Федеральное государственное унитарное предприятие
«Российский федеральный ядерный центр –
Всероссийский научно-исследовательский институт экспериментальной физики»

УТВЕРЖДЕН
07623615.00427-09 32 01-ЛУ

КОМПЛЕКС ПРОГРАММ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ «СИСТЕМА ПОЛНОГО ЖИЗНЕННОГО ЦИКЛА ИЗДЕЛИЙ «ЦИФРОВОЕ ПРЕДПРИЯТИЕ»

ПРОГРАММНЫЙ МОДУЛЬ «СИСТЕМА ИНТЕГРИРОВАННОЙ ЛОГИСТИЧЕСКОЙ ПОДДЕРЖКИ» (ОСНОВНАЯ ВЕРСИЯ 4)

Руководство системного программиста

07623615.00427-09 32 01

Листов 68

Инв № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
35-17161	08.11.2021			

2021

АННОТАЦИЯ

Настоящий документ содержит руководство системного программиста ПМ ИЛП (Основная версия 4).

Документ является составной частью документации, разработанной в соответствии с Техническим заданием на разработку программного модуля «Система интегрированной логистической поддержки» инв. № 35-5996-дсп от 12.07.2021 [1].

Руководство системного программиста включает:

- общие сведения о программе (назначение и функции ПМ ИЛП, требования к техническим и программным средствам);
- описание структуры программы;
- сведения о настройке программы;
- описание проверки работоспособности программы и мер для обнаружения модификации ПО или расхождения между оригиналом и версией, полученной пользователем;
- описание дополнительных возможностей.

Сообщения оператору указаны по мере работы программы в процессе ввода данных.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Назначение и функции программы

ПМ ИЛП предназначен для обеспечения информационной поддержки видов деятельности, осуществляемых разработчиком изделия совместно с другими участниками жизненного цикла изделия и направленных на формирование системы технической эксплуатации изделия, обеспечивающей эффективное использование изделия при приемлемой стоимости его жизненного цикла.

Функциями ПМ ИЛП являются:

1) формирование информационной модели изделия и системы его технической эксплуатации в форме БД АЛП;

2) решение задач сбора, обработки и анализа информации об изделии и системе его эксплуатации;

3) моделирование процессов технической эксплуатации изделий при различных сценариях применения, и оценки достигаемых показателей готовности парка изделия и соответствующих финансовых затрат;

4) оценка показателей безотказности как изделия в целом, так и его систем и СЧ;

5) хранение данных в соответствии с заданной информационной моделью.

Описание функций ПМ ИЛП приведено в следующих документах:

- 07623615.00427-09 13 01-2 Описание программы. Часть 2;
- 07623615.00427-09 13 01-3 Описание программы. Часть 3;
- 07623615.00427-09 13 01- 4 Описание программы. Часть 4;
- 07623615.00427-09 13 01-5 Описание программы. Часть 5;
- 07623615.00427-09 13 01-6 Описание программы. Часть 6;
- 07623615.00427-09 13 01-7 Описание программы. Часть 7;
- 07623615.00427-09 13 01-8 Описание программы. Часть 8.

1.2 Сведения о технических и программных средствах, обеспечивающих выполнение программы

ПЭВМ, предназначенная для работы ПМ ИЛП, должна удовлетворять определенным требованиям к ПО и техническим средствам.

1.2.1 Требования к техническим средствам

Для функционирования ПМ ИЛП необходимы следующие аппаратные средства:

1) для сервера СУБД и сервера приложений (включая сервер СХД) необходим компьютер, удовлетворяющий следующим требованиям:

- процессор: архитектура x64, частота не менее 3 ГГц и количество ядер не менее 8;
- оперативная память: 8Gb и более;
- жесткий диск: 1Tb и более;
- сетевая карта: скорость передачи данных 100 Мбит/с и выше;
- видеокарта и монитор, обеспечивающие разрешение экрана 1280x1024 или более;
- клавиатура и манипулятор типа «мышь».

Рекомендуется использовать высокоскоростной жесткий диск;

2) для клиентского рабочего места необходим персональный компьютер, удовлетворяющий следующим минимальным требованиям:

- процессор: архитектура x64, частота не менее 2 ГГц и количество ядер не менее 2;
- оперативная память: 4Gb и более (для ОС Windows 8Gb и более);
- жесткий диск: 256Gb и более;
- сетевая карта: скорость передачи данных 100 Мбит/с и выше;
- видеокарта и монитор, обеспечивающие разрешение экрана 1280x1024 или более;
- клавиатура и манипулятор типа «мышь».

Не рекомендуется использовать видеокарту Intel(R) Q45/Q43 Express Chipset;

3) локальная вычислительная сеть, обеспечивающая пропускную способность не менее 1000 Мбит/с.

1.2.2 Требования к ПО

Для функционирования ПМ ИЛП необходимы следующие программные средства:

1) ОС:

а) сервер СУБД и сервер приложений (включая сервер СХД) может работать на следующих ОС:

- Astra Linux Special Edition версии 1.6 (64-х разрядная версия);
- Microsoft Windows Server 2016 и новее (64-х разрядная версия) или Microsoft Windows 10 (64-х разрядная версия);

б) клиентская часть ПМ ИЛП может работать на следующих ОС:

- Astra Linux Special Edition версии 1.6 (64-х разрядная версия);
- Microsoft Windows 10 (64-х разрядная версия);

При использовании ОС Astra Linux необходимо установить пакеты (и для сервера, и для клиента):

- «libpq-dev»;
- «libsasl2-dev»;
- «python-dev»;
- «libldap2-dev»;
- «libssl-dev»;
- «qml»;
- «qtquickcontrols2-5-dev»;
- «qtdeclarative5-dev»;
- «qtlocation5-dev»;
- «qtmultimedia5-dev»;
- «dh-make» (из стандартного дистрибутива Astra Linux Special Edition);
- «qml-module-qtlocation»;
- «qml-module-qtpositioning»;
- «qtpositioning5-dev»;

При использовании в ОС Astra Linux домена ALD необходимо дополнительно установить следующие пакеты;

- все пакеты, имя которых начинается с «krb5»;
- все пакеты, имя которых начинается с «ald-»;
- все пакеты, имя которых начинается с «fly-admin-ald-».

Допускается работа сервера приложений и клиента ПМ ИЛП на разных ОС. При использовании механизма собственной аутентификации такая работа не налагает дополнительных требований. При использовании в кроссплатформенной среде доменной

аутентификации необходимо, чтобы используемые для работы сервера приложений и клиентской части компьютеры входили в общий домен;

2) для аутентификации в домене необходимо наличие домена Active Directory (AD) в случае использования ОС Windows или домена Astra Linux Domain (ALD) в случае использования ОС Astra Linux. Описание настроек доменной среды AD / ALD и ПМ ИЛП для доменной аутентификации приведено в 3.6;

3) СУБД:

- в ОС Astra Linux Special Edition версии 1.6 (64-х разрядная версия): СУБД PostgreSQL версии 9.6 (64-х разрядная версия), в качестве СУБД также может выступать СХД программного модуля;

- в ОС Microsoft Windows 10 (64-х разрядная версия): СУБД PostgreSQL версии 9.6 (64-х разрядная версия), СУБД Oracle версии 12c (64-х разрядная версия), в качестве СУБД также может выступать СХД программного модуля;

4) ПО для просмотра файлов в формате «*.xlsx», содержащих результаты расчетов.

2 СТРУКТУРА ПРОГРАММЫ

2.1 Структура программы и ее составные части

В ПМ ИЛП используется трехуровневая архитектура «клиент – сервер приложений – СУБД». Подробное описание структуры ПМ ИЛП приведено в 07623615.00427-09 13 01-1 Описание программы. Часть 1. В данном документе приведены общие сведения о структуре ПМ ИЛП.

Общая концептуальная схема программной архитектуры ПМ ИЛП приведена на рисунке 1.

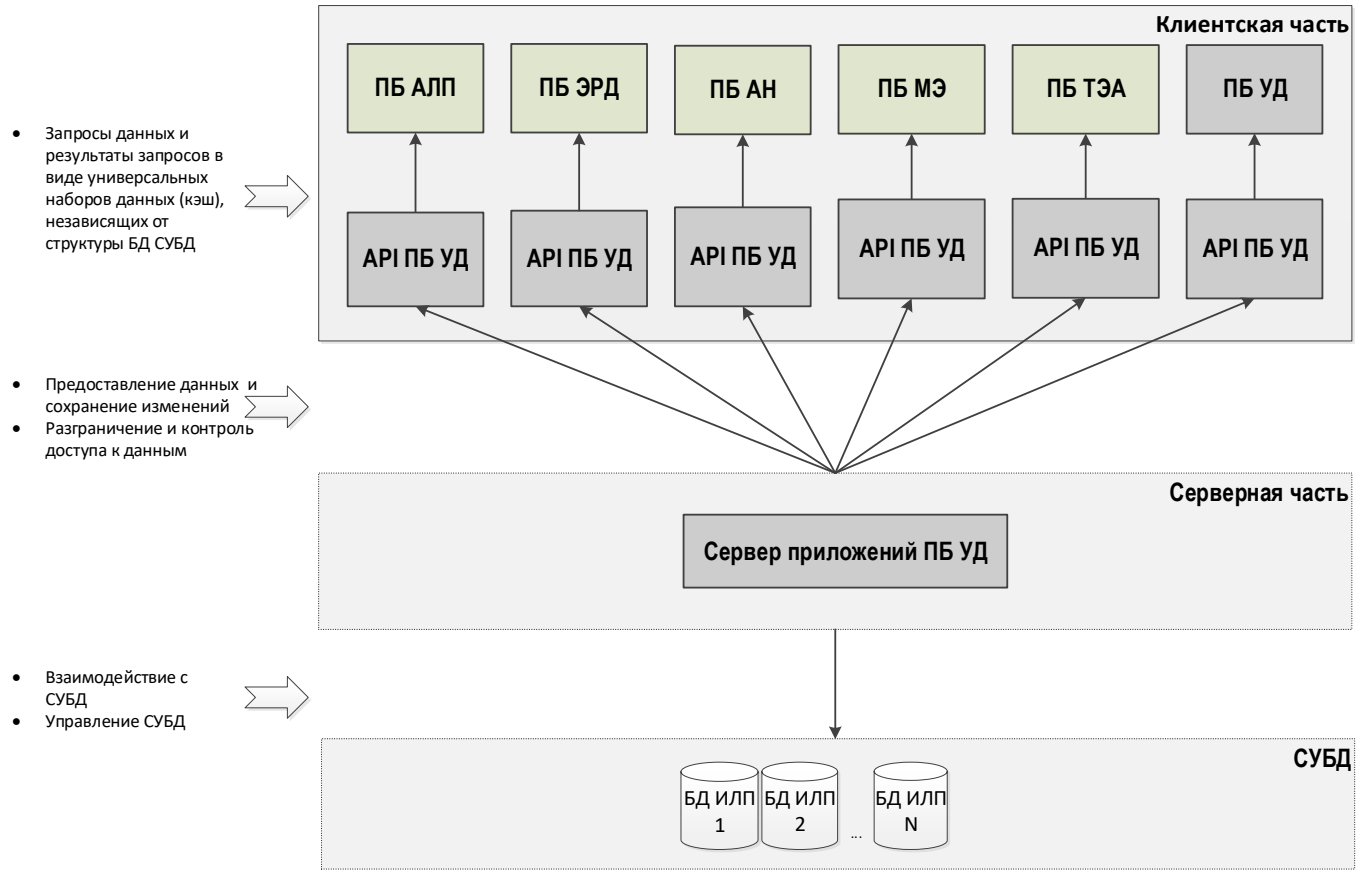

Рисунок 1 – Архитектура и состав компонентов ПМ ИЛП

Клиентская часть ПМ ИЛП состоит из набора программных компонентов ПБ АЛП, ПБ АН, ПБ ЭРД, ПБ МЭ, ПБ ТЭА и клиентской части ПБ УД.

ПБ УД предназначен для решения задач, связанных с сетевым взаимодействием, хранением и передачей данных, обеспечением их целостности, защитой от несанкционированного доступа и других задач, не связанных с прикладной логикой. ПБ УД состоит из компонентов данных и исполняемых компонентов, обеспечивающих доступ и настройку компонентов данных.

Компоненты ПБ УД:

- обеспечивают доступ к данным ИЛП с использованием трехуровневой архитектуры «клиент – сервер приложений – СУБД»;
- обеспечивают доступ к БД ИЛП для ПБ АЛП, ПБ ЭРД, ПБ МЭ, ПБ АН и ПБ ТЭА через сервер приложений;
- обеспечивают редактирование информационной модели БД ИЛП для ПБ АЛП, ПБ ЭРД, ПБ МЭ, ПБ АН и ПБ ТЭА и сохранение схемы данных;
- предоставляют низкоуровневый прикладной программный интерфейс доступа к локальным данным (кэш клиента) для ПБ АЛП, ПБ ЭРД, ПБ МЭ, ПБ АН и ПБ ТЭА;
- предоставляют низкоуровневый прикладной программный интерфейс доступа к данным в БД ПМ ИЛП для ПБ АЛП, ПБ ЭРД, ПБ МЭ, ПБ АН и ПБ ТЭА;
- предоставляют прикладной программный интерфейс для взаимодействия с внешними системами через обменные файлы в части группы функций для импорта и экспорта данных;
- предоставляют прикладной программный интерфейс для обновления штатных механизмов, реализующих меры защиты информации, путём регламентированной замены или добавления соответствующих файлов в развёрнутом экземпляре ПМ ИЛП в части группы функций для обновления механизмов идентификации, аутентификации и авторизации;
- обеспечивают настройку УЗ пользователей и групп пользователей, существующих только в контексте ПМ ИЛП для ПБ АЛП, ПБ ЭРД, ПБ МЭ, ПБ АН и ПБ ТЭА;
- обеспечивают механизм контроля состава, проверки соответствия и запуска ПБ ПМ ИЛП на клиенте и на сервере;

- обеспечивают управление параметрами авторизации подключений, включая ограничение числа параллельных сеансов и ограничение времени бездействия субъекта в сеансе;

- обеспечивают механизм регистрации событий безопасности, связанных с доступом к данным ПМ ИЛП;

- обеспечивают разграничение и контроль доступа субъектов к данным ПМ ИЛП в БД под управлением СУБД Oracle;

- реализуют механизм, обеспечивающий процессы идентификации и аутентификации, включая взаимодействие с компонентами ОС и Secret Net Studio 8.

ПМ ИЛП работает с единой интегрированной БД (БД ИЛП). Звено СУБД ПМ ИЛП реализуется ПБ УД и осуществляет взаимодействие серверной части ПМ ИЛП с СУБД, в качестве которой может выступать:

- СХД;
- СУБД PostgreSQL (в ОС Microsoft Windows и ОС Astra Linux);
- СУБД Oracle (в ОС Microsoft Windows).

ПБ УД выполняет функции администрирования и настройки СХД. Администрирование и настройка СУБД PostgreSQL и Oracle выполняются заимствованными компонентами соответствующей СУБД или через прикладной программный интерфейс (API) клиентской части СУБД с использованием диалогового взаимодействия администратора БД ИЛП через графический интерфейс серверных компонентов ПБ УД.

2.2 Связи между составными частями программы

Взаимодействие между ПБ АЛП, ПБ ЭРД, ПБ АН, ПБ МЭ и ПБ ТЭА осуществляется через общую БД. Доступ к БД для ПБ АЛП, ПБ ЭРД, ПБ МЭ, ПБ АН и ПБ ТЭА осуществляется через сервер приложений ПБ УД.

Описание взаимодействия между составными частями ПМ ИЛП приведено в 07623615.00427-09 13 01-1 Описание программы. Часть 1.

Все изменения в БД выполняются в режиме реального времени, поэтому они автоматически становятся доступны для всех ПБ, которые работают с БД.

При функционировании в разных БД передача данных из ПБ МЭ в ПБ АЛП возможна посредством обменного «*.xml» файла, формат которого описан в 07623615.00427-09 13 01-8 Описание программы. Часть 8. Книга 35.

2.3 Связи программы с другими программами

В ПМ ИЛП реализован прикладной программный интерфейс для взаимодействия с другими программами через обменные файлы. Описание прикладного интерфейса приведено в 07623615.00427-09 13 01-8 Описание программы. Часть 8. Книга 7.

3 НАСТРОЙКА ПРОГРАММЫ И СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

3.1 Установка ПМ ИЛП

Установка ПМ ИЛП выполняется с использованием инсталлятора. Инструкции по установке приведены в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 1.

После установки ПМ ИЛП следует настроить программу. Инструкции по настройке программы приведены в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 1.

3.2 Общие сведения о настройке ПМ ИЛП

Настройка программы включает следующие этапы:

- подготовительные действия к созданию БД при работе с СУБД PostgreSQL (создание папки для размещения БД и назначение ей необходимых прав доступа) или СУБД Oracle (создание сетевой службы для доступа сервера приложений к БД). При работе с СУБД PostgreSQL настройка выполняется на компьютере с сервером СУБД PostgreSQL, а при работе с СУБД Oracle – на компьютере с Oracle Client. Подготовительные действия описаны в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 2. Подразделы 3.2, 3.3, 3.4;

- формирование БД на основе информационной модели БД в СХД, СУБД PostgreSQL и СУБД Oracle описано в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 2. Подразделы 3.2, 3.3, 3.4;

- запуск сервера приложений при работе с СУБД PostgreSQL или СУБД Oracle. Запуск сервера приложений описан в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 1. Пункт 3.2.2;

- настройка логики работы и элементов интерфейса ПМ ИЛП с помощью «Модуля настроек и опций БД» описана в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 1. Пункт 3.2.3;

- настройка параметров подключения к БД, необходимых для работы сервера приложений с БД (адрес компьютера с промежуточным сервером приложений, номер

порта, по которому работает сервер приложений, и имя БД). Настройка доступа к БД описана в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 1. Подраздел 3.3.

Описание применяемых технических и организационных мер, используемых для обнаружения модификации ПО или любого расхождения между оригиналом и версией, полученной пользователем, в объеме, достаточном для правильной настройки и безопасного применения программы, приведено в 4.2.

