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

УТВЕРЖДЕН
07623615.00096-05 90 01-ЛУ

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

Программный модуль «Система информационного анализа»

Руководство администратора

07623615.00096-05 90 01

Листов 34

2021

АННОТАЦИЯ

В документе приводится общее описание программного модуля «Система информационного анализа» комплекса программ в защищенном исполнении «Система полного жизненного цикла изделий «Цифровое предприятие» и его компонентный состав.

Представлена информация о составе дистрибутивного пакета и необходимых процедурах, требуемых для установки и настройки программного модуля.

Указаны команды запуска и остановки, а также общие алгоритмы проверки доступности программного модуля.

Полное наименование: программный модуль «Система информационного анализа».

Краткое наименование: СИА.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение программы

СИА обеспечивает унификацию технологий формирования отчетности и анализа данных в едином рабочем пространстве и предназначен для отображения значений интегральных показателей и отчетных форм, получаемых на основании произвольных наборов данных, представленных в реляционной форме, а также многомерного анализа производственных данных. При этом первичная информация для СИА поставляется из смежных систем путем исполнения соответствующих сценариев интеграции.

Результаты представляются пользователю в виде легко читаемых графиков и таблиц для принятия управленческих решений.

СИА позволяет отслеживать эффективность выполнения процессов деятельности предприятия через индикативную модель, позволяющую измерять/рассчитывать конечные состояния объектов/процессов требуемой предметной области («экономика», «производство», «закупки», «персонал» и т.п.).

СИА не накладывает ограничений на типы/виды процессов деятельности, для которых предполагается осуществлять мониторинг их исполнения.

Основными условиями возможности применения СИА в части контроля процессов являются:

- процесс должен быть автоматизирован;
- процесс иметь конечные состояния, фиксируемые в ИС;
- должны быть определены алгоритмы мониторинга состояний процесса.

1.2. Функции программы

СИА обеспечивает механизмы аналитической обработки и многомерного анализа производственных данных с визуализацией результатов.

СИА выполняет следующие основные функции:

- хранение и управление данными о структуре информационных панелей, представляющих данные в виде таблиц и различного рода диаграмм;

- хранение и управление информацией об используемых в информационных панелях наборах данных;
- хранение и управление макетами регламентированных отчетов;
- хранение и управление схемами построения «OLAP» отчетности;
- хранение и управление параметрами подключения к источникам данных;
- хранение и управление параметрами отображения объектов в виртуальной файловой системе;
- доступ к обрабатываемым данным;
- предоставление средств построения статических отчетов;
- предоставление пользователю интерфейса работы с многомерными моделями данных («OLAP» отчетность с использованием языка «MDX»);
- структуризация и отображение данных на информационных панелях;
- возможность обработки основных событий, возникающих в результате действий пользователя;
- предоставление средств регулируемого углубления («drill-down») в данные;
- функциональность редактора для определенных типов элементов репозитория;
- управление стартовыми страницами, автоматически открываемыми при входе пользователя;
- просмотр значений переменных окружения;
- управление расписанием (планировщик) автоматически выполняемых задач;
- управление сценариями, автоматически выполняемыми при входе пользователя;
- мониторинг деятельности пользователей в отношении объектов виртуальной файловой системы;
- организация доступа пользователя через графический интерфейс браузера.

1.3. Состав технических и программных средств

СИА реализована в архитектуре «клиент - сервер». В серверную часть входят:

- сервер(ы) баз данных (сервер БД) – хранение и обработка прикладных и системных данных;
- сервер службы каталогов (сервер «LDAP») – управление доменом и пользователями домена;
- сервер приложений (сервер СИА) – реализация программных средств информационного анализа на платформе «Java» и сервере «Tomcat», позволяющего запустить аналитическую платформу.

Минимальные требования к серверу СИА и серверу БД (только для системных баз данных):

- процессор: «x86-64», от 2х ядер;
- оперативная память: 8 ГБ;
- сетевой интерфейс: 1000 Мб/сек;
- дисковая подсистема: 32 ГБ для ОС, 32 ГБ для данных.

Состав ПО на рабочем месте пользователя:

- операционная система: «Astra Linux SE»;
- браузер: «Firefox» или «Chromium» из состава «Astra Linux SE».

Состав ПО на серверах:

- операционная система: «Astra Linux SE»;
- сервер СИА: «Tomcat» и компоненты СИА на платформе «Java»;
- сервер БД: СУБД «Синергия-БД» / «PostgreSQL».

Для создания и/или модификации некоторых объектов СИА рекомендуется использовать следующие приложения с открытым кодом:

- приложение «Редактор сценариев интеграции» («Pentaho Data Integration»), позволяющее редактировать сценарии интеграции («ETL»);
- приложение «Редактор отчетов» («Pentaho Report Designer»), позволяющее редактировать отчеты;
- приложение «Редактор схем OLAP» («Pentaho Schema Workbench»), позволяющее определять схемы многомерных кубов;

- приложение «Редактор метаданных» («Pentaho Metadata Editor»), позволяющее редактировать метамодели.

Источниками производственных данных для СИА являются смежные информационные системы («PDM», «ILS», «MDM» и т.п.). Доступ к ним осуществляется посредством драйверов «JDBC» (для баз данных) и/или по протоколам «HTTP»/«HTTPS» (для веб-сервисов).

Исполнение сценариев интеграции данных смежных систем обеспечивается КСИ, либо встроенным инструментарием СИА (подсистемой «ETL»).

КСИ представляет расширенную функциональность интеграции данных, а именно:

- управление сообщениями в распределенной вычислительной среде;
- реализация выделенных серверов трансформации и управление ими;
- реализация собственного репозитория трансформаций с возможностью подключения к репозиторию СИА.

2. СТРУКТУРА ПРОГРАММЫ

СИА обеспечивает выполнение следующих функций:

- ведение репозитория (подсистема метаданных);
- хранение и доступ к данным (подсистема обработки данных);
- исполнение задач трансформации, расположенных в репозитории СИА (подсистема «ETL») или исполняемых смежным КСИ;
- визуализация и аналитическая обработка данных (подсистема визуализации и анализа);
- управление системными параметрами (подсистема технологических сервисов).

