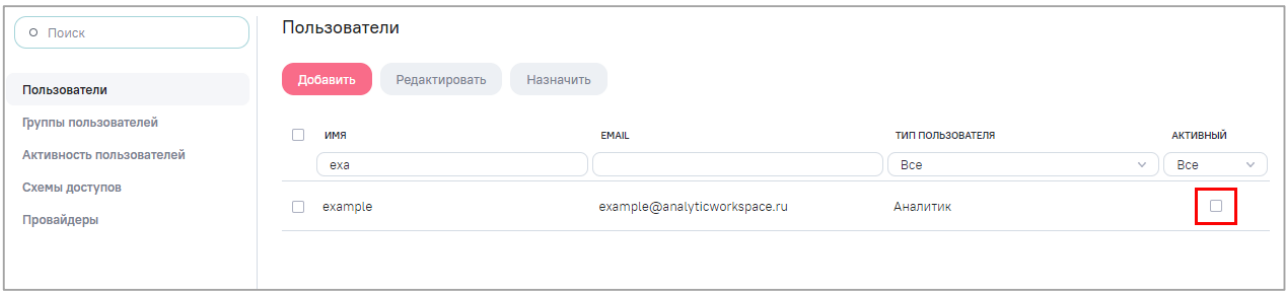


Рисунок 59 – Блокировка учетной записи пользователя в интерфейсе просмотра списка пользователей

– в интерфейсе просмотра списка пользователей, включая блокировку сразу нескольких – установите «флажки» напротив необходимых записей и нажмите на кнопку «Назначить» на панели инструментов. Откроется окно (Рисунок 57). Переведите переключатель параметра «Активный» в состояние выключен (влево) и нажмите на кнопку «Применить».

Заблокированного пользователя можно разблокировать, т.е. сделать активным.

По всем столбцам реализована сортировка по возрастанию/убыванию (Рисунок 56). Нажмите на наименование необходимого столбца, список пользователей отсортируется по возрастанию. Повторно нажмите на наименование столбца, список пользователей отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список пользователей отобразится без сортировки, и скроется кнопка сортировки.

В AW предусмотрена возможность настройки разделения прав доступа к разделам AW и к выполнению определенных операций с помощью установки пользовательских ролей.

Список пользовательских ролей (типов пользователей):

Примечание – Доступно создание только пользователей с типом «Аналитик» в соответствии с доступными пользовательскими квотами лицензии.

– «Аналитик» – специалист, обладающий правами на создание и изменение виджетов.

Примечание – Максимальное количество активных пользователей роли определяется лицензионными ограничениями по количеству пользовательских лицензий.

Описание предоставления доступа пользователей с типом «Аналитик» к объектам AW приведено в таблице ниже (Таблица 40).

Таблица 40 – Предоставление доступа пользователей с типом «Аналитик» к объектам AW

Описание права доступа к объектам AW	**Аналитик**
Доступ к разделу «Виджеты»	+
Просмотр и экспорт доступного виджета	+
Добавление виджета	+
Редактирование доступного виджета	+
Администрирование AW	-

Примечание – В таблице выше (Таблица 40) доступным называется объект AW, который создан текущим пользователем или к которому предоставлены соответствующие права.

15.6.1.1 Создание пользователей Компонента анализа данных

Доступно создание пользователей как в разделе «Пользователи» (с помощью кнопки «Добавить»), так и автоматическое создание пользователей при установке «флажка» в поле «Разрешить создание новых пользователей через внешнее управление» при настройке провайдера (п. 15.6.5).

Для создания учетной записи пользователя нажмите на кнопку «Добавить» на панели инструментов (Рисунок 56). Откроется окно создания нового пользователя (Рисунок 60), в котором заполните поля:

– «Логин» – введите логин (целое слово без пробелов латинскими буквами);

– «Тип пользователя» – выберите из выпадающего списка тип пользователя «Аналитик». Описание типов пользователя приведено в п. 15.6.1;

Примечание – В момент сохранения новой учетной записи пользователя или измененной учетной записи выполняется проверка доступных пользовательских лицензионных квот. Если доступных квот на требуемый тип пользователя нет – не сохраняются внесенные изменения. Доступно создание только пользователей с типом «Аналитик» в соответствии с доступными пользовательскими квотами лицензии.

- «Электронная почта» – введите электронную почту;
- «Пароль» – введите пароль. При установке «флажка» в поле «Предварительная проверка через LDAP сервер» необязательно указывать и подтверждать пароль;
- «Повторите пароль» – повторно введите пароль;
- установите «флажок» в поле «Активный». При создании нового пользователя «флажок» установлен автоматически;
- установите «флажок» в поле «Предварительная проверка через LDAP сервер» для прохождения авторизации через LDAP сервер.

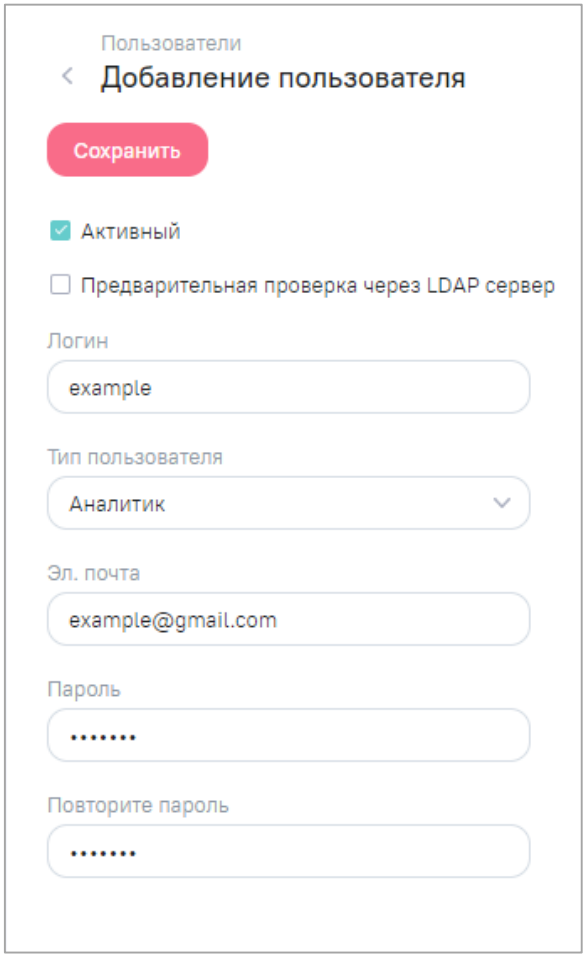
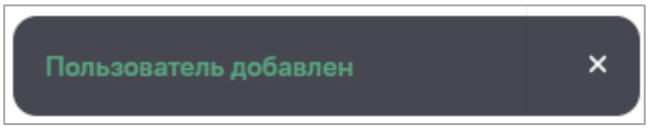


Рисунок 60 – Окно создания нового пользователя

Нажмите на кнопку «Сохранить». В случае успешного сохранения отобразится уведомление о внесенных изменениях 

.

Поле «Активный» позволяет временно отключить возможность входа в AW для созданного пользователя, не удаляя его совсем (снимите «флажок» или нажмите на кнопку «Блокировать пользователя»).

15.6.1.2 Редактирование пользователей Компонента анализа данных

Для изменения учетной записи пользователя установите «флажок» напротив необходимой записи и нажмите на кнопку «Редактировать» на панели инструментов (Рисунок 56). Откроется окно редактирования учетной записи пользователя (Рисунок 61).

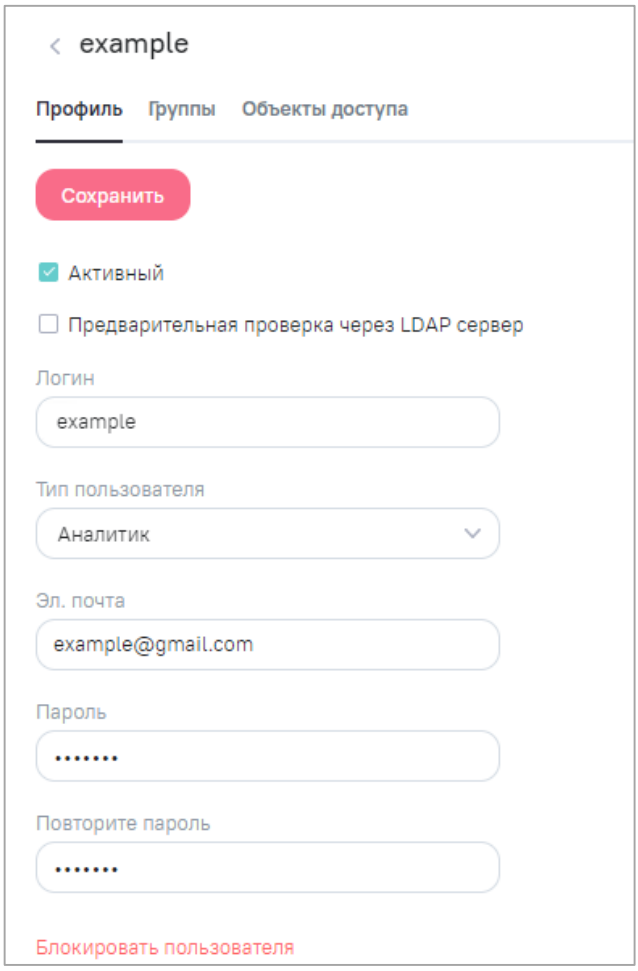


Рисунок 61 – Окно редактирования учетной записи пользователя

Операции изменения параметров и прав для существующего пользователя со стороны технического администратора AW включают возможности:

– изменение следующих данных пользователя:

- логин;
- тип пользователя;
- адрес электронной почты;
- пароль.

- блокировка или активация пользователя:
  - для блокировки пользователя снимите «флажок» в поле «Активный» или нажмите на кнопку «Блокировать пользователя»;
  - для активации пользователя установите «флажок» в поле «Активный».
- установка или снятие LDAP аутентификации – установите или снимите «флажок» в поле «Предварительная проверка через LDAP сервер»;
- просмотр и управление правами пользователя через принадлежность к группам пользователей.

Добавление доступа пользователю к группам и объектам доступны как для созданного (нового) пользователя, так и для изменяемого существующего. Переход к ним выполняется через окно редактирования выбранного пользователя.

Для существующего (созданного) пользователя в интерфейсе редактирования (Рисунок 61) отображаются вкладки «Группы» и «Объекты доступа».

Вкладка «Группы» содержит интерфейс просмотра и настройки групп, к которым отнесен данный пользователь, с целью передачи пользователю назначенных группе разрешений.

По умолчанию созданные пользователи включаются в те группы, которые указаны в качестве базовых групп в карточке соответствующего провайдера (п. 15.6.5).

Для включения пользователя в группы нажмите на кнопку «Добавить». Откроется окно, в котором доступен список системных и пользовательских групп с возможностью множественного выбора (Рисунок 62). Ранее добавленные группы в списке отображаются с установленным «флажком» и недоступны для повторного выбора. Для выбора всех групп установите «флажок» в поле «Выбрать все» и нажмите на кнопку «Применить».

Для выбора определенной группы в поле поиска начните вводить название группы, к которой необходимо предоставить права (Рисунок 62). В выпадающем списке отобразятся группы согласно параметрам поиска. Установите «флажки» напротив необходимых групп или установите «флажок» в поле «Выбрать найденные» для выбора групп, соответствующим параметрам поиска. Нажмите на кнопку «Применить».

Примечания

1 После каждой установки «флажка» в поле «Выбрать найденные» при разных значениях, введенных в поле поиска, новые значения будут добавляться к старым, а не заменять их.

2 В соответствии с доступными пользовательскими квотами лицензии можно создать только пользователей с типом «Аналитик» и выбрать для них только системные группы «Просмотр виджетов», «Просмотр уведомлений», «Просмотр личного кабинета» и пользовательские группы.

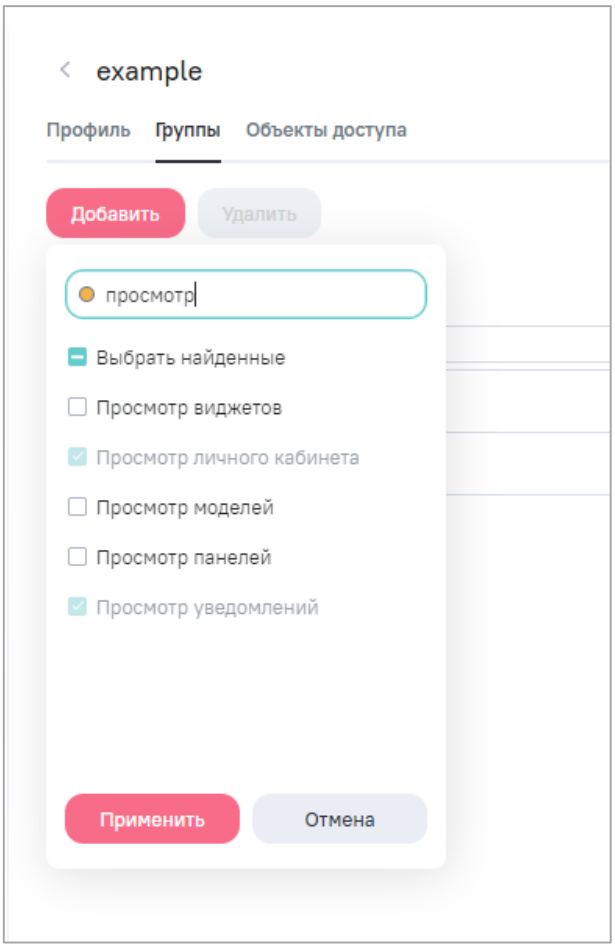


Рисунок 62 – Добавление пользователя в группы

Добавленные группы отображаются в общем списке групп данного пользователя. Пользователь получает все назначенные группе разрешения.

Для удаления пользователя из групп установите «флажки» напротив необходимых записей (Рисунок 63) и нажмите на кнопку «Удалить».

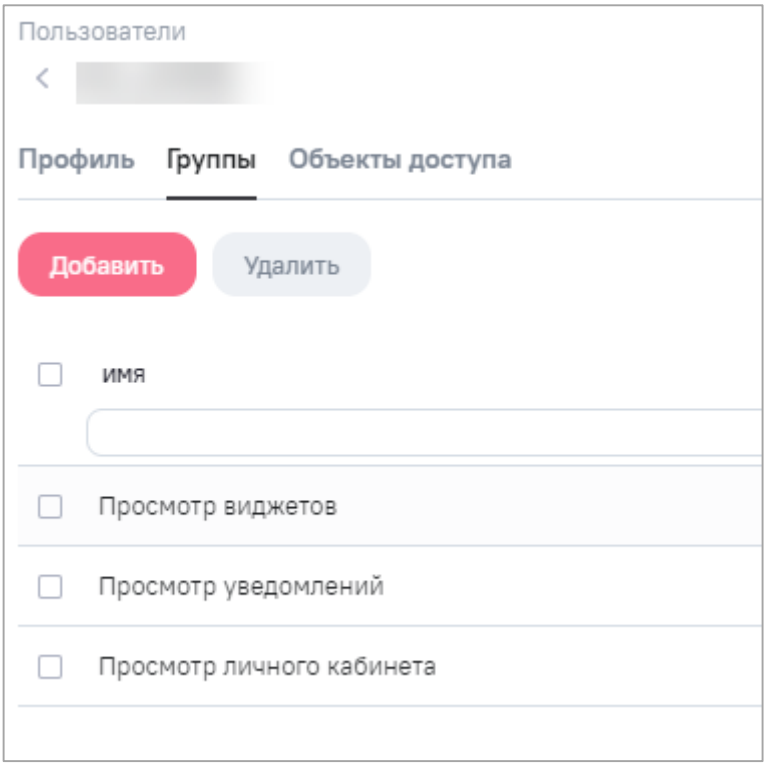


Рисунок 63 – Вкладка «Группы» – управление списком групп пользователя

Пользователь получает права доступа к объектам AW, если:

- они созданы им;
- права на них предоставлены ему другими пользователями – владельцами (создателями) объектов или имеющими права на их администрирование;
- права на них предоставлены ему техническим администратором AW.

Предоставление данных прав доступа выполняется в контексте конкретного объекта описано ниже.

Вкладка «Объекты доступа» (Рисунок 64) содержит интерфейс только для просмотра списка фактически установленных данному пользователю прав доступа к объектам AW. Данный список содержит поля:

- «Наименование» – наименование объекта, к которому предоставлен доступ;
- «Тип» – тип объекта AW;
- «Дата создания» – дата и время создания объекта;
- «Дата изменения» – дата и время изменения объекта.

Для удобства поиска прав в списке он содержит возможности фильтрации выводимой информации по всем перечисленным выше полям.

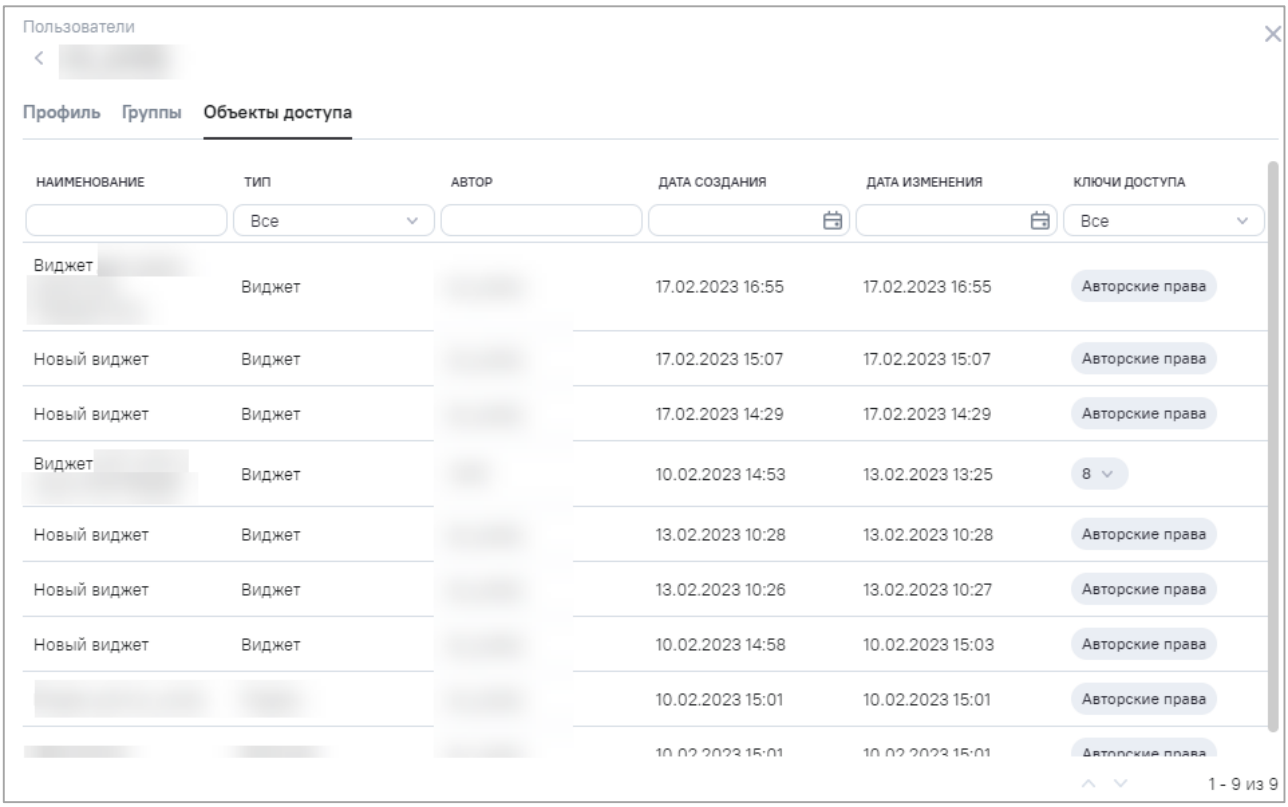


Рисунок 64 – Вкладка «Объекты доступа» – просмотр списка установленных пользователю прав доступа к объектам AW

15.6.2 Работа с группами пользователей

Группы пользователей предназначены для формирования, хранения и массового присвоения пользователям стандартных наборов разрешений. В AW реализованы два вида групп пользователей: системные и пользовательские (Рисунок 65).

На обеих вкладках («Системные» и «Пользовательские») по всем столбцам реализована сортировка по возрастанию/убыванию. Нажмите на наименование необходимого столбца, список групп пользователей отсортируется по возрастанию. Повторно нажмите на наименование столбца, список групп пользователей отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список групп пользователей отобразится без сортировки, и скроется кнопка сортировки.