Сообщения оператору, выдаваемые в ходе выполнения настройки, указаны по мере работы программы в процессе ввода данных.

3.3 Настройка ПМ ИЛП в ОС Microsoft Windows

3.3.1 Настройка сервера СУБД

Настройка сервера СУБД включает настройку СУБД Oracle, СУБД PostgreSQL или СХД, создание записей БД и создание БД.

Настройка СХД состоит из следующих шагов:

1) определить каталог для размещения БД СХД и каталога со словарями;

2) задать пути к каталогу размещения БД и пути к словарям в файле конфигурации «AplTransport.ini»;

3) создать БД СХД утилитой «Приложение для администрирования СХД».

Настройка СУБД PostgreSQL состоит из следующих шагов:

1) создать в каталоге, заданном при установке СУБД PostgreSQL, папку для размещения БД;

2) задать для созданной папки разрешения на полный доступ для системной группы пользователей «NETWORK SERVICE» или другого пользователя, с правами которого работает служба СУБД PostgreSQL;

3) создать запись БД утилитой «Администратор БД для PostgreSQL»;

4) сгенерировать БД ПМ ИЛП в PostgreSQL утилитой «Администратор БД для PostgreSQL».

Настройка СУБД Oracle состоит из следующих шагов:

1) создать сетевую службу (alias) с помощью утилиты Net Manager (из каталога установки Oracle Client);

2) создать запись БД утилитой «Администратор БД для Oracle»;

3) сгенерировать БД утилитой «Администратор БД для Oracle».

Подробнее настройка сервера СУБД рассматривается в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 2.

3.3.2 Настройка сервера приложений

Настройка сервера приложений выполняется в соответствии с 3.5.

Перед настройка сервера приложений необходимо выполнить настройку сервера СУБД, которая включает:

- создание записей БД СХД утилитой «Приложение для администрирования СХД» (при использовании БД СХД);
- создание записей БД PostgreSQL утилитой «Администратор БД для PostgreSQL» (при использовании СУБД PostgreSQL);
- создание записей БД Oracle утилитой «Администратор БД для Oracle» (при использовании СУБД Oracle);
- установку параметров доступа к домену и способов аутентификации путем изменения файла настроек «AplTransport.ini» (см. 3.6.2.1);
- установка параметров журнала информационной безопасности путем изменения файла настроек «AplTransport.ini».

3.3.3 Настройка клиента

Для настройки клиента необходимо:

1) настроить УЗ пользователей;
2) настроить подключения к БД.

3.4 Настройка ПМ ИЛП в ОС Astra Linux

3.4.1 Настройка сервера СУБД

Настройка сервера СУБД включает настройку СУБД PostgreSQL или СХД, создание записей БД и создание БД.

Настройка СХД состоит из следующих шагов:

1) определить каталог для размещения БД СХД и каталога со словарями;

2) задать пути к каталогу размещения БД и пути к словарям в файле конфигурации «AplTransport.ini»;

3) создать БД СХД утилитой «Приложение для администрирования СХД».

Настройка СУБД PostgreSQL состоит из следующих шагов:

1) создать в каталоге «/var/lib/postgresql/9.6», используемом для размещения БД PostgreSQL, папку для размещения БД;

2) задать для созданной папки разрешения на полный доступ для пользователя, под которым работает служба СУБД PostgreSQL;

3) создать запись БД утилитой «Администратор БД для PostgreSQL»;

4) сгенерировать БД ПМ ИЛП в PostgreSQL утилитой «Администратор БД для PostgreSQL».

Настройка сервера СУБД рассматривается в 07623615.00427-09 34 01-1 Руководство оператора. Часть 1. Книга 2.

3.4.2 Настройка сервера приложений

Настройка сервера приложений выполняется в соответствии с 3.5.

Настройка сервера включает следующие действия:

- создание записей БД СХД утилитой «Приложение для администрирования СХД» (при использовании БД СХД);
- создание записей БД PostgreSQL утилитой «Администратор БД для PostgreSQL» (при использовании СУБД PostgreSQL);
- установка параметров доступа к домену и способов аутентификации путем изменения файла настроек «AplTransport.ini» (см. 3.6.2.1);
- установка параметров журнала информационной безопасности путем изменения файла настроек «AplTransport.ini».

3.4.3 Настройка клиента

Необходимо:

1) настроить УЗ пользователей;

2) настроить подключения к БД.

3.5 Процедуры настройки сервера приложений и выбор конкретной БД для работы сервера приложений

По умолчанию каждый сервер приложений использует свой порт: 7239 для PostgreSQL, 7240 для СХД и 7241 для Oracle. Это обеспечивает возможность их одновременной работы на одном компьютере. Если необходимо изменить рабочий порт сервера, то необходимо выполнить следующие действия:

1) запустить интерпретатор командной строки в ОС Windows или терминал Fly для ОС Astra Linux;

2) запустить из него нужный сервер приложений с ключом «/p:», указав номер свободного порта. Например:

- «aplPGServer /p:7239» для работы с БД PostgreSQL;
- «aplLiteServer /p:7240» для работы с СХД;
- «aplOraServer /p:7241» для работы с БД Oracle (для ОС Windows).

При работе в ОС Astra Linux при запуске сервера из командной строки необходимо указывать полный путь к серверу приложений. Например, если ПМ ИЛП находится в папке «/opt/PM_ILP», то команда на запуск в командной строке или команда в ярлыке должна быть такой:

- «/opt/PM_ILP/aplPGServer /p:7239» (для запуска сервера приложений для PostgreSQL с рабочим портом 7239);
- «/opt/PM_ILP/aplLiteServer /p:7240» (для запуска сервера приложений для СХД с рабочим портом 7240).

В настроечном файле «AplTransport.ini» номер порта при запуске сервера приложений не задается.

Номер порта, по которому работает сервер приложений, отображается в окне сервера приложений при его запуске (рисунок 2).

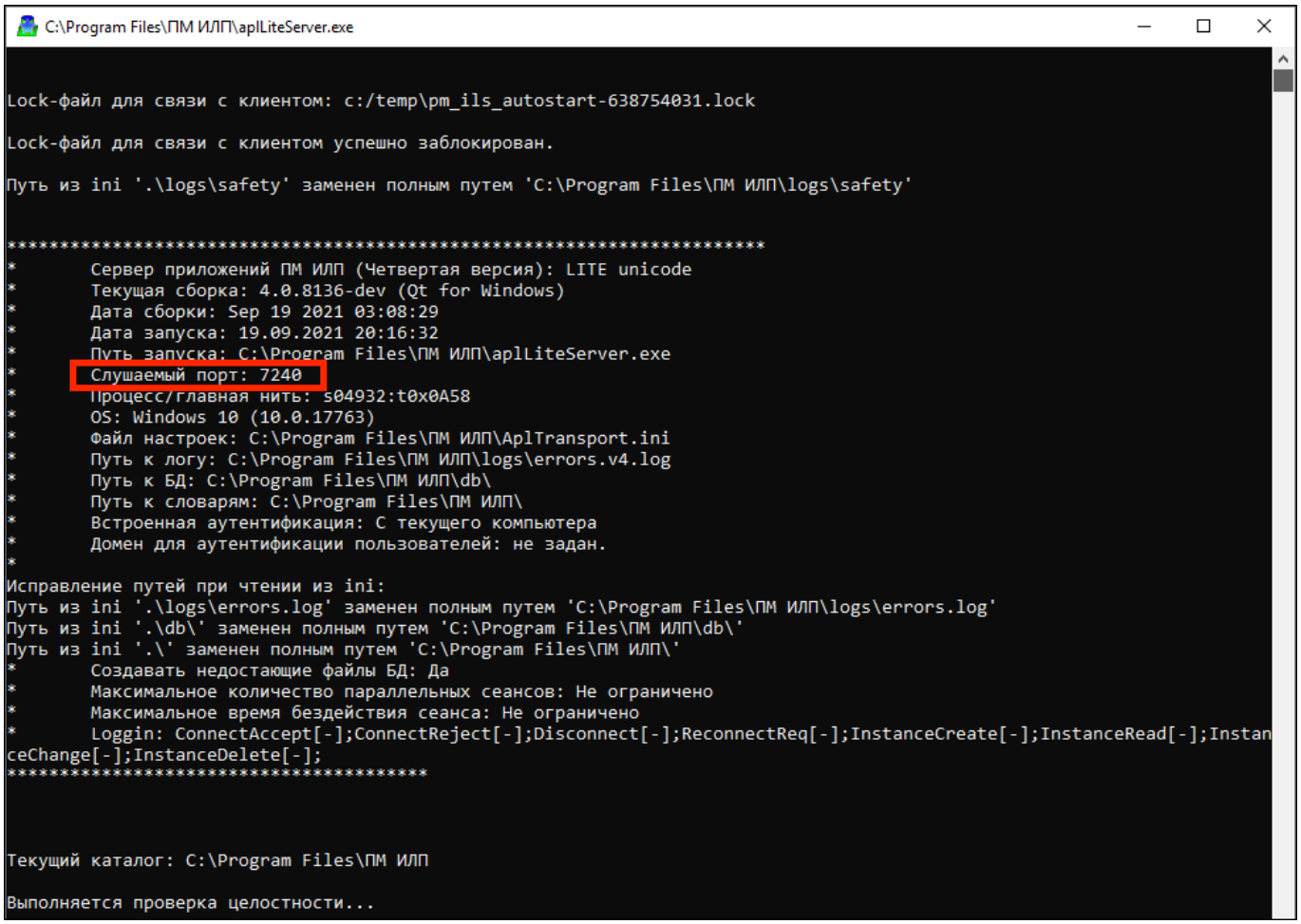

Рисунок 2 – Пример окна сервера приложений «aplLiteServer.exe» в ОС Windows

Для вывода информации о текущем состоянии сервера приложений и подключениях клиентов к нему необходимо запустить веб-браузер и в его адресной строке ввести IP адрес машины, на которой запущен сервер приложений, и номер порта, например: «http://192.168.56.51:7240» (рисунок 3).

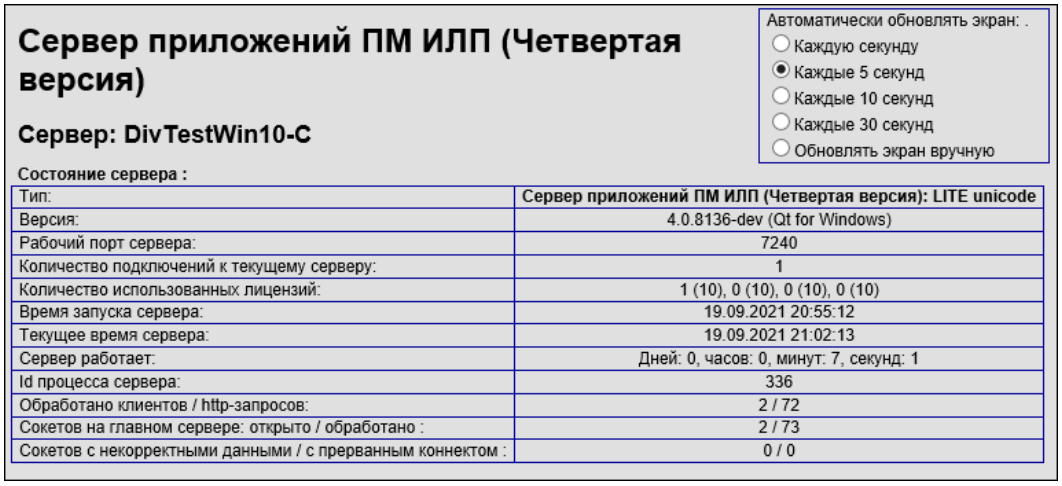

Рисунок 3 – Пример вывода информации о сервере приложений в веб-браузере

При настройке подключения клиента к БД для каждой БД указывают адрес сервера, где размещена БД, и номер порта, по которому работает сервер приложений.

Для настройки подключения необходимо выполнить следующие действия:

1) запустить на машине клиента ПМ ИЛП. В результате откроется диалоговое окно «Установка соединения с БД» (рисунок 4);

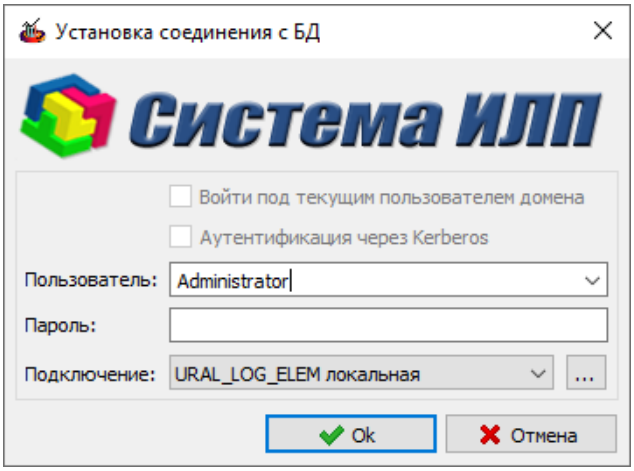

Рисунок 4 – Окно «Установка соединения с БД»

2) для настройки подключений нажать на кнопку ... «Настройка списка подключений» рядом с полем выбора подключения (см. рисунок 4);

3) откроется диалоговое окно «Настройка списка подключений» (рисунок 5). Здесь выводятся все подключения, которые содержатся в секции [ConnectionsList] файла настроек «AplTransport.ini» (рисунок 6). Для каждого подключения в файле настроек указано имя подключения, адрес компьютера, номер порта и имя БД. Тип сервера приложений не указывается, так как он определяется номером рабочего порта;

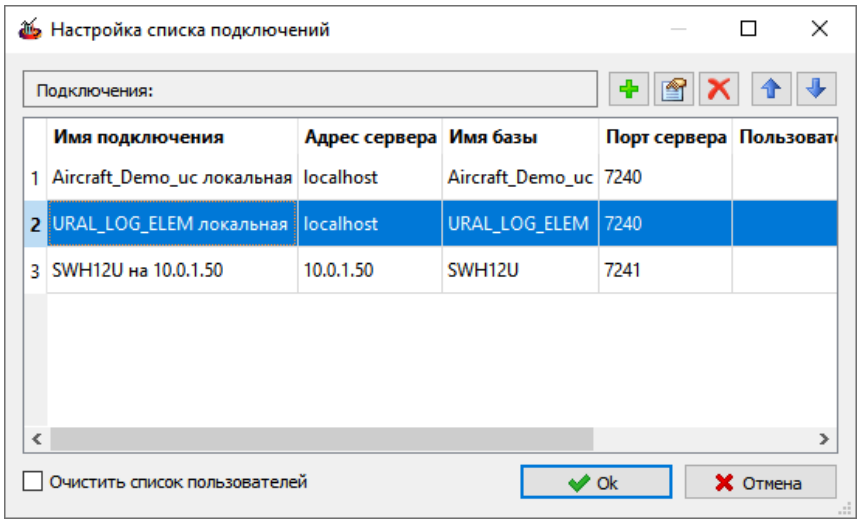

Рисунок 5 – Настройка списка подключений к БД

```
;Список подключений к БД
[ConnectionsList]
0=Aircraft_Demo_uc локальная=localhost:7240/Aircraft_Demo_uc
1=URAL_LOG_ELEM локальная=localhost:7240/URAL_LOG_ELEM
2=SWH12U на 10.0.1.50=10.0.1.50:7241/SWH12U
```

Рисунок 6 – Пример списка подключений к БД в файле «AplTransport.ini»

4) для изменения параметров подключения выбрать подключение и нажать на кнопку  «Редактировать свойства подключения» (см. рисунок 5). После этого откроется окно «Настройка параметров подключения» (рисунок 7);

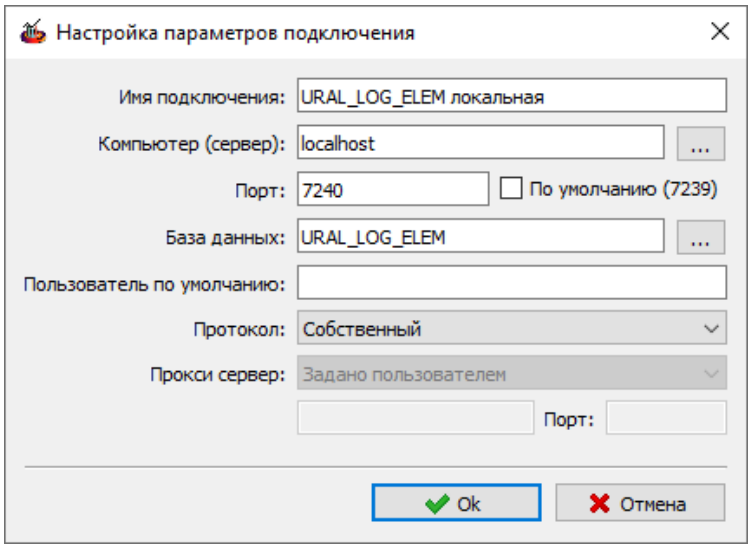

Рисунок 7 – Настройка параметров подключения к БД

5) для изменения имени подключения отредактировать поле «Имя подключения» (см. рисунок 7);

6) в поле «Компьютер (сервер)» указать IP адрес или имя удаленного сервера или «localhost», если БД находится на локальном компьютере;

7) в поле «База данных» выбрать БД, нажав на кнопку  справа от него (см. рисунок 7). В соответствии с указанным в окне «Настройка параметров подключения» адресом компьютера и рабочим портом сервера приложений отправляется запрос серверу приложений на передачу списка БД, с которым он работает на этом компьютере. Сервер приложений читает соответствующую ему секцию в файле настроек «AplTransport.ini» ([BasesLite] для СХД, [BasesPostgres] для PostgreSQL и [BasesOra] для Oracle) и возвращает список БД клиенту ПМ ИЛП. Клиент выводит его в открывшемся окне «Выберите Базу данных» (рисунок 8). Списки БД на стороне сервера приложений формируются при создании БД с помощью утилит «Администратор БД» для СХД, PostgreSQL и Oracle;

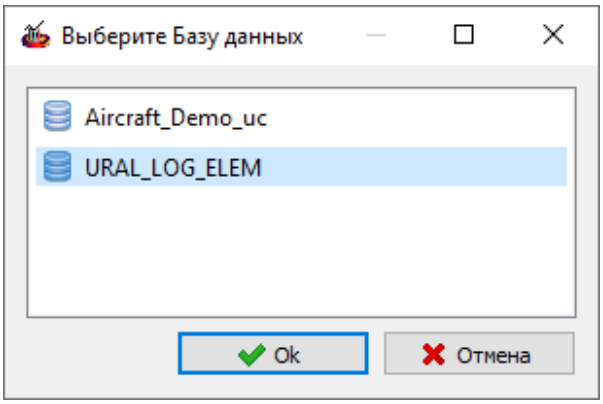

Рисунок 8 – Окно «Выберите Базу данных» со списком БД

8) в окне «Настройка параметров подключения» выбрать БД и нажать на кнопку «Ok» для сохранения измененных данных и закрытия окна (см. рисунок 8). Измененные данные о подключении автоматически будут сохранены в секции [ConnectionsList] файла настроек «AplTransport.ini» (см. рисунок 6);

9) для создания нового соединения нажать на кнопку  в окне «Настройка списка подключений» (см. рисунок 5). В открывшемся окне «Настройка параметров подключения» задать имя подключения, компьютер, порт, базу данных и пользователя по умолчанию. Нажать на кнопку «Ok» для сохранения данных и закрытия окна. Данные по созданному подключению будут сохранены на компьютере клиента в файле «AplTransport.ini» в секции [ConnectionsList];

10) для удаления параметров подключения нажать на кнопку  в окне «Настройка списка подключений» (см. рисунок 5). В открывшемся диалоговом окне нажать на кнопку «Да» для подтверждения действия и закрытия диалогового окна (рисунок 9);

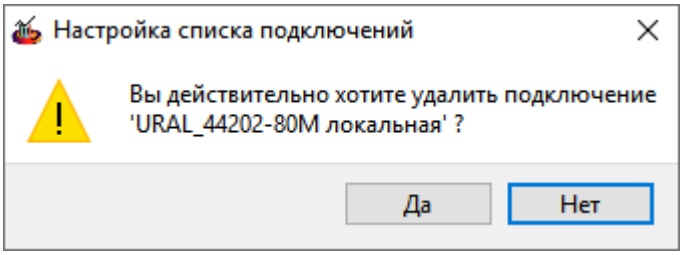

Рисунок 9 – Диалоговое окно при удалении подключения к БД

11) для выбора БД для подключения раскрыть список в поле «Подключение» в окне «Установка соединения с БД» (рисунок 10).