Схема функциональной структуры СИА представлена на рис. 1.

Структурная схема СИА

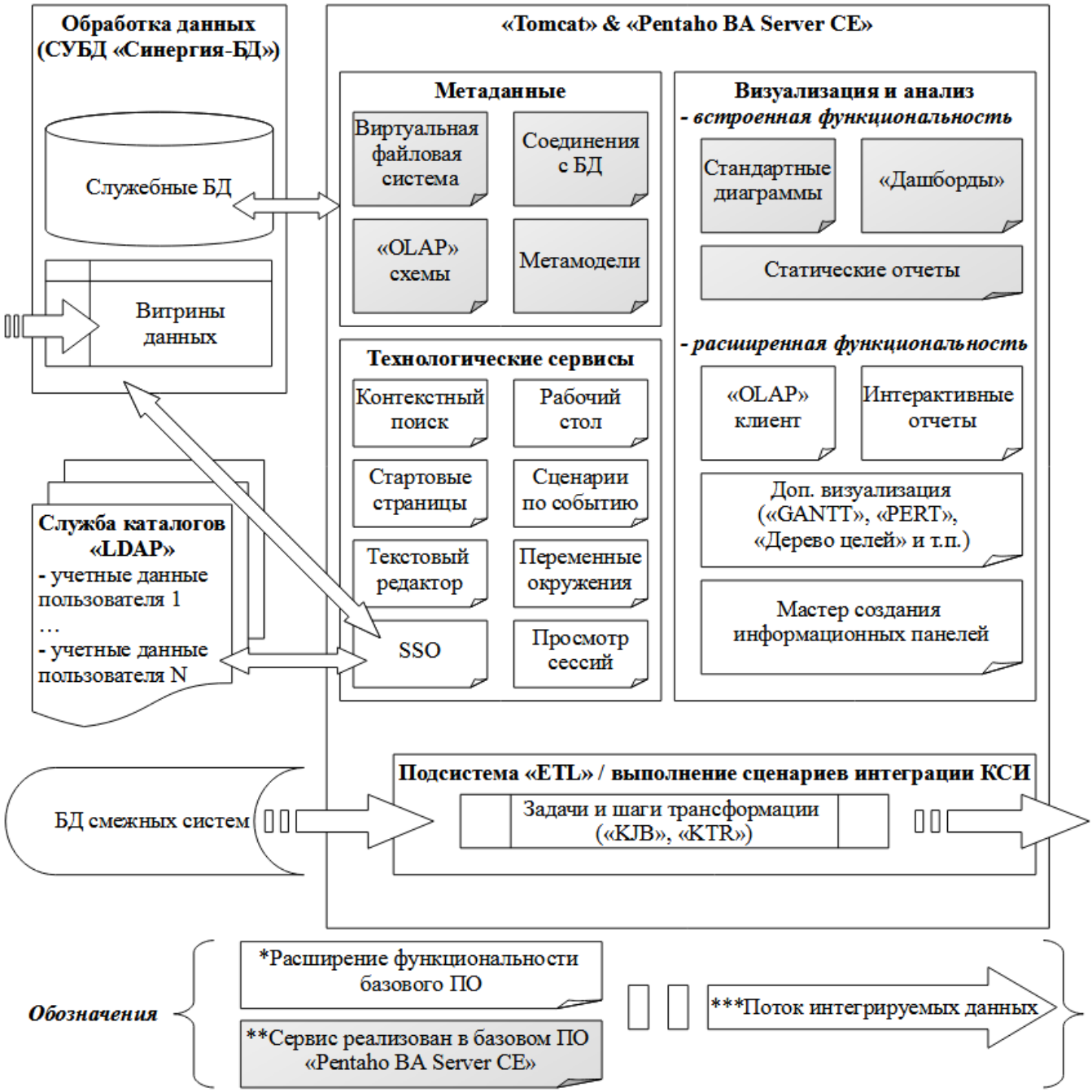

Рисунок 1

2.1. Подсистема метаданных

Подсистема обеспечивает хранение данных об основных элементах СИА и их структуре, таких как:

- наборы настроек подключений к источникам данных («Connections»);
- сценарии формирования наборов данных (запросы и задачи «ETL»);
- информационные панели (их структура и связь с данными);

- статические отчеты;
- схемы-описания «OLAP» кубов и сохраненные запросы к ним;
- метамодели данных, позволяющие трансформировать физическую структуру хранения данных в объектную модель понятную конечному пользователю;
- метаданные виртуальной файловой системы, предназначенные для отображения системных объектов в виде элементов структуры каталогов репозитория.

Виртуальная файловая система поддерживает следующие возможности:

- организация структуры каталогов;
- копирование, переименование и перемещение элементов;
- удаление элементов в «корзину»;
- импорт/экспорт элементов.

2.2. Подсистема обработки данных

Функциональность подсистемы реализуется СУБД.

Подсистема предназначена для:

- обеспечения доступа к хранимым данным;
- хранения системных данных – системный репозиторий;
- хранения прикладных данных – пользовательские БД и витрины данных.

2.3. Подсистема «ETL»

Подсистемой обеспечиваются:

- чтение метаданных процедур «ETL»;
- выполнение процедур «ETL»;
- вывод результатов выполнения процедур «ETL» в файл и/или базу данных.

2.4. Подсистема визуализации и анализа

Подсистема обеспечивает доступ к информации для решения прикладных задач обработки данных, включая формирование различного рода диаграмм (тренд, сравнительная, круговая и т.п.), генерацию отчетов, выполнение анализа данных с использованием «OLAP» технологий.

К инструментам, обеспечивающим визуализацию аналитической информации, относятся:

- информационные панели;
- средства генерации отчетов;
- «OLAP» средства.

«OLAP» средства реализуют функции создания динамической отчетности с использованием языка «MDX» и представляют графический инструмент анализа данных, позволяющий:

- проводить анализ показателей деятельности на основе операционных данных;
- собирать, обобщать и представлять данные в виде легко читаемых графиков и аналитических таблиц;
- создавать и обрабатывать «информационные кубы» – виртуальные информационные центры, которые содержат данные, существенные для анализа, выявления тенденций развития и принятия стратегических решений.