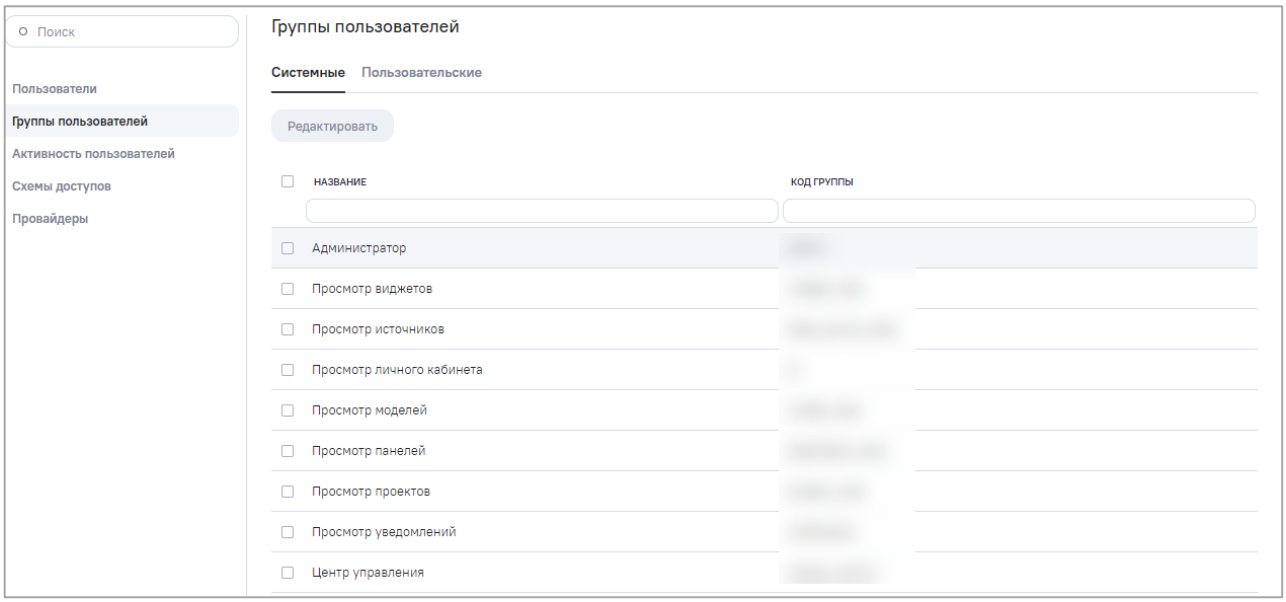


Рисунок 65 – Интерфейс управления группами пользователей

15.6.2.1 Вкладка «Системные»

Системные группы – встроенные группы, которые невозможно удалить или добавить новую даже техническому администратору AW. Системные группы обычно предназначены для выдачи пользователям комплекса разрешений, необходимых для работы в соответствующих функциональных блоках AW. Встроенными группами являются (Рисунок 66):

- «Администратор» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям администрирования AW;
- «Просмотр виджетов» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с виджетами;
- «Просмотр источников» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с источниками данных;
- «Просмотр личного кабинета» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям личного кабинета пользователя;
- «Просмотр моделей» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с моделями;
- «Просмотр панелей» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с информационными панелями;
- «Просмотр уведомлений» – предоставляет включенным в нее пользователям доступ к интерфейсу и функциям работы с центром уведомлений.

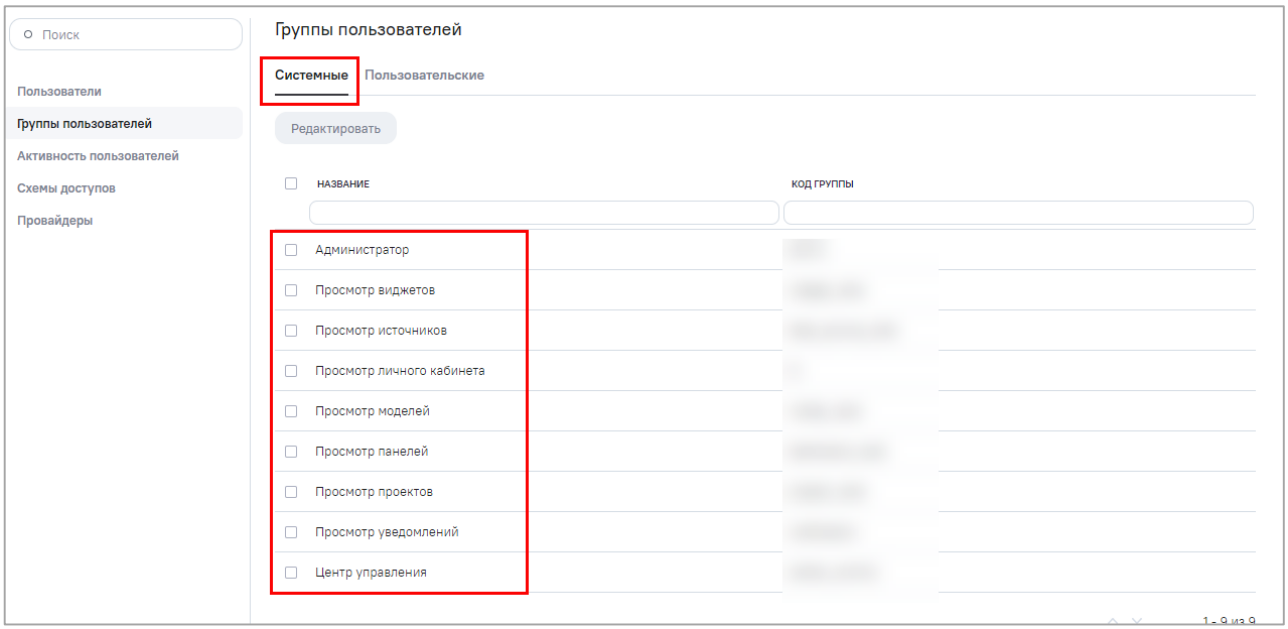


Рисунок 66 – Системные группы

Примечание – В соответствии с доступными пользовательскими квотами лицензии можно создать только пользователей с типом «Аналитик» и выбрать для них только системные группы «Просмотр виджетов», «Просмотр уведомлений», «Просмотр личного кабинета».

Доступ к системным группам зависит от типа пользователя. Описание предоставления доступа к системным группам для пользователей с типом «Аналитик» приведено в таблице ниже (Таблица 41).

Таблица 41 – Предоставление доступа системных групп пользователей к объектам AW для пользователей с типом «Аналитик»

№	Системная группа	Тип пользователя «Аналитик»
1	«Администратор» – доступ к разделу и функциям администрирования AW	-
2	«Просмотр виджетов»:	+
2.1	– доступ к разделу «Виджеты»	+
2.2	– просмотр и экспорт доступного виджета	+
2.3	– добавление виджета	+
2.4	– редактирование доступного виджета	+
3	«Просмотр личного кабинета»	+
4	«Просмотр уведомлений»	+

Примечание – В таблице выше (Таблица 41) доступным называется объект AW, который создан текущим пользователем или к которому предоставлены соответствующие права.

15.6.2.1.1 Редактирование системных групп пользователей

Для перехода к редактированию дважды нажмите левой кнопкой мыши на выбранной в списке системной группе или установите «флажок» напротив необходимой строки и нажмите на кнопку «Редактировать». Редактирование позволяет управлять составом группы на вкладке «Пользователи».

Для включения пользователей в группу нажмите на кнопку «Добавить». Откроется окно, в котором доступен список учетных записей пользователей AW с возможностью множественного выбора (Рисунок 67). Ранее добавленные пользователи в списке отображаются с установленным «флажком» и недоступны для повторного выбора. Для выбора всех пользователей установите «флажок» в поле «Выбрать все» и нажмите на кнопку «Применить».

Для выбора определенного пользователя в поле поиска начните вводить логин пользователя (Рисунок 67). В выпадающем списке отобразятся логины пользователей согласно параметрам поиска. Установите «флажки» напротив необходимых записей или установите «флажок» в поле «Выбрать найденные» для выбора пользователей, соответствующих параметрам поиска. Нажмите на кнопку «Применить».

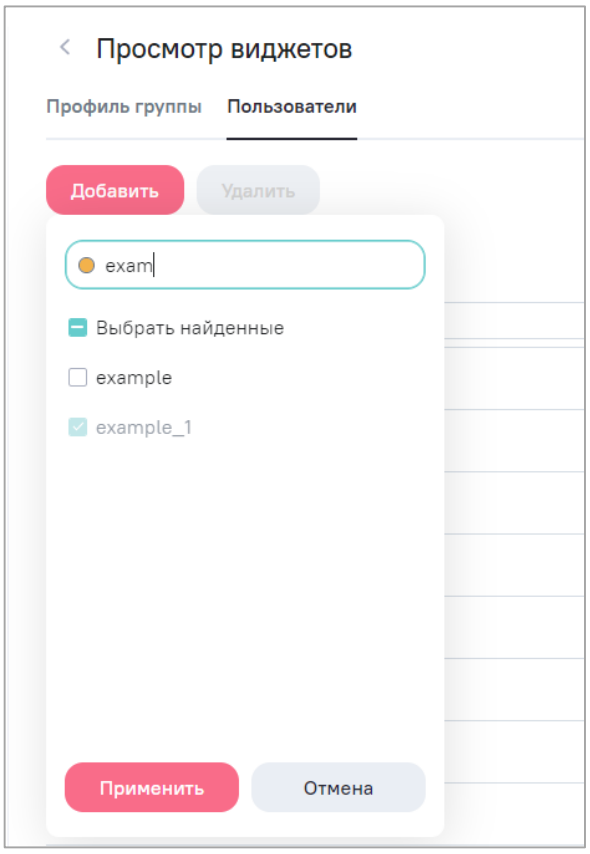


Рисунок 67 – Управление составом системных групп

Добавленные учетные записи пользователей отображаются в общем списке пользователей данной группы (Рисунок 68). Пользователи получают все назначенные группе разрешения.

Примечание – Список учетных записей пользователей формируется в зависимости от доступности системной группы типу пользователя, указанному в учетной записи (Таблица 41).

Для удаления пользователей из группы установите «флажки» напротив необходимых учетных записей в списке и нажмите на кнопку «Удалить».

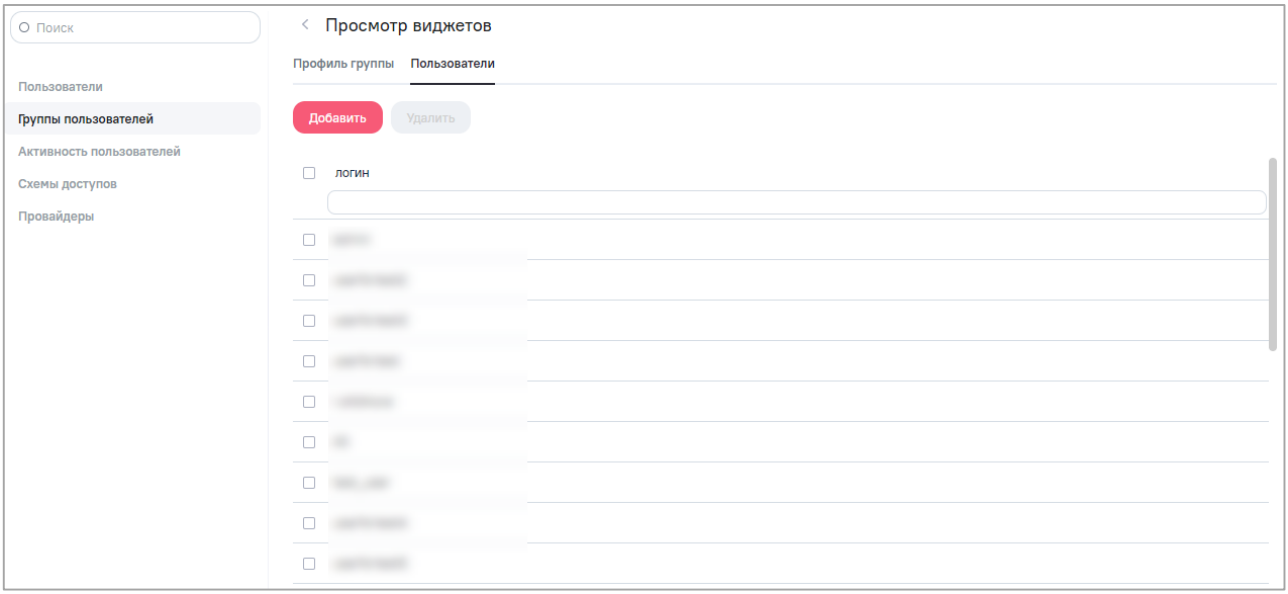


Рисунок 68 – Вкладка «Пользователи» – управление списком пользователей, включенных в группу

15.6.2.2 Вкладка «Пользовательские»

Пользовательские группы – группы, создаваемые, редактируемые и удаляемые техническим администратором AW, позволяющие создать и сохранить целевой набор разрешений на доступ к объектам AW (конкретным виджетам) и присвоить эти права нескольким пользователям (Рисунок 69).

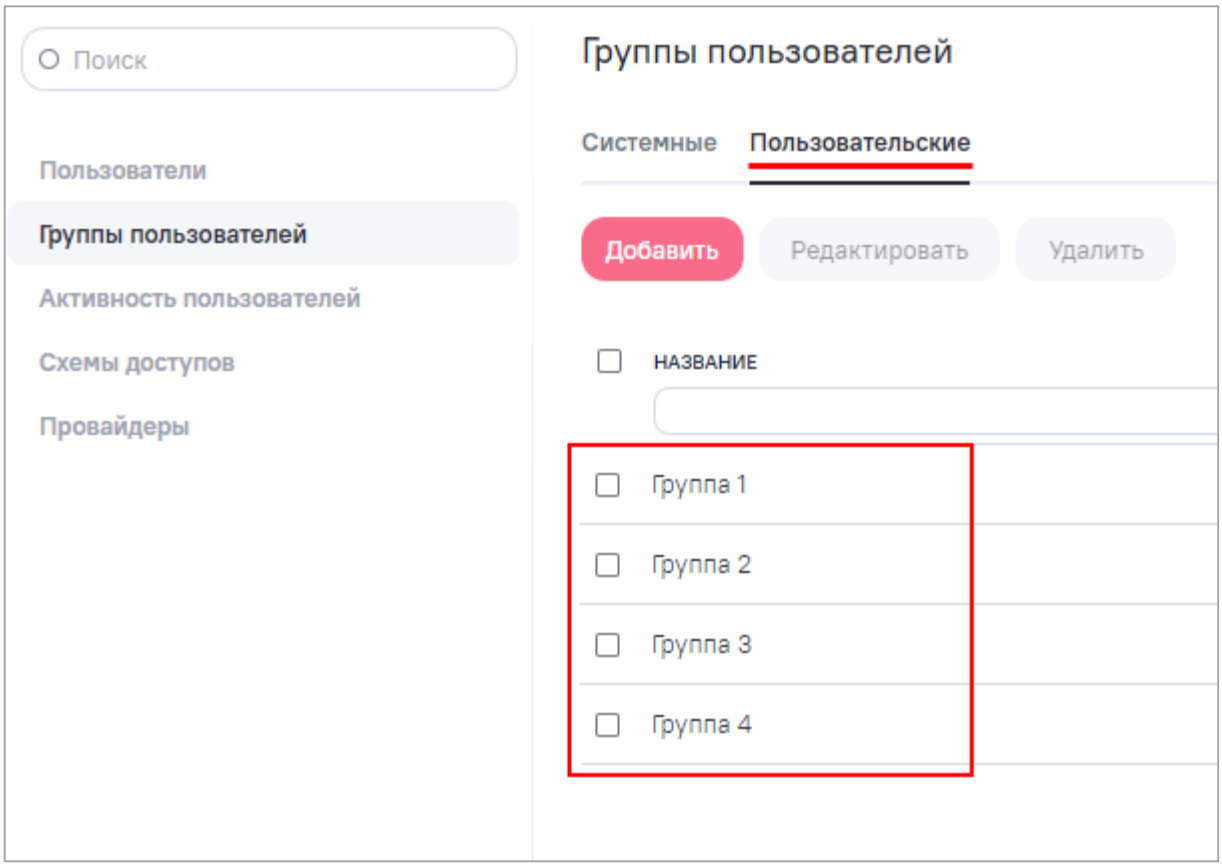


Рисунок 69 – Пользовательские группы

Интерфейс управления пользовательскими группами позволяет выполнять:

- создание групп пользователей AW (кнопка «Добавить»);
- редактирование групп пользователей AW;
- удаление групп пользователей AW.

15.6.2.2.1 Создание пользовательских групп

Для добавления новой пользовательской группы заполните поля:

- «Код группы» – введите код группы (латинскими буквами, одним словом, без пробелов), который может быть использован при авторизации пользователя через внешний провайдер;
- «Наименование» – введите наименование группы.

Нажмите на кнопку «Сохранить». Откроется интерфейс редактирования пользовательской группы (Рисунок 70).

15.6.2.2.2 Редактирование пользовательских групп

Чтобы отредактировать группу, дважды нажмите левой кнопкой мыши по группе в списке или установите «флажок» напротив необходимой строки. Нажмите на кнопку

«Редактировать». Откроется окно редактирования пользовательской группы на вкладке «Профиль группы» (Рисунок 70).

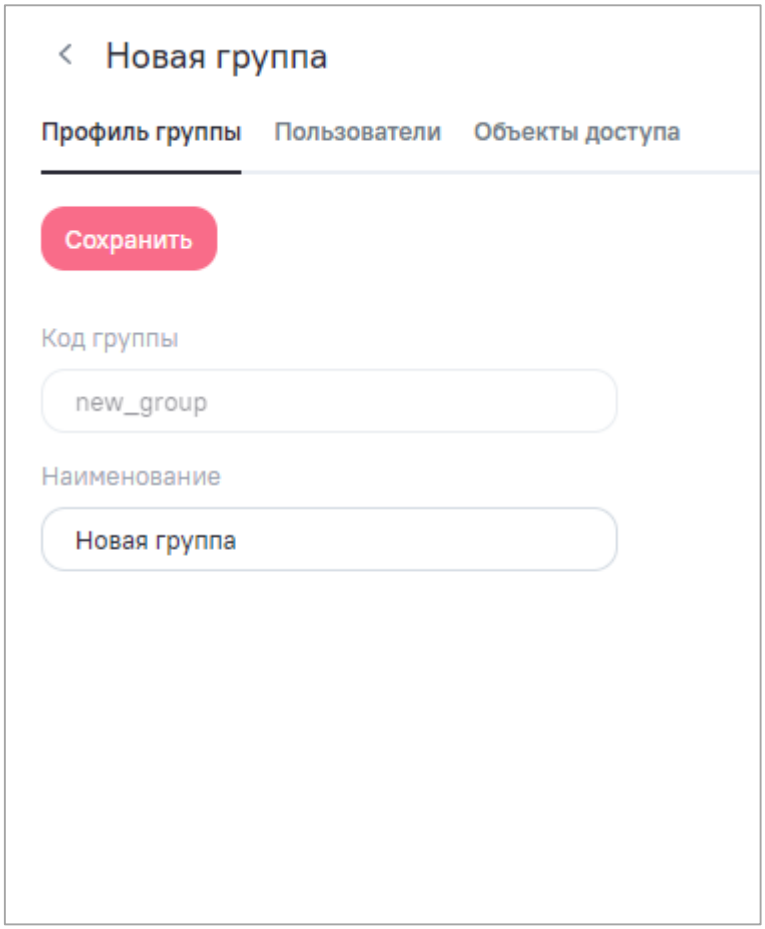


Рисунок 70 – Редактирование пользовательской группы

При редактировании группы можно изменить ее наименование (на вкладке «Профиль группы»), а также управлять составом группы (добавить или исключить пользователей на вкладке «Пользователи») или просматривать объекты доступа (на вкладке «Объекты доступа»).

Для включения пользователей в группу нажмите на кнопку «Добавить». Откроется окно, в котором доступен список учетных записей пользователей AW с возможностью множественного выбора (Рисунок 71). Ранее добавленные пользователи в списке отображаются с установленным «флажком» и недоступны для повторного выбора. Для выбора всех пользователей установите «флажок» в поле «Выбрать все» и нажмите на кнопку «Применить».