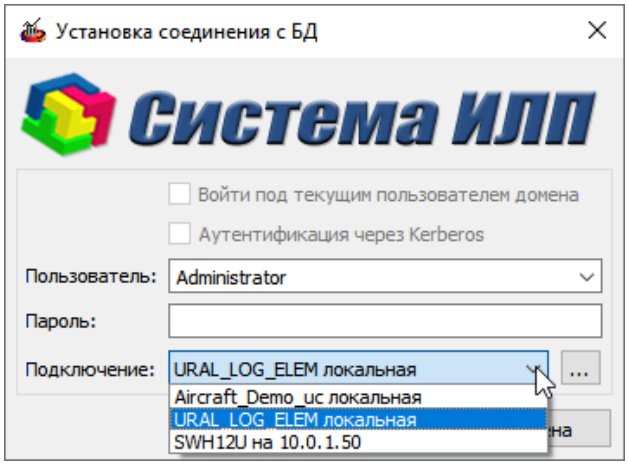

Рисунок 10 – Выбор БД для подключения

Выбор конкретной БД осуществляется сервером приложений при выборе конкретного подключения.

3.6 Идентификация и аутентификация

3.6.1 Общие сведения

При работе ПМ ИЛП без использования доменной среды единственным механизмом аутентификации пользователей является собственный механизм аутентификации. В этом случае используются пара логин – пароль из УЗ пользователей, заданных в БД ПМ ИЛП (рисунок 11).

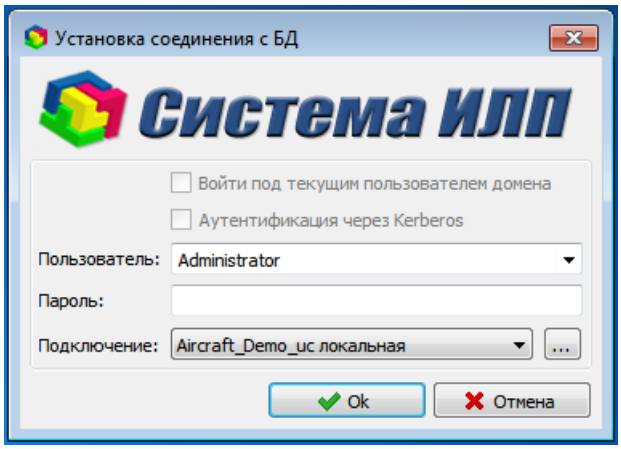

Рисунок 11 – Окно «Установка соединения с БД» (аутентификация в локальной среде)

При работе ПМ ИЛП в доменной среде основным способом аутентификации является аутентификация в домене. При этом логины пользователей, заданные в ПМ ИЛП должны совпадать с логинами пользователей, заданных в домене. ПМ ИЛП может взаимодействовать как с доменами Active Directory (при работе в ОС Windows), так и с доменами Astra Linux Domain (при работе в ОС Astra Linux).

Аутентификация под доменным пользователем возможна двумя методами (рисунок 12):

1) прямым обращением к контроллеру домена;

2) аутентификация через API Kerberos.

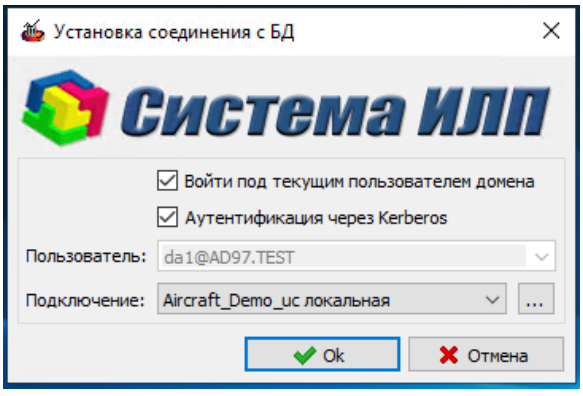

Рисунок 12 – Окно «Установка соединения с БД» (аутентификация в доменной среде)

Аутентификация прямым обращением к контроллеру домена использует параметры сессии текущего пользователя ОС и при обращении к контроллеру домена только подтверждает актуальность и полномочия текущего пользователя, поэтому она возможна только для текущего пользователя домена.

Аутентификация через API Kerberos выполняется путем итерационных обращений к API на стороне клиента и на стороне сервера приложений и обмена зашифрованными пакетами; такой механизм позволяет выполнять аутентификацию только под текущим пользователем домена и обеспечивает высокую степень надежности и безопасности аутентификации пользователя.

Для повышения степени безопасности аутентификации ПМ ИЛП можно ограничить или совсем отключить механизм собственной аутентификации и отключить аутентификацию прямым обращением к контроллеру домена.

3.6.2 Настройка ПМ ИЛП

Настройка ПМ ИЛП состоит из двух стадий:

- необходимо задать настройки доступа к домену путем изменения файла настроек «AplTransport.ini» в каталоге сервера приложений;
- необходимо создать УЗ пользователей ПМ ИЛП с помощью ПБ «Конфигуратор пользователей».

3.6.2.1 Настройка сервера приложений для использования доменной аутентификации

При необходимости можно включить автоматическое создание в ПМ ИЛП УЗ при первом подключении доменного пользователя путем изменения файла «AplTransport.ini» на стороне сервера приложений.

Для аутентификации путем прямого обращения к контроллеру домена и для проверки нахождения УЗ пользователя в доменной группе, разрешающей использование ПМ ИЛП при аутентификации с помощью API Kerberos необходимо задать на стороне сервера приложений в файле «AplTransport.ini» в группе [LocalServer] следующие параметры:

- LdapServer= – имя контроллера домена;
- LdapUser= – имя пользователя домена, который имеет право на чтение информации о других пользователях в формате <имя пользователя>@<полное имя домена>, например, da1@ad97.test;
- LdapPwd= – пароль пользователя домена, заданного параметром LdapUser;

- LdapGroupe= – группа пользователей в домене, которым разрешен вход в ПМ ИЛП;

- LdapUsersGroupeInDb= – имя группы пользователей ПМ ИЛП, в которой при необходимости будет создана УЗ пользователя ПМ ИЛП. Указанная группа будет создана в БД ПМ ИЛП автоматически при создании первого пользователя (при условии разрешения автоматического создания пользователей). Посмотреть ее наличие и входящих в нее пользователей можно в ПБ «Конфигуратор пользователей» в разделе «Рабочие группы». Параметр необходимо задавать, только если надо автоматически создавать в БД ПМ ИЛП УЗ пользователя. Пример такой группы с автоматически созданным пользователем, приведен на рисунке 13;

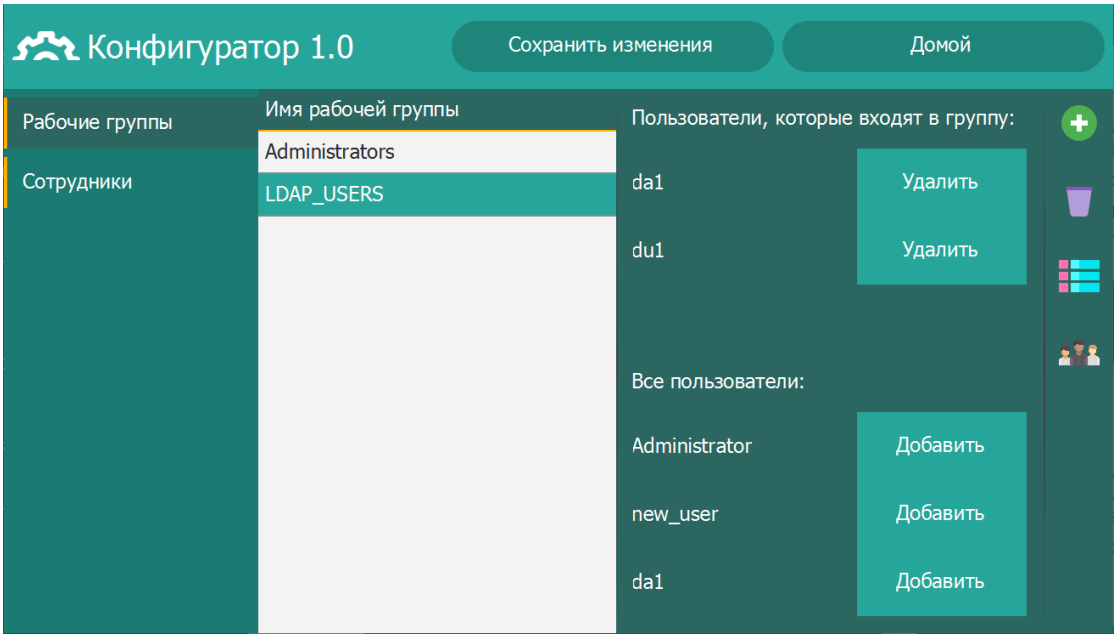

Рисунок 13 – Группа пользователей LDAP_USERS, в которую автоматически добавлен пользователь в результате доменной аутентификации

- AutoCreateLdapUsers= – задает поведение при отсутствии в БД ПМ ИЛП УЗ пользователя, одноименного пользователю домена. При значении «1» сервер приложений будет автоматически создавать УЗ пользователя ПМ ИЛП с логином, совпадающим с логином доменного пользователя, и помещать созданного пользователя в группу, заданную параметром «LdapUsersGroupeInDb».

Параметры LdapUser и LdapPwd необходимо задавать только при работе с AD в ОС Windows; при работе с ALD в Astra Linux их необходимо оставлять пустыми.

При доменной аутентификации через API Kerberos необходимо дополнительно задать на стороне сервера приложений в «AplTransport.ini» в группе [LocalServer] следующие параметры:

- SPN= – имя SPN, зарегистрированного в домене;
- Keytab= – путь к файлу «keytab» (только при аутентификации в ALD). При указании пути к файлу «keytab» можно использовать относительные пути.

После изменения настроек необходимо перезапустить сервер приложений.

Пример параметров при аутентификации в ALD домене «ald99.test» с контроллером домена «ald99dc.ald99.test», доменной группой «Пользователи ПМ ИЛП», группой в БД ПМ ИЛП «LDAP_USERS» и файлом «keytab ils-ald99srv.keytab», расположенном в каталоге установки ПМ ИЛП:

```
[LocalServer]
…
;Настройки подключения к серверу LDAP для доменной авторизации
LdapServer=ald99dc.ald99.test
LdapUser=
LdapPwd=
LdapGroupe=Пользователи ПМ ИЛП
LdapUsersGroupeInDb=LDAP_USERS
SPN=ils/ald99srv.ald99.test@ALD99.TEST
Keytab=./ils-ald99srv.keytab
AutoCreateLdapUsers=1
```

Пример параметров при аутентификации в AD домене «ad97.test» с контроллером домена «dc97.ad97.test», пользователем доменов для чтения информации «da1@ad97.test», доменной группой «Пользователи ПМ ИЛП» и группой для создания пользователей БД ПМ ИЛП «LDAP_USERS»:

```
;Параметры сервера приложений
[LocalServer]
…
;Настройки подключения к серверу LDAP для доменной авторизации
LdapServer=dc97.ad97.test
LdapUser=da1@ad97.test
LdapPwd=11
LdapGroupe=Пользователи ИЛП
LdapUsersGroupeInDb=LDAP_USERS
SPN=ils/ad97-srv.ad97.test
```

Для отключения аутентификации в домене прямым обращением к контроллеру домена необходимо задать на стороне сервера приложений в файле «AplTransport.ini» параметр [LocalServer] «LdapAuthentication». Значение «0» запрещает аутентификацию прямым обращением к контроллеру домена, значение «1» или отсутствие параметра – разрешает. Пример настроек для запрета аутентификации прямым обращением к контроллеру домена:

```
[LocalServer]
LdapAuthentication=0
```

Для ограничения или отключения собственной аутентификации необходимо задать на стороне сервера приложений в файле «AplTransport.ini» параметр [LocalServer] InternalAuthentication. Параметр может принимать следующие значения:

- «All» – собственная аутентификация разрешена со всех адресов;
- «Local» – собственная аутентификация разрешена только клиентам с текущего компьютера (значение по умолчанию);
- «Deny» – собственная аутентификация запрещена всем клиентам.

Если параметр не задан, используется значение «Local». Пример разрешения собственной аутентификации для всех адресов:

```
[LocalServer]
InternalAuthentication=All
```

Настройки управления аутентификацией так же вступают в силу после перезапуска сервера приложений.

При ограничении собственной аутентификации следует учесть, что первоначальная настройка новой БД ПМ ИЛП должна выполняться встроенным пользователем «Administrator», авторизующимся исключительно через механизм собственной аутентификации.

3.6.2.2 Настройка УЗ

Настройка УЗ выполняется в ПБ «Конфигуратор пользователей» в разделе «Сотрудники».

При аутентификации собственным механизмом в УЗ обязательно надо задать логин и пароль пользователя. Логин используется при идентификации, пароль – при аутентификации пользователя.

При аутентификации в домене логин УЗ должен совпадать с логином доменного пользователя. Можно запретить УЗ участвовать в собственной аутентификации, для этого необходимо в параметрах УЗ указать, что она предназначается только для аутентификации в домене; для таких УЗ задавать пароль не обязательно (рисунок 14).

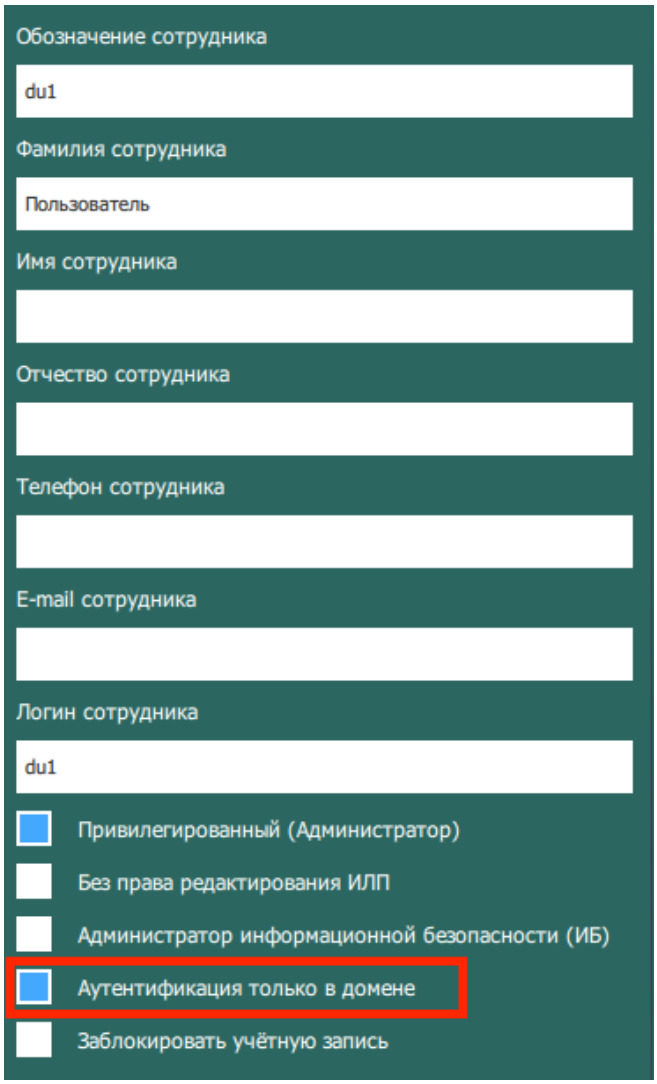

Рисунок 14 – Флаг по умолчанию «Аутентификация только в домене» в свойствах автоматически созданного пользователя

В процессе создания УЗ можно прочитать из домена параметры пользователя и одновременно проконтролировать правильность созданной УЗ с помощью функции «Получить пользователя из домена». Для работы этой функции необходимо, чтобы в файле «AplTransport.ini» на стороне сервера приложений были заданы параметры LdapServer, LdapUser, LdapPwd и LdapGroupe для домена AD и LdapServer и LdapGroupe для домена ALD (см. 3.6.2.1).