«OLAP» средства включают в себя два основных компонента:

- «OLAP» сервер, обеспечивающий формирование модели данных и выполнение необходимых операций с ними (посредством выполнения MDX выражений);
- «OLAP» клиент, предоставляющий пользователю визуальный интерфейс к многомерной модели данных, обеспечивая его возможностью удобно манипулировать данными для выполнения задач анализа данных.

2.5. Подсистема технологических сервисов

Подсистема обеспечивает:

- реализацию технологии единого входа в сеть («SSO»), обеспечивающей сквозную аутентификацию пользователя для взаимодействующих программ: «браузер» – «сервер СИА» – «контроллер домена» – «СУБД»;
- выполнение операций с источниками данных (соединения с базами данных, схемы «OLAP», метамодели и пр.);

- представление пользователю инструмента «Рабочий стол», обеспечивающего возможность создания «ярлыков» для быстрого запуска инструментов и/или файлов отчетов и информационных панелей;
- функциональность редактора информационных панелей – инструмент создания интерактивных страниц для мониторинга ключевых показателей деятельности предприятия;
- функциональность текстового редактора для элементов репозитория;
- управление стартовыми страницами, автоматически открываемыми при входе пользователя;
- просмотр значений переменных окружения;
- управление расписанием (планировщик) автоматически выполняемых задач (например: запуск интеграционного сценария по расписанию);
- просмотр текущих и закрытых (журнал) сессий пользователей и информации о связанных с ними объектах виртуальной файловой системы;
- возможность локализации пользовательского интерфейса;
- управление сценариями (в т.ч. сценариями интеграции), автоматически выполняемыми при входе пользователя.

3. АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

СИА поддерживает возможность сквозной аутентификации пользователей с использованием сервера «Kerberos». Схема взаимодействия программных компонентов для такого типа аутентификации представлена на на рис. 2.

Взаимодействие компонентов при аутентификации «Kerberos»

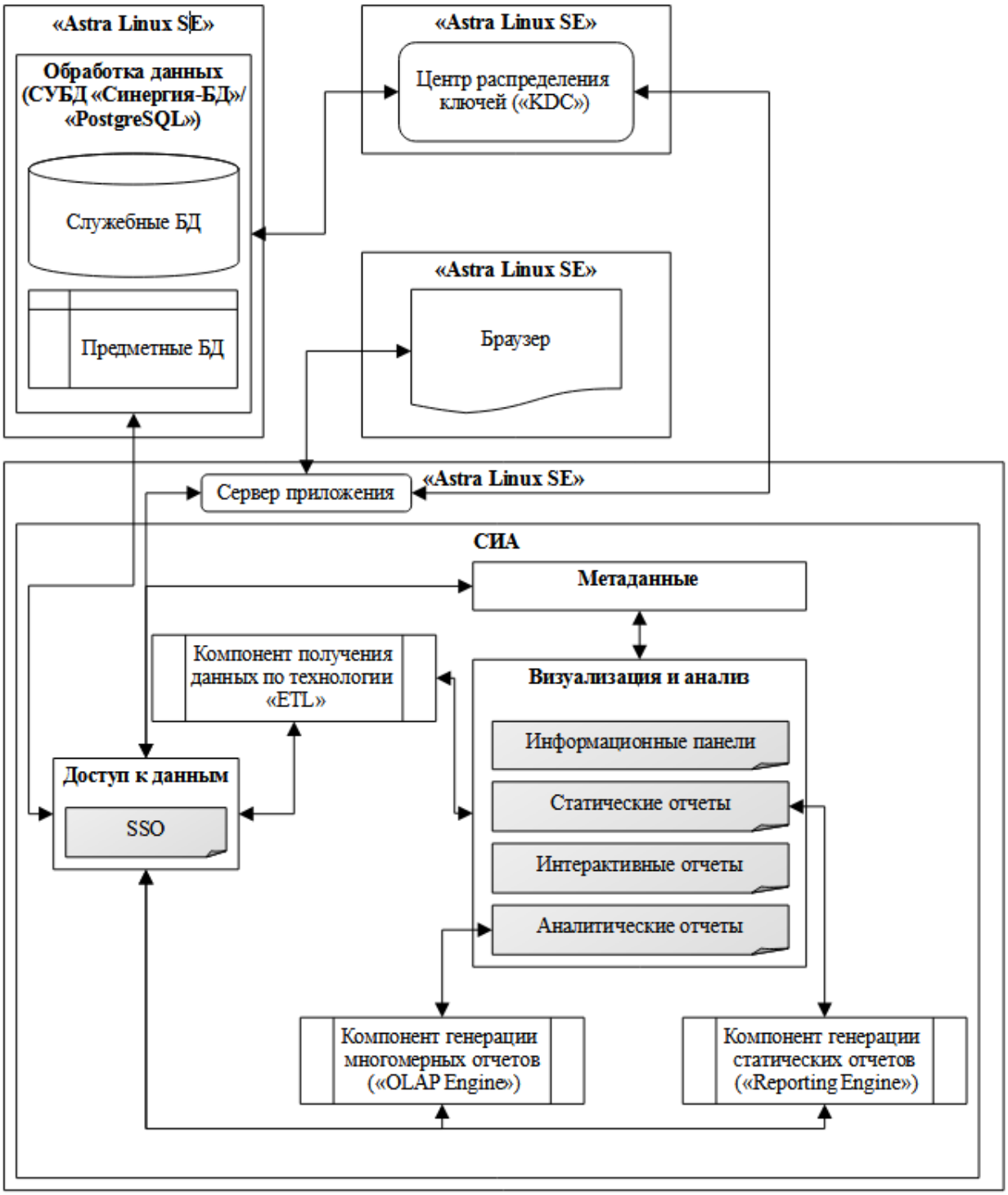

Рисунок 2

Ключевая особенность такого способа аутентификации – доступ к данным осуществляется в контексте доменного пользователя согласно правилам СУБД.