Для выбора определенного пользователя в поле поиска начните вводить логин пользователя (Рисунок 71). В выпадающем списке отобразятся логины пользователей согласно параметрам поиска. Установите «флажки» напротив необходимых записей или

установите «флажок» в поле «Выбрать найденные» для выбора пользователей, соответствующих параметрам поиска. Нажмите на кнопку «Применить».

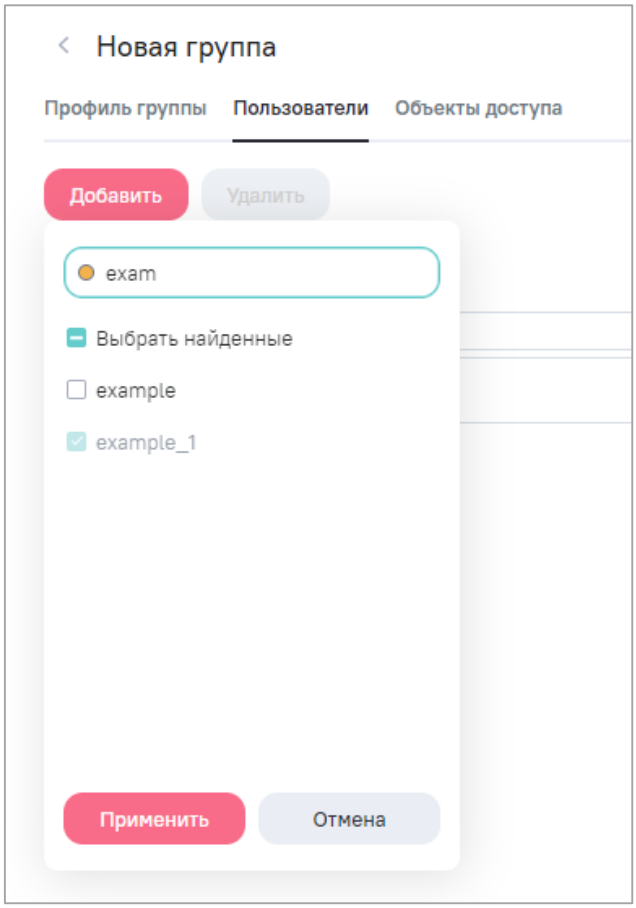


Рисунок 71 – Управление составом пользовательских групп

Примечание – После каждой установки «флажка» в поле «Выбрать найденные» при разных значениях, введенных в поле поиска, новые значения будут добавляться к старым, а не заменять их.

Добавленные учетные записи пользователей отображаются в общем списке пользователей данной группы (Рисунок 72). Пользователи получают все назначенные группе разрешения.

Для удаления пользователей из группы установите «флажки» напротив необходимых учетных записей в списке и нажмите на кнопку «Удалить».

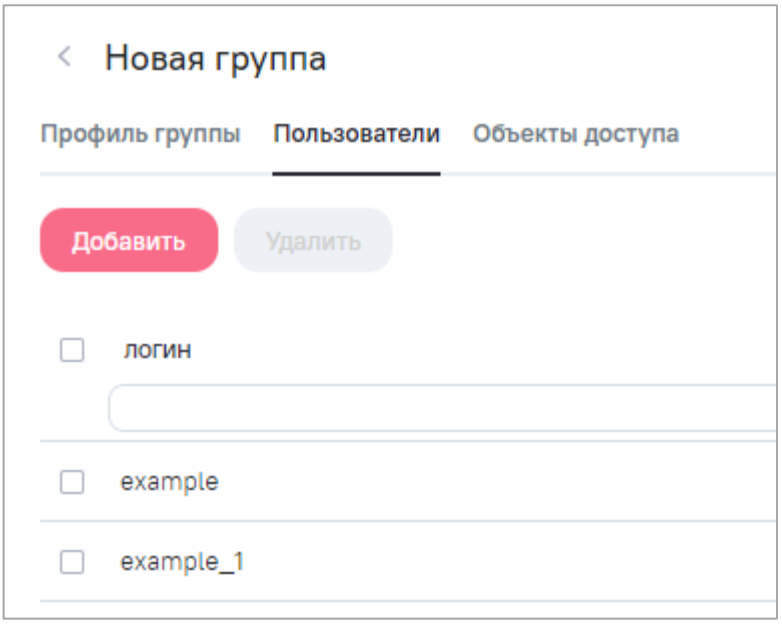


Рисунок 72 – Вкладка «Пользователи» – управление списком пользователей, включенных в группу

Группа пользователей получает права доступа к объектам AW, если:

– права ей предоставлены другими пользователями – владельцами (создателями) объектов или имеющими права на их администрирование;
– права ей предоставлены техническим администратором AW.

Предоставление данных прав доступа выполняется в контексте конкретного объекта описано ниже.

Вкладка «Объекты доступа» содержит интерфейс только для просмотра списка фактически установленных данной группе прав доступа к объектам AW (Рисунок 73). Данный список содержит поля:

– «Наименование» – наименование объекта, к которому предоставлен доступ;
– «Тип» – тип объекта AW;
– «Дата создания» – дата и время создания объекта;
– «Дата изменения» – дата и время изменения объекта.

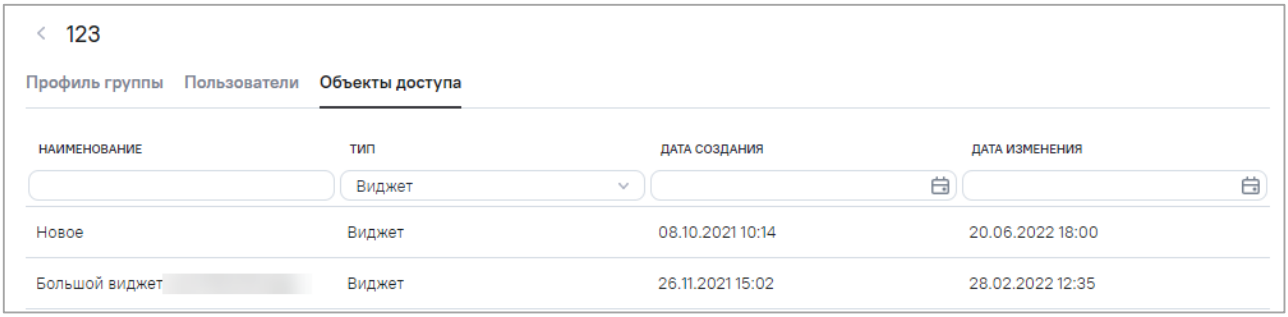


Рисунок 73 – Просмотр списка объектов доступа пользовательских групп

Для удобства поиска прав в списке есть возможность фильтрации выводимой информации по всем полям.

15.6.2.2.3 Удаление пользовательских групп

AW позволяет удалить ранее созданную (существующую) пользовательскую группу в интерфейсе просмотра списка групп пользователей. Для этого выберите нужную группу пользователей и нажмите на кнопку «Удалить». Аналогично можно выбрать и удалить сразу несколько пользовательских групп.

Перед удалением откроется окно подтверждения действия.

15.6.3 Работа с активностью пользователей

Активность пользователей выводит информацию о пользовательских сессиях в виде таблицы со следующими полями (Рисунок 74):

- «Имя» – логин пользователя;
- «IP-адрес»;
- «Дата и время входа»;
- «Дата и время выхода»;
- «Время активности».

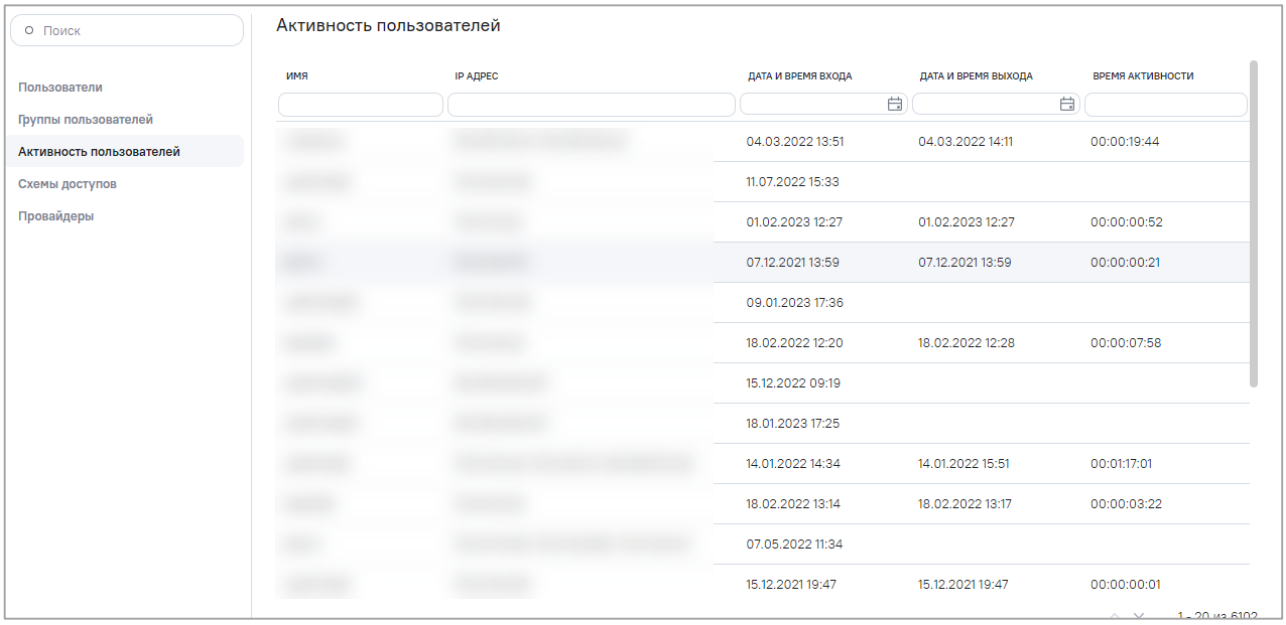


Рисунок 74 – Окно «Активность пользователей»

По столбцу «Имя» реализована сортировка по возрастанию/убыванию. Нажмите на наименование столбца, список записей отсортируется по возрастанию. Повторно нажмите на наименование столбца, список записей отсортируется по убыванию. Нажмите на

наименование столбца в третий раз, список записей отобразится без сортировки, и скроется кнопка сортировки.

15.6.4 Управление схемами доступов

Схема доступов является дополнительным слоем между данными провайдеров и данными пользователей AW. Упрощает настройку прав доступа к данным модели при добавлении нового провайдера.

Интерфейс управления схемой доступов (Рисунок 75) позволяет выполнять:

– создание атрибутов доступа;

– редактирование атрибутов доступа;

– удаление атрибутов доступа.

Схема доступов представляет собой список атрибутов доступа, которые передаются внешними провайдерами в AW при авторизации пользователя (п. 15.8).

В AW есть встроенные атрибуты доступа «login» (логин), «email» (E-mail), «state» (статус) и «user_roles» (роль). По ним сопоставляется учетная запись пользователя, и обновляются его данные. Встроенные атрибуты не подлежат редактированию и удалению.

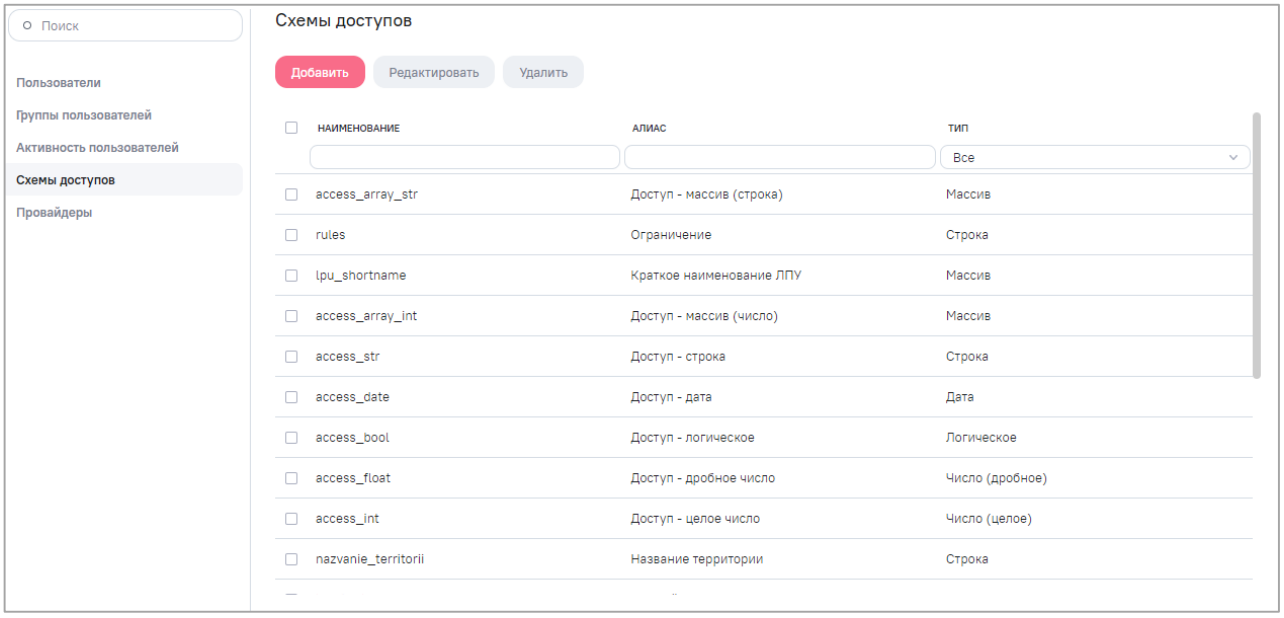


Рисунок 75 – Интерфейс управления схемами доступа

По всем столбцам реализована сортировка по возрастанию/убыванию. Нажмите на наименование необходимого столбца, список записей отсортируется по возрастанию. Повторно нажмите на наименование столбца, список записей отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список записей отобразится без сортировки, и скроется кнопка сортировки.

Чтобы принимать от провайдера атрибуты пользователя в виде массива данных, в том числе ролей пользователей, в схеме доступов для данных атрибутов выберите тип данных «Массив» (Рисунок 76).

15.6.4.1 Создание атрибутов доступа

Чтобы создать атрибут доступа, нажмите на кнопку «Добавить» в интерфейсе управления схемами доступа (Рисунок 75).

Откроется окно добавления нового атрибута доступа (Рисунок 76). Для добавления атрибута укажите следующие параметры:

- «Наименование» – целое слово без пробелов латинскими буквами, уникальное в рамках схемы;
- «Алиас»;
- «Тип» – выберите значение из выпадающего списка. Доступны следующие значения:
- «Число (целое)»;
- «Число (дробное)»;
- «Логическое»;
- «Строка»;
- «Дата»;
- «Массив».

Нажмите на кнопку «Сохранить». В случае успешного сохранения отобразится уведомление о внесенных изменениях «Атрибут добавлен».

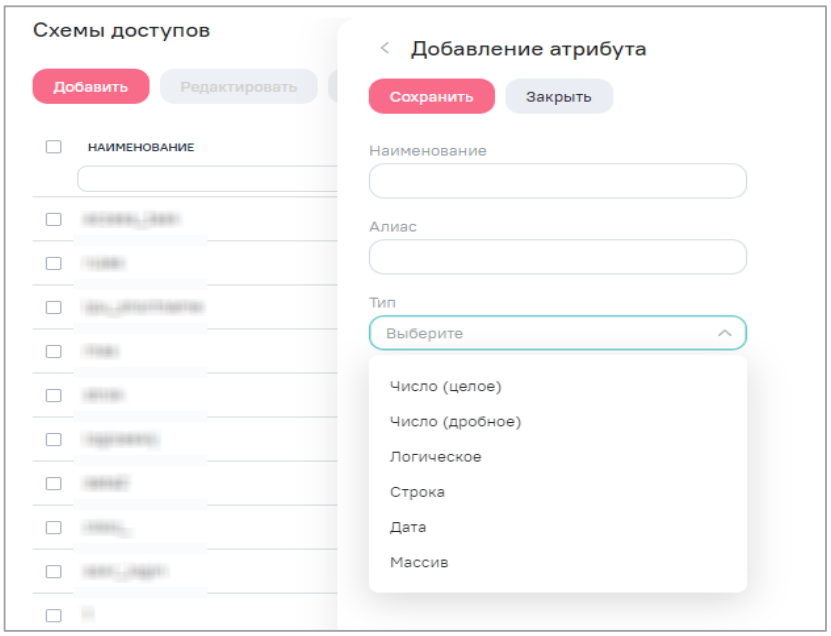


Рисунок 76 – Окно создания атрибута доступа

15.6.4.2 Редактирование атрибутов доступа

Чтобы отредактировать атрибут, дважды нажмите левой кнопкой мыши по записи в списке или установите «флажок» напротив необходимой строки и нажмите на кнопку «Редактировать» (Рисунок 77).

При редактировании атрибута можно изменить его наименование, алиас, а также тип данных.

Примечание – Редактировать можно только те атрибуты, которые не задействованы ни в одном из провайдеров (15.6.5.3).

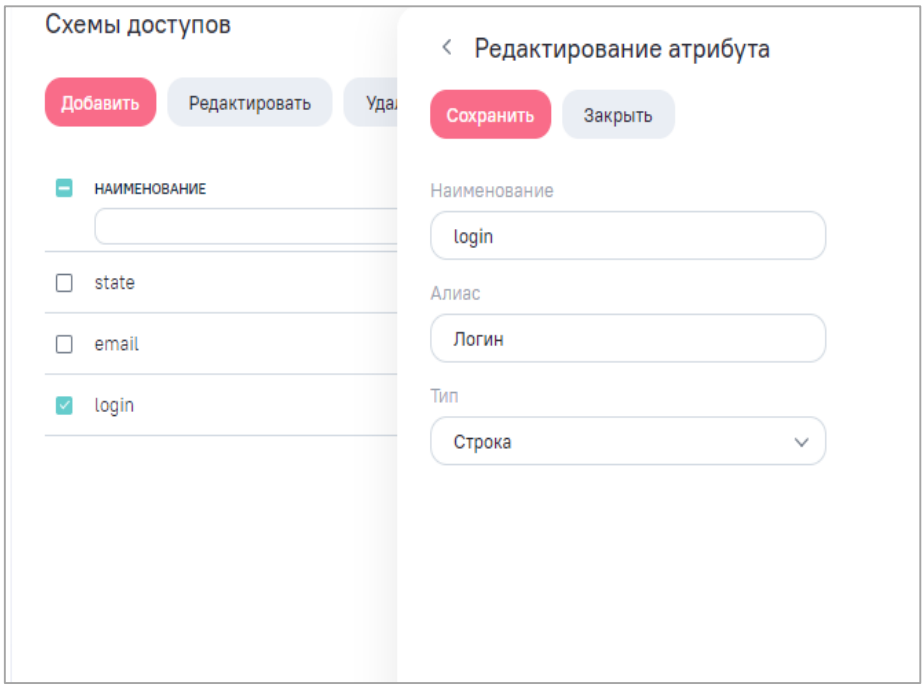


Рисунок 77 – Редактирование атрибута доступа

15.6.4.3 Удаление атрибутов доступа

Ранее созданный атрибут можно удалить в интерфейсе просмотра списка атрибутов доступа. Для этого выберите нужный атрибут и нажмите на кнопку «Удалить». Чтобы удалить несколько атрибутов, установите напротив них «флажки» и нажмите на кнопку «Удалить».

Перед удалением атрибута (нескольких атрибутов) откроется окно подтверждения действия.

Примечание – Удалить можно только те атрибуты, которые не задействованы ни в одном из провайдеров (п. 15.6.5).

15.6.5 Управление провайдерами

Раздел «Провайдеры» предназначен для настройки взаимодействия AW с провайдерами пользователей: системами идентификации, аутентификации и авторизации (ИА). В AW есть внутренний провайдер «AW» с типом «Локальный (user_permissions)», который используется только для технического администратора AW. Также в AW можно настроить авторизацию через внешний сервис аутентификации по протоколам Open ID Connect и LDAP.

С помощью OpenID Connect и LDAP пользователи могут проходить аутентификацию и авторизацию в нескольких облачных приложениях через единую точку с использованием одного логина и пароля.

Данный раздел представляет собой реестр всех настроенных провайдеров пользователей (Рисунок 78). В реестре отображается информация о провайдерах в полях:

– «Наименование»;

– «Тип»;

– «Активность».