Для этого необходимо выполнить следующие действия:

1) открыть рабочее окно «Сотрудники»;

2) создать нового сотрудника, нажав кнопку «Создать нового сотрудника»;

3) заполнить поле «Обозначение сотрудника» и нажать кнопку «Сохранить изменения»;

4) выбрать созданного сотрудника из списка;

5) нажать кнопку «Получить пользователя из домена» (рисунок 15);

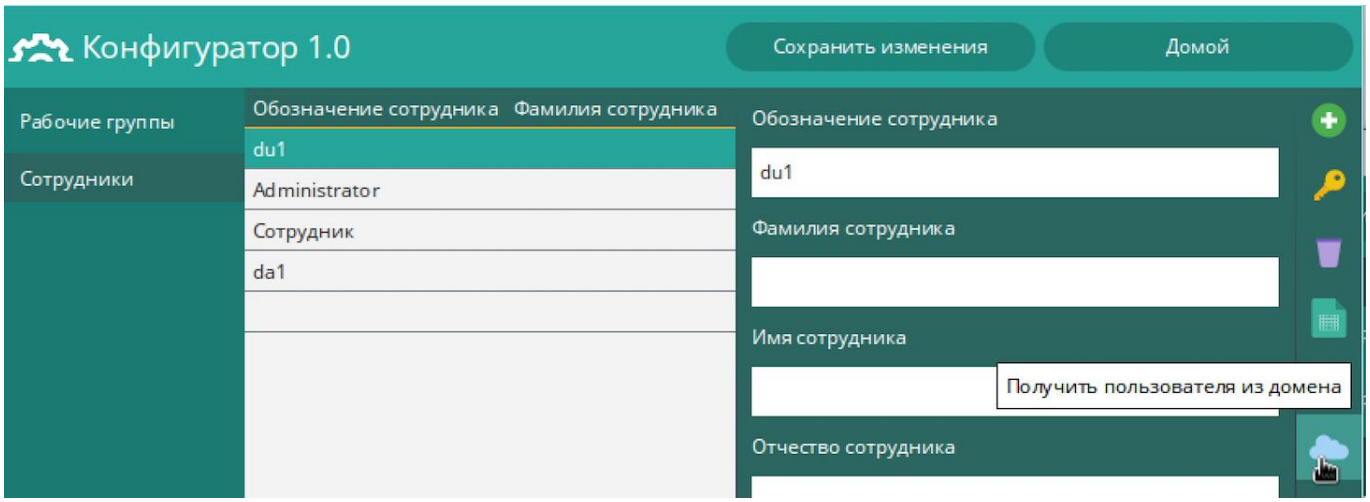

Рисунок 15 – Получение пользователя из домена

6) если сотрудник с таким обозначением существует в домене, то его данные будут взяты из УЗ домена и загружены в БД ИЛП (рисунок 16). Если логин не был задан, присваивается значение, указанное в обозначении сотрудника;

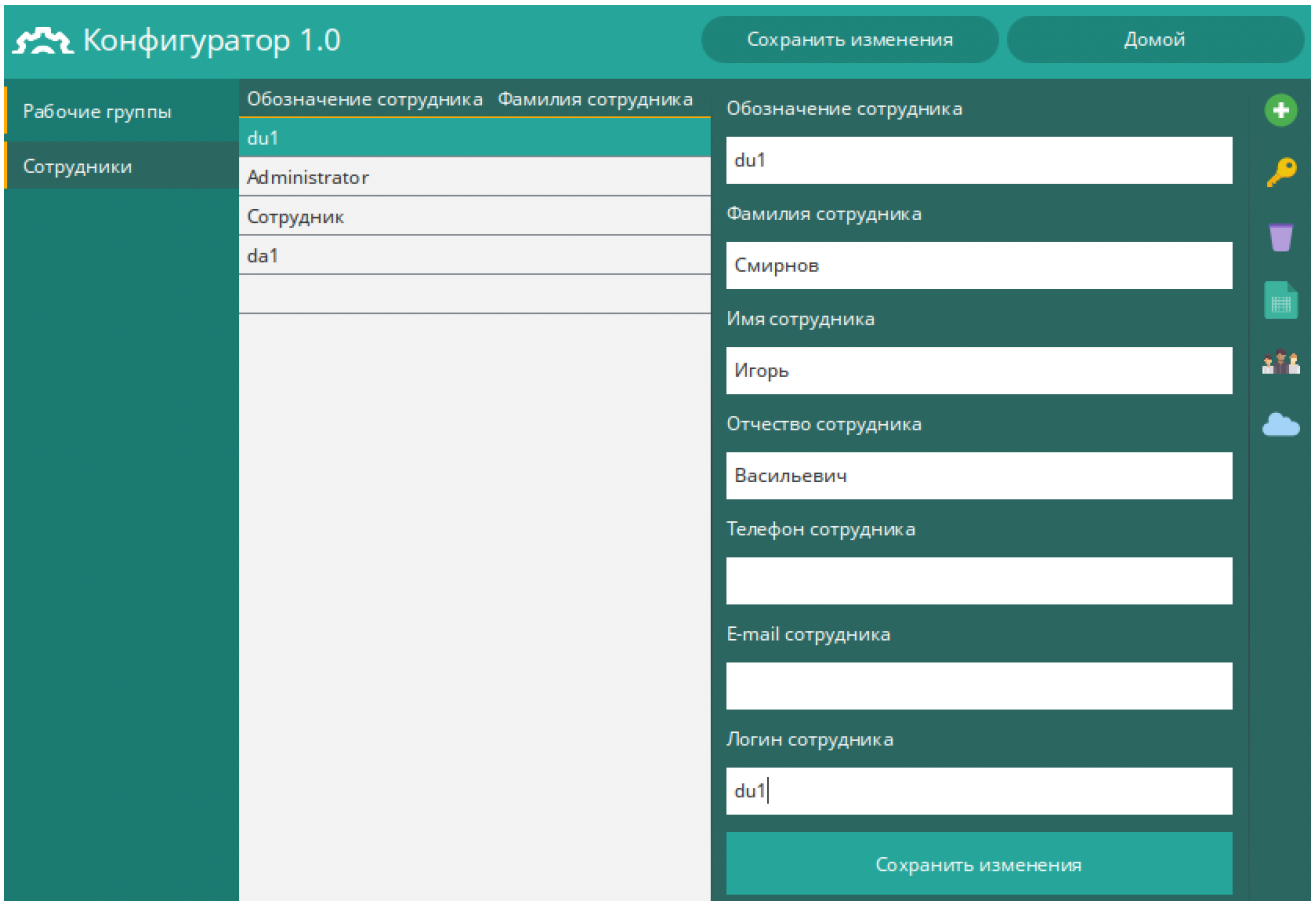

Рисунок 16 – Данные сотрудника, загруженные из УЗ в домене

7) нажать на кнопку «Сохранить изменения».

3.6.3 Настройка Kerberos в Astra Linux Directory

3.6.3.1 Общие сведения

Для работы Kerberos в Astra Linux на всех компьютерах должны быть установлены следующие пакеты:

- krb5-kdc;
- krb5-kpropd;
- krb5-multidev;
- krb5-user;
- krb5-config;
- krb5-admin-center.

Так же должны быть установлены все пакеты, от которых зависят перечисленные.

Общие сведения о настройке:

1) настройки данных о принципалах – в файле «/etc/krb5/krb5.conf». В нем указываются возможные REALM (с адресами серверов KDC) и преобразование имен доменов в REALM;

2) для корректной работы необходима работа обратного преобразования IP в адрес (обратный DNS). Проверяется вызовом «nslookup <server ip address>». (Для установки программы «nslookup», необходимо установить пакет «dnsutils»).

Если определение доменного имени по IP через DNS недоступно (например, при отсутствии DNS сервера), то можно прописать необходимые адреса в файле «/etc/hosts» (рекомендуется) или установить значение переменной «rdns» в значение «false» на клиентах в файле «krb5.conf» (не рекомендуется);

3) для работы сервиса (сервера) необходимо задать на компьютере с сервером приложений путь к файлу «keytab». Это выполняет сервер приложений путем установки переменной окружения «KRB5_KTNAME», которая должна содержать полный путь к файлу:

```
setenv("KRB5_KTNAME","/usr/krb5-ils.keytab",1);
```

4) для сборки программ, использующих Kerberos, необходимо установить пакет «ald-dev»:

```
sudo apt-get install  ald-dev
```

5) если аутентификация не проходит:

а) первым делом необходимо смотреть на соответствие времени; при разнице в показаниях часов больше, чем на 5 минут, Kerberos считает пакеты данных не валидными. В частности, на виртуальных машинах VMware по умолчанию отключено использование системных часов. Поэтому даже у работающих на одном сервере виртуализации виртуальных машин может возникнуть большая разница во времени;

б) убедится, что сервер запущен от имени пользователя домена. Сервер, запущенный от имени локального пользователя компьютера, не сможет участвовать в аутентификации;

6) при возникновении ошибки «Возможно, неверные имя пользователя или пароль» при коннекте под текущим пользователем необходимо убедиться, что:

а) клиент не запущен под пользователем root (через sudo …);

б) вход в систему был осуществлен под пользователем домена.

3.6.3.2 Создание SPN для сервиса аутентификации

Для создания SPN необходимо на контроллере домена в сеансе пользователя «superadmin» запустить утилиту «kadmin» (рисунок 17).

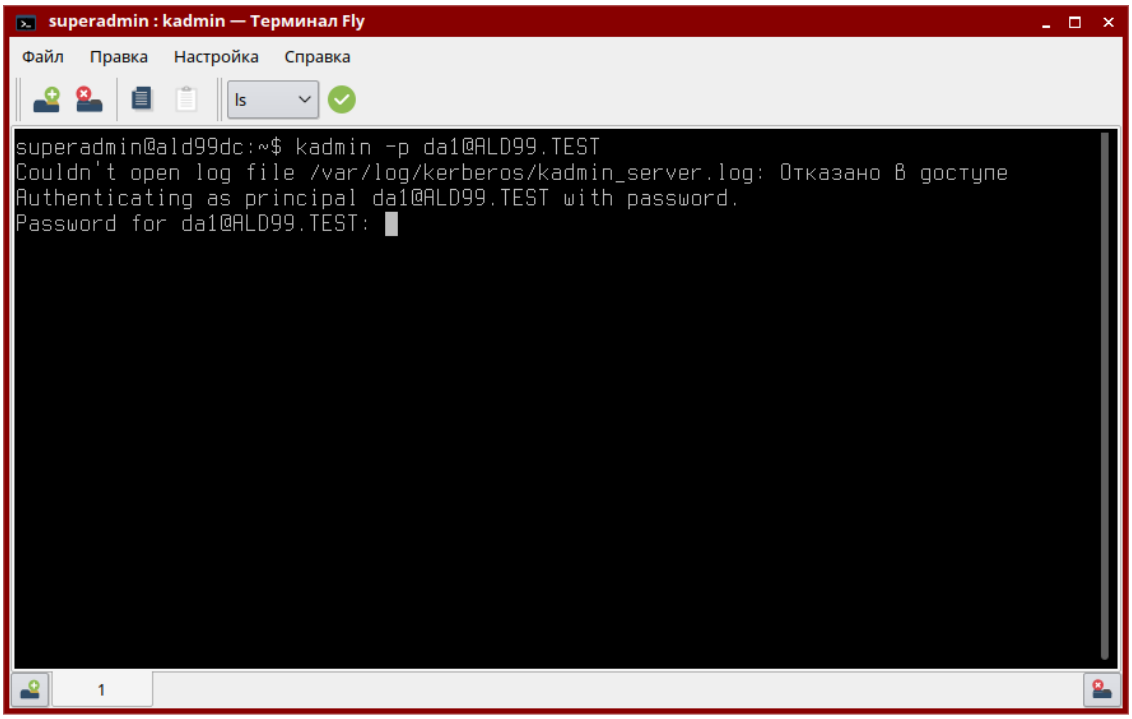

Рисунок 17 – Запуск утилиты «kadmin»

Пример формата запуска утилиты «kadmin»:

```
kadmin -p <UPN>
```

В приведенном примере формата запуска утилиты «kadmin»:

- «-p» – указание о вводе имени принципала;
- «<UPN>» – UPN администратора домена.

Пример, где `«da1@ALD99.TEST»` – UPN администратора домена, можно просто – «da1»:

```
kadmin -p da1@ALD99.TEST
```

После ввода пароля запустится утилита «kadmin» (рисунок 18).

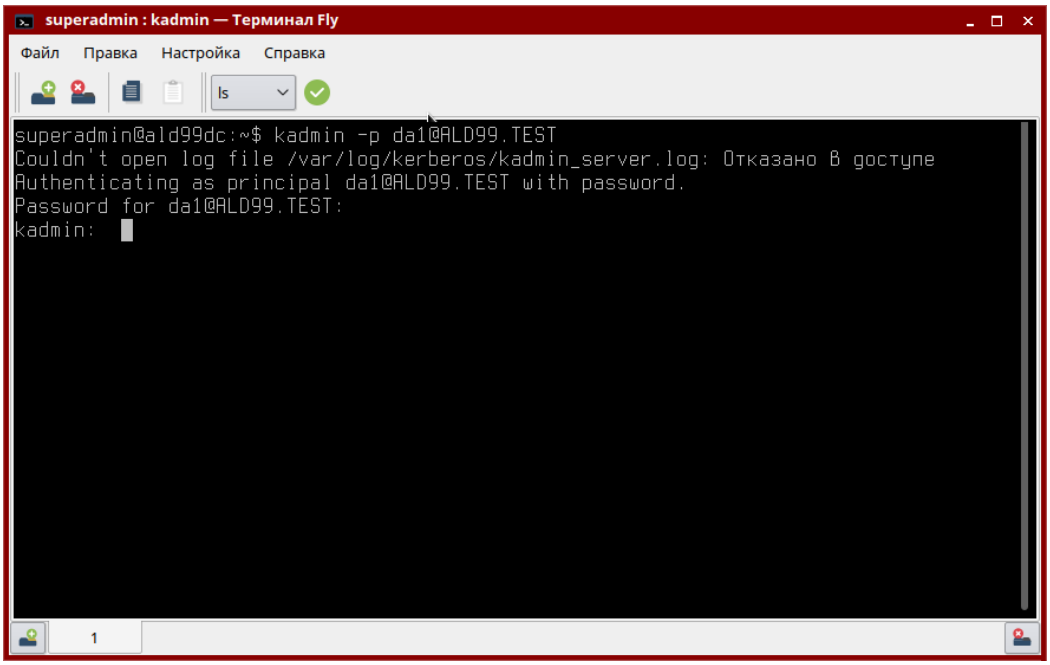

Рисунок 18 – Ввод пароля

Для регистрации принципала сервиса необходимо выполнить команду «addprinc».

Пример команды:

```
addprinc -randkey  ils/ald99srv.ald99.test@ALD99.TEST
```

В приведенном примере команды:

- «-randkey» – команда генерации случайного пароля. Этот вариант является рекомендованным, так как он не позволит выполнить злоумышленнику аутентификацию от имени сервиса;

- «ils/ald99srv.ald99.test@ALD99.TEST» – SPN для сервиса (рисунок 19).

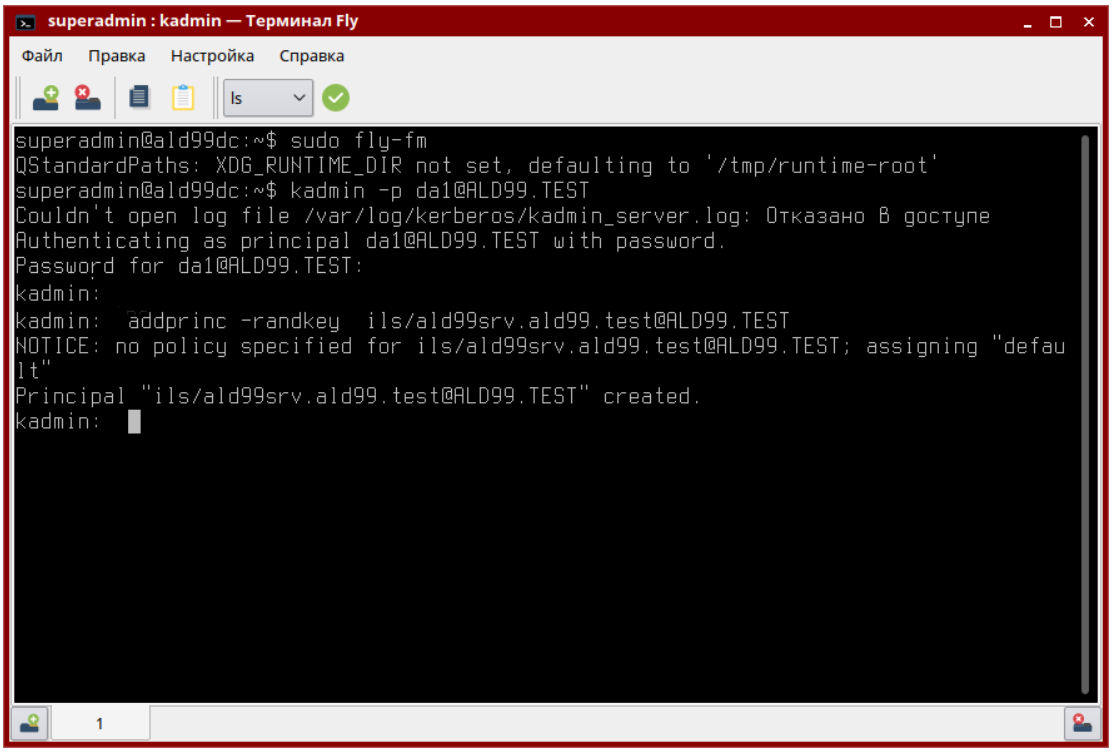

Рисунок 19 – Регистрация SPN

Далее необходимо выгрузить данные принципала сервиса в файл «keytab» (рисунок 20). Это делается командой «ktadd».