Подобная схема обусловлена применением в автоматизированных системах в защищенном исполнении, т.к. предполагает использование доверенных (сертифицированных) средств разграничения доступа ОС и СУБД и их отсутствие в СИА.

При визуализации информации из БД с использованием протокола «Kerberos» задача разграничения доступа возлагается на подсистему обработки данных, которая реализуется средствами СУБД. На уровне СУБД определяется, у каких пользователей есть права на доступ к тем или иным объектам БД.

Аутентификация пользователей в системе осуществляется согласно схеме, представленной на рис. 3.

Схема сквозной аутентификации пользователей

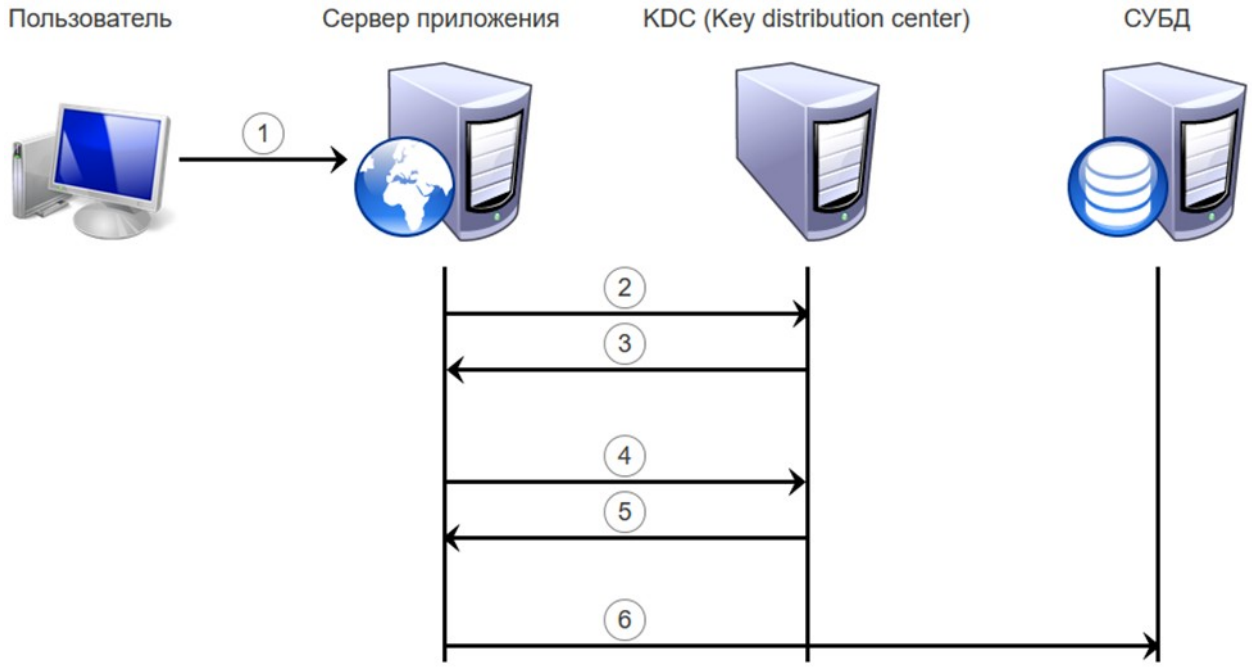

Рисунок 3

Пользователь авторизуется в операционной системе и браузер обращается к серверу приложения, чтобы получить доступ к необходимым ему данным (1). Сервер приложения обращается к «KDC» с запросом первичной аутентификации (2).

«KDC» – служба, работающая на защищенном сервере. «KDC» хранит базу данных с информацией об учётных записях всех клиентов сети. Вместе с

информацией о каждом абоненте в базе данных «KDC» хранится криптографический ключ, известный только этому абоненту и службе «KDC». Этот ключ служит для связи клиента с центром дистрибуции ключей.

После успешного подтверждения его подлинности, «KDC» выдает первичное удостоверение пользователя для доступа к сетевым ресурсам – «Ticket Granting Ticket» («TGT») (3). Затем, пользователь, предъявляя «TGT» (4), получает от «KDC» удостоверение для доступа к конкретному сетевому ресурсу – «Ticket Granting Service» («TGS») (5).

После получения «TGS», пользователь обращается с ним к СУБД (6) и, после взаимной проверки подлинности, получает доступ к запрашиваемым данным согласно матрице доступа.

В рассматриваемом случае считается, что все пользователи домена допущены к визуальному интерфейсу СИА, имеют равный доступ к объектам виртуальной файловой системы СИА («видят» все отчеты, информационные панели и т.п.), данные в которых выводятся согласно политикам доступа, определенных в СУБД.

Если существует необходимость ограничить список пользователей, допущенных к СИА, предлагается использовать защищенный веб-сервер «Apache2», входящий в состав «Astra Linux SE».

В этом случае при обращении к СИА клиентский браузер передает веб-серверу «Apache2» учетные данные «Kerberos».

Если значения параметров не заданы – учетные данные «Kerberos» не передаются веб-серверу и происходит отказ в доступе.

Веб-сервер, обращаясь к «LDAP» службе каталогов, проверяет действительность представленных данных. В случае успешного прохождения проверки пользователю выводится веб-страница СИА.

Доступ субъектов к интерфейсу СИА ограничен разрешительным списком, задаваемым в конфигурационном файле веб-сервера.

Взаимодействие веб-сервера и СИА осуществляется по протоколу «AJP» (по определенному порту), который обеспечивает проксирование запросов к серверу СИА и передачу запрашиваемой информации.

Для того, чтобы ограничить возможность доступа пользователей / программ непосредственно к серверу СИА и использовать только веб-сервер «Apache2» следует:

- средствами сетевого экранирования ОС «Astra Linux» закрыть порт «AJP» для всех «ip» адресов кроме веб-сервера командой «iptables»;
- отключить любые возможности доступа к СИА (порты доступа 8080 и т.п.) за исключением «AJP».