По всем столбцам реализована сортировка по возрастанию/убыванию. Нажмите на наименование необходимого столбца, список провайдеров отсортируется по возрастанию. Повторно нажмите на наименование столбца, список провайдеров отсортируется по убыванию. Нажмите на наименование столбца в третий раз, список провайдеров отобразится без сортировки, и скроется кнопка сортировки.

Интерфейс управления провайдерами позволяет выполнять:

– создание провайдера;

– редактирование провайдера;

– удаление провайдера.

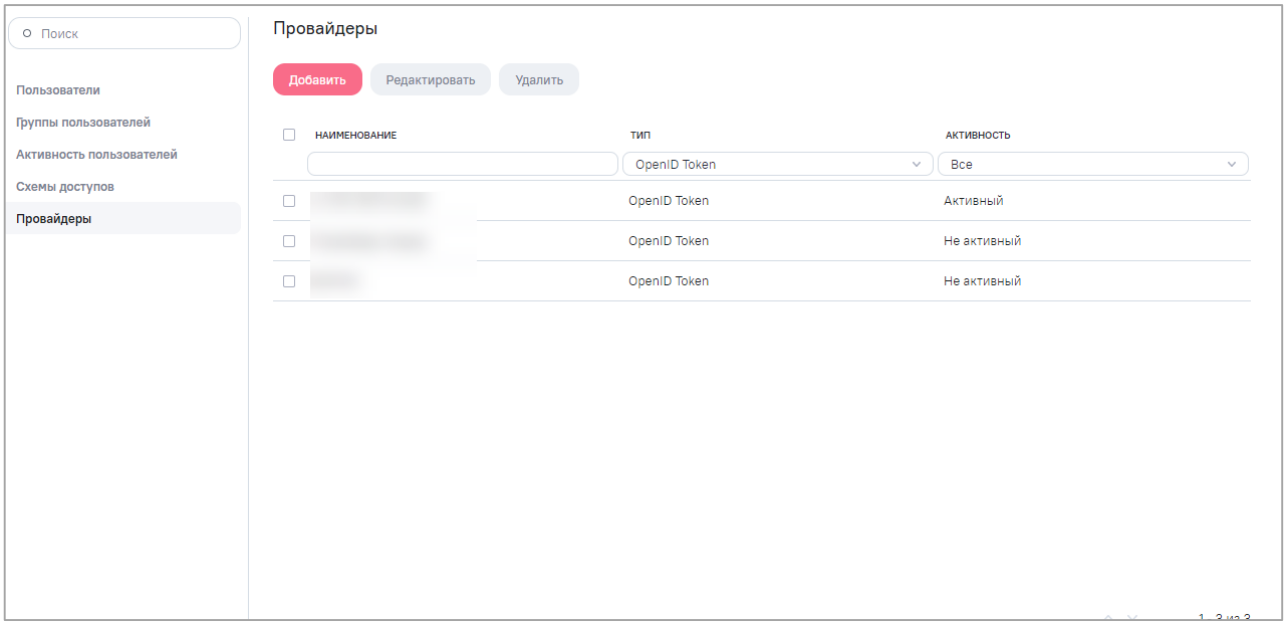


Рисунок 78 – Интерфейс управления провайдерами

Чтобы настроить взаимодействие, произведите настройку для обоих участников взаимодействия: провайдера (поставщика учетных записей) и AW (поставщика сервиса). Для настройки взаимодействия AW с провайдером выполните шаги, описанные в п. 15.6.5.3.

Примечание – Предполагается, что взаимодействие провайдера (поставщика учетных записей) с AW настроено и учетные записи зарегистрированы.

15.6.5.1 Создание внешнего провайдера

Чтобы создать внешний провайдер, нажмите на кнопку «Добавить» в интерфейсе управления провайдерами.

Откроется окно создания и настроек провайдера (Рисунок 79), которое состоит из вкладок:

- «Основное»;
- «Параметры»;
- «Маппинг схемы».

Для ввода данных провайдера в AW заполните обязательные поля на вкладках «Основное» и «Параметры» и нажмите на кнопку «Сохранить». В случае успешного сохранения отобразится уведомление о внесенных изменениях: «Провайдер сохранен».

Вкладка «Основное» предназначена для ввода стартовой информации о провайдере (Рисунок 79). Заполните поля:

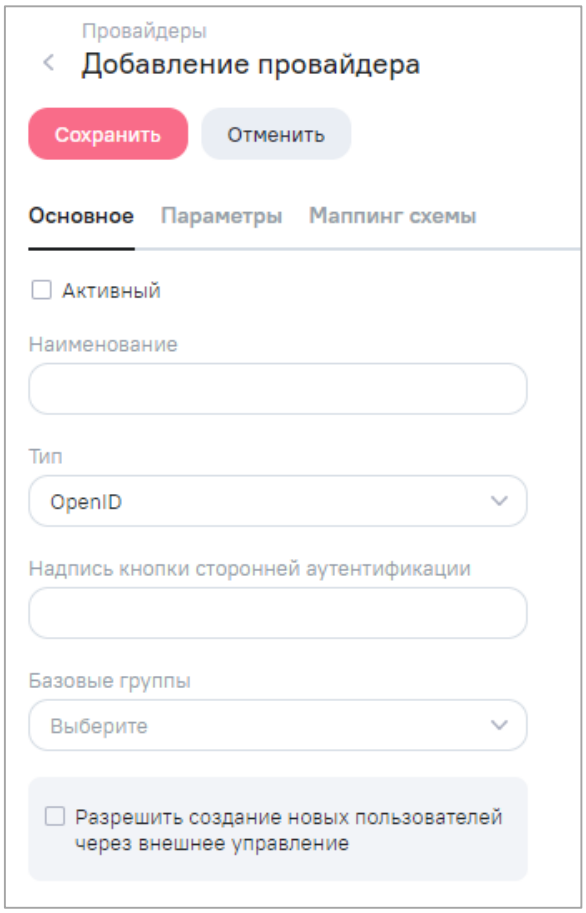


Рисунок 79 – Создание провайдера, вкладка «Основное»

- «Активный» – установите «флажок» в поле, чтобы провайдер стал активным;
- «Наименование» – введите дружественное имя провайдера в AW, поле обязательно для заполнения;

- «Тип» – выберите из выпадающего списка разновидность провайдера в зависимости от протокола взаимодействия. Поддерживаются четыре типа провайдеров:
  - внутренний – «Локальный (user_permissions)»;
  - внешние:
- «OpenID»;
- «OpenID Token»;
- «LDAP».

Примечание – Для перехода пользователей из ПП М3 в AW используется только провайдер «OpenID Token».

- «Надпись кнопки сторонней аутентификации» – введите надпись кнопки, которая будет отображаться на странице авторизации AW и выполнять переход на страницу авторизации провайдера (для провайдеров типа «OpenID»);
- «Базовые группы» – выберите одно или несколько значений из выпадающего списка системных и пользовательских групп пользователей. Выбранные группы будут присваиваться пользователям автоматически при создании (для всех типов провайдеров) и при авторизации пользователя через SSO (для провайдеров типа «OpenID», «OpenID Token», «LDAP»);
- «Разрешить создание новых пользователей через внешнее управление» – установите «флажок» в параметр, при включении которого в AW будет создаваться новый пользователь в случае его отсутствия. Если «флажок» не установлен, новый пользователь получит уведомление: «Для указанного в запросе пользователя не создана учетная запись. Необходимо обратиться к Администратору Системы». При установке «флажка» в поле «Разрешить создание новых пользователей через внешнее управление» отобразится дополнительное поле «Тип пользователя», в котором в выпадающем списке выберите тип пользователя, с которым будут создаваться новые пользователи, учитывая квоты на тип пользователя в лицензии (Рисунок 80).

Примечание – Если при создании пользователя через провайдера не окажется свободных пользовательских лицензионных квот, то учетная запись будет создана с неактивным статусом.

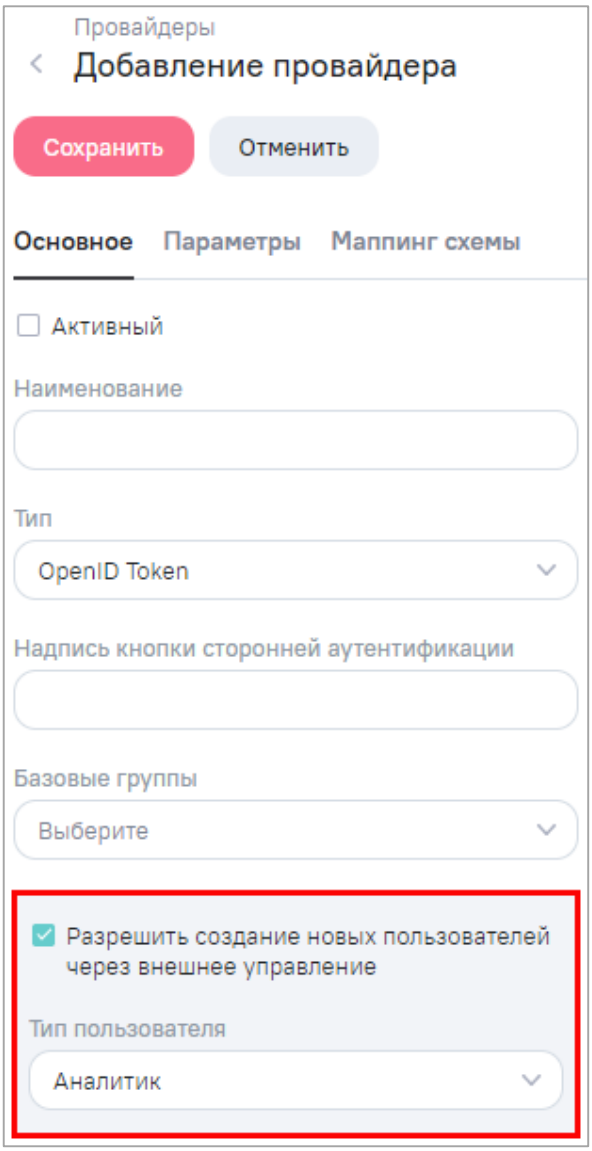


Рисунок 80 – Создание провайдера, вкладка «Основное». Поле «Разрешить создание новых пользователей через внешнее управление»

Внешний провайдер с типом «OpenID Token» построен на базе провайдера с типом «OpenID». Отличительной чертой является то, что данный тип провайдера не отображается в окне авторизации AW и для его настройки достаточно указать:

– на вкладке «Основное» – наименование и тип;

– на вкладке «Параметры» – идентификатор ИА и внешний URL.

Провайдер с типом «OpenID Token» применяется для бесшовного перехода в AW внутри стороннего приложения через единую точку входа и в случае работы с API AW.

Вкладка «Параметры» предназначена для ввода идентифицирующей информации о взаимодействии AW и внешнего провайдера. Данную информацию передает администратор провайдера при регистрации заявки на подключение AW к

промышленному/тестовому контору ИА. Состав полей на вкладке зависит от типа провайдера, выбранного на вкладке «Основное».

Для типов провайдеров «OpenID» и «OpenID Token» вкладка содержит поля (Рисунок 81):

- «Идентификатор ИА» – поле обязательное для заполнения;
- «Секретный ключ доступа» – поле обязательное для заполнения только для провайдера типа «OpenID»;
- «Внешний URL» – поле обязательное для заполнения.

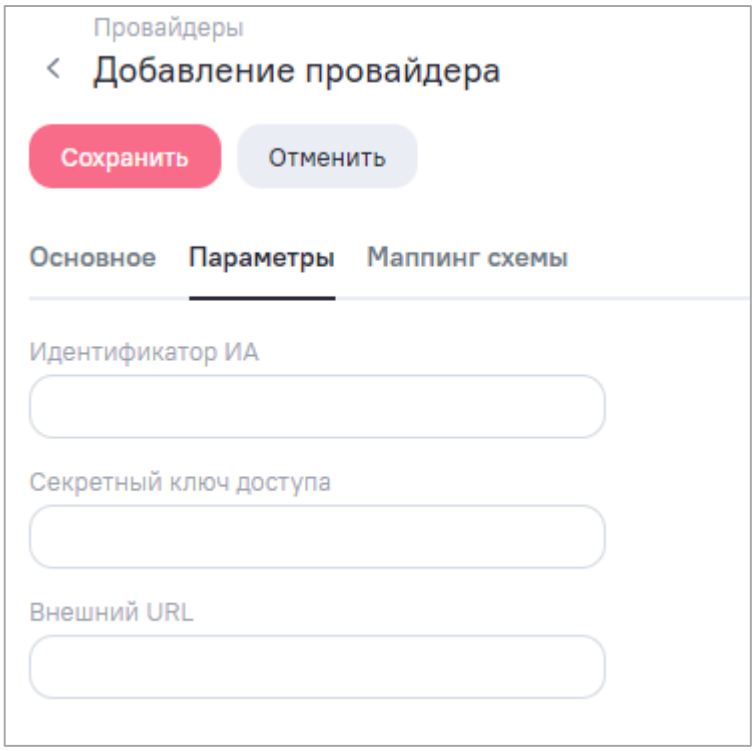


Рисунок 81 – Создание провайдера, вкладка «Параметры» для типов провайдеров «OpenID» и «OpenID Token»

Вкладка «Маппинг схемы» содержит интерфейс для задания правил сопоставления атрибутов доступа схемы и атрибутов доступа провайдера пользователей (Рисунок 82). Вкладка содержит:

- параметр «Без соответствия» – при включении параметра отображаются атрибуты доступа схемы, которым не задано соответствие с атрибутами провайдера;
- таблицу соответствия:
- в первом столбце перечислены все атрибуты доступа схемы, объявленные в разделе AW «Схемы доступов» (п. 15.6.4);

– во втором столбце можно указать соответствующие атрибуты, передаваемые провайдером при взаимодействии:
  – для «user_roles» – «preferred_username»;
  – «email» – «email».

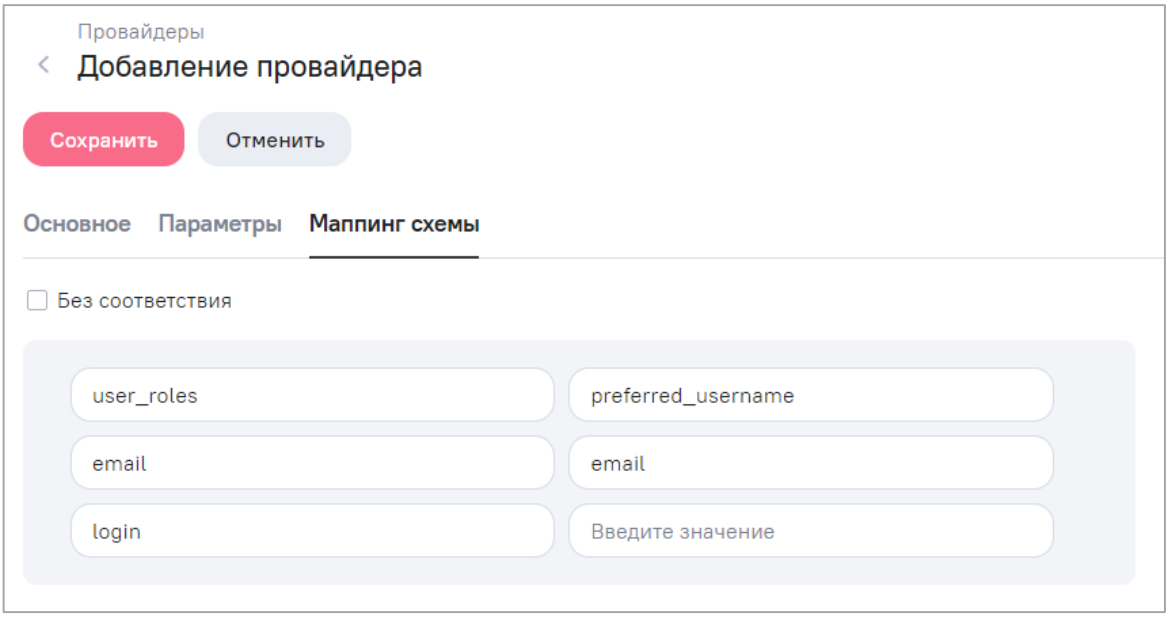


Рисунок 82 – Создание провайдера, вкладка «Маппинг схемы»

При стандартной конфигурации приложения последующую настройку в данном разделе производить не требуется.

Примечание – Реализован «мягкий» маппинг данных внешних провайдеров. Если у пользователя есть атрибут, не указанный в схеме, значение сохраняется в списке дополнительных атрибутов. И наоборот, если при формировании критериев доступа на модель у пользователя нет используемого атрибута, то его значение ищется в списке дополнительных атрибутов.

После заполнения правил соответствия атрибутов доступа схемы с атрибутами доступа провайдера и после сохранения данных провайдера, можно дополнительно задать соответствия к атрибутам пользователей в соответствующем атрибуте доступа.

Для этого на вкладке «Маппинг схемы» справа от атрибута доступа нажмите на кнопку [..]. Откроется окно «Маппинг атрибутов» для выбранного атрибута доступа.

Окно «Маппинг атрибутов» содержит интерфейс для задания правил сопоставления атрибутов пользователей внешнего провайдера и атрибутов пользователей, используемых в AW (Рисунок 83).

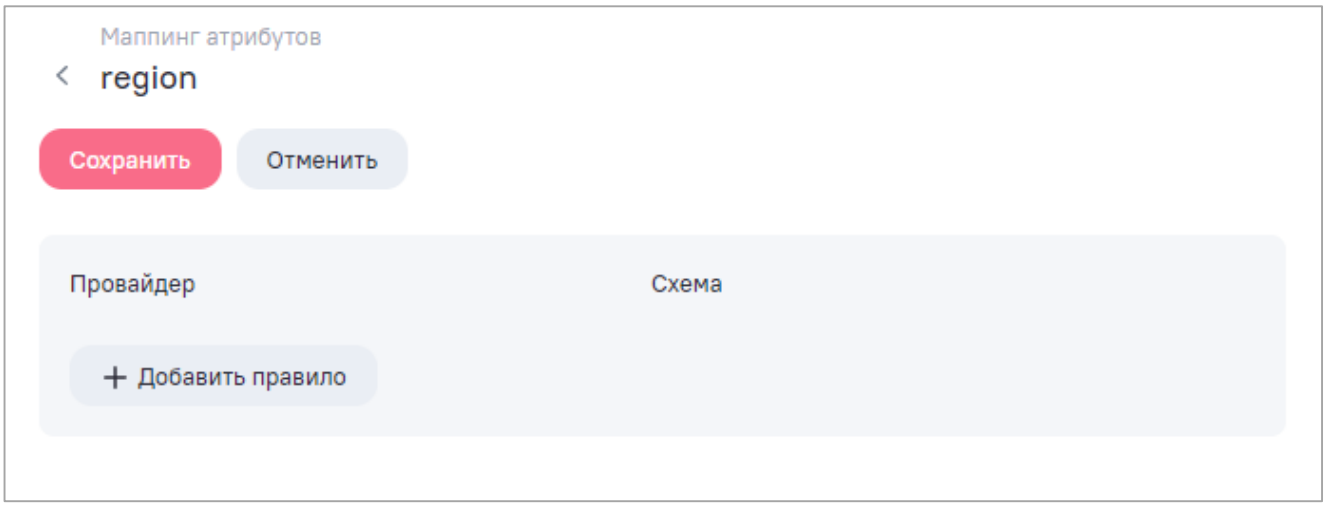


Рисунок 83 – Окно «Маппинг атрибутов»

На вкладке можно задать дополнительные правила сопоставления и группировки атрибутов. Правила сопоставления атрибутов пользователей применяются при входе пользователя в AW через провайдера.

Для создания правила нажмите на кнопку «Добавить правило». Отобразятся поля для ввода параметров. В поле «Провайдер» введите название атрибута, передаваемого провайдером, а в поле «Схема» укажите значение, которое будет использоваться при настройке правил доступа в моделях (Рисунок 84). Создайте необходимое количество правил. Чтобы удалить правило, нажмите на кнопку  напротив необходимого правила.

