

1.3. Термины и определения

Сокращение, термин	Полное наименование, определение
ЕСМЭВ	Единая система межведомственного электронного взаимодействия, обеспечивающая взаимодействие информационных систем в соответствии с МР версии 3
ВИС	Ведомственные информационные системы, обеспечивающие предоставление государственных и (или) муниципальных услуг, операторами которых являются региональные органы исполнительной власти или органы местного самоуправления
ИС	Информационные системы, обеспечивающие предоставление государственных и (или) муниципальных услуг
СЗИ	Средства защиты информации
Электронный сервис	Программная система, идентифицируемая строкой URI, чьи публичные интерфейсы и привязки определены и описаны посредством XML. Описание этой программной системы может быть найдено другими программными системами, которые могут взаимодействовать с ней согласно этому описанию посредством сообщений, основанных на XML, и передаваемых с помощью Интернет-протоколов
ЭП	Электронная подпись
ЭП-ОВ	Электронная подпись ОИВ
ЭП-СП	Электронная подпись, формируемая от имени должностного лица органа власти, участвующего в межведомственном информационном взаимодействии при оказании государственных услуг
Участник	Региональные органы исполнительной власти и подведомственные им государственные организации, территориальные органы федеральных органов исполнительной власти, территориальные подразделения государственных внебюджетных фондов, органы местного самоуправления муниципальных образований и подведомственные им муниципальные организации, многофункциональные центры предоставления государственных и муниципальных услуг, участвующие в предоставлении государственных и муниципальных услуг в электронном виде
Потребитель	Участник межведомственного информационного взаимодействия, который формирует запросы Поставщикам информации о получении сведений в рамках предоставления государственных и муниципальных услуг (функций) в электронном виде и обрабатывает ответы Поставщиков информации
Поставщик	Участник межведомственного информационного

Име. № дубл.	Име. № дубл.
Взам. инв. №	Взам. инв. №
Подпись и дата	Подпись и дата
Име. № подл.	Име. № подл.

Изм.	Лист	№ документа	Подпись	Дата	Руководство системного администратора	Лист
						4

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	Подпись и дата

	взаимодействия, который формирует и предоставляет ответы на запросы Потребителей информации о получении сведений в рамках предоставления государственных и муниципальных услуг (функций) в электронном виде
ОИВ	Орган исполнительной власти
р-сведения	Сведения, предоставляемые Участниками по запросам федеральных органов исполнительной власти в рамках предоставления ими государственных услуг или исполнения государственных функций в электронном виде
ф-сведения	Сведения, предоставляемые федеральными органами исполнительной власти, подведомственными им государственными организациями, государственными внебюджетными фондами по запросам Участников в рамках предоставления Участниками государственных и муниципальных услуг или исполнения государственных и муниципальных функций в электронном виде
FTP	Протокол передачи файлов, предназначенный для передачи файлов по ТСР-сетям
Парсинг	Синтаксический анализ и разбор электронного сообщения, производимый специальной программой или скриптом
ФОИВ	Федеральный орган исполнительной власти
МВ взаимодействие	Структурированный набор данных, пересылаемый по каналам МВ
Каналы МВ	Технологические каналы связи, используемые для передачи МВ сообщений
МВ сообщений	Электронные сообщения (запрос, ответ) передаваемые в рамках МВ взаимодействия
МР версии 3	Методические рекомендации по работе с единой системой межведомственного электронного взаимодействия версии 3.4.0.0 или старше, утвержденные Подкомиссией по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности»

Изм.	Лист	№ документа	Подпись	Дата	<i>Руководство системного администратора</i>	<i>Лист</i>
						5

2. Описание Системы

2.1. Назначение Системы

Назначением Системы является поддержка процессов межведомственного взаимодействия Участников при оказании государственных услуг. Назначением Системы является:

- Маршрутизация МВ сообщений;
- Проведение форматно-логического контроля передаваемых сообщений;
- Гарантированная доставка МВ сообщений;
- Простановка ЭП-ОВ на МВ сообщениях;
- Журналирование процесса МВ взаимодействия;
- Интеграция с ЕСМЭВ.

2.2. Состав Системы

В качестве системного программного обеспечения используется:

- СУБД Postgres Pro Standard 10.5.3 в качестве хранилища данных;
- Tomcat v.8.0.32 в качестве Web-сервера и сервера приложений;
- RabbitMQ v.3.6.10 в качестве шины взаимодействия компонентов Системы.

Требования к общесистемному и специализированному программному обеспечению для реализации функций Системы в минимально необходимом объёме представлены в Таблице №1.