4. ПОДГОТОВКА И УСТАНОВКА ПРОГРАММЫ

Установку СИА рекомендуется выполнять в следующей последовательности:

- подготовка и конфигурирование серверов;
- сборка из исходных кодов (в случае варианта поставки в исходных кодах);
- установка и настройка СИА и программного окружения (ОС, СУБД, виртуальная машина «Java»);
- установка и настройка веб-сервера «Apache2» (опционально).

Дистрибутив, тексты программ (в случае варианта поставки в исходных кодах) и вспомогательные файлы, требуемые для сборки и установки СИА, поставляются на машинном носителе (инсталляционный пакет).

Каталоги инсталляционного пакета:

- «build_tools» – инструменты сборки программных компонентов СИА;
- «dependencies» – вспомогательные файлы для сборки программных компонентов СИА;
- «jdk» – дистрибутив «Java Development Kit» («JDK»);
- «pdi» – дистрибутив «Pentaho Data Integration»;
- «samples» – примеры информационных панелей и демонстрационная база данных;
- «scripts» – вспомогательные программы сборки и установки;
- «service» – скрипт создания службы запуска СИА;
- «src» – тексты программных компонентов СИА.

Файлы инсталляционного пакета:

- «build.cfg» – конфигурационный файл, содержащий параметры сборки СИА из исходных кодов;
- «build.sh» – скрипт сборки компонентов СИА из исходных кодов;
- «install.cfg» – конфигурационный файл, содержащий параметры установки СИА;
- «install.sh» – скрипт установки СИА.

4.1. Подготовка и конфигурирование серверов

СИА предполагает наличие следующих (виртуальных) серверов:

- сервер с исходными кодами и/или дистрибутивом системы (далее – «siasrc») и дистрибутивом операционной системы, доступным по протоколу «FTP»;
- сервер службы каталогов «LDAP» (далее – «sialdap») – обеспечивает возможность входа пользователей в СИА без ввода «логина»/пароля с использованием технологии единого входа в сеть («SSO»);
- сервер(ы) СУБД (далее – «siadb») – сервер для хранения системных данных и сервер для хранения прикладных данных (могут быть объединены);
- сервер СИА (далее – «sia») – сервер, обеспечивающий функционирование системы информационного анализа.

Перед установкой СИА необходимо выполнить следующие действия:

- присвоить всем серверам статические «ip» адреса;
- присвоить всем серверам соответствующие имена (в файлах «/etc/hosts», «/etc/hostname»);
- обеспечить возможность доступа ко всем серверам по протоколу «SSH»;
- обеспечить размещение «FTP» репозитория ОС «Astra Linux SE» на сервере «siasrc» на который будут ссылаться другие серверы при установке системы.

Выполнение инструкций настоящего руководства необходимо осуществлять под учетной записью пользователя (далее – «user»), имеющей возможность выполнять команды от имени суперпользователя («sudo»). Такая учетная запись должна быть определена на всех серверах.

После конфигурирования серверов необходимо скопировать файлы инсталляционного пакета на сервер «siasrc» в домашний каталог пользователя «user» в каталог «install».

4.1.1. Разрешение подключения к серверу по протоколу «SSH»

Для обеспечения доступа к серверу под управлением ОС «Astra Linux SE» необходимо:

- проверить наличие пакета командой:

```
sudo apt list ssh
```

- в случае, если пакет отсутствует, установить его командой:

```
sudo apt install ssh
```

- для разрешения доступа по «SSH» выполнить команды:

```
sudo systemctl enable ssh
sudo systemctl start ssh
```

Указанные команды выполняются для всех серверов, участвующих в установке системы.

4.1.2. Создание локального репозитория

Для создания в ОС «Astra Linux SE» репозитория из «ISO» образов установочных дисков необходимо на сервере «`siasrc`»:

- создать каталог для размещения репозитория:

```
sudo mkdir -p /srv/repo/smolensk/main
```

- «примонтировать» образ установочного диска (если на компьютере нет каталога «`/media/cdrom`» – то создать каталог «`/media/cdrom`»):

```
[ -d /media/cdrom ] || sudo mkdir /media/cdrom
sudo mount /путь_к_ISO-образу /media/cdrom
```

- скопировать файлы из образа в каталог репозитория:

```
sudo cp -a /media/cdrom/* /srv/repo/smolensk/main
```

- «отмонтировать» «ISO» образ диска:

```
sudo umount /media/cdrom
```

- установить «FTP» сервер:

```
sudo apt install vsftpd
```

- в конфигурационный файл «/etc/vsftpd.conf» внести следующие данные:

```
listen=YES
listen_ipv6=NO
#Анонимный доступ разрешен
anonymous_enable=YES
local_enable=NO
anon_root=/srv/repo
no_anon_password=YES
hide_ids=YES
```

- перезапустить сервис «FTP»:

```
sudo systemctl restart vsftpd
```

- настроить источники пакетов (файл «/etc/apt/sources.list»):

```
deb ftp://ip_адрес_сервера_siasrc/smolensk/main smolensk
main contrib non-free
```

Ссылка на созданный «FTP» репозиторий для других серверов настраивается автоматически в процессе установки СИА (согласно последнему пункту инструкции – через файл «/etc/apt/sources.list»).

4.2. Сборка из исходных кодов

Сборка из исходных кодов осуществляется на сервере «siasrc» при запуске сценария:

```
cd $HOME/install
./build.sh
```

В процессе исполнения сценария сборки СИА на сервере «siasrc» осуществляется:

- установка пакетов «rsync», «dos2unix», «sshpass», «zip», «xrdp»;
- распаковка архивов с исходными кодами (в каталог «$HOME/sia/», причем имя «sia» задается в конфигурационном файле «build.cfg» параметром «appName»);
- распаковка архивов с зависимостями (в каталог «$HOME»);
- для текстов программ (в каталоге «$HOME/sia/») выполняется преобразование кодировки файлов (командой «dos2unix»).