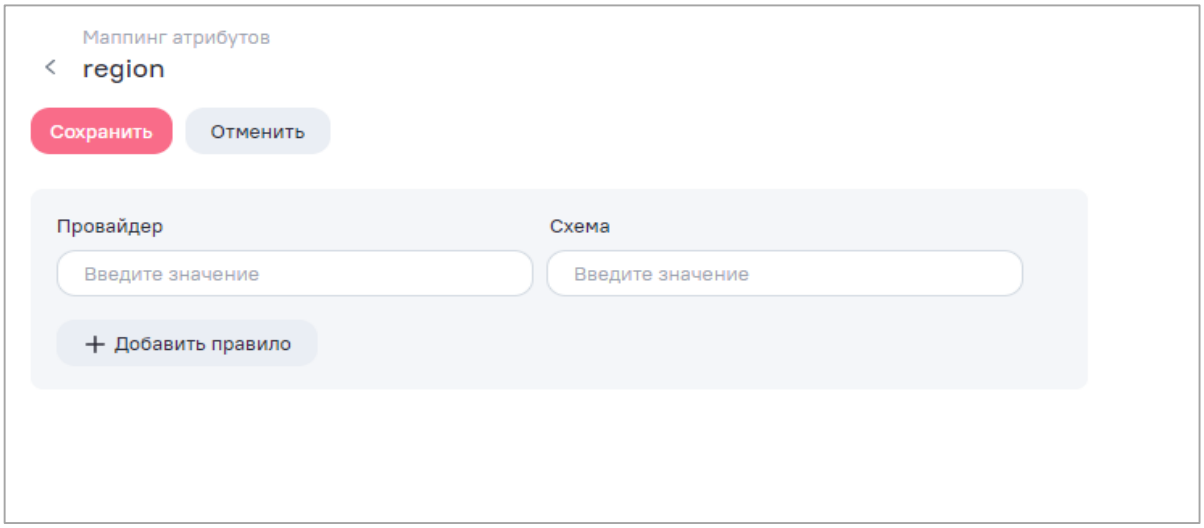


Рисунок 84 – Создание провайдера, добавление правила сопоставления

Атрибуты доступа, которые содержат маппинг атрибутов пользователей, отмечены пиктограммой  (Рисунок 85).

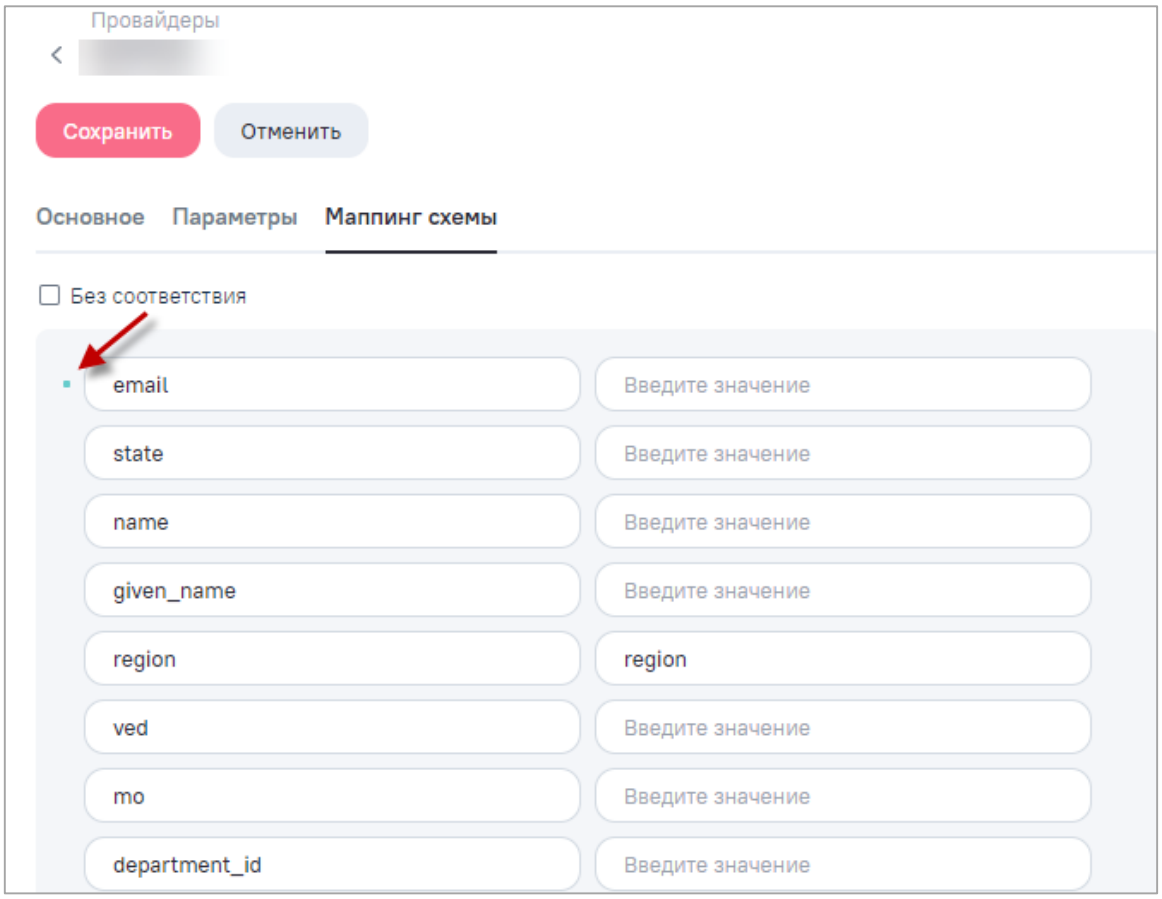


Рисунок 85 – Отображение атрибута, который содержит маппинг атрибутов пользователей

15.6.5.2 Редактирование провайдера

Чтобы отредактировать провайдер, дважды нажмите левой кнопкой мыши по провайдеру в списке или установите «флажок» напротив строки провайдера и нажмите на кнопку «Редактировать».

Доступно изменение следующих параметров и настроек провайдера:

- на вкладке «Основное»:
- активация и деактивация провайдера – для этого установите или снимите «флажок» в поле «Активный»;
- изменение наименования в поле «Наименование»;
- изменение типа провайдера в поле «Тип»;
- изменение надписи кнопки сторонней аутентификации в поле «Надпись кнопки сторонней аутентификации»;
- выбор списка базовых групп в поле «Базовые группы»;

- установка или снятие разрешения на создание новых пользователей через внешнее управление – для этого установите или снимите «флажок» в поле «Разрешить создание новых пользователей через внешнее управление»;
- настройка параметров подключения на вкладке «Параметры»;
- добавление соответствий атрибутов доступа схемы и атрибутов доступа провайдера на вкладке «Маппинг схемы»;
- управление соответствиями атрибутов пользователей провайдера с атрибутами пользователей, используемых в Компонене, на вкладке «Маппинг схемы».

Окно редактирования внешнего провайдера аналогично окну добавления провайдера (п. 15.6.5.1).

Окно редактирования внутреннего провайдера содержит вкладки «Основное», «Маппинг схемы».

Примеры настроек внутреннего и внешних провайдеров представлены в п. 15.6.5.

Для сохранения внесенных изменений убедитесь, что заполнены обязательные поля на вкладках «Основное» (для внешнего и внутреннего провайдера) и «Параметры» (для внешнего провайдера). Нажмите на кнопку «Сохранить». В случае успешного сохранения отобразится уведомление о внесенных изменениях – «Провайдер сохранен».

15.6.5.3 Удаление провайдера

Ранее созданный провайдер можно удалить:

- в интерфейсе редактирования выбранного провайдера – ссылка «Удалить» на вкладке «Основное»;
- в интерфейсе просмотра списка провайдеров – выберите нужный провайдер и нажмите на кнопку «Удалить». Аналогично можно выбрать и удалить сразу несколько провайдеров.

Перед удалением откроется окно подтверждения действия. В AW невозможно удалить активные провайдеры, а также внутренний провайдер «AW» с типом «Локальный (user_permissions)», который используется для технического администратора AW, провайдер «AW» можно только деактивировать.

15.6.6 Пользовательский сценарий авторизации через внешний провайдер «OpenID Token» по протоколу OpenID Connect

При авторизации через внешний провайдер по протоколу OpenID Connect:

а) технический администратор AW подает заявку администратору провайдера на подключение AW к тестовому/промышленному контуру провайдера, в которой указывает:
   - протокол взаимодействия;
   - необходимость запрашивать согласие у пользователя на передачу данных в AW в процессе аутентификации;
   - список атрибутов для передачи из провайдера;
   - коды ролей (коды групп) пользователей.

б) администратор провайдера создает роли для AW;

в) необходимые учетные записи заводятся по соответствующим заявкам техническим администратором AW и администратором провайдера;

г) взаимодействие пользователей через провайдер может происходить по следующим сценариям:
   - основной принцип взаимодействия пользователей:

- пользователь авторизуется в стороннем приложении с помощью единой точки входа;
- работает с разделами стороннего приложения;
- нажимает на кнопки для перехода к AW, после чего переходит в AW, минуя форму авторизации (AW получает access_token от сторонней системы).
   - сценарии, по которым осуществляется бесшовный переход из стороннего приложения в AW:

- пользователь сторонней системы переходит в соответствующий раздел для дальнейшей работы с объектами AW – при нажатии на кнопку открывается окно стороннего приложения (реестр/таблица) со списком доступных пользователю объектов из AW и доступными операциями. При открытии объекта, например, на просмотр открывается окно AW, и все дальнейшие операции с объектом происходят в интерфейсе AW;
- пользователь сторонней системы переходит в соответствующий раздел для перехода и дальнейшей работы в AW – при нажатии на кнопку раздела открывается раздел AW с доступными пользователю объектами и доступными операциями. Все дальнейшие операции происходят в интерфейсе AW;

- пользователю сторонней системы предоставляется кнопка со ссылкой ресурса AW – при нажатии на кнопку открывается окно AW на просмотр виджета по ссылке. Все дальнейшие операции с виджетом происходят в интерфейсе AW;
- в сторонней системе пользователь нажимает на кнопку для открытия объекта AW – при нажатии на кнопку открывается окно AW на просмотр или редактирование объекта. Все дальнейшие операции с объектом происходят в интерфейсе AW.

д) отработка сценариев взаимодействия при кросс-авторизации:

- для сценария 1: 1 вариант – взаимодействие с API AW:

- сторонняя система отправляет в провайдер запрос на предоставление access token, который она может использовать для доступа к ресурсам AW от имени пользователя;
- провайдер проводит аутентификацию пользователя. Затем при необходимости отправляет пользователю запрос на согласие в предоставлении доступа. После чего отправляет в стороннюю систему access token;
- сторонняя система делает POST запрос к api/auth-provider/verify-code (верификация кода авторизации) с обязательными параметрами: id – идентификатор провайдера в AW, code – access_token, полученный от провайдера;
- если все проверки на стороне AW пройдены успешно, то в ответ сторонняя система получает token AW. Дальше его используют для последующих запросов к API AW.

- для сценариев 2, 3, 4: 2 вариант – фронтовое взаимодействие пользователей с AW (через web-браузер):

- сторонняя система отправляет в провайдер запрос на предоставление access token, который она может использовать для доступа к ресурсам AW от имени пользователя;
- провайдер проводит аутентификацию пользователя. Затем при необходимости отправляет пользователю запрос на согласие в предоставлении доступа. После чего отправляет в стороннюю систему access token;
- сторонняя система отправляет запрос на frontend AW /auth/verify-code/ с обязательными параметрами: id – идентификатор провайдера в AW, code – access_token, полученный от провайдера, и дополнительными параметрами:

sessionId – идентификатор сессии пользователя и redirectUrl – URL AW, запрашиваемый пользователем;

- frontend AW перехватывает запрос и обращается к backend AW, backend обращается к провайдеру;
- если все проверки на стороне AW пройдены успешно, то генерируется внутренний token AW. Дальше frontend использует его для открытия запрашиваемого ресурса в redirectUrl (например, /app/widgets, при отсутствии адреса в redirectUrl пользователю откроется первый доступный раздел AW).

15.6.7 Принципы создания новых пользователей и обновления их доступов к разделам Компонента анализа данных

Для внешних провайдеров с типом «OpenID Token»:

а) когда в AW через кросс-авторизацию переходит пользователь без учетной записи, AW проверяет настройку провайдера:
   - если нет «флажка» в поле «Разрешить создание новых пользователей через внешнее управление», то открывается сообщение об ошибке «Для указанного в запросе пользователя не создана учетная запись. Необходимо обратиться к Администратору Системы»;
   - если установлен «флажок» в поле «Разрешить создание новых пользователей через внешнее управление», то в AW создается новая учетная запись пользователя с определенными параметрами: логин, электронная почта, группы.

б) если установлен «флажок» в поле «Разрешить создание новых пользователей через внешнее управление», AW проверяет, какие коды ролей (групп) передал провайдер для Компо AW нента (блок endpoint с идентификатором AW в ИА):
   - если в блоке ролей имеются коды ролей, которые соответствуют кодам групп пользователей AW (системным или пользовательским группам), то в карточку пользователя добавляются эти группы;
   - далее проверяется настройка базовых групп: если в настройках провайдера указаны базовые группы пользователя, то в учетную запись пользователя добавляются базовые группы из настройки.

в) когда в AW через кросс-авторизацию переходит пользователь с учетной записью в AW, то:

- в учетной записи пользователя удаляются все настройки по доступным группам (даже те, которые были добавлены техническим администратором AW вручную);
- далее группы записываются снова по тому же принципу, что и при создании учетной записи.

15.7 Атрибутный доступ к данным

При стандартной конфигурации приложения настройки в последующих разделах производить не требуется.

15.7.1 Общие принципы

Атрибутный доступ к данным включает получение пользователем доступа к отдельным строкам данных модели на основании значений параметров (атрибутов) его учетной записи, полученных от провайдера. Данный универсальный принцип позволяет реализовать множество различных сценариев управления доступом, таких как:

- доступ только к области ответственности специалиста, например:
- данным по деятельности собственной и нижестоящих организационных структур;
- данным по собственному региону и его субъектам.
- разделение доступа к данным по времени (периоду) к которому они относятся:
  - доступ только к данным созданным соответствующим периоду работы сотрудника;
  - доступ определенных категорий сотрудников только к историческим данным (данным за прошедшие периоды).

В настройках целевой модели (доступ к которой ограничивается атрибутными правилами) задаются условия, использующие сравнение значений атрибутов пользователя и выбранных полей данных модели. Если такие условия заданы для модели – доступ к каждой строке данных предоставляется дифференциально каждому конкретному пользователю. Если для модели не заданы условия атрибутного доступа – доступ к строкам не ограничивается.

Ограничения атрибутного доступа применяются в интерфейсе просмотра виджетов.

Атрибутный доступ только накладывает дополнительные ограничения, независимо от его применения, у пользователя должны быть обеспечены права для работы с соответствующим разделом AW и даны, как минимум, на права просмотр для соответствующего объекта AW (виджета).

15.7.2 Настройка схемы доступов

Раздел «Схемы доступов» (п. 15.6.4) доступен пользователям, наделенным административными правами через встроенную системную группу «Администратор».

Схема доступов представляет собой список атрибутов доступа, которые передаются внешними провайдерами в AW при входе в AW.

В AW есть встроенные атрибуты доступа «login» (логин), «email» (E-mail), «state» (статус) и «user_roles» (роль). По ним сопоставляется учетная запись пользователя, и обновляются его данные. Встроенные атрибуты не подлежат редактированию и удалению.

Настройте схему доступов так, чтобы она содержала все необходимые атрибуты пользователей, которые необходимы для атрибутного доступа к данным моделей, например:

- оргструктурную принадлежность (департамент, подразделение, ведомство и т.д.);
- территориальную привязку (регион, город и т.д.);
- принадлежность к определенным ролям (руководитель, бухгалтер, ответственный за, и т.д.);
- дополнительные атрибуты, делающие информацию более понятной и наглядной (ФИО пользователя, название организационной единицы, название территории).

Чтобы принимать от провайдера атрибуты пользователя в виде массива данных, в том числе ролей пользователей, в схеме доступов для данных атрибутов выберите тип данных «Массив».

Настройка атрибутов доступа в схеме доступов описана в п. 15.6.4. На рисунке ниже (Рисунок 86) представлен пример настроенной схемы доступов.

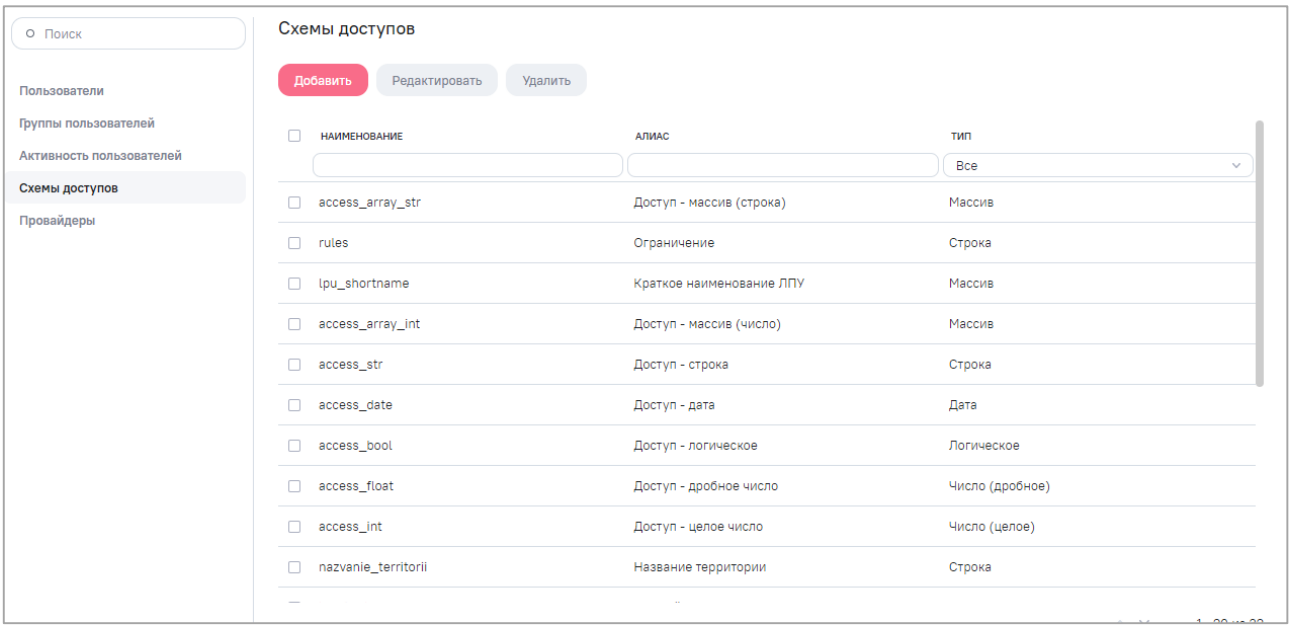


Рисунок 86 – Пример настройки схемы доступов

15.7.3 Настройка провайдера пользователя

Раздел «Провайдеры» (п. 15.6.5) доступен пользователям, наделенным административными правами через встроенную системную группу «Администратор». Раздел предназначен для настройки взаимодействия AW с провайдерами пользователей. Также в AW есть возможность настроить авторизацию через внешний сервис аутентификации по протоколу Open ID Connect.

Чтобы настроить взаимодействие, произведите настройки для обоих участников взаимодействия: провайдера (поставщика учетных записей) и AW (поставщика сервиса). Для настройки взаимодействия AW с провайдером выполните шаги, описанные в п. 15.6.5.1.

Примечание – Предполагается, что взаимодействие провайдера (поставщика учетных записей) с AW настроено, и учетные записи зарегистрированы.

На рисунках (Рисунок 87 – Рисунок 89) представлен пример настроенного внешнего провайдера «OpenID».