Пример команды «ktadd»:

```
ktadd -k /_TEST/ils-ald99srv.keytab ils/ald99srv.ald99.test@ALD99.TEST
```

В приведенном примере команды «ktadd»:

- «-k» – команда формирования файла «keytab»;
- «/_TEST/ils-ald99srv.keytab» – путь к формируемому файлу «keytab»;
- «ils/ald99srv.ald99.test@ALD99.TEST» – SPN сервиса.

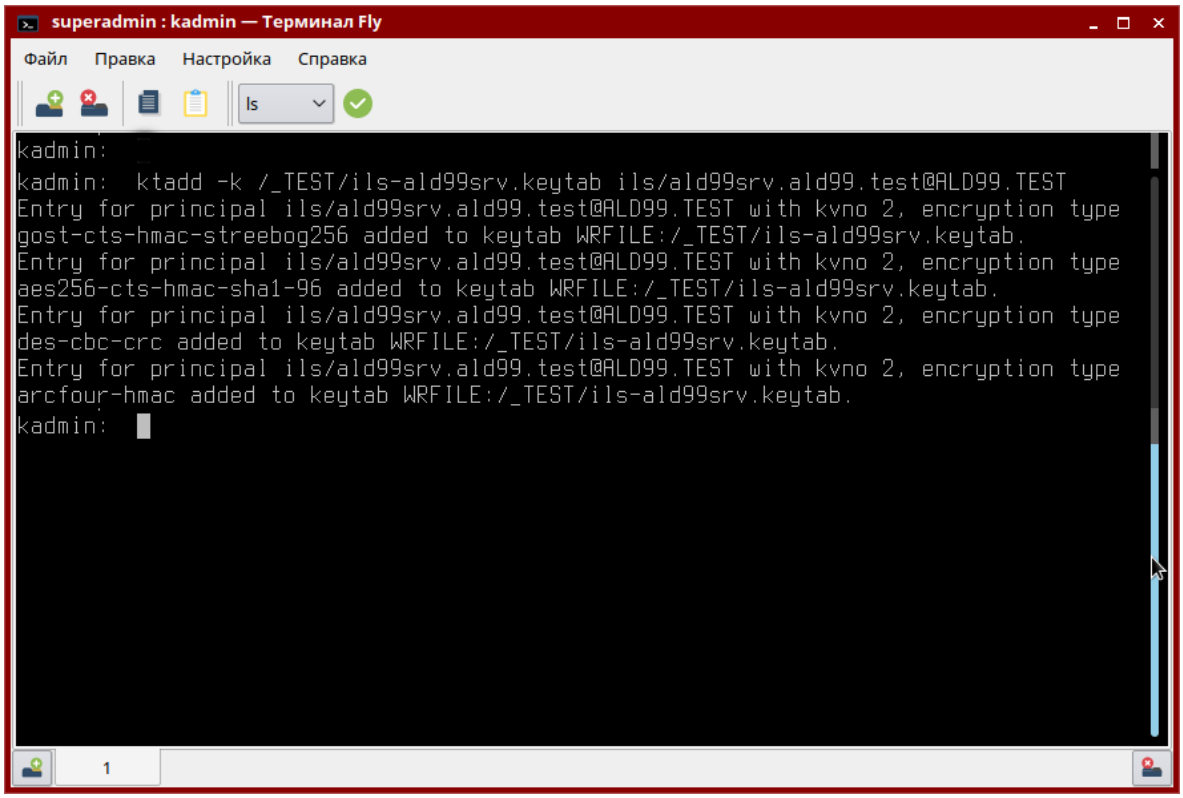

Рисунок 20 – Формирование файла «keytab»

Полученный файл «keytab» (в примере «/_TEST/ils-ald99srv.keytab») необходимо перенести на компьютер с севером приложений (указанный в SPN) и задать в файле параметров сервера приложений «AplTransport.ini» следующие параметры в группе [LocalServer]:

- «Keytab» – указать путь к файлу «keytab». Можно использовать относительные пути; отсчет ведется от каталога расположения файла «AplTransport.ini»;

- «SPN» – необходимо задать имя созданного SPN.

Настройки файла «AplTransport.ini» для доменной авторизации см. 3.6.2.1.

3.6.3.3 Дополнительные настройки для настройки работы с Kerberos в Astra Linux Directory

Дополнительные настройки для настройки работы с Kerberos в Astra Linux Directory:

1) использование утилиты klist.

При запуске без параметров отображает список билетов в КЭШе.

При вызове с параметром «-k» и указанием файла отображает список SPN в файле «keytab». Формат вызова: `klist -k <файл keytab>;`

2) использование утилита «ktutil». Позволяет работать с содержимым файла «keytab». Для работы используются команды:

- чтение файла keytab в память: «read_kt»;
- отображение списка записей в памяти: «list»;
- запись содержимого памяти в файл «keytab» на диске: «write_kt»;
- удаление записи: «delent»;
- выход: «quit».

Примеры использования приведены в таблице 1.

Таблица 1 – Примеры использования

Выполняемое действие	**Команда**
Отображение списка записей в файле	> klist -k mykeytab version_number username@DOMAIN version_number username@DOMAIN
Объединение нескольких в keytab файлов в один	> ktutil ktutil: read_kt mykeytab-1 ktutil: read_kt mykeytab-2 ktutil: read_kt mykeytab-3 ktutil: write_kt krb5.keytab ktutil: quit
Удаление записи	> ktutil ktutil: read_kt mykeytab ktutil: list ... slot# version# username@DOMAIN version# ... ktutil: delent slot#

3.6.3.4 Формирование файла «keytab»

Формирование файла «keytab» так же может понадобиться для авторизации пользователя ActiveDirectory на сервере, работающем под управлением Linux (возможно не для всех версий Linux). В этом случае для сервиса необходимо:

- создать пользователя домена для сервиса, работающего под Linux;
- зарегистрировать для него SPN;

- сформировать файл «keytab».

Файл «keytab» формируется вызовом команды «ktpass». При этом для пользователя формируется ключ шифрования в соответствии с нужным алгоритмом. Ключ шифрования может быть создан на основе явно заданного пароля или же на основе случайного пароля (рекомендуется во избежание авторизации в домене под пользователем сервиса).

Команда «ktpass» имеет следующие параметры:

- «/out» – задает имя файла keytab;
- «/princ» – SPN;
- «/mapuser» – пользователь домена (для сервиса);
- «/pass» – пароль пользователя. Задается явно или же при указании «rndpass» может генерироваться случайным образом;
- «/ptype» – тип принципала (сервис «KRB5_NT_SRV_HST» или пользователь «KRB5_NT_SRV_INST»). Рекомендуется универсальный «KRB5_NT_PRINCIPAL»;
- «/crypto» – алгоритм для ключа шифрования. Может задаваться один из конкретных алгоритмов («DES-CBC-CRC», «DES-CBC-MD5», «RC4-HMAC-NT», «AES256-SHA1», «AES128-SHA1»), но указав «ALL» можно сгенерировать ключи для всех алгоритмов.

Пример вызова:

```
ktpass /princ ils/ad97-srv.ad97.test@ad97.test /mapuser iu /pass rndpass /ptype KRB5_NT_PRINCIPAL /crypto ALL /out c:\ils.keytab
```

3.6.4 Настройка Kerberos в Windows Active Directory

3.6.4.1 Общие сведения

Так как Kerberos интегрирован в AD (а не является внешней системой, как в ALD) его использование значительно проще. Достаточно создать пользователя домена и зарегистрировать для него нужный SPN. Однако, использование Kerberos в AD имеет ряд особенностей, отличающих его от канонического Kerberos. Главной особенностью является привязка принципалов к записям домена, причем записью может являться не только доменный пользователь, но и компьютер. А так как запись компьютера имеет ряд ограничений, в том числе при работе с сетью, то такой вариант вызывает множество проблем и не является рекомендованным.

Основным режимом является работа сервиса под доменным пользователем. Причем это может быть пользователь заданный, как для сотрудника имеющего право входа на компьютер, так и специальный пользователь для сервиса.

При регистрации SPN, указанное имя привязывается к записи пользователя домена и расшифровать TGS для этого SPN сможет только сервис, запущенный под этим пользователем.

Регистрация одинаковых SPN для нескольких пользователей не допускается.

У каждого объекта AD есть многозначный атрибут «servicePrincipalName», в котором хранятся все имена SPN. Просмотреть атрибут можно с помощью редактора атрибутов Active Directory («ADSI Edit»). Если SPN предназначен для локальной УЗ «System» компьютера, то SPN будет храниться в атрибуте «servicePrincipalName» УЗ «Computers» в AD. Это значение не следует записывать напрямую; оно должно обновляться только через вызов «DsWriteAccountSpn» (но его можно обновить напрямую с использованием таких инструментов, как «ADSI Edit»).

Если клиент запрашивает соединение со службой, то центр дистрибуции ключей (Key Distribution Center – KDC) выполняет в лесу поиск УЗ пользователей и компьютеров, для которых зарегистрирован SPN. Если KDC обнаруживает регистрацию в более чем одной УЗ, то запрос проверки подлинности завершается неудачей, что указывает на ложную регистрацию службы.

3.6.4.2 Формат SPN

При всех операциях с SPN используется формат SPN:

```
<service_class>/<host>.<domain-name>[:<port>]
```

В приведенном формате SPN:

- <service_class> – имя класса сервиса. Примерами классов сервисов являются: http, ftp, ldap, smb, host, termsrv. В случае ПМ ИЛП используется префикс ils;
- <host> – имя компьютера;
- <domain-name> – имя домена. При задании можно использовать как полную, так и краткую запись. Но при этом это будут разные SPN. Например, «ils/srv.ad.test» и «ils/srv» – это разные SPN. Обычно, при регистрации сервиса Windows автоматически создает SPN для всех вариантов записи, но при регистрации SPN «вручную» это происходит не всегда;

- <port> – порт. Необязательная часть позволяющая задать несколько SPN с одинаковым именем сервиса. С портами TCP явно никак не связана, хотя может совпадать с номерами TCP портов, которые используют сервисы. Например, если имя сервиса «http», но порты 80 и 8080 используют разные экземпляры web серверов, то для каждого из них можно задать свой SPN используя номера портов: http/www.abcd.com:80 и http/www.abcd.com:8080.

3.6.4.3 Операции с SPN

Операции с SPN:

1) регистрация SPN.

Все операции с SPN необходимо выполнять на контроллере домена в командной строке, запущенной с правами администратора.

Регистрация SPN осуществляется командой «setspn» с ключем «-s». Формат вызова:

```
setspn -s <SPN> <account>
```

В приведенном формате вызова:

- <SPN> – SPN в описанном выше формате;

- <account> – имя УЗ домена, с которым связывается SPN и от имени которого сервис будет участвовать в аутентификации.

При задании имени УЗ домена она будет интерпретировать <account> как имя компьютера, если такой компьютер существует, и как имя пользователя в противном случае. Однако, тип УЗ можно задать, явно указав при вызове «setspn» модификаторы: «-C», если используется УЗ компьютера, и «-U», если используется УЗ пользователя.

Пример:

```
setspn -s ils/ad101-srv.ad101.test da1
```

Примечание. Зарегистрировать SPN можно также командой «setspn -a», но она не выполняет проверки существования записи и не рекомендуется к использованию. В поздних версиях ОС Windows вызов команды «setspn -a» автоматически заменяется на вызов команды «setspn -s».

2) удаление (отмена регистрации) SPN.

Удаление SPN осуществляется командой «setspn» с ключем «-d». Формат вызова:

```
setspn –d <SPN> <account>
```

В приведенном формате вызова:

- <SPN> – SPN в описанном выше формате;
- <account> –имя УЗ домена, с которым связан SPN.

Пример:

```
setspn -d ils/ad97-srv.ad97.test da1
```

3) удаление всех SPN связанных с УЗ.

Удаление всех SPN связанных с УЗ осуществляется командой «setspn» с ключем «-R». Формат вызова:

```
setspn -R <user-account>
```

В приведенном формате вызова – <account> – имя УЗ домена;

4) отображение списка SPN записей.

Отображение списка SPN осуществляется командой «setspn» с ключем «-L». Формат вызова:

setspn -L <user-account>

или

setspn -L <host>

В приведенном формате вызова:

- <user-account> – имя УЗ пользователя домена;
- <host> –имя компьютера, который указан в SPN.

Примеры:

```
setspn -L da1
setspn -L ad97-cli
setspn -L ad97-cli.ad97.test
```

5) проверка наличия SPN записи.

Проверка наличия SPN записи осуществляется командой «setspn» с ключом «-Q». Пример вызова:

setspn -Q ils/ad97-srv.ad97.test

6) поиск дублирующихся записей SPN.

Поиск дублирующихся записей SPN осуществляется командой «setspn» с ключом «-X». Пример вызова:

setspn -X

После регистрации SPN необходимо указать его на сервер приложений ПМ ИЛП в файле «AplTransport.ini» параметром [LocalServer] SPN (см. 3.6.1).

3.6.4.4 Операции с кэшем билетов в текущей сессии

Операции с кэшем билетов выполняются командой «klist».

Просмотреть список билетов в текущем кэше можно, вызвав «klist» без параметров или указав параметр «tickets»:

```
klist
klist tickets
```

Просмотреть список билетов в текущем кэше для конкретного хоста можно, вызвав «klist» с параметром «get» и указанием полного имени хоста, указанного в SPN:

```
klist get host/ad97-srv.ad97.test@AD97.TEST
```

Просмотреть начальный TGT (полученный при входе пользователя на компьютер) можно, вызвав «klist» с параметром «tgt»:

```
klist tgt
```

Очистить текущий кэш билетов можно, вызвав «klist» с параметром «purge»:

```
klist purge
```

3.6.5 Алгоритм аутентификация с использованием API Kerberos

Порядок действий при использовании протокола Kerberos следующий:

1) предварительная настройка (перед запуском ПМ ИЛП): в AD/ALD выбирается пользователь, под которым должен работать сервер приложений. Вызовом специальной утилиты (из ОС) для этого пользователя регистрируется SPN (Service Principal Name), как в ОС Windows, так и в ОС Astra Linux. Дополнительно в ОС Astra Linux другой утилитой создаётся ключевой файл «KeyTab». Этот SPN и путь к «KeyTab» прописываются в файле настроек ПМ ИЛП «AplTransport.ini»;

2) запускается сервер приложений. Он должен запускаться строго под УЗ пользователя, на которого зарегистрирован SPN;

3) запускается клиент ПМ ИЛП. Клиент открывает диалоговое окно «Установка соединения с БД», в котором можно установить флаг «Аутентификация через Kerberos». После выбора подключения клиент запрашивает с сервера приложений SPN. Дальше клиент обращается к API Kerberos, передаёт ему SPN и пустые строки в полях логин и пароль. Так как логин и пароль не заданы, Kerberos использует УЗ текущего доменного пользователя, под которым был произведен вход в ОС;

4) клиент ПМ ИЛП формирует входной буфер (на первом шаге буфер пустой). Дальше идёт итерационный процесс обмена буферами данных между клиентом, API Kerberos на стороне клиента, сервером приложений и API Kerberos на стороне сервера приложений;

5) клиент ПМ ИЛП передаёт в API Kerberos входной буфер (при первом шаге пустой, при последующих – буфер, полученный с сервера приложений) и ждёт выходной буфер с данными. В процессе подготовки выходного буфера Kerberos запрашивает контроллер домена, проверяет валидность SPN, логина/пароля или полномочий текущего пользователя ОС Windows или ОС Astra Linux. Перед выдачей буфер шифруется (расшифровать его можно только ключом пользователя, на которого зарегистрирован SPN), поэтому подменить что-либо в этом буфере нельзя. Так же Kerberos возвращает статус выполнения. Возможны следующие статусы выполнения:

- статус ошибки – в этом случае процедура аутентификации прерывается;
- статус необходимости дополнительных данных – в этом случае полученный буфер нужно передать серверу и ждать ответа;
- статус успешности аутентификации;

6) если буфер от Kerberos не пустой, клиент ПМ ИЛП передаёт полученный буфер серверу приложений. Сервер приложений отправляет его в API Kerberos, там буфер расшифровывается ключом текущего доменного пользователя, проверяется данными, полученными с контроллера домена; формируется новый буфер и статус выполнения, которые возвращаются серверу приложений;

7) если получен статус «ошибка», то сервер приложений возвращает клиенту ошибку;

8) если получен статус «нужны дополнительные данные» или «аутентификация успешна», то сервер отправляет клиенту полученный из Kerberos буфер, и выполняется п. 3). Если получен статус «аутентификация выполнена», то сервер так же запрашивает в API Kerberos имя аутентифицированного пользователя и запоминает его в контексте пользовательского сеанса.

Итерационный процесс прерывается на клиенте, когда после обработки буфера получен статус «аутентификация выполнена» и нет буфера для оправки серверу приложений. Поскольку клиент не знает, под кем он аутентифицировался, то после

аутентификации клиент запрашивает у сервера параметры аутентифицированного пользователя.

Поскольку при формировании буфера и на стороне клиента, и на стороне сервера идёт обращение к контроллеру домена, то такой метод аутентификации работает только в доменной среде. Поэтому при запуске клиента не под доменным пользователем флаг «Аутентификация через Kerberos» будет заблокирован.

3.6.6 Принципы взаимодействия с Secret Net Studio 8

3.6.6.1 Настройка Secret Net для взаимодействия с ПМ ИЛП

Использование системы Secret Net в минимальных настройках не влияет на работу ПМ ИЛП. В то же время, при использовании некоторых функций SecretNet может потребоваться дополнительная настройка.

1) контроль целостности.

При формировании модели защищаемых данных необходимо исключить из контроля файлы БД СХД (в случае использования БД СХД), файлы журналов сервера приложений, файлы журналов клиентских приложений и журналов информационной безопасности. По умолчанию файлы БД СХД располагаются в каталоге «\db» каталога установки ПМ ИЛП, файлы журналов располагаются в подкаталогах «\logs» и «\logs\safety»; при необходимости файлы БД СХД и журналы можно перенести в каталог, отличный от каталога установки ПМ ИЛП. Для переноса необходимо внести изменения в файл настроек параметров работы ПМ ИЛП «AplTransport.ini», а также вручную перенести необходимые файлы.