Кроме этого, осуществляется установка следующего программного обеспечения:

- «Java Development Kit» («JDK») версии 1.8.0_282-b08 или выше;
- «Apache Maven» версии 3.6.3 или выше;
- «Gradle» версии 6.6.1 или выше;
- «Node.js» версии 14.16.0 или выше (включая «npm» версии 6.14.11 или выше);
- «Apache Ant» версии 1.10.9 или выше (включая «Apache Ivy» версии 2.5.0 или выше).

После выполнения подготовительных процедур осуществляется сборка программных компонентов СИА.

Дистрибутивы, полученные в результате сборки, помещаются в каталог «`$HOME/sia/dist/app`».

В состав дистрибутива также включаются:

- «Java Development Kit» – среда функционирования СИА (каталог «`$HOME/sia/dist/app`»);
- «Pentaho Data Integration» – необходим для установки пакета локализации (каталог «`$HOME/sia/dist/pdi`»).

Далее приведены команды и порядок сборки компонентов:

- «data-access»:

```
mvn clean install -DskipTests
```

- «cda»:

```
mvn clean install -DskipTests
```

- «cde»:

```
mvn clean install -DskipTests
```

- «cdf»:

```
mvn clean install -DskipTests
```

- «pentaho-commons-gwt-modules»:

```
mvn clean install -DskipTests
```

- «pentaho-commons-database»:

```
mvn clean install -DskipTests
```

- «pentaho-platform-plugin-reporting»:

```
mvn clean install -Dmaven.test.skip=true
```

- «postgresql-driver»:

```
mvn clean install -DskipTests
```

- «pentaho-karaf-assembly»:

```
mvn clean install -DskipTests
```

- «pentaho-platform»:

```
mvn clean install -DskipTests
```

- «platform-extensions»:

```
gradle clean –offline
gradle build --offline
```

- «russian-language-pack»:

```
ant clean resolve build-language-pack -DlangCode=ru
```

- «startupRuleEngine»:

```
ant clean-all resolve dist
```

- «usersessions»:

```
"ant clean-all resolve dist
```

- «cte»:

```
ant clean-all resolve dist
```

- «cst»:

```
ant clean-all resolve dist
```

- «environmentDisplay»:

```
ant clean-all resolve dist
```

- «tree-editor»:

```
gradle clean –offline
gradle build --offline
```

- «interactive-reports»:

```
gradle clean –offline
gradle build –offline -xtest
```

- «panelsEditor»:

```
gradle clean –offline
gradle build --offline
```

- «desktop»:

```
gradle clean –offline
gradle build --offline
```

- «cde-extensions-pack»:

```
ant clean-all resolve dist
```

- «mondrian»:

```
ant build
```

- «saiku»:

```
mvn clean install -DskipTests
```

4.3. Установка программы

Для запуска программы установки СИА на сервере «siasrc» следует выполнить сценарий:

```
cd $HOME/install
./install.sh
```

4.3.1. Описание конфигурации

Перед началом установки СИА на сервере «siasrc» следует определить значения основных параметров, задаваемых в файле «$HOME/install/install.cfg».

4.3.1.1. Параметры конфигурации сервера с дистрибутивом системы

В отношении сервера «siasrc» выполняются настройки:

- «srcIP» – «IP» адрес сервера;

- «srcAdminUsr» – имя учетной записи пользователя, имеющего возможность выполнять команды от имени суперпользователя («sudo»);

- «srcAdminPwd» – пароль для этой учетной записи (если значение не определено – потребуется ввод с клавиатуры во время установки).

4.3.1.2. Параметры конфигурации сервера приложения

В отношении сервера «sia»:

- «appIP» – «IP» адрес сервера;
- «appAdminUsr» – имя учетной записи пользователя, имеющего возможность выполнять команды от имени суперпользователя («sudo»);
- «appAdminPwd» – пароль для этой учетной записи (если значение не определено – потребуется ввод с клавиатуры во время установки);
- «dirApp» – каталог, куда будет установлена система;
- «appUsr» – пользователь, от имени которого запускается система (владелец каталога «dirApp»);
- «appUsrPwd» – пароль этого пользователя (если значение не определено – потребуется ввод с клавиатуры во время установки);
- «appUsrPwdForceChange» – флаг (принимает значение «1» или «0»), определяющий необходимость / отсутствие необходимости изменения пароля пользователя «appUsr», если пользователь был создан ранее;
- «installDemo» – флаг (принимает значение «1 или «0»), определяющий необходимость / отсутствие необходимости установки демонстрационного примера.

4.3.1.3. Параметры конфигурации сервера службы каталогов

В отношении сервера «sialdap» выполняются настройки:

- «ldapIP» – «IP» адрес сервера;
- «ldapAdminUsr» – имя учетной записи пользователя, имеющего возможность выполнять команды от имени суперпользователя («sudo»);
- «ldapAdminPwd» – пароль для этой учетной записи (если значение не определено – потребуется ввод с клавиатуры во время установки);
- «domainName» – имя устанавливаемого домена;
- «domainAdminUsr» – администратор домена;

- «domainAdminPwd» – пароль администратор домена (если значение не определено – потребуется ввод с клавиатуры во время установки);
- «testUser» – имя доменного пользователя для тестирования входа в систему;
- «testUserPwd» – пароль этого пользователя (если значение не определено – потребуется ввод с клавиатуры во время установки).

4.3.1.4. Параметры конфигурации сервера баз данных

В отношении сервера «siadb» выполняются настройки:

- «dbIP» – «IP» адрес сервера;
- «dbAdminUsr» – имя учетной записи пользователя, имеющего возможность выполнять команды от имени суперпользователя («sudo»);
- «dbAdminPwd» – пароль для этой учетной записи (если значение не определено – потребуется ввод с клавиатуры во время установки);
- «demoDbName» – имя демонстрационной БД (следует указать в случае значения флага «installDemo» равного «1»).