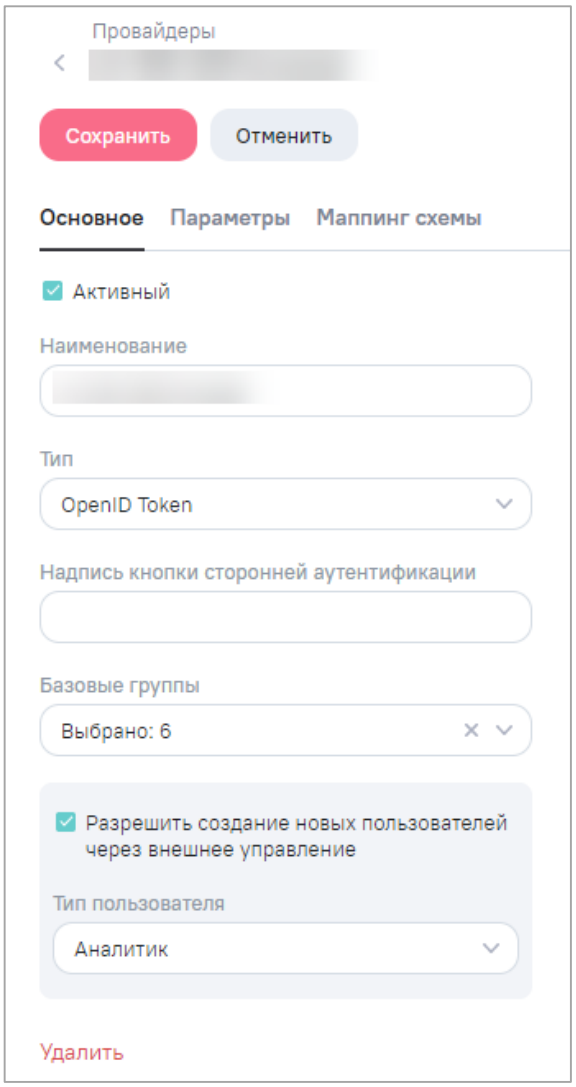


Рисунок 87 – Пример настройки внешнего провайдера, вкладка «Основное»

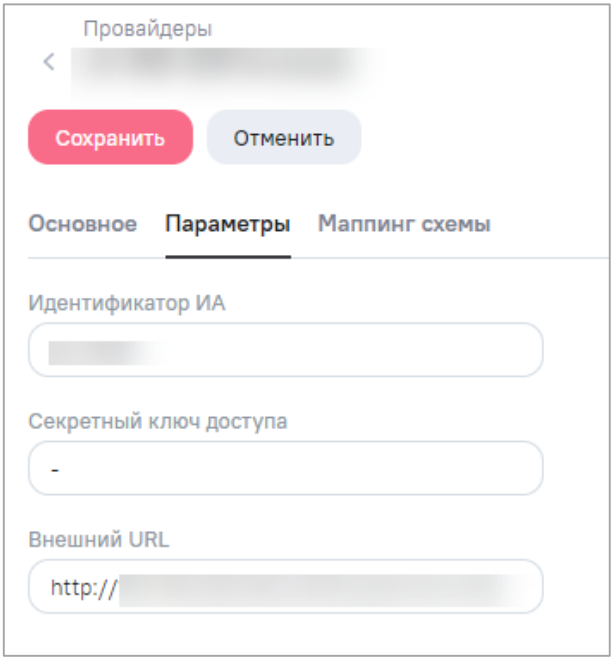


Рисунок 88 – Пример настройки внешнего провайдера, вкладка «Параметры»

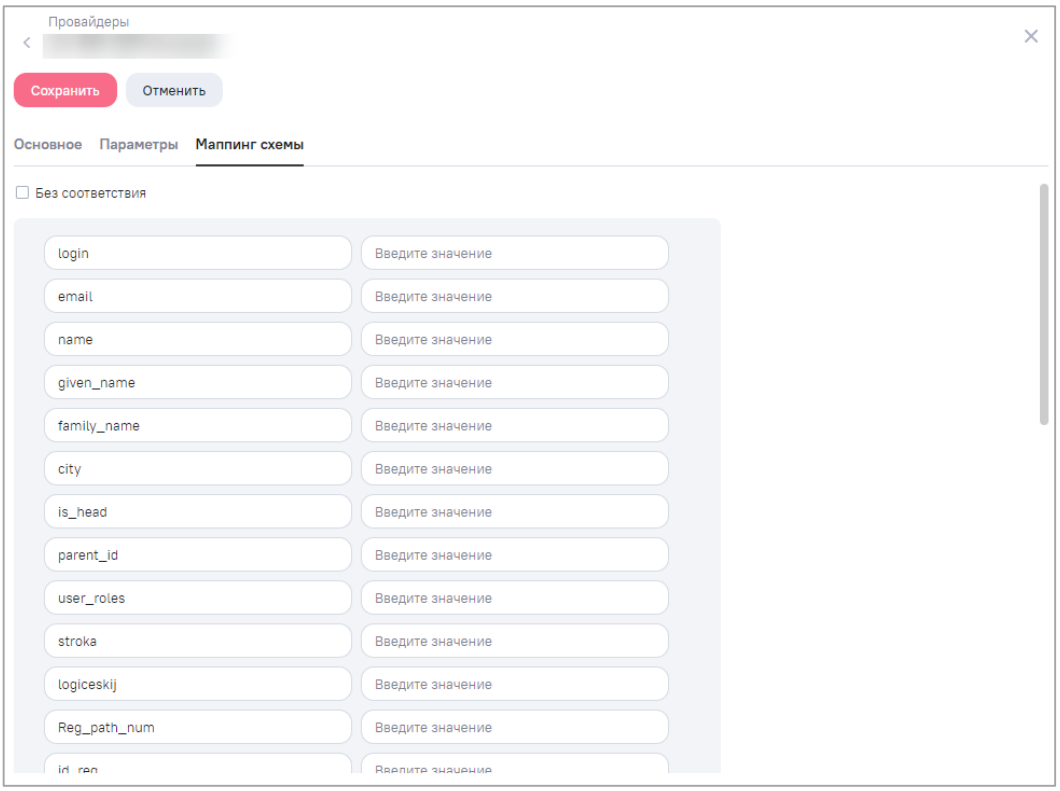


Рисунок 89 – Пример настройки внешнего провайдера, вкладка «Маппинг схемы»

15.7.4 Сценарии настройки атрибутного доступа

Сценарии настройки атрибутного доступа представлены в таблице ниже (Таблица 42).

Таблица 42 – Сценарии настройки атрибутного доступа

Состояние внешнего провайдера	Состояние внутреннего провайдера «AW»	Этапы настройки атрибутного доступа
Активный	Активный (локальная аутентификация разрешена)	– настройка схемы доступов; – настройка модели данных «user_permissions»; – настройка внутреннего провайдера «AW» на вкладке «Маппинг схемы»; – настройка внешнего провайдера на вкладках «Маппинг схемы» и «Маппинг атрибутов»; – настройка правил доступа к данным пользовательской модели
Не активный	Не активный (локальная аутентификация запрещена)	– настройка схемы доступов; – настройка внешнего провайдера на вкладках «Маппинг схемы» и «Маппинг атрибутов»; – настройка правил доступа к данным пользовательской модели

15.8 Центр управления

Примечание – При стандартной конфигурации приложения настройку в данном разделе производить не требуется.

В функции технического администратора AW входят задачи управления:

– информацией о AW (п. 15.8.1);

– лицензиями (п. 15.8.2);

– драйверами (п. 15.8.3).

Вы можете авторизоваться, используя логин и пароль по умолчанию:

tech_admin

123456

В целях безопасности после первого входа в AW пароль необходимо изменить.

Для перехода в Центр управления нажмите на кнопку  в главном меню AW. Откроется Центр управления в подразделе «Система» (Рисунок 90).

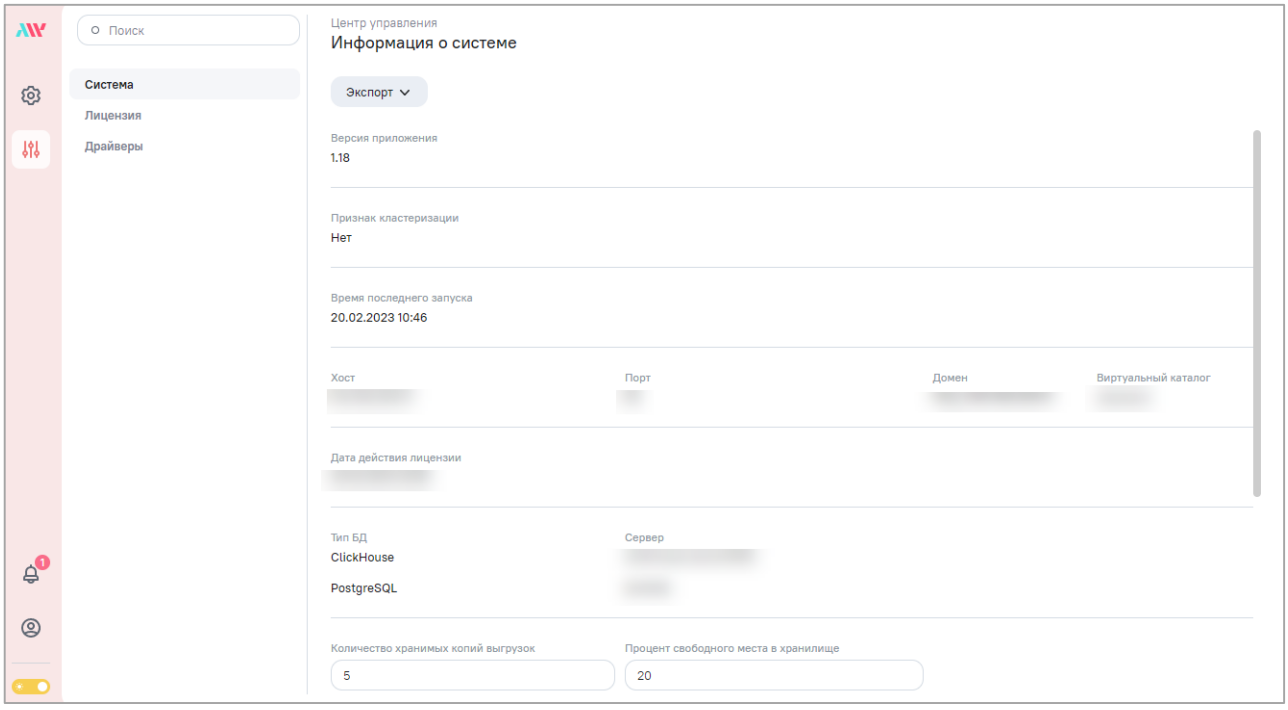


Рисунок 90 – Центр управления, подраздел «Система»

15.8.1 Подраздел «Система»

В подразделе «Система» (Рисунок 90) отображается информация о AW в следующих полях:

– «Версия приложения» – данные доступны только для просмотра;

- «Признак кластеризации» – данные доступны только для просмотра;
- «Время последнего запуска» – данные доступны только для просмотра;
- «Хост» – данные доступны только для просмотра;
- «Порт» – данные доступны только для просмотра;
- «Домен» – данные доступны только для просмотра;
- «Виртуальный каталог» – данные доступны только для просмотра;
- «Дата действия лицензии» – данные доступны только для просмотра;
- «Тип БД» – данные доступны только для просмотра;
- «Сервер» – данные доступны только для просмотра;
- «Количество хранимых копий выгрузок» (параметр «count_of_stored_files») – измените значение при необходимости, по умолчанию установлено значение «5». При превышении лимита реализуется метод по удалению старого неактуального набора данных по текущему объекту AW данного пользователя;
- «Процент свободного места в хранилище» (параметр «free_storage_space») – измените значение при необходимости, по умолчанию установлено значение «10». Позволяет резервировать свободное место в хранилище для работы AW;
- «Время жизни файла выгрузки (сек)» (параметр «file_lifetime») – измените значение при необходимости, по умолчанию установлено значение «604800» (7 дней). Проверяется по cron, по истечении срока реализуется механизм удаления старых данных из хранилища. Время указывается в секундах, если параметр равен «0» или значение не указано, то считается, что установлено значение «Неограниченное время жизни выгрузки», т.е. разрешено хранение всех версий выгрузок неограниченное количество времени;
- «Частота запуска очистки (сек)» (параметр «storage_cleared_start_interval») – измените значение при необходимости, по умолчанию установлено значение «86400» (1 день). Запускается принудительный механизм очистки хранилища:
  - сначала очищается хранилище от копий, остаются только последние выгрузки пользователя по объектам AW (на один объект AW по одной выгрузке);
  - если необходимое место не освобождено, то удаляются самые старые файлы до тех пор, пока не будет освобождено необходимое пространство, регулируемое параметром «free_storage_space».
- «Website» – измените значение при необходимости;
- «Все стили» – данные доступны только для просмотра;

– «Стиль приложения» – измените значение при необходимости, по умолчанию установлено значение «default».

Для выгрузки информации о AW нажмите на кнопку «Экспорт» и в выпадающем списке выберите пункт «Экспорт информации» (Рисунок 91). На персональный компьютер выгрузится файл формата .csv.

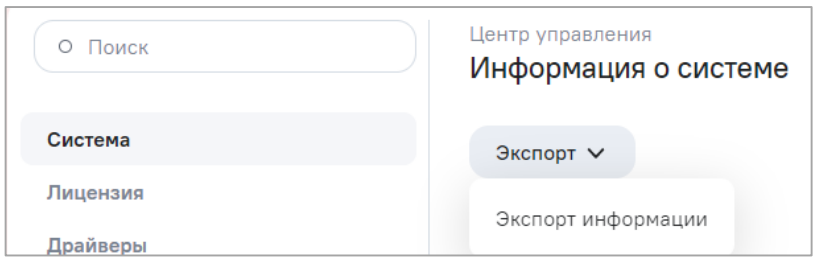


Рисунок 91 – Кнопка «Экспорт» в подразделе «Система»

При необходимости измените адрес сайта AW в поле «Website». При нажатии на ссылку «Официальный сайт» в окне авторизации (Рисунок 49) откроется сайт с адресом, указанным в поле «Website».

15.8.2 Лицензия

15.8.2.1 Лицензионная политика

Виды лицензии по типу доступа:

– «Триальный» (Trial) – демонстрационная (бесплатная) версия программного обеспечения. Не имеет ограничений в функциональности, но имеет ограниченный срок работы – AW будет работать только 14 дней и будет обрабатывать ограниченное количество данных – только 5 моделей с максимальным размером 524 МБ. Предоставляется возможность ознакомиться с интерфейсом и функциональностью AW;

Примечание – AW функционирует, пока не наступит дата окончания действия лицензии. Но недоступна конкретному пользователю, у которого истек срок триального доступа, при этом есть 7 дней на экспорт объектов через личный кабинет на сайте.

– «Корпоративный» (On-premise) – коммерческое программное обеспечение. Для работы с такой программой ее нужно купить. Устанавливается на серверах Заказчика. Никаких ограничений в функциональности такого программного обеспечения нет, лицензией лишь варьируется количество активных пользователей и их роли. После истечения срока действия лицензии программное обеспечение продолжает функционировать, но не обновляется до новых версий AW;

Лицензии AW с типом доступа «Триальный», «Корпоративный» – именные, т.е. содержат квоты на количество активных пользователей типа «Аналитик». Для данной пользовательской роли предусмотрено разделение прав доступа к разделам AW и к выполнению определенных операций.

Список пользовательских ролей (типов пользователей):

– «Аналитик» – специалист, обладающий всеми правами на создание и изменение информационных панелей и виджетов, а также правом на просмотр доступных и предварительно настроенных моделей.

Настройка типов пользователей описана в п. 15.6.1.

15.8.2.2 Загрузка и активация лицензий

Для работы с лицензиями в Центре управления перейдите в подраздел «Лицензия» (Рисунок 92). Работа с лицензиями включает операции добавления и замены файла лицензии, активации и деактивации лицензий, просмотра информации о загруженных файлах лицензий.

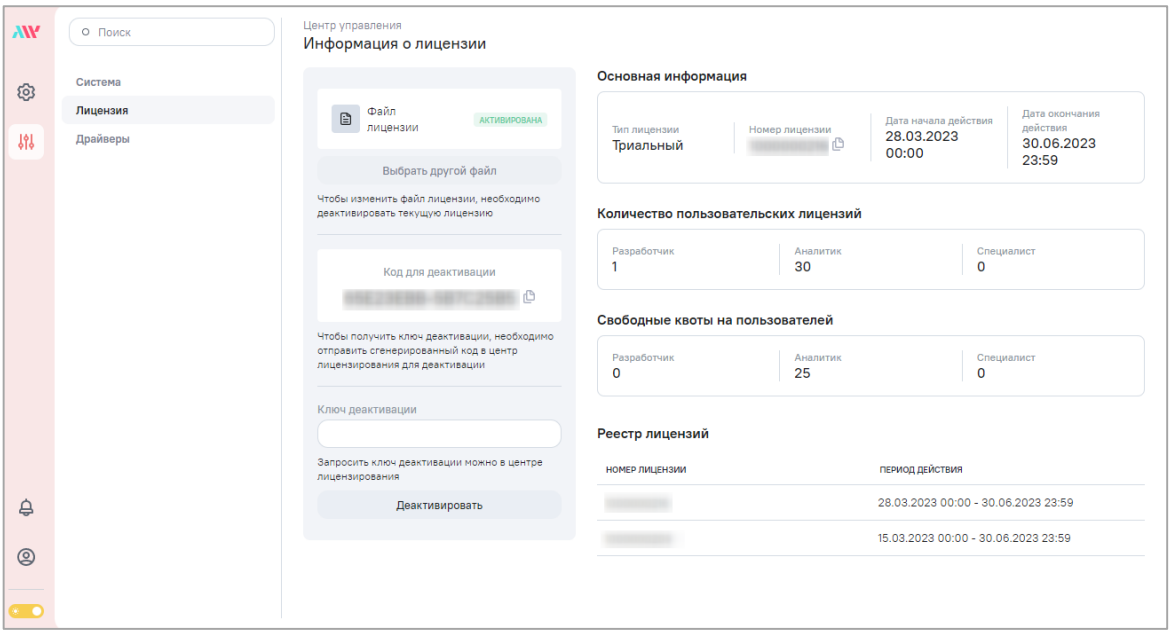


Рисунок 92 – Центр управления, подраздел «Лицензия»

В подразделе отображается информация о текущей лицензии в следующих полях:

– «Код для активации»/ «Код для деактивации» – код, сгенерированный Компоненом, для получения ключа активации/деактивации лицензии;

– блок «Основная информация»:

  – «Тип лицензии» – тип лицензии, соответствующий виду лицензии по типу доступа (см. п. 15.8.2.1);

- «Номер лицензии» – номер лицензии, сгенерированный администратором центра лицензирования при создании лицензии;
- «Дата начала действия» – дата начала действия лицензии;
- «Дата окончания действия» – дата окончания действия лицензии.

– блок «Количество пользовательских лицензий» – именные лицензии, определяющие квоты на количество активных пользователей типа «Аналитик» (см. п. 15.8.2.1);

– блок «Свободные квоты на пользователей» – количество доступных пользовательских квот для создания учетных записей пользователей типа «Аналитик» (см. п. 15.8.2.1);

– блок «Реестр лицензий» – информация о ранее загруженных лицензиях в табличном виде, в столбцах:

- «Номер лицензии» – номер лицензии, сгенерированный администратором центра лицензирования при создании лицензии;
- «Период действия» – дата начала и дата окончания действия лицензии.

Для просмотра информации о ранее загруженной лицензии дважды нажмите на запись о лицензии. Откроется окно «Информация о лицензии» (Рисунок 93).

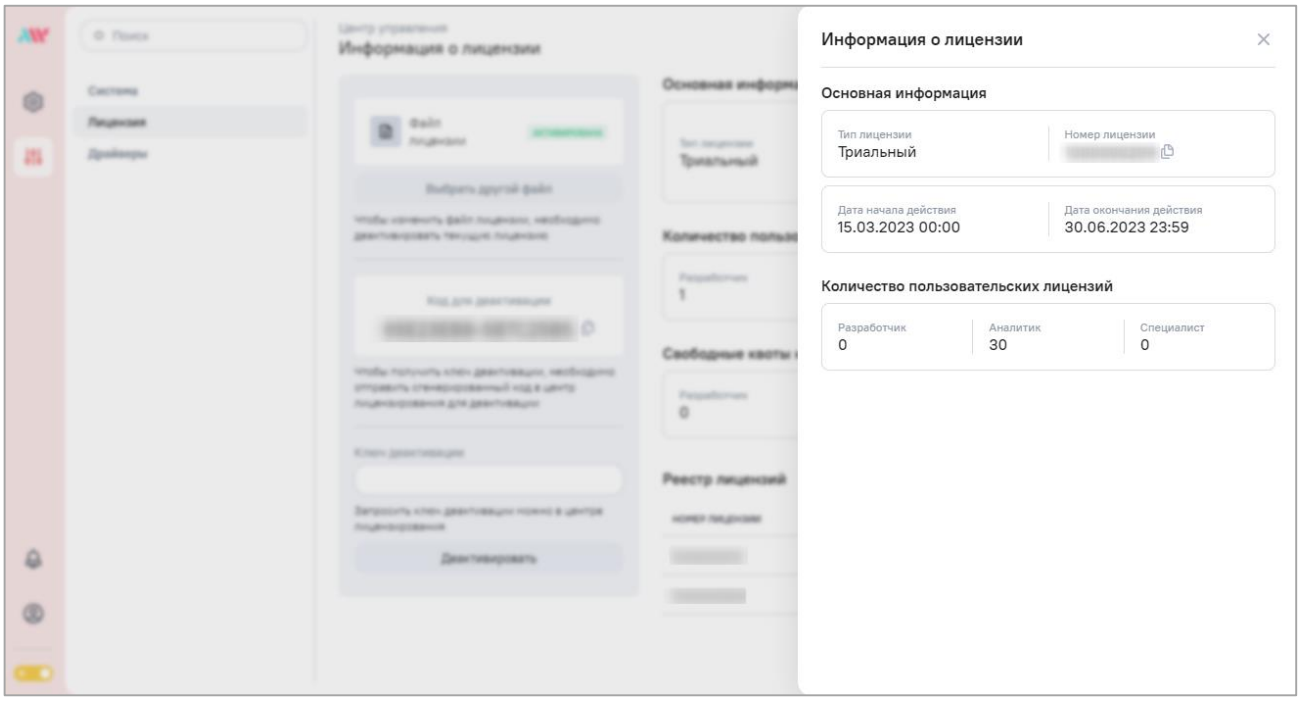


Рисунок 93 – Окно «Информация о лицензии»

После загрузки файла лицензии в AW необходимо выполнить активацию лицензии.