Сам файл настроек AplTransport.ini следует добавлять в модель защищаемых данных после выполнения настроек подключений;

2) персональный межсетевой экран.

ПМ ИЛП передает данные через сетевое соединение, поэтому при разработке политики ограничения сетевого доступа необходимо предусмотреть правила, разрешающие входящие TCP соединения на стороне сервера приложений и исходящие соединения на стороне клиентских модулей. По умолчанию ПМ ИЛП использует следующие порты TCP:

- сервер приложений для PostgreSQL: 7239;

- сервер приложений СХД: 7240;
- сервер приложений для Oracle: 7241.

В случае необходимости можно назначить другие порты для работы серверов приложений.

При использовании сервера приложений для работы с СУБД PostgreSQL или сервера приложений для работы с СУБД Oracle также необходимо разрешить доступ к СУБД PostgreSQL и СУБД Oracle со стороны серверов приложений и утилит администрирования БД ПМ ИЛП. По умолчанию СУБД PostgreSQL использует порт TCP 5432, СУБД Oracle использует TCP порт 1521; за более точными сведениями о настройках СУБД следует обращаться к администраторам СУБД;

3) полномочное управление доступом и уровнями конфиденциальности.

Перед работой сервера приложений в конфиденциальных сессиях необходимо предварительно изменить уровень конфиденциальности каталогов, содержащих файлы с БД СХД, со всеми входящими файлами (в случае использования БД СХД), каталогов с журналами клиентских приложений и каталогов с журналами информационной безопасности. Также необходимо включить автоматическое присваивание уровня конфиденциальности вновь создаваемым файлам и каталогам.

При использовании СУБД PostgreSQL в защищенном исполнении (например, от компании «PostgresPro») необходимо настроить уровни конфиденциальности в соответствии с руководством конкретной сборки СУБД PostgreSQL.

3.6.6.2 Рекомендации по повышению безопасности системы

Рекомендации по повышению безопасности системы:

1) ограничение доступа к серверу приложений ПМ ИЛП и защита передаваемых данных от прослушивания и подмены.

В сервере приложений ПМ ИЛП есть функция «белый список», позволяющая разрешить доступ к серверу приложений только для определенных компьютеров. Однако она не позволяет управлять доступом на уровне отдельных пользователей и групп пользователей доменной среды. Кроме того, ПМ ИЛП передает данные между клиентом и сервером в открытом, не защищенном виде. Для ограничения доступа на уровне пользователей и защиты передаваемых данных рекомендуем сделать следующие настройки:

- в разделе настроек «Авторизация сетевых соединений» включить защиту соединений. Параметры обработки сетевых пакетов установить в зависимости от степени важности передаваемых данных: при необходимости защиты только от подмены оставить включенной опцию «Подпись пакета целиком», при необходимости защиты данных от прослушивания включить опцию «Шифрование с контролем целостности»;

- в разделе настроек «Персональный межсетевой экран» в группе настроек «Правила, регламентирующие доступ к сетевым сервисам данного компьютера» создать два правила. Первое правило – запрет на доступ к портам серверов приложений (по умолчанию это TCP порты 7239, 7240 и 7241) для группы «everyone». Второе правило – разрешение на доступ к этим портам для группы «authenticated» (в случае, если надо только ограничить доступ с компьютеров, не входящих в домен), или разрешение на доступ к этим портам для конкретной группы доменных пользователей. Разрешающее правило необходимо расположить в списке выше запрещающего, чтобы его приоритет был выше. Эти правила запретят доступ к серверу приложений для ПМ ИЛП, запущенному от имени пользователей, не входящих в домен (в первом случае) или не входящих в конкретную группу доменных пользователей (во втором случае).

При использовании СУБД PostgreSQL или СУБД Oracle также рекомендуется разрешить доступ к серверу СУБД к портам СУБД только для тех компьютеров, на которых будет работать серверная часть ПМ ИЛП. По умолчанию СУБД PostgreSQL использует TCP порт 5432, СУБД Oracle использует TCP порт 1521; за более точными сведениями о серверах СУБД и их настройках следует обращаться к администраторам СУБД;

2) ограничение доступа при использовании конфиденциальных сессий.

При работе ПМ ИЛП в конфиденциальных сессиях SecretNet никак не ограничивает возможность сетевого соединения клиента и сервера, запущенных с разными настройками конфиденциальности, из-за чего возникает риск утечки конфиденциальной информации. При необходимости работы ПМ ИЛП в конфиденциальных сессиях рекомендуем задать правила межсетевого экрана, разрешающие доступ к серверу ПМ ИЛП только для текущего компьютера;

3) ограничения запуска сервера приложений при использовании аутентификации Kerberos.

При аутентификации через API Kerberos процесс сервера приложений должен быть запущен под той же УЗ, для которой зарегистрирован SPN; при запуске сервера приложений под другой УЗ аутентификация завершится ошибкой. Рекомендуется назначить для серверов приложений дискреционный доступ, разрешающий запуск только для того пользователя, для которого зарегистрирован SPN. Так же можно при настройке разрешающего правила межсетевого экрана указать в поле «Допустимые субъекты безопасности» того доменного пользователя, для которого был зарегистрирован SPN.

3.7 Настройка ограничения неуспешных попыток аутентификации

3.7.1 Общие сведения

Основным режимом аутентификации пользователей в ПМ ИЛП является аутентификация в домене. Поэтому настройка сложности пароля, ограничение количества неуспешных попыток входа и прочие политики безопасности настраиваются с помощью средств управления доменом.

3.7.2 Настройка ограничения неуспешных попыток аутентификации и политики сложности пароля в Windows Active Directory

Настройка выполняется на контроллере домена. Заданные параметры действуют как на вход в ОС, так и на вход в ПМ ИЛП с помощью API Kerberos.

Для настройки:

1) чтобы настроить политику паролей, откройте консоль управления доменными политиками («Group Policy Management console»). Для этого выполните команду gpmc.msc или в меню «Пуск» выберите пункт «Средства администрирования Windows / Управление групповой политикой»;

2) разверните ваш домен и найдите политику «Default Domain Policy», нажмите на неё правой кнопкой мыши и выберите пункт меню «Edit». В отдельном окне откроется редактор управления групповыми политиками;

3) политики паролей находятся в следующем разделе редактора «GPO»: «Конфигурация компьютера» -> «Конфигурация Windows» -> «Параметры безопасности» -> «Политики учетных записей» -> «Политика паролей». В данном разделе можно

установить минимальный и максимальный срок действия пароля, минимальную длину пароля, степень сложности пароля;

4) политики блокировки УЗ находятся в следующем разделе редактора «GPO»: «Конфигурация компьютера» -> «Конфигурация Windows» -> «Параметры безопасности» -> «Политики учетных записей» -> «Политика блокировки учетной записи». В данном разделе можно установить количество неуспешных входов до блокировки, время блокировки и параметры сброса счетчика неудачных попыток входа;

5) чтобы отредактировать настройки параметра политики, дважды нажмите на нее. Чтобы включить политику, включите переключатель «Определить следующий параметр политики» и укажите необходимую настройку.

После изменения политики в редакторе политик до ее применения на контроллере домена может пройти некоторое время.

Чтобы принудительно сбросить блокировку заблокированного пользователя, откройте консоль управления доменными пользователями. Для этого выполните команду «dsa.msc» или в меню «Пуск» выберите пункт «Средства администрирования Windows / Пользователи и компьютеры Active Directory». В дереве найдите группу «Users», в ней найдите УЗ пользователя и откройте ее двойным нажатием мыши. Перейдите на вкладку «Учетная запись», установите переключатель «Разблокируйте учетную запись. Учетная запись на этом контроллере домена заблокирована». Нажмите «Применить» или закройте диалог кнопкой «Ok». Разблокировка занимает некоторое время.

3.7.3 Настройка ограничения неуспешных попыток аутентификации и политики сложности пароля в Windows без домена

Для настройки:

1) чтобы настроить политику паролей, откройте консоль управления локальными политиками. Для этого выполните команду «gpedit.msc» или в меню «Пуск» выберите пункт «Средства администрирования Windows / Локальная политика безопасности»;

2) политики паролей находятся в следующем разделе: «Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Политики учетных записей -> Политика паролей». В данном разделе можно установить минимальный и максимальный срок действия пароля, минимальную длину пароля, степень сложности пароля;

3) политики блокировки УЗ находятся в следующем: «Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Политики учетных записей -> Политика блокировки учетной записи». В данном разделе можно установить количество неуспешных входов до блокировки, время блокировки и параметры сброса счетчика неудачных попыток входа;

4) чтобы отредактировать настройки параметра политики, дважды щелкните по ней. Чтобы включить политику, включите переключатель «Определить следующий параметр политики» и укажите необходимую настройку.

Чтобы принудительно сбросить блокировку заблокированного пользователя, откройте консоль управления локальным компьютером. Для этого выполните команду «compmgmt.msc» или в меню «Пуск» выберите пункт «Средства администрирования Windows / Управление компьютером». В дереве найдите группу «Локальные пользователи/ Пользователи», в ней найдите УЗ пользователя и откройте ее двойным нажатием мыши. Перейдите на вкладку «Общие» и снимите переключатель «Заблокировать учетную запись». Нажмите «Применить» или закройте диалог кнопкой «Ok».

3.7.4 Настройка ограничения неуспешных попыток аутентификации и политики сложности пароля в Astra Linux Domain

Настройка выполняется на контроллере домена. Для выполнения настройки необходимо войти в ОС с максимальным уровнем целостности под УЗ пользователя, имеющего администраторские права (то есть пользователь должен входить в группу «astra-admin»).

Для настройки:

1) запустите утилиту «Доменная политика безопасности». Для этого в меню «Пуск» выберите «Настройки / Доменная политика безопасности», или если отображается сокращенное меню «Настройки», то откройте «Настройки / Панель управления», в панели управления перейдите в раздел «Сеть» и в нем выберите «Доменная политика безопасности»;

2) введите логин и пароль доменной УЗ, имеющей привилегии «Администратор домена» и привилегии «Использование средств администрирования домена»;

3) политики блокировки УЗ и политики паролей находятся в разделе «Политики паролей / default». В данном разделе можно установить количество неуспешных входов до

блокировки, время блокировки, параметры сброса счетчика неудачных попыток входа, минимальный и максимальный срок действия пароля, минимальную длину пароля, степень сложности пароля;

4) при необходимости в разделе «Политики паролей» можно создать новую политику паролей и применить ее к отдельным пользователям или группам пользователей.

Чтобы принудительно сбросить блокировку заблокированного пользователя, запустите утилиту «Доменная политика безопасности», введите логин и пароль доменной административной УЗ, выберите в разделе «Пользователи» УЗ пользователя и на вкладке «Политика» нажмите кнопку «Сброс» в строке счетчика неуспешных попыток входа.

3.7.5 Настройка ограничения неуспешных попыток аутентификации в Astra Linux SE без домена

Для выполнения настройки необходимо войти в ОС с максимальным уровнем целостности под УЗ пользователя, имеющего администраторские права (то есть пользователь должен входить в группу «astra-admin»).

Для настройки:

1) запустите утилиту «Управления политиками безопасности». Для этого в меню «Пуск» выберите «Настройки / Политика безопасности». Если меню «Настройки» сокращенное, то откройте «Настройки / Панель управления», в панели управления перейдите в раздел «Безопасность» и в этом разделе выберите «Политика безопасности»;

2) политики блокировки УЗ находятся в разделе «Политики учетной записи / Блокировка». При настройке следует учитывать состояние переключателя «Индивидуальные настройки»; если он установлен, для каждого пользователя действуют персональные настройки блокировки. Задать их можно в разделе «Пользователи» в настройках пользователя на вкладке «Блокировка»;

3) политики паролей находятся в разделе «Политики учетной записи / Политика паролей».

Чтобы принудительно сбросить блокировку заблокированного пользователя, запустите утилиту «Управления политиками безопасности», выберите в разделе «Пользователи» УЗ пользователя и на вкладке «Блокировка» нажмите кнопку «Сброс» в строке счетчика неуспешных попыток входа.

3.8 Настройка ПМ ИЛП для обновления механизмов аутентификации путем использования сторонней библиотеки.

В ПМ ИЛП заложена возможность аутентификации через внешний модуль, разработанный эксплуатирующей организацией. Модуль должен быть выполнен в виде динамической библиотеки («*.dll» для ОС Windows или «lib*.so» для ОС Astra Linux). Динамическая библиотека должна экспортировать функции, указанные в заголовочном файле «ExtAuth_global.h», входящем в состав примера такой библиотеки «ExternalAuthenticationSample», поставляющимся вместе с исходными текстами ПМ ИЛП.

Перед использованием библиотеки внешней аутентификации необходимо подготовить обновленный файл с контрольными суммами файлов ПМ ИЛП. Для этого надо выполнить следующее:

- установить используемый дистрибутив ПМ ИЛП в максимальной конфигурации, то есть выбрать для установки все компоненты ПМ ИЛП;
- поместить в папку с установленным ПМ ИЛП файл библиотеки внешней аутентификации, например «ExternalAuthentication.dll» или «libExternalAuthentication.so»;
- добавить в файл «list_controlled_files.txt» в отдельную строчку имя файла библиотеки внешней аутентификации; в случае использования ОС Astra Linux имя файла можно указать в формате Windows, например, «ExternalAuthentication.dll»;
- в случае использования ОС Windows открыть консоль cmd, перейти в папку с ПМ ИЛП и запустить команду:

«CalcFilesHash.exe -d 512 -o hashes_of_files.4.0.XXXX.xml -t -p list_controlled_files.txt»,

где «hashes_of_files.4.0.XXXX.xml» – это имя файла с эталонными хешами из каталога ПМ ИЛП;

- в случае использования ОС Astra Linux открыть терминал fly-term, перейти в папку с ПМ ИЛП и запустить команду:

«./CalcFilesHash -d 512 -o hashes_of_files.4.0.XXXX.xml -t -p list_controlled_files.txt»,

- где «hashes_of_files.4.0.XXXX.xml»– это имя файла с эталонными хешами из каталога ПМ ИЛП;
- после завершения программы CalcFilesHash необходимо проконтролировать наличие в файле «hashes_of_files.4.0.XXXX.xml» хеш-суммы файла библиотеки;

- полученный файл «hashes_of_files.4.0.XXXX.xml» необходимо сохранить для использования с текущим дистрибутивом ПМ ИЛП и текущей версией библиотеки внешней аутентификации. При каждом изменении версии используемой библиотеки внешней аутентификации или при смене версии дистрибутива ПМ ИЛП или необходимо повторно выполнить пересчет контрольных сумм.

Настройка ПМ ИЛП для обновления механизма аутентификации выполняется, как на стороне сервера приложений, так и на стороне клиента. Необходимо выполнить следующее:

1) переписать в каталог установки ПМ ИЛП файл библиотеки внешней аутентификации, например, «ExternalAuthentication.dll» для ОС Windows, или «libExternalAuthentication.so» для ОС AstraLinux;

2) добавить в файл «AplTransport.ini» параметр [Safety] ExternalAuth=<имя внешней библиотеки> без префикса и расширения. Пример:

```
[Safety]
ExternalAuth=ExternalAuthentication
```

На стороне сервера приложений необходимо заменить файл контрольных сумм «hashes_of_files.4.0.XXXX.xml» файлом, полученным при пересчете контрольных сумм.

Без обновления файла контрольных сумм сервер приложений выдаст ошибку проверки целостности (рисунок 21).

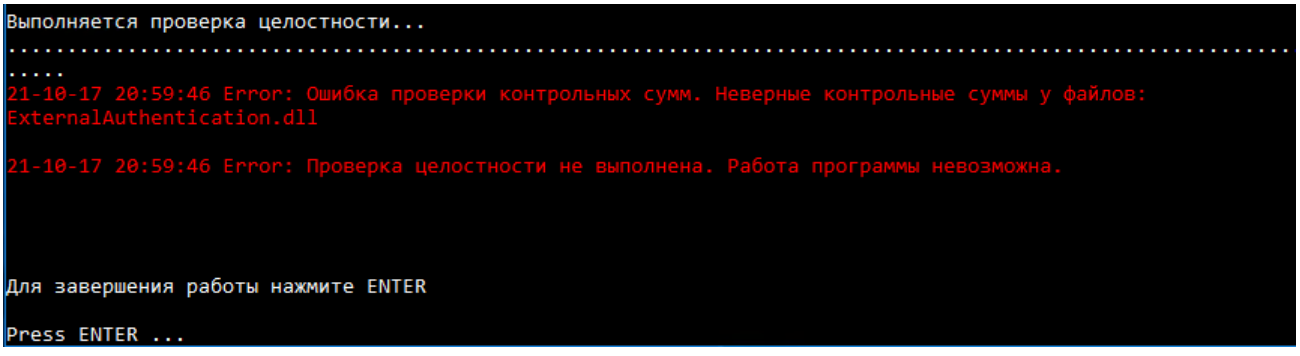

Рисунок 21 – Пример сообщения об ошибке при отсутствии хеш-суммы.

После настройки ПМ ИЛП и замены файла контрольных сумм сервер приложений при запуске загружает библиотеку внешней аутентификации и выводит в терминальное окно ее имя и путь к файлу библиотеки (рисунок 22).