4.3.2. Описание процедуры установки

В процессе исполнения сценария установки СИА осуществляются следующие действия:

- конфигурация репозитория и установка пакетов «rsync», «dos2unix», «sshpass», «zip», «xrdp» на серверах «sia», «sialdap», «siadb»;
- установка СУБД на сервере «siadb» и ее конфигурация для доступа пользователей с использованием механизмов сквозной аутентификации (тип аутентификации – «GSS»);
- копирование дистрибутива на сервер «sia», распаковка архивов дистрибутива в каталог, определенный конфигурационным параметром «dirApp»;
- установка и конфигурация контроллера домена на сервере «sialdap» и клиентов домена на серверах «sia», «siadb»;

- установка и настройка СИА и его программных компонентов;
- конфигурация СИА для доступа пользователей с использованием механизмов сквозной аутентификации;
- установка пакета локализации (русификации) базовой платформы;
- установка демонстрационного примера (определяется конфигурационным параметром «installDemo»);
- создание «тестового» доменного пользователя;
- создание службы запуска СИА;
- запуск СИА.

4.4. Совместное применение с веб-сервером

Веб-сервер «Apache2» может выступать в роли обратного прокси-сервера и использоваться для организации единой точки доступа к серверу СИА.

Для обеспечения доступа к СИА через веб-сервер «Apache2» необходимо установить сам веб-сервер и дополнительные модули к нему, выполнив команды:

```
apt-get install apache2
apt-get install libapache2-mod-proxy-html libapache2-mod-auth-kerb
a2enmod proxy
a2enmod proxy_http
```

Для аутентификации пользователей посредством «Kerberos» необходимо:

- отключить модуль аутентификации через «PAM»:

```
a2dismod auth_pam
```

- активировать модуль «auth_kerb»:

```
a2enmod auth_kerb
```

- в директории «/etc/apache2/sites-available/» создать конфигурационный файл виртуальных хостов «host.conf»:

```
<VirtualHost *:80>
  ServerName localhost
  ErrorLog /var/log/apache2/ajp.error.log
  CustomLog /var/log/apache2/ajp.log combined

  DocumentRoot /var/www/
```

```
<Directory />
  AddDefaultCharset Off
  Order deny,allow
  Allow from all
  AuthType Kerberos
  KrbServiceName host/apache-srv.vniief.local@VNIIEF.LOCAL
  Krb5Keytab /etc/web.keytab
  KrbMethodNegotiate on
  KrbMethodK5Passwd off
  KrbSaveCredentials on
  KrbLocalUserMapping on
  require valid-user
</Directory>

<Proxy "http://apache-srv.vniief.loc/pentaho/*">
  AddDefaultCharset Off
  Order deny,allow
  Allow from all

  AuthType Kerberos
  KrbServiceName host/apache-srv.vniief.loc@VNIIEF.LOC
  Krb5Keytab /etc/web.keytab
  KrbMethodNegotiate on
  KrbMethodK5Passwd off
  KrbSaveCredentials on
  KrbLocalUserMapping on

  require valid-user
</Proxy>

<Proxy "ajp://sia-srv.vniief.loc:8009/pentaho/*">
  AddDefaultCharset Off
  Order deny,allow
  Allow from all

  AuthType Kerberos
  KrbServiceName host/apache-srv.vniief.loc@VNIIEF.LOC
  Krb5Keytab /etc/web.keytab
  KrbMethodNegotiate on
  KrbMethodK5Passwd off
  KrbSaveCredentials on
  KrbLocalUserMapping on
```

```
        require valid-user

    </Proxy>

    ProxyPass /pentaho ajp://sia-srv.vniief.loc:8009/pentaho
    ProxyPassReverse /pentaho ajp://sia-
srv.vniief.loc:8009/pentaho

</VirtualHost>
```

- активировать виртуальный хост:

```
a2ensite /etc/apache2/sites-available/host.conf
```

- перезапустить сервер «apache2»:

```
service apache2 restart
```

Теперь сервер СИА может быть доступен по адресу:

```
http://apache-srv.vniief.loc/pentaho
```

Все подчеркнутые значения зависят от инфраструктуры предприятия.

Обратите внимание на выделенный цветом параметр «`require`». Он определяет доступ пользователей:

- значение «`valid-user`» определяет, что все аутентифицированные на контроллере домена пользователи имеют к доступ;
- для ограничения списка допущенных пользователей следует задать значение параметра в виде списка их имен, разделенных символом пробела («`require user-01 user-02`» и т.п.).

Веб-сервер для аутентификации пользователей использует «Kerberos». Указанный в «`host.conf`» файл ключей «`/etc/web.keytab`» необходимо скопировать с сервера «`sia`», расположенного по аналогичному пути.

Взаимодействие веб-сервера и СИА осуществляется по протоколу «AJP» (по определенному порту), который обеспечивает проксирование запросов к серверу СИА и передачу запрашиваемой информации.

Настройка протокола «AJP» для СИА осуществляется в файле «`./pentaho-server/tomcat/conf/server.xml`», например:

```
<Connector URIEncoding="UTF-8" port="8009" protocol="AJP/1.3"
redirectPort="8443"/>
```

Для того, чтобы ограничить возможность доступа пользователей / программ непосредственно к серверу СИА и использовать только веб-сервер «Apache2» следует:

- средствами сетевого экранирования ОС «Astra Linux SE» закрыть порт «AJP» для всех, кроме веб-сервера командой «iptables»:

```
iptables -A INPUT -p tcp ! -s apache-srv.vniief.loc --dport
8009 -j DROP
```

- добавить исполнение этого правила при загрузке ОС – в файле «/etc/network/if-up.d» создать файл «iptables»:

```
#!/bin/sh
iptables -A INPUT -p tcp ! -s apache-srv.vniief.loc --dport
8009 -j DROP
```

- добавить файлу атрибут «исполняемый»:

```
chmode +x /etc/network/if-up.d/iptables
```

- в файле «/pentaho-server/tomcat/conf/server.xml» удалить строки, определяющие порты доступа («8080» и т.п.) за исключением «AJP»:

```
<Connector URIEncoding="UTF-8" port="8009"
protocol="AJP/1.3" redirectPort="8443"/>
```

4.5. Запуск и остановка программы

Для запуска СИА на сервере «sia» в директории «/etc/systemd/system» расположен файл «pentaho.service».