Принцип активации лицензии: после загрузки файла лицензии в AW генерируется код, который необходимо отправить в центр лицензирования AW для получения ключа

активации лицензии. После внесения ключа активации в AW можно активировать лицензию.

Для открытого контура активация происходит в полуавтоматическом режиме, т.к. может быть установлена связь с центром лицензирования AW. Для загрузки и активации новой лицензии выполните следующие действия:

а) загрузите новую лицензию в подразделе «Лицензия» – нажмите на кнопку «Импорт файла лицензии» и выберите файл лицензии (Рисунок 94);

Примечание – На момент загрузки новой лицензии в AW не должно быть активированной лицензии.

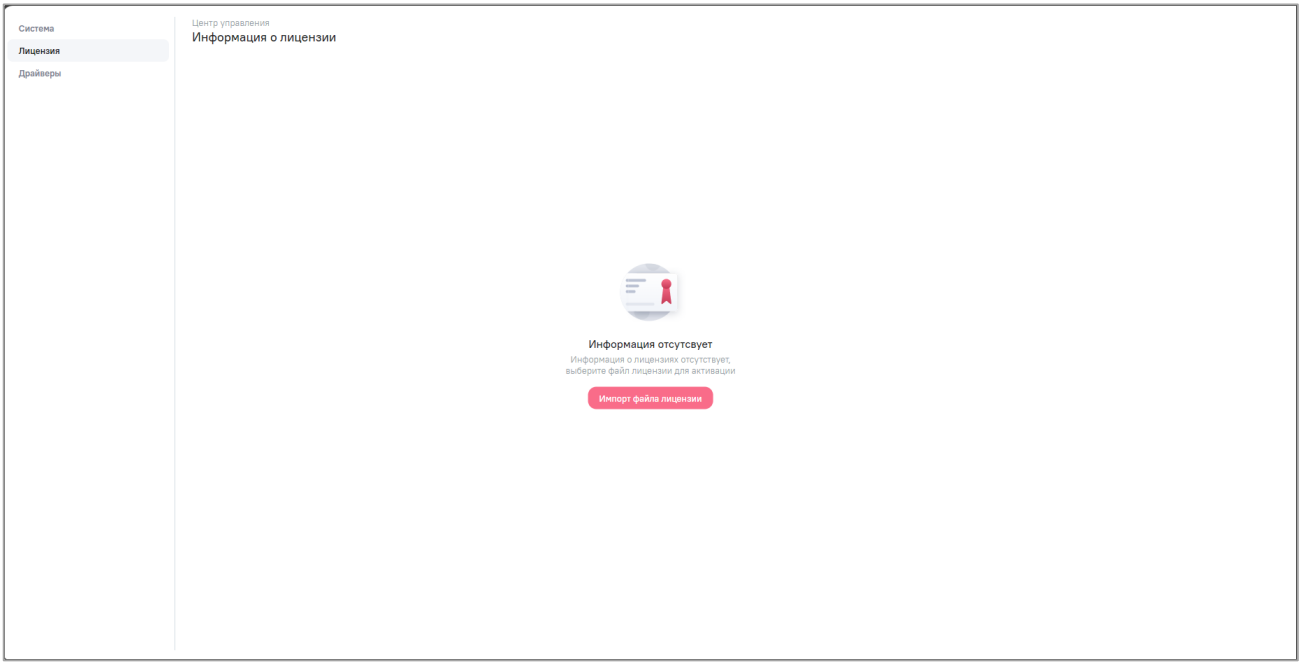


Рисунок 94 – Стартовая страница добавления новой лицензии

б) активируйте лицензию – нажмите на кнопку «Активировать» (Рисунок 95).

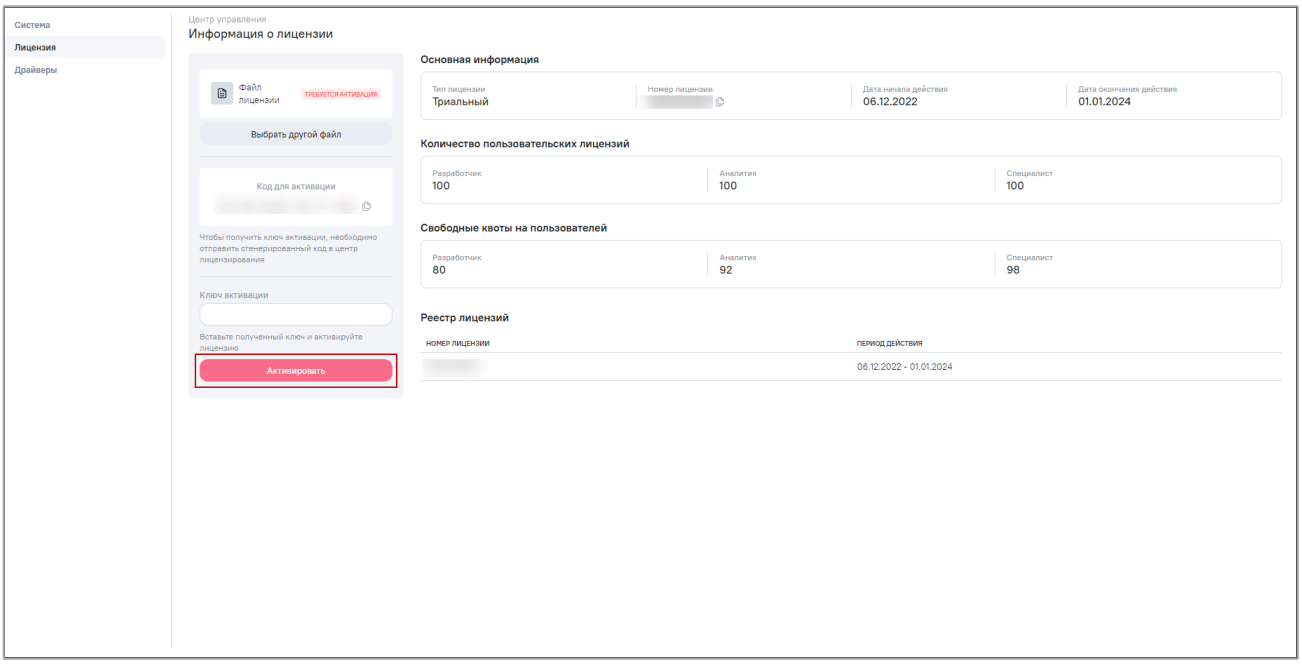


Рисунок 95 – Активации лицензии в открытом контуре

В закрытом контуре получение кода и внесение ключа активации происходит в ручном режиме техническим администратором AW.

Для загрузки и активации новой лицензии выполните следующие действия:

а) загрузите новую лицензию в подразделе «Лицензия» – нажмите на кнопку «Импорт файла лицензии» и выберите файл лицензии (Рисунок 94);

Примечание – На момент загрузки лицензии в AW не должно быть активированной лицензии.

б) скопируйте код для активации лицензии – нажмите на кнопку  рядом с кодом активации (Рисунок 96). Отобразится уведомление о том, что код скопирован;

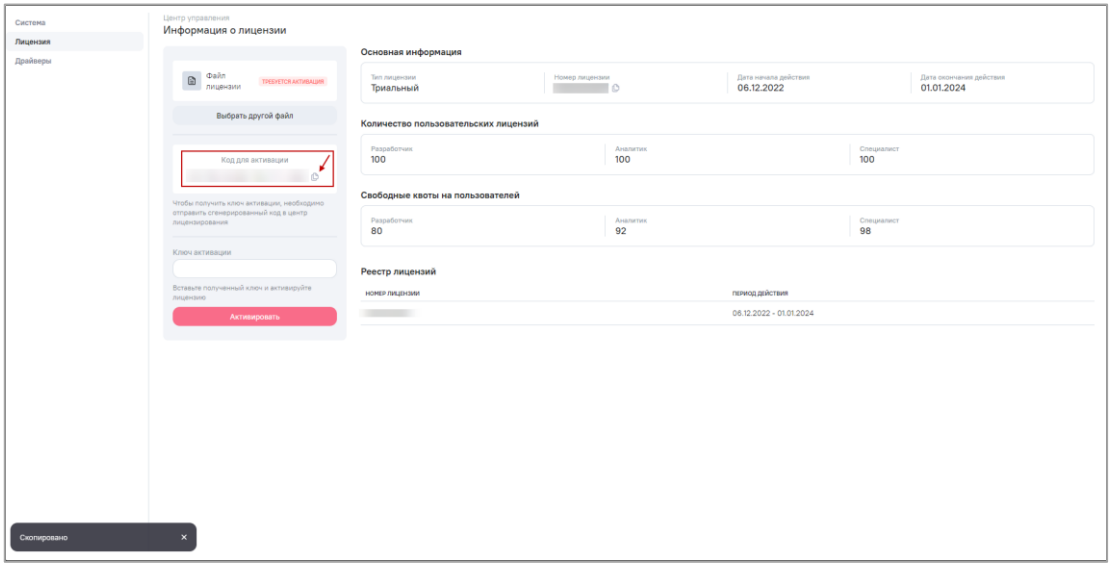


Рисунок 96 – Копирование кода для активации лицензии

в) полученный код передайте администратору центра лицензирования (сотруднику, предоставившему файл лицензии) для получения ключа активации;

г) активируйте лицензию – укажите ключ активации, полученный от администратора центра лицензирования, и нажмите на кнопку «Активировать» (Рисунок 97).

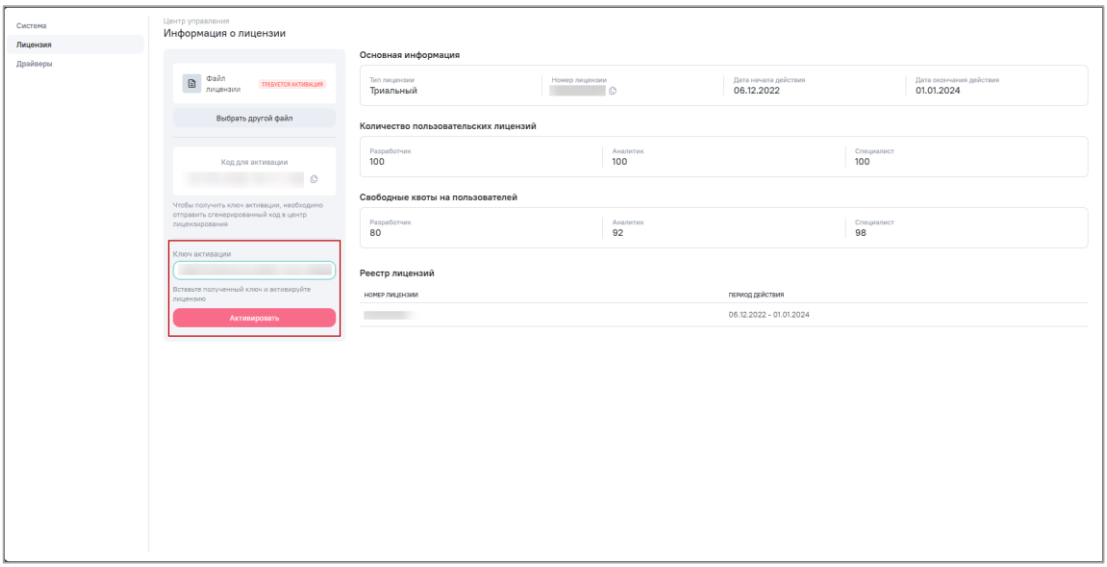


Рисунок 97 – Активации лицензии в закрытом контуре

15.8.2.3 Деактивация и замена

Для замены файла лицензии необходимо деактивировать старую лицензию.

Принцип деактивации лицензии: для каждой активированной лицензии в AW генерируется код, который необходимо отправить в центр лицензирования AW для получения ключа деактивации лицензии. После внесения ключа деактивации в AW, можно деактивировать лицензию.

Для открытого контура деактивация происходит в полуавтоматическом режиме, т.к. может быть установлена связь с центром лицензирования AW.

Для деактивации старой лицензии и замены файла лицензии выполните следующие действия:

а) деактивируйте лицензию – нажмите на кнопку «Деактивировать» (Рисунок 98);

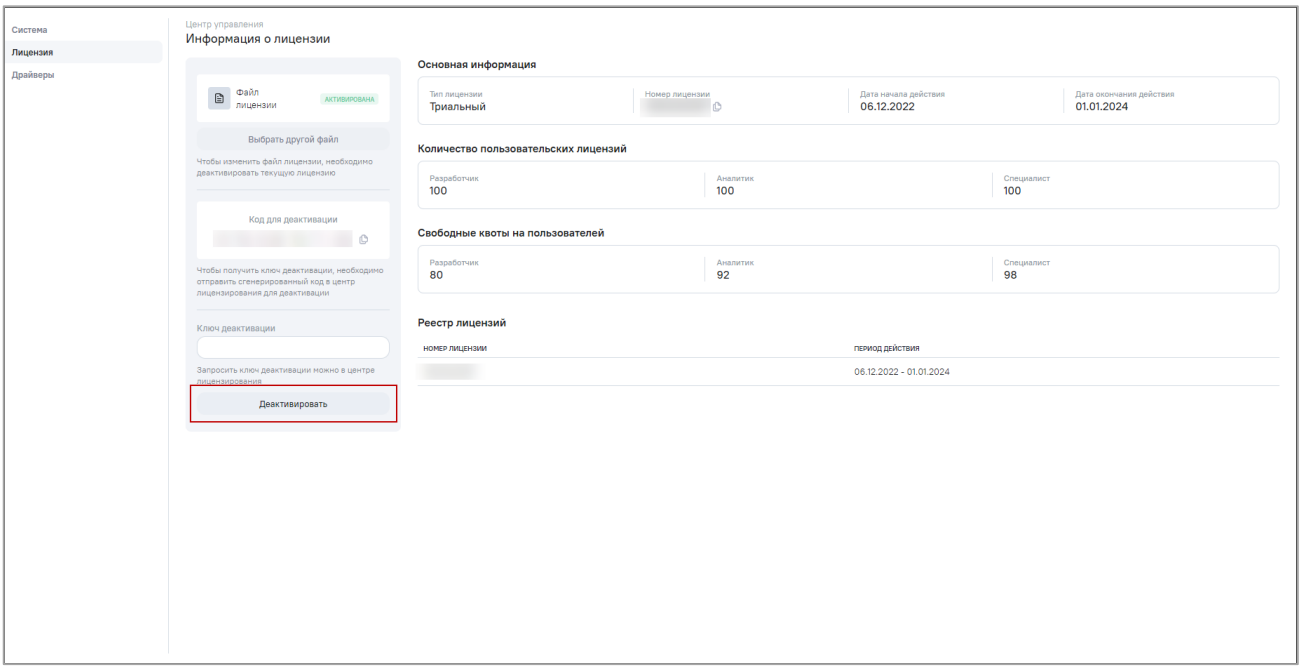


Рисунок 98 – Деактивации лицензии в открытом контуре

б) замените файл лицензии – нажмите на кнопку «Выбрать другой файл» и выберите файл лицензии (Рисунок 99);

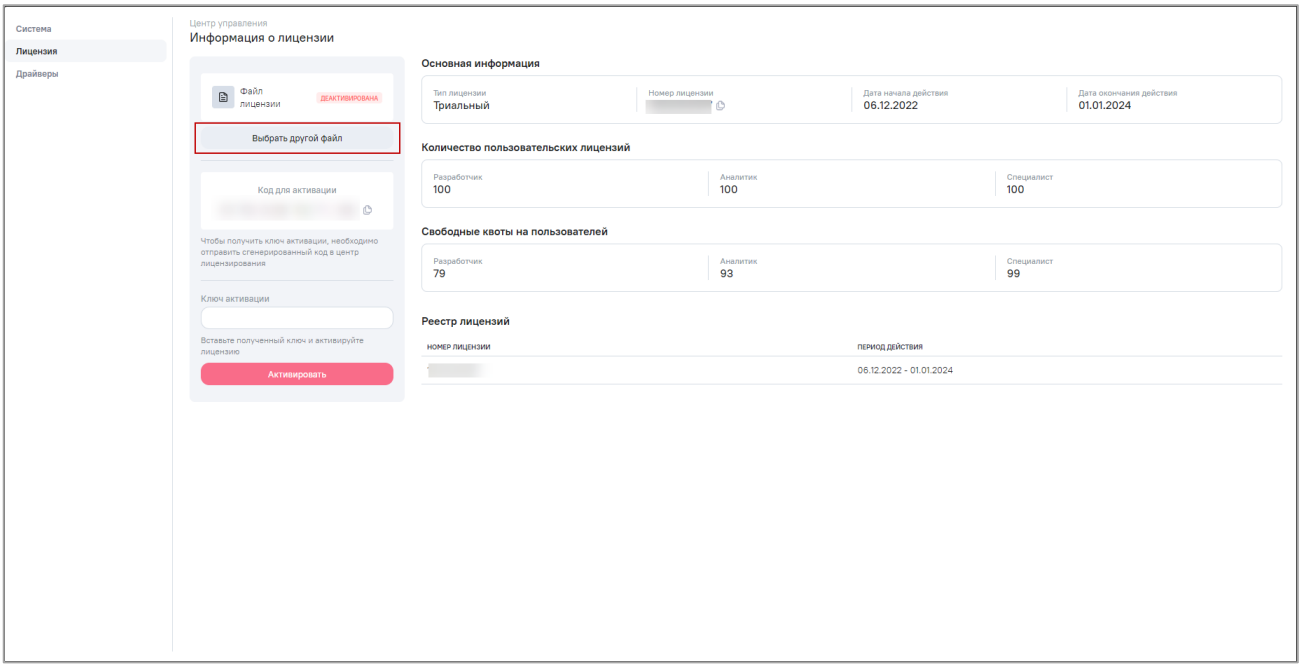


Рисунок 99 – Замена файла лицензии

в) активируйте лицензию – нажмите на кнопку «Активировать» (Рисунок 95).

В закрытом контуре получение кода и внесение ключа деактивации происходит в ручном режиме техническим администратором AW.