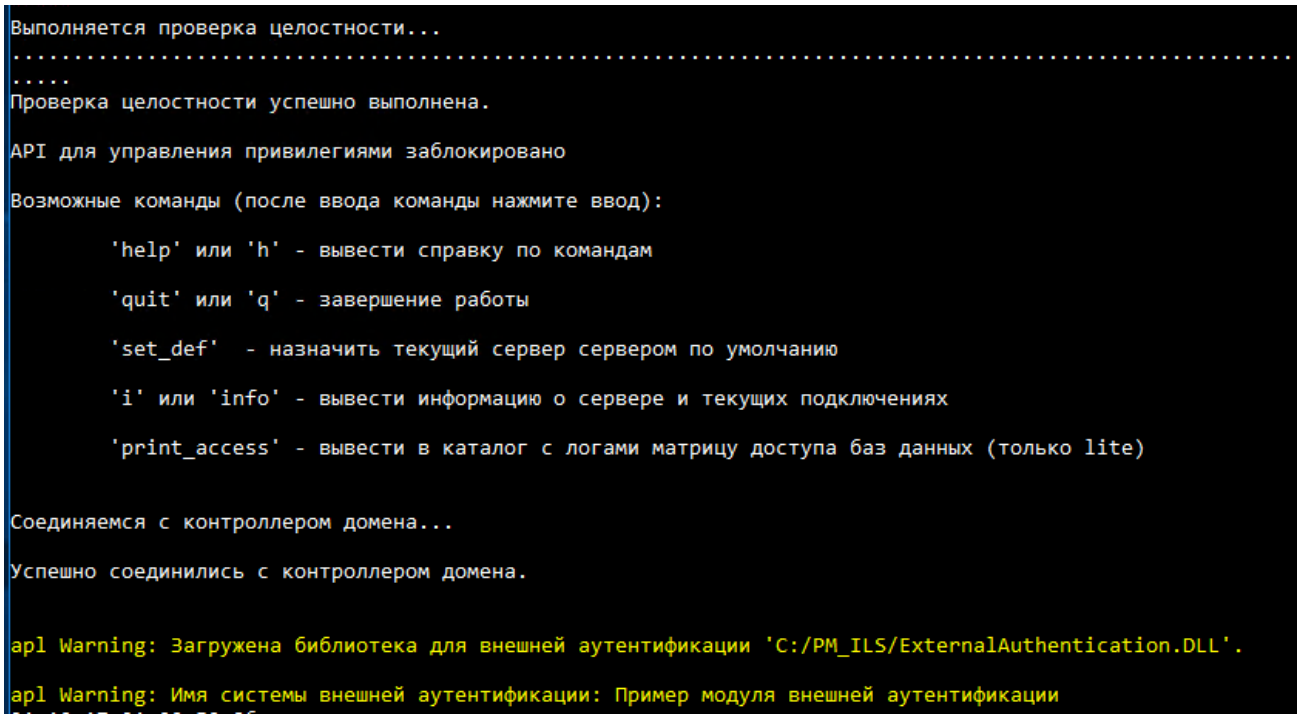

Рисунок 22 – Пример сообщений при запуске сервера с библиотекой внешней аутентификации

Использование внешней библиотеки аутентификации влияет на безопасность работы ПМ ИЛП, поэтому эти сообщения оформлены как предупреждения.

Библиотека внешней аутентификации скрывает стандартное окно «Установка соединения» ПМ ИЛП.Определение подключения к серверу приложений, идентификация и аутентификация пользователя производится средствами самой библиотеки как на стороне клиента ПМ ИЛРП, так и на стороне сервера приложений.

В случае, если настройки были проведены некорректно, аутентификация прерывается. На рисунке 23 приведен пример сообщение об ошибке, появляющегося при запуске ПМ ИЛП, если библиотека аутентификации была задана на клиенте, но не задана на сервере.

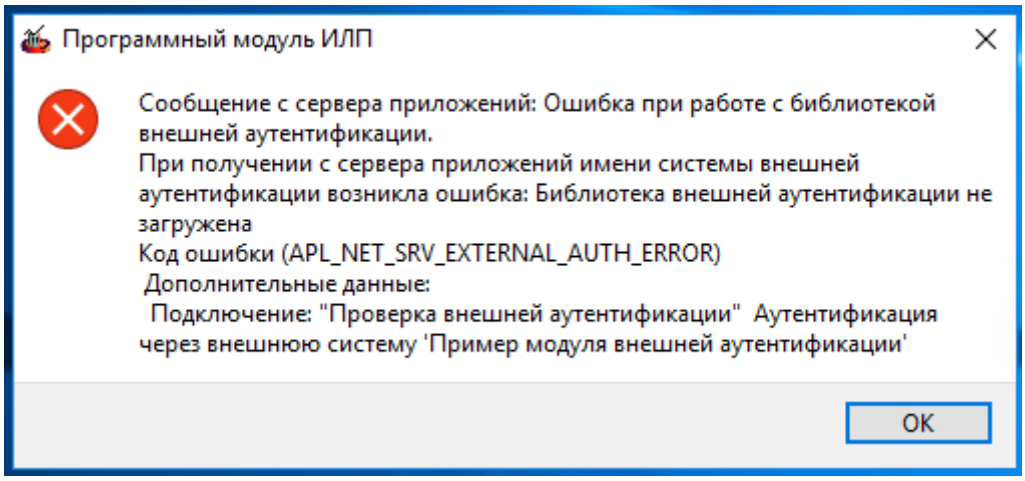

Рисунок 23 – Пример сообщения об ошибке, если библиотека аутентификации задана на клиенте, но не задана на сервере

На рисунке 24 приведен пример сообщения, появляющегося при запуске ПМ ИЛП, если на сервере приложений библиотека внешней аутентификации задана, а на клиенте не задана.

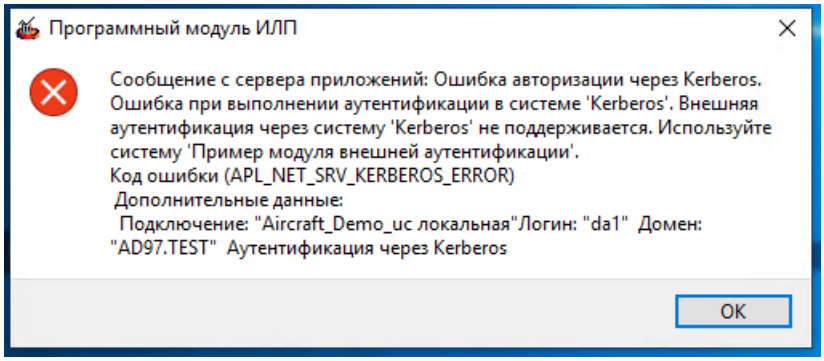

Рисунок 24 – Пример сообщения об ошибке, если на сервере приложений библиотека внешней аутентификации задана, а на клиенте не задана, при аутентификации через Kerberos

4 ПРОВЕРКА ПРОГРАММЫ И СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

4.1 Способы проверки

После настройки программы следует убедиться в возможности подключения к БД. Для этого выполняют следующие проверки на машине клиента ПМ ИЛП:

- для СХД:
  1) запустить «Администратор БД для СХД»;
  2) создать БД;
  3) запустить ПМ ИЛП;
  4) добавить БД в список подключений;
  5) установить соединение с БД;
- для БД PostgreSQL:
  1) запустить «Администратор БД для PostgreSQL»;
  2) создать запись в списке БД;
  3) заблокировать БД, сгенерировать БД, разблокировать БД;
  4) запустить ПМ ИЛП;
  5) добавить БД в список подключений;
  6) установить соединение с БД;
- для БД Oracle:
  1) запустить «Администратор БД для Oracle»;
  2) создать запись в списке БД;
  3) заблокировать БД, сгенерировать БД, разблокировать БД;
  4) запустить ПМ ИЛП;
  5) добавить БД в список подключений;
  6) установить соединение с БД.

Примеры некоторых ошибок, которые могут встретиться при проверке:

1) при установке соединения с БД запускается окно сервера приложений СХД, в котором выводится сообщение об ошибке (рисунок 25). Соединение с БД не устанавливается (рисунок 26).

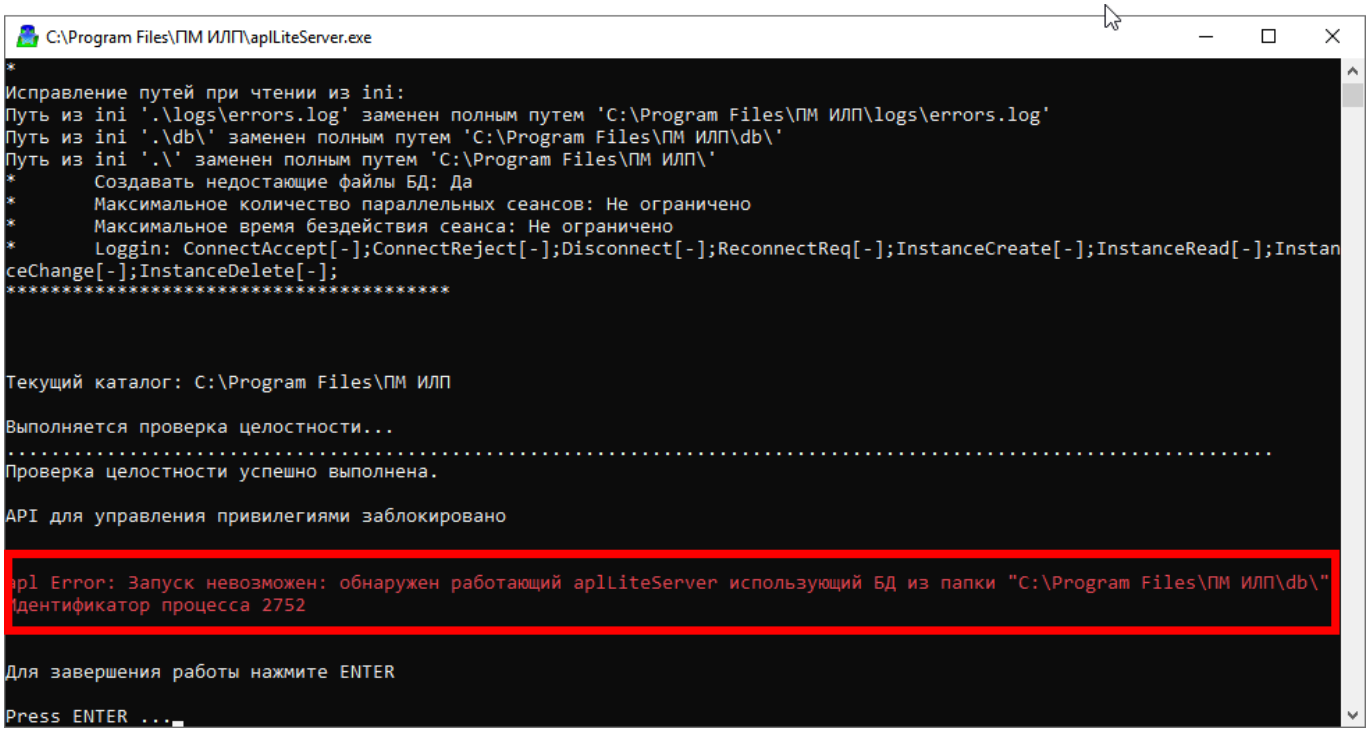

Рисунок 25 – Окно сервера приложений с сообщением об ошибке соединения с БД

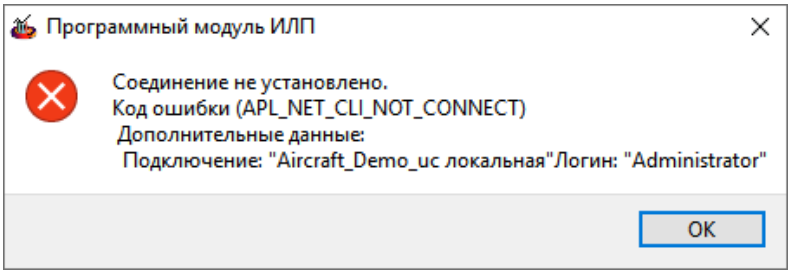

Рисунок 26 – Сообщение оператору об ошибке соединения

Причиной ошибки является неправильно указанный порт в настройках соединения с БД на локальном компьютере (см. рисунок 7). Указанный порт не используется ни одним из серверов приложений, поэтому система пытается запустить сервер приложений СХД по этому порту. Если же сервер приложений СХД уже работает, но использует другой порт, возникает ошибка.

Для устранения ошибки следует указать в настройках соединения с БД корректный номер порта, который использует соответствующий типу БД сервер приложений;

2) при подключении к БД появляется сообщение о том, что имя БД в параметрах подключения указано неверно (рисунок 27). Для устранения ошибки указать в параметрах подключения имя существующей БД (см. рисунок 7);

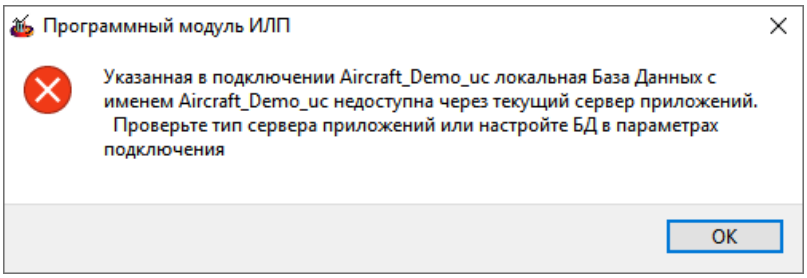

Рисунок 27 – Ошибка при неправильно указанном имени БД

3) при подключении к БД появляется сообщение о том, что список БД отсутствует (рисунок 28). Причина заключается в том, что в настройках подключения указан порт, по которому работает сервер приложения, но для него не создано ни одной БД. Для устранения ошибки необходимо указать порт, по которому работает сервер приложений, соответствующей данной БД;

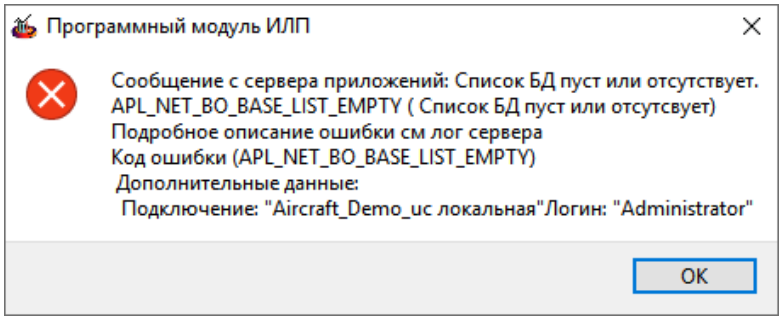

Рисунок 28 – Сообщение об ошибке, если для используемого сервера приложений не создано ни одной БД

4) при подключении к БД появляется сообщение о том, что данная БД недоступна через указанный сервер приложений (рисунок 29). Ситуация аналогична, приведенной на рисунке 25. Отличие в том, что по указанному порту уже запущен сервер приложений, но его тип не соответствует указанной БД. Для устранения ошибки следует указать в настройках соединения с БД корректный номер порта, который использует соответствующий типу БД сервер приложений;

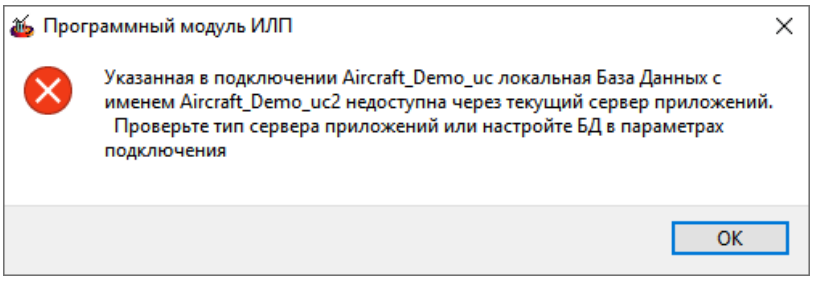

Рисунок 29 – Сообщение об ошибке, если БД недоступна через указанный сервер приложений

5) при подключении к БД появляется сообщение о том, что сервер не ответил на запрос (рисунок 30). Ошибка возникает при подключении к БД на удаленном компьютере, если по указанному порту не работает ни один сервер приложения. Для устранения ошибки запустить сервер приложений, соответствующий типу БД;

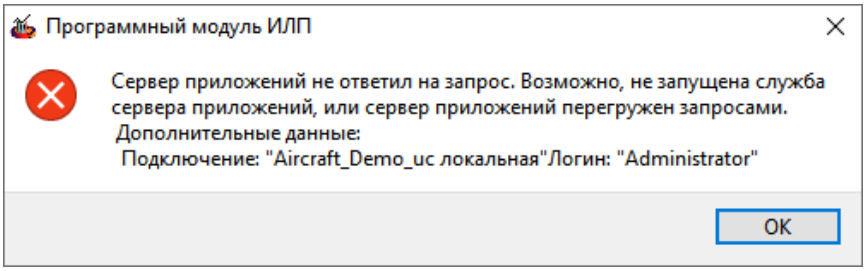

Рисунок 30 – Сообщение об ошибке, если сервер не ответил на запрос

6) при попытке подключения к БД Oracle или PostgreSQL появляется сообщение о том, что БД заблокирована (рисунок 31). Для устранения ошибки необходимо разблокировать БД в утилите «Администратор БД» для Oracle или PostgreSQL;

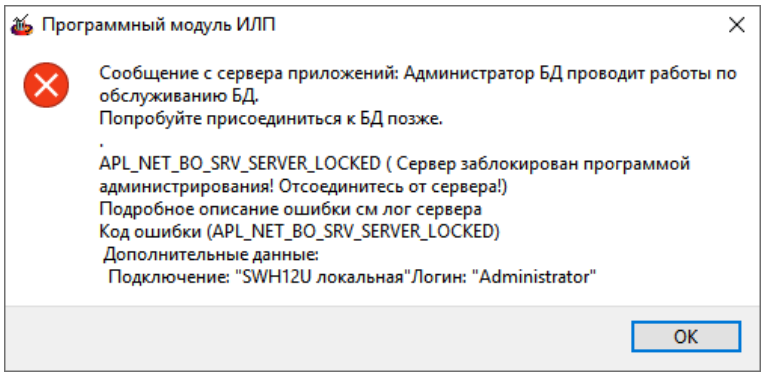

Рисунок 31 – Сообщение о том, что БД заблокирована

7) при попытке создать БД в «Администраторе БД для PostgreSQL» появляется сообщение об ошибке (рисунок 32 и рисунок 33).