Структура файла представляется в виде шаблона:

```
[Unit]
Description=APP_NAME
After=network.target

[Service]
Type=forking
ExecStart=APP_PATH/START_CMD_FILE
ExecStop=APP_PATH/STOP_CMD_FILE
User=SERVICE_USER

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

В приведенном шаблоне:

- «APP_NAME» – имя приложения (например, «pentaho»);
- «APP_PATH» – путь к каталогу с командами запуска и остановки приложения (например, «/opt/sia/pentaho-server»);
- «START_CMD_FILE», «STOP_CMD_FILE» – команды запуска и остановки приложения («start-pentaho.sh» и «stop-pentaho.sh» соответственно);
- «SERVICE_USER» – имя пользователя (владельца каталога «APP_PATH») от которого выполняется запуск команд «START_CMD_FILE» и «STOP_CMD_FILE» (например, «user»).

Для регистрации сервиса запуска СИА выполняются команды («$FILE» - полный путь до файла описания сервиса, в рассматриваемом случае - «/etc/systemd/system/pentaho.service»):

```
chown root:root "$FILE"
chmod 0777 "$FILE"
chmod a+r "$FILE"
systemctl daemon-reload
```

После регистрации сервиса запуск СИА осуществляется командой:

```
sudo systemctl start pentaho
```

Остановка СИА осуществляется командой:

```
sudo systemctl start pentaho
```

В случае изменения настроек конфигурационных файлов СИА требуется его перезапуск. При этом перед запуском рекомендуется удалить содержимое каталогов:

- «./pentaho-solutions/system/logs/audit»;
- «./pentaho-solutions/system/jackrabbit/repository», включая удаление самого каталога «repository»;
- «./tomcat/logs»;
- «./tomcat/temp»;
- «./tomcat/work».

В процессе работы приложения ведется журнал, отражающий результаты основных системных событий.

Файлы журнала СИА расположены в каталоге «./tomcat/logs».

Сообщения журнала представлены следующими основными типами:

- «INFO» – информационные сообщения;
- «WARNING» – предупреждение;
- «ERROR» – сообщения об ошибке.

5. ПРОВЕРКА ПРОГРАММЫ

Для работы с СИА следует в адресной строке браузера ввести адрес вида:

`<протокол>://<адрес СИА>:<порт>/<имя_веб_приложения>`

Адрес и имя веб-приложения определяются на этапе развертывания и передаются пользователям СИА средствами, определенными в регламентах взаимодействия служб предприятия.

В случае ввода корректной адресной информации в окне браузере отобразится интерфейс пользователя СИА (рис. 4).

Главная страница СИА

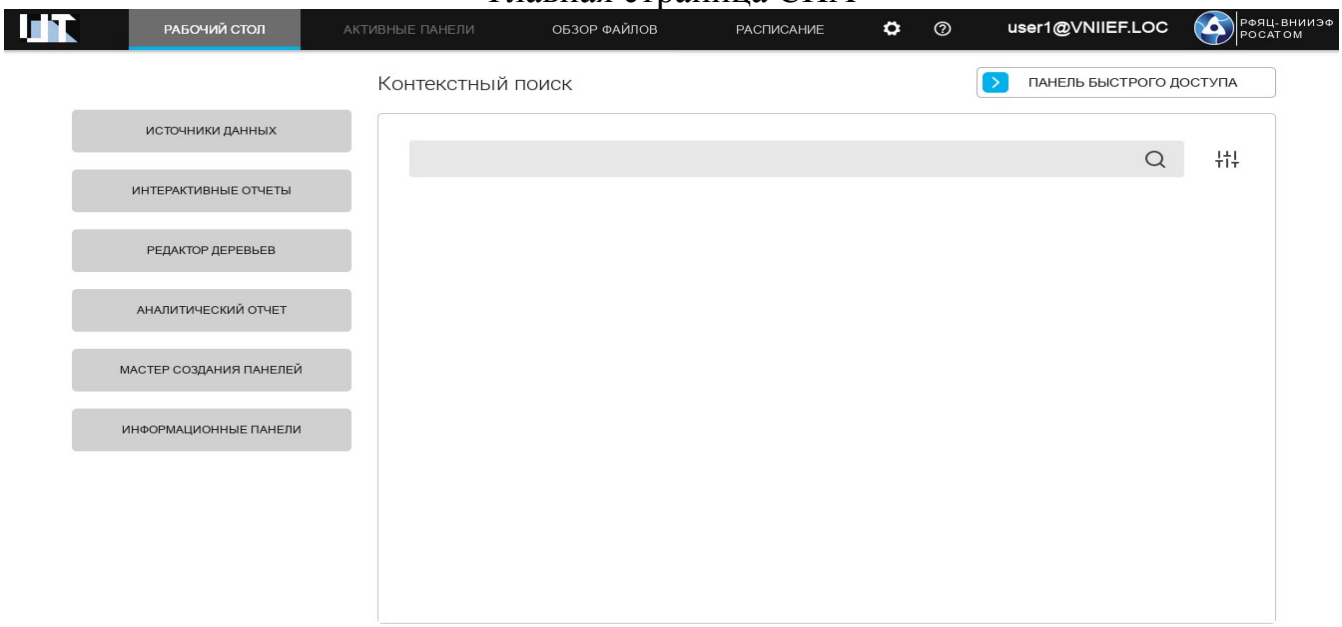

Рисунок 4

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	–	база данных
ИС	–	информационная система
КСИ	–	программный модуль «Комплекс средств интеграции» комплекса программ в защищенном исполнении «Система полного жизненного цикла изделий «Цифровое предприятие»
ОС	–	операционная система
ПО	–	программное обеспечение
СИА	–	программный модуль «Система информационного анализа» комплекса программ в защищенном исполнении «Система полного жизненного цикла изделий «Цифровое предприятие»
СУБД	–	система управления базами данных
СУБД «Синергия-БД»	–	программный модуль «Система управления базами данных «Синергия-БД» комплекса программ в защищенном исполнении «Система полного жизненного цикла изделий «Цифровое предприятие»

Лист регистрации изменений

Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в докум.*	*№ документа*	*Подп.*	*Дата*
	измененных	*замененных*	*новых*	*аннулированных*				