Для деактивации старой лицензии и замены файла лицензии выполните следующие действия:

а) скопируйте код для деактивации лицензии – нажмите на кнопку  рядом с кодом деактивации (Рисунок 100). Отобразится уведомление о том, что код скопирован;

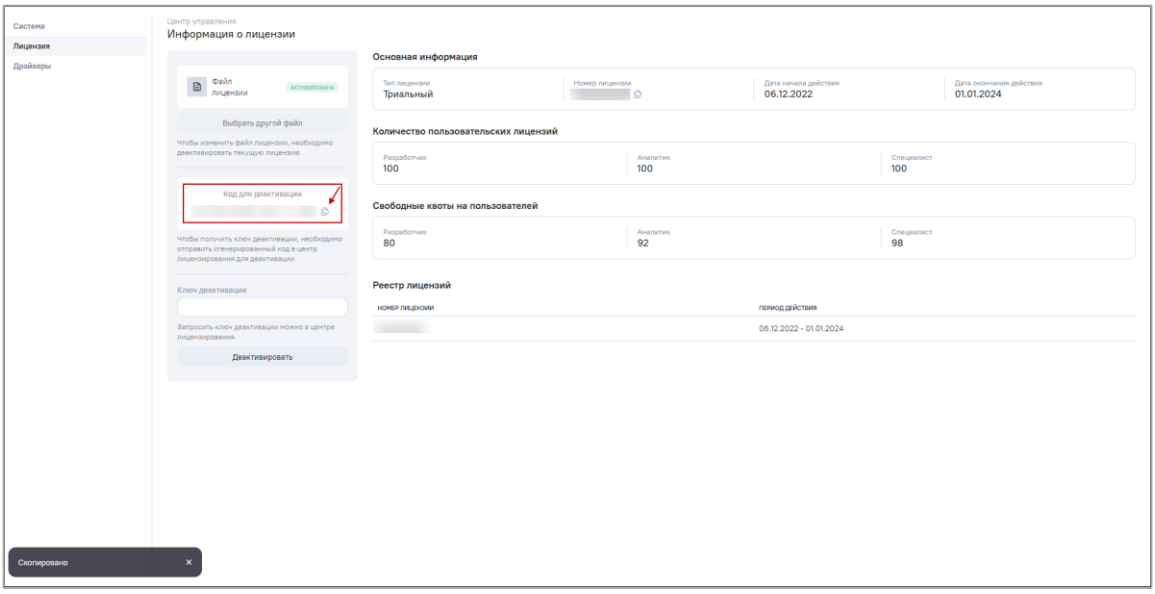


Рисунок 100 – Копирование кода для деактивации лицензии

б) полученный код передайте администратору центра лицензирования (сотруднику, предоставившему файл лицензии) для получения ключа деактивации;

в) деактивируйте лицензию – укажите ключ деактивации, полученный от администратора центра лицензирования, и нажмите на кнопку «Деактивировать» (Рисунок 101);

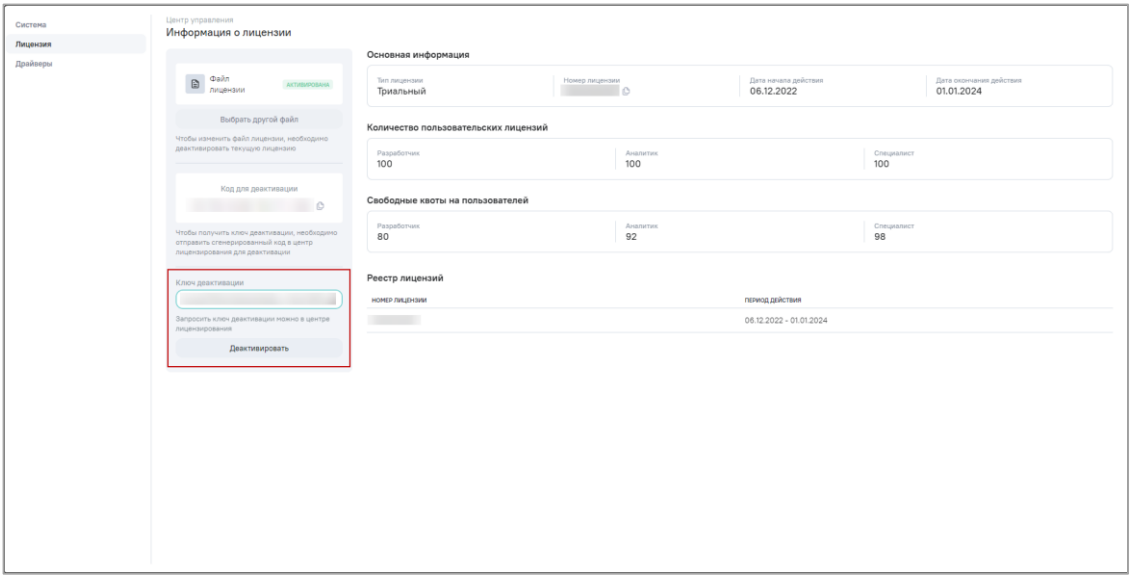


Рисунок 101 – Деактивации лицензии в закрытом контуре

г) замените файл лицензии – нажмите на кнопку «Выбрать другой файл» и выберите файл лицензии (Рисунок 99);

д) активируйте лицензию в соответствии с описанием активации для закрытого контура, приведенного выше.

15.8.3 Драйверы

Подраздел «Драйверы» не используется.

15.9 Аварийные ситуации

Возникающие при работе с AW нештатные ситуации и способы их решения описаны в таблице ниже (Таблица 43).

Таблица 43 – Описание нештатных ситуаций

Сообщение/ название ошибки	Причина появления	Вывод ошибки на экране/ консоли	Действия пользователя/ способы устранения
404 – not found	В адресную строку введен неверный адрес	404 – not found	Проверьте правильность ввода ссылки в адресной строке web-браузера
Ошибка валидации данных	Неверно введен логин/пароль	При авторизации в AW отображается уведомление об ошибке: «Ошибка валидации данных». В консоли: "success":false,"error":{"code":422,"message":"Ошибка валидации данных"},"data":{"username":"Не удалось авторизоваться в системе"}}	В окне идентификации пользователя заново заполните поля «Логин» и «Пароль», предварительно проверив, не включена ли клавиша <Caps Lock> и правильность выбора раскладки языка
Файл не найден	Файл лицензии не вмонтирован	"success":false,"error":{"code":401,"message":" Лицензия: Файл не найден"}}	Обратитесь к техническому администратору компонента анлиза данных
Ошибка чтения/записи	Нет прав чтения записи в файл лицензии	"success":false,"error":{"code":401,"message":"Лицензия:Ошибка чтения/записи"}}	Обратитесь к техническому администратору компонента анлиза данных
Ошибка формата	Нарушение целостности данных файла лицензии и теперь его невозможно расшифровать	"success":false,"error":{"code":401,"message":"Лицензия: Ошибка формата"}	Обратитесь к техническому администратору компонента анлиза данных
Срок действия лицензии еще не наступил		{"success":false,"error":{"code":401,"message":"Лицензия: Срок действия лицензии еще не наступил "}}	Обратитесь к техническому администратору компонента анлиза данных

Сообщение/ название ошибки	Причина появления	Вывод ошибки на экране/ консоли	Действия пользователя/ способы устранения
Срок действия лицензии истек		{"success":false,"error":{"code":401,"message":"Лицензия: Срок действия лицензии истек"}}	Обратитесь к техническому администратору компонента анлиза данных
Неверная дата	Была попытка изменения даты и времени на сервере		Обратитесь к техническому администратору компонента анлиза данных
Ошибка домена	Файл лицензии не привязан к домену	{"success":false,"error":{"code":401,"message":"Лицензия: Ошибка домена"}}	Обратитесь к техническому администратору компонента анлиза данных
Указан некорректный id провайдера	В файле svody.config в секции Bars.Authorization в параметре «ProviderId» некорректно задан id провайдера	При переходе в раздел «Список аналитических выборок» ошибка «Подсистема аналитики временно недоступна.Обратитесь к администратору» При этом в логах в файле AW.log: |ERROR|AW|Ошибка авторизации в AW| {"success":false,"error":{"code":404,"message":"Не найдено: 5"}}| System.Net.Http.HttpRequestException: Response status code does not indicate success: 404 (Not Found).	В файле svody.config в секции Bars.Authorization в параметре «ProviderId» задать корректный id провайдера Id провайдера указан в AW

16 Настройка отображения метрик сервиса форм

В приложении сервиса форм реализована возможность экспорта различных метрик в Prometeus. Для просмотра и мониторинга значений метрик рекомендуется использовать инструменты визуализации Grafana, т.к. в Grafana есть встроенная поддержка источников данных prometeus.

Таким образом, перед тем как включить сбор метрик, необходимо (желательно на отдельном сервере) развернуть и настроить приложение Prometeus и Grafana.

16.1 Установка Prometeus

Установка приложения Prometeus осуществляется согласно официальным инструкциям, расположенным на сайте разработчика продукта Prometeus: https://prometheus.io.

После проведения установки Prometeus дальнейшее конфигурирование проходит после установки приложения Grafana.

16.2 Установка Grafana

Установка приложения Grafana осуществляется согласно официальным инструкциям, расположенным на сайте разработчика продукта Grafana: https://grafana.com.

После успешного проведения установки Grafana можно переходить к конфигурированию приложений

16.3 Настройка метрик со стороны ПП МЗ

Чтобы включить функциональность метрик, необходимо отредактировать файл конфигурации metrics.json в папке Config:

```
{
  "metrics": {
    "enabled": true,
    "port": 12345
  }
}
```

Значение `enabled = false` позволяет отключить сбор метрик во время работы приложения.

Значение `port` задает номер локального порта на сервере, где развернуто приложение, на котором будет доступна конечная точка с данными метрик в формате prometeus по url вида http://localhost:{port}/metrics.

16.4 Метрики, реализованные в приложении сервиса отчетных форм

Таблица 44 – Метрики, реализованные в приложении сервиса отчетных форм

Метрика	Значение
Http	
http_request_duration_seconds	время выполнения http-запроса в секундах
http_requests_received_total	общее количество обработанных запросов
http_requests_in_progress	количество активных запросов
Grpc	
grpc_requests_received_total	общее количество пришедших GRPC-запросов
Dotnet	
dotnet_gc_allocated_bytes_total	общее количество байт, выделенное для управляемой кучи
dotnet_gc_pause_ratio	процент времени, которое процесс приложение потратил на сборку мусора
dotnet_jit_il_bytes	общее количество байт, выделенное при компиляции IL-кода
dotnet_gc_heap_size_bytes	размер поколений и кучи больших объектов в байтах
dotnet_total_memory_bytes	общий объем выделенной памяти рантайму DotNet
dotnet_threadpool_timer_count	количество активных таймеров пула потоков рантайма DotNet
dotnet_gc_collection_count_total	количество сборок мусора с разбивкой по поколениям
dotnet_exceptions_total	количество исключений
dotnet_collection_count_total	общее количество сборок мусора
Группа метрик по работе с threadpool	
Группа метрик по работе с сокетами	
Метрики ОС	
Группа метрик "system_"	отражает показатели работы dotnet runtime
node_memory_PageFileFree	максимальный объем памяти, который может быть выделен процессу

Метрика	Значение
node_memory_MemoryLoad	число от 0 до 100, указывающее приблизительный процент используемой физической памяти (0 означает отсутствие использования памяти, а 100 — полное использование памяти)
node_memory_VirtualTotal	размер виртуального адресного пространства процесса в байтах. Это значение зависит от типа процесса, типа процессора и конфигурации операционной системы. Например, это значение составляет приблизительно 2 ГБ для большинства 32-разрядных процессов на процессоре x86 и приблизительно 3 ГБ для 32-разрядных процессов, которые поддерживают большие адреса и работают в системе с настройкой на 4 гигабайта.
node_filesystem_avail_bytes	Свободное место на диске
node_cpu_seconds_total	время работы ЦП в различных режимах
node_filesystem_size_bytes	общий размер всех дисков файловой системы
node_memory_MemFree	объем доступной физической памяти в байтах. Это объем физической памяти, который может быть немедленно повторно использован без предварительной записи ее содержимого на диск
node_memory_MemTotal	общий объем оперативной памяти
Метрики приложения сервиса форм	
cells_chunk_read_time	время в мс чтения набора значений ячеек из БД
cells_chunk_mirror_read_time 0	время в мс чтения набора значений ячеек зеркала данных формы из БД
cells_chunk_snapshot_read_time	время в мс чтения набора значений ячеек слепка данных формы из БД
cell_read_time	время в мс чтения значения одной ячейки из БД
cell_mirror_read_time	время в мс чтения значения зеркала одной ячейки из БД
cell_snapshot_read_time	время в мс чтения значения слепка одной ячейки из БД
cells_cache_hit	количество чтений из кэша значений ячеек
opened_forms	количество открытых форм

17 Настройка ssl-сертификата

Примечание: Инструкция по настройке носит рекомендательный характер.

В случае использовая приложения как модуля в рамках другой системы, либо из ПП МЗ необходимо открывать другое приложение (дизайнер отчетных форм, AW и т.д.), то обязательно нужно настроить доступ по https-протоколу. Сертификат должен быть доверенным, не самоподписным. Сертификаты, выданные через Госуслуги полностью подходят для работоспособности ПП МЗ.

Сами сертифкаты обычно выдают с расширением .crt или .pem. Совместно с сертификатом также выдается ключ с раширением .key. Сертификат и ключ могут быть предоставлены одним файлом. Секретный ключ следует хранить в файле с ограниченным доступом (права доступа должны позволять главному процессу nginx читать этот файл).

Ниже описан пример конфигурации nginx в качестве прокси-сервера для терминирования SSL трафика (настройка https).

Примечание: Для AW и нужен свой отдельный домен. Для остальных компонентов ПП МЗ можно использовать одно доменное имя.

17.1 Настройка приложения ПП МЗ

1. Найдите файл nginx.conf и создайте его резервную копию. Обычно этот файл находится в /`etc/nginx/nginx.conf`.
2. Откройте этот файл в текстовом редакторе и измените секцию server:

```
server {
  listen 80;
  listen 443 ssl;
  server_name your_domain.com;
  ssl_certificate /etc/ssl/certs/your_domain.crt;
  ssl_certificate_key /etc/ssl/certs/your_domain.key;
  }
```

17.2 Настройка сервера AW:

1.Перейдите в директорию, где расположен AW, например:

```
cd /opt/aw/
```

2.Остановите контейнеры AW:

```
docker-compose down
```

3.Создайте резервную копию конфигурационных файлов:

```
cp /opt/aw/docker/nginx/nginx.conf
/opt/aw/docker/nginx/nginx.conf.bak
```

4.Сохраните резервную копию конфигов AW (.env, а так же два файла .yml из директории AW)

5.Скопируйте файлы сертификата и ключа в директорию /opt/aw/docker/nginx/ например:

```
cp /path/to/your_domain.crt /opt/aw/docker/nginx/
cp /path/to/your_domain.key /opt/aw/docker/nginx/
```

6. Откройте файл `/opt/aw/docker/nginx/nginx.conf` в текстовом редакторе.

7. Добавьте следующую секцию в файл:

```
listen 443 ssl;
        ssl_certificate     /etc/ssl/your_domain.crt;
        ssl_certificate_key /etc/ssl/your_domain.key;
```

8. Открываем docker-compose.yml , расположенный по пути `/opt/aw/docker-compose.yml`

в текстовом редакторе и добавляем в секции:

- ports:

```
${AW_FRONTEND_HTTP_PORT:-80}:80
```

Добавляем порт 443 для HTTPS:

```
${AW_FRONTEND_HTTPS_PORT:-443}:443
```

Дальше:

После строки

```
restart: always
```

Измените секцию `volumes` для проброса сертификата и ключа в контейнер:

- volumes:

```
./docker/nginx/nginx.conf:/etc/nginx/nginx.conf
```

добавляем сюда:

```
./docker/nginx/cert_mz63_2.pem:/etc/ssl/your_domain.crt
```

```
./docker/nginx/cert_mz63_2.key:/etc/ssl/your_domain.key
```

9. Сохраните изменения. Поднимите контейнеры с пересозданием:

```
docker-compose up -d --force-recreate
```

18 Аварийные ситуации

Возникающие при работе с ПП МЗ нештатные ситуации, причины их возникновения и способы решения описаны в таблице (Таблица 45).

Таблица 45 – Аварийные ситуации

№	Название ошибки	Причины возникновения	Способы устранения
1	Ошибка 404	Сервер не может распознать запрос, отправленный web-браузером	Удалите cookie из web-браузера
2	«OutOfMemoryException»	Необработанная ошибка работы приложения встречается при недостатке оперативной памяти на Web-сервере.	При появлении такой ошибки необходимо проверить количество свободной оперативной памяти на Web-сервере приложения ПП МЗ.
3	Ошибка компиляции макросов формы	Возникает при открытии отчетной формы и означает отсутствие нужной Api. Библиотеки должны храниться в каталоге «AddInLib» на одном уровне с «bin»	Необходимо обновить файлы в папке «AddInLib» на web-сервере из дистрибутива
4	Ошибка подключения к БД. Сообщение «Не найден файл настроек»	Отсутствие возможности прочесть файл «Приложение.барс»	Необходимо проверить содержимое файла «Приложение.барс», работоспособность СУБД
5	Отображение даты в печатной форме на английском языке	Дата отображается в виде «January, 1»	Добавьте в файл «svody.config» секцию: <globalization> <Culture>ru-RU</Culture>

№	Название ошибки	Причины возникновения	Способы устранения
			<UiCulture>ru-RU</UiCulture> </globalization>
7	Сообщение «Время сессии истекло»	Сработал тайм-аут на запрос, либо приложение перезапустилось. Возможна критичная ошибка, которая приводит к отказу приложения	Повторно авторизуйтесь в ПП МЗ.
8	Если в логе при открытии Списка АВ ошибка |ERROR|AW|Ошибка авторизации в AW| {"success":false,"error":{"code":404,"message":"Не найдено: 5"}}| System.Net.Http.HttpRequestException: Response status code does not indicate success: 404 (Not Found). at System.Net.Http.HttpResponseMessage.EnsureSuccessStatusCode() at BARS.Svody.Web.Host.Areas.Security.Aw.OpenIdAwAuthClient.GetTokenAsync()* at System.Net.Http.HttpResponseMessage.EnsureSuccessStatusCode() at BARS.Svody.Web.Host.Areas.Security.Aw.OpenIdAwAuthClient.GetTokenAsync()	Некорректная настройка авторизации, поэтому она не проходит.	Необходимо в конфиге ПП МЗ проверить корректность заданного Id <ProviderId>5</ProviderId>

Лист регистрации изменений

Изм.	Версия ПП МЗ	Версия документа	Дата внесения изменений	Автор изменений	Краткое описание изменений
1	5.0	1	09.07.2021	Школьная Е.О.	Документ создан
2	5.0	1	27.10.2021	Жукова А.И.	Добавлены п.: 12, 12.1
3	5.1	1	21.04.2021	Халитов М.Т.	Добавлены п. 13 и п.14.
4	5.1	2	09.06.2022	Рахимова Н.Д.	Добавлены п.: 7 – 12
5	5.1.1	1	27.06.2022	Пырихина Е.В.	Обновлен п. 13.1
6	5.2	1	25.11.2022	Пашукова М.И.	Документ актуализирован в рамках совершенствования ПП МЗ
7	5.2.3	1	13.02.2023	Хомик А.В.	Исправлены орфограф. и пунктуационные ошибки. Актуализированы: Определения, обозначения и сокращени, п. 4.8
8	5.2.4	1	14.03.2023	Валиева З.И.	Документ актуализирован в рамках совершенствования ПП МЗ, п.12
9	5.2.5	1	17.03.2023	Лебедева А.Р.	Обновление информации по AW
10	5.3	1	28.04.2023	Хомик А.В.	Добавлены п.: 15.5 – 15.9. Обновлены п.: 10.1, 14.1.1, 14.1.2.
11	5.3.0	2	15.06.2023	Тарасевич Е.В.	Актуализированы: 2.3, 3.2, 4.6, 4.7, 5, 5.5, 5.6, 6.5, 6.6, 7.5, 9.1, 10.1, 12.1, 16. Добавлено: 16.4
12	5.3.0	3	30.06.2023	Пырихина Е.В.	Документ отформатирован по ГОСТ 2.105-2019
13	5.3.2	1	13.09.2023	Тарасевич Е.В.	Добавлен п. 15.5, п. 16.3. Актуализированы: п. 2, п. 4.6, п. 5.5, п. 6.5, п. 7.5, п. 7.4, п. 10.1, п. 18
14	5.3.3	1	03.10.2023	Савельева Е.В.	Документ отформатирован. Актуализированы Определения, обозначения и сокращения
15	5.3.4	1	16.10.2023	Салахов С.Р.	Добавлены п.: 4.12, 5.11, 6.11, 7.11 Актуализированы п.: 2.4, 2.6, 4.10, 5.9, 6.9, 7.9
16	5.3.4	2	17.10.2023	Салахов С.Р.	Актуализированы п.: 10.11 , 15.9
17	5.3.6	1	09.11.2023	Тарасевич Е.В.	Актуализирован п. 10.4
18	5.3.9	1	19.01.2024	Салахов С.Р.	Актуализирован п. 10.4

Изм.	Версия ПП МЗ	Версия документа	Дата внесения изменений	Автор изменений	Краткое описание изменений
19	5.3.11	1	09.02.2024	Салахов С.Р.	Актуализирован п. 10.4