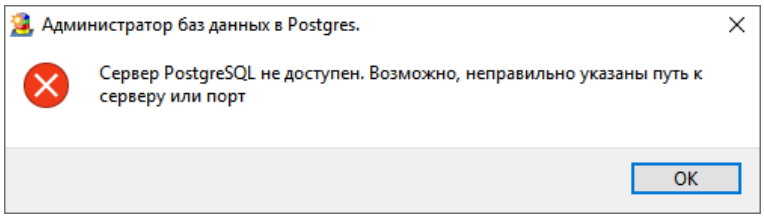

Рисунок 32 – Сообщение об ошибке при попытке создать БД PostgreSQL

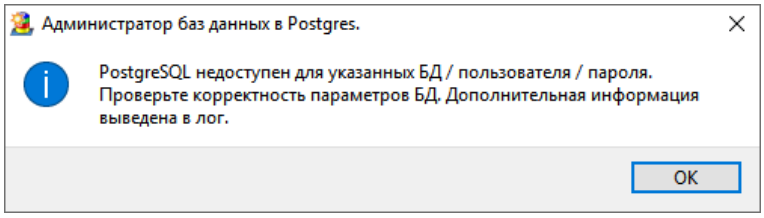

Рисунок 33 – Сообщение об ошибке при попытке создать БД PostgreSQL

По указанному в записи БД адресу компьютера и порту не работает сервер PostgreSQL (рисунок 34).

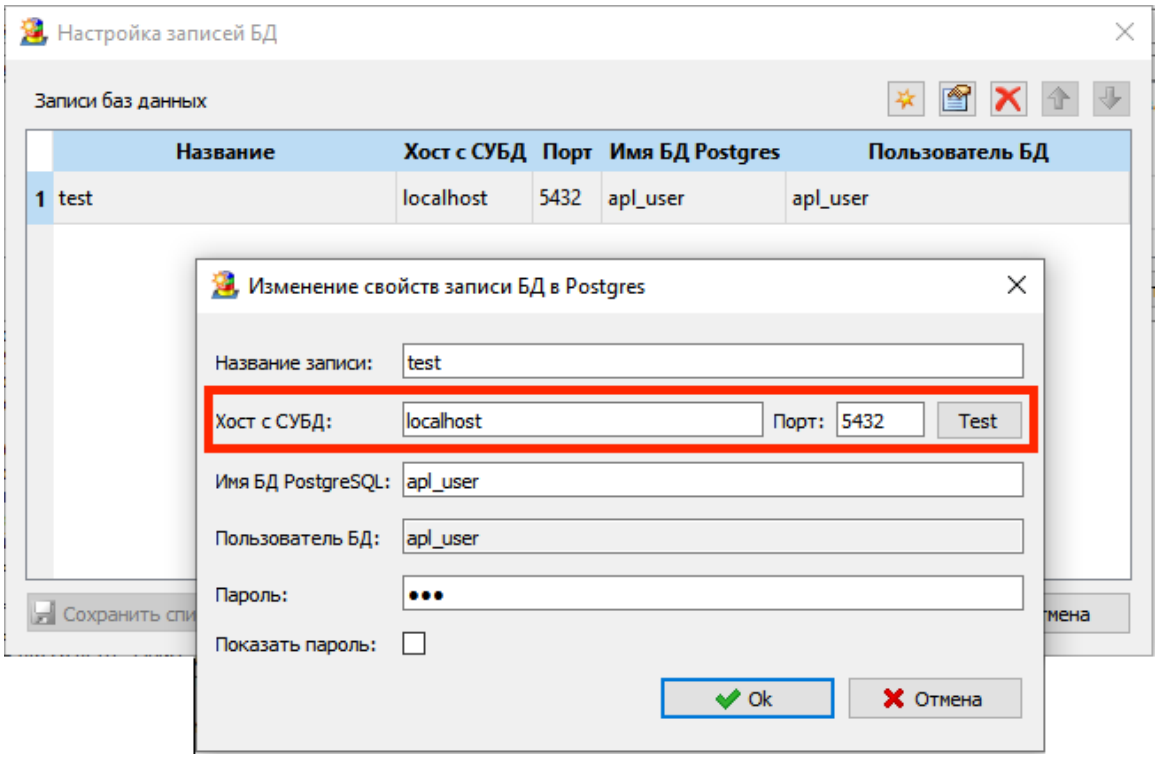

Рисунок 34 – Настройка параметров БД для PostgreSQL

Проверить, установлена ли СУБД PostgreSQL на указанном компьютере, запущен ли сервер PostgreSQL, правильно ли для него указан порт;

8) если при запуске «Администратора БД для Oracle» появляется сообщение об ошибке, приведенное на рисунке 35, это означает, что на компьютере не установлен Oracle Client. Если необходимо, установить Oracle Client на машине клиента ПМ ИЛП;

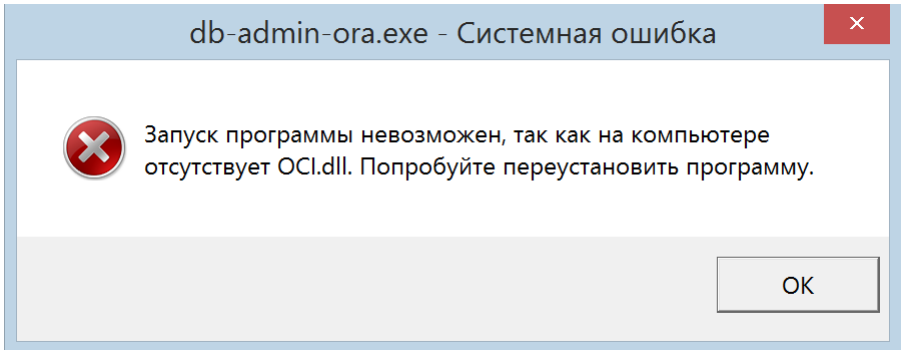

Рисунок 35 – Ошибка при запуске Администратора БД для Oracle в случае, если на компьютере не установлен Oracle Client

9) при попытке заблокировать БД в «Администраторе БД» для Oracle появляется сообщение о том, что Oracle недоступен для указанного Alias (рисунок 36).

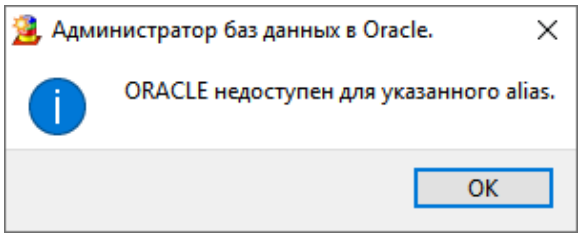

Рисунок 36 – Пример сообщения «Oracle недоступен для указанного Alias»

Причиной ошибки может быть неправильно указанный Alias в свойствах записи БД (рисунок 37).

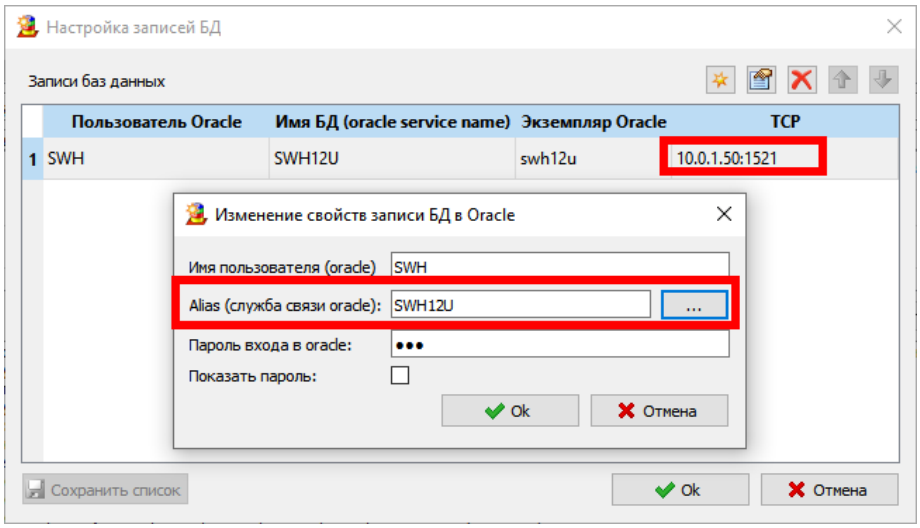

Рисунок 37 – Настройка Alias для записи БД Oracle

Если Alias указан правильно, необходимо проверить, запущена ли по адресу, указанному для БД в столбце «TCP» (см. рисунок 37), служба Oracle Listener, а также служба «OracleService<имя_алиас>» (рисунок 38). При необходимости создать и настроить Listener на машине Oracle Serve и Alias на машине Oracle Client, и запустить их.

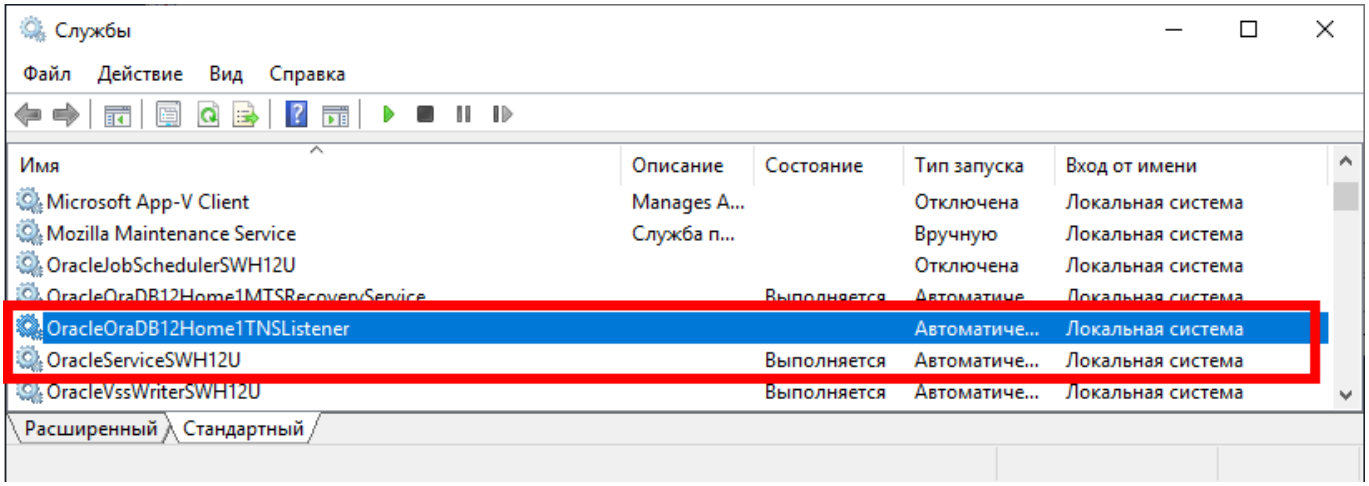

Рисунок 38 – Службы Oracle для Listener и Alias

При попытке подключиться к БД Oracle в окне «Установка соединения с БД» в случае, когда не работает служба Listener или Alias, также появляется сообщение о том, что Oracle недоступен (рисунок 39). Запустить соответствующие службы.

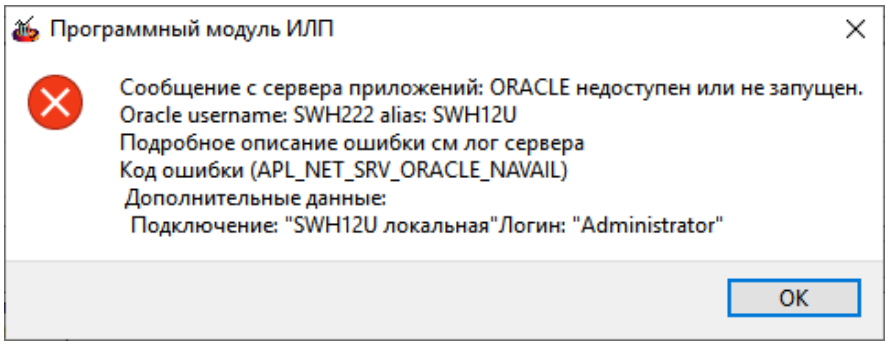

Рисунок 39 – Сообщение о недоступности Oracle при попытке подключиться к БД

При работе с БД Oracle обрабатываются следующие коды ошибок:

- OCI_SUCCESS – успешное выполнение;
- OCI_SUCCWSS_WITH_INFO – успешное выполнение с замечаниями;
- OCI_NEED_DATA – выполнение прервано из-за недостатка входных данных;
- OCI_NO_DATA – выборка завершилась, так как закончились данные;
- OCI_ERROR – ошибка выполнения. Описание конкретной ошибки берется из Oracle дополнительной функцией;
- OCI_INVALID_HANDLE – недопустимый контекст службы, соединения или дескриптор оператора.

При работе с БД PostgreSQL возможны следующие коды ошибок (некоторые из них, например, для асинхронного выполнения, в ПМ ИЛП не встречаются):

- PGRES_COMMAND_OR – успешное завершение команды, не возвращающей никаких данных;
- PGRES_TUPOES_OR – успешное завершение команды, возвращающей данные (такой, как SELECT или SHOW);
- PGRES_COPY_OUT – начат перенос данных Copy Out (с сервера);
- PGRES_COPY_IN – начат перенос данных Copy In (на сервер);
- PGRES_SINGLE_TUPLE – структура PGresult содержит только одну результирующую строку, возвращенную текущей командой. Этот статус имеет место только тогда, когда для данного запроса был выбран режим построчного вывода;
- PGRES_EMPTY_QUERY – строка, отправленная серверу, была пустой;
- PGRES_BAD_RESPONSE –ответ сервера не был распознан;
- PGRES_NONFATAL_ERROR – произошла не фатальная ошибка (уведомление или предупреждение);
- PGRES_FATAL_ERROR – критическая ошибка.

4.2 Применяемые технические и организационные меры, используемые для обнаружения модификации ПО или любого расхождения между оригиналом и версией, полученной пользователем, в объеме, достаточном для правильной настройки и безопасного применения программы

Организационные меры, используемые для обнаружения модификации ПО или любого расхождения между оригиналом и версией, полученной пользователем, должны быть определены организацией-правообладателем ПО в своих организационно-распорядительных документах и должны в себя включать:

- средства маркировки дистрибутива (при его передаче пользователю на носителе);
- средства контрольного суммирования поставляемого дистрибутива программы;
- средства аутентификации (верификации) контрольных сумм при передаче дистрибутива и контрольных сумм по каналам связи;
- определение и утверждение конфигурация эталонных параметров ПО (оригинал);
- определение порядка установки, настройки и эксплуатации ПО в соответствии с эксплуатационной документацией на ПМ ИЛП, определены роли и права этих ролей на выполнение установки, настройки и эксплуатации ПО;
- определен порядок действий при обнаружении расхождений между оригиналом и версией, полученной пользователем, и их устранении;
- определен порядок аудита версий ПО, установленного у пользователей, на соответствие оригиналу.

Технические меры, используемые для обнаружения модификации ПО или любого расхождения между оригиналом и версией, полученной пользователем, включают:

- настройку прав разрешенных действий пользователей ПО;
- контроль и протоколирование действий пользователей;
- встроенные средства контроля целостности сервера приложений и клиента ПМ ИЛП, которые описан в 07623615.00427-09 13 01-2 Описание программы. Часть 2. Книга 1.

На этапе разработки ПО указанные меры реализуются путем выполнения следующих шагов:

- исследование существующих у разработчика процессов в границах области действия мер по разработке безопасного ПО, связанных с идентификацией инструментальных средств разработки, отладки и тестирования;

- выбор способов обнаружения модификации ПО или любого расхождения между оригиналом и версией, полученной пользователем, для программ (и их частей) которые распространяются на физических носителях;

- выбор способов обнаружения модификации ПО или любого расхождения между оригиналом и версией, полученной пользователем, для программ (и их частей) которые распространяются по каналам связи;

- разработка процедуры обнаружения модификации файлов программы (или отдельных ее частей, например, обновлений);

- назначение работников, ответственных за реализацию меры по разработке безопасного ПО (в части контроля несанкционированной модификации кода), ознакомление их с документацией, касающейся реализации меры по разработке безопасного ПО.

При передаче дистрибутива и обновлений на носителе основными мерами контроля модификаций являются:

- маркировка дистрибутивного комплекта отличительными знаками (защитными знаками);

- использование контрольных сумм для идентифицированного перечня файлов.

При передаче дистрибутива и обновлений по каналам связи помимо контрольных сумм должны также использоваться средства двухключевой криптографии (хэш-суммы с подписью доверенным сертификатом), обеспечивающие возможность проверить доверенность источника при проверке контрольной суммы (защита от подделки контрольной суммы. Проверка осуществляется путем проверки сертификатов, выдаваемых доверенным удостоверяющим центром. Инфраструктура открытых ключей является элементом среды функционирования и предоставляется заказчиком (разработчик формирует подпись с помощью собственного сертификата, который должен быть включен заказчиком в число доверенных для обеспечения контроля дистрибуции).

Независимо от способа передачи дистрибутива и обновлений к мерам контроля несанкционированных модификаций относятся:

- организационно-технические меры обеспечения доверенной загрузки рабочей среды на компьютерах пользователей;

- использование штатных средств дистрибуции (установочного комплекта), содержащих проверку целостности и контрольных сумм модулей дистрибутива и обновлений.

5 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Дополнительные возможности – отсутствуют.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

AD	–	Active Directory;
API	–	прикладной программный интерфейс (англ., Application programming interface);
ALD	–	Astra Linux Domain;
SPN	–	имя сервиса в домене (англ., Service Principal Name);
АЛП	–	анализ логистической поддержки;
БД	–	база данных;
ИЛП	–	интегрированная логистическая поддержка;
ОС	–	операционная система;
ПБ АЛП	–	программный блок анализа логистической поддержки;
ПБ АН	–	программный блок анализа надежности;
ПБ МЭ	–	программный блок мониторинга эксплуатации;
ПБ ТЭА	–	программный блок технико-экономического анализа и моделирования процессов эксплуатации;
ПБ УД	–	программный блок управления данными интегрированной логистической поддержки;
ПМ ИЛП	–	программный модуль «Система интегрированной логистической поддержки»;
ПО	–	программное обеспечение;
ПЭВМ	–	персональная электронная вычислительная машина;
СУБД	–	система управления базами данных;
СХД	–	собственное хранилище данных;
СЧ	–	составная часть;
УЗ	–	учетная запись.

ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

[1] Комплекс программ в защищенном исполнении «Система полного жизненного цикла изделий «Цифровое предприятие»». Техническое задание на разработку программного модуля «Система интегрированной логистической поддержки»
инв. № 35-5996-дсп от 12.07.2021.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					