Таблица № 1. Требования к ОПО и СПО

Тип	Назначение	Наименование
Операционная система	Обеспечение работы СУБД	CentOSv6.x.
	Обеспечение работы Web-сервера	CentOSv6.x.
	Обеспечение работы сервера приложений	CentOSv6.x.

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

Изм.	Лист	№ документа	Подпись	Дата	Руководство системного администратора	Лист
						6

Тип	Назначение	Наименование
СУБД	Хранилище данных	Postgres Pro Standard 10.5.3
Web-сервер	Обеспечение доступа пользователей к внешнему интерфейсу Системы посредством WEB-интерфейса	Tomcat v.8.0.32
Сервер приложений	Обеспечение функционирования внутреннего интерфейса Системы	Tomcat v.8.0.32
Шина взаимодействия	Обеспечение взаимодействия между компонентами Системы	RabbitMQ v.3.6.10

Технологии, используемые при создании Системы:

- Spring Framework — универсальный фреймворк с открытым исходным кодом для Java-платформы. (www.springsource.org/)
- Vaadin – открытый набор библиотек для создания RIA веб-приложений (<https://vaadin.com/>).
- Junit – библиотека для модульного тестирования программного обеспечения на языке Java. (junit.org/)
- Spring MVC — фреймворк для разработки приложений в соответствии с шаблоном проектирования Model-view-controller. (www.springsource.org/)
- Spring Security - фреймворк, предоставляющий механизмы построения систем аутентификации и авторизации, а также другие возможности обеспечения безопасности и отказоустойчивости. (docs.spring.io/spring-security/)
- RabbitMQ - платформа, реализующая систему обмена сообщениями между компонентами программной системы (<http://www.rabbitmq.com/>) на основе стандарта AMQP

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

						<i>Руководство системного администратора</i>	<i>Лист</i>
							7
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>			

2.3. Описание модулей Системы

1. Модуль управления ЖЦ МВ-сообщений;
2. Модуль взаимодействия с внешними ИС;
3. Модуль контроля МВ-сообщений;
4. Подсистема мониторинга;
5. Модуль (подсистема) ЭП;
6. Модуль (подсистема) журналирования;
7. Модуль администрирования и управления;
8. Модуль хранения данных.

Модуль управления ЖЦ МВ-сообщений

Модуль управления жизненным циклом МВ-сообщений обеспечивает жизненный цикл электронного сообщения в Системе (смена статуса, запуск процесса обработки электронного сообщения), формирование очереди электронных сообщений, формирование подтверждений о доставке сообщений и иных служебных сообщений, запуск процесса опроса внешней очереди электронных сообщений (опрос очереди Потребителя данных ЕСМЭВ с целью получения ответа).

Модуль определяет получателя данных. На основании данных, переданных в запросе, определяется вид запрашиваемых сведений, затем на основании вида сведений определяется, какому Поставщику должен быть направлен запрос.

Процесс опроса очередей в ЕСМЭВ обеспечивает возможность регулирования и соблюдение ограничения на частоту опроса очередей, определенные в МР версии 3.

Модуль взаимодействия с внешними ИС

Модуль взаимодействия с внешними ИС обеспечивает обмен данными с ИС и с ЕСМЭВ. Модуль включает в себя:

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					<i>Руководство системного администратора</i>	Лист
						8
Изм.	Лист	№ документа	Подпись	Дата		

- электронный сервис, предоставляющий ИС методы для передачи и получения электронных сообщений, для управления жизненным циклом электронного сообщения, для получения статусов взаимодействия и статистики;
- FTP-сервер для передачи и получения вложений;
- функции, обеспечивающие обмен данными с ЕСМЭВ.

Модуль контроля МВ-сообщений

Модуль контроля МВ-сообщений обеспечивает целостность и непротиворечивость данных передаваемых Участниками МВ взаимодействия.

Модуль обеспечивает:

- Идентификацию ИС Участника;
- Идентификацию вида сведения;
- Проверку прав доступа ИС Участника;
- Форматно-логический контроль и проверка соответствия формату видов сведений;
- Проверка наличия вложенных файлов в соответствии со списком вложений.

Подсистема мониторинга

Подсистема мониторинга обеспечивает централизованный мониторинг за состоянием информационных компонентов Системы, а также уведомление ответственных лиц при наступлении критических событий.

Подсистема обеспечивает следующие функции прикладного мониторинга:

мониторинг наличия в очереди доставки ответов потребителей Системы в ЕСМЭВ ожидаемых ответов на запросы в разрезе ВС и поставщиков сведений;
анализ кода ошибок и предупреждений в логах межведомственного взаимодействия и отправка уведомлений ответственному лицу на e-mail.

Модуль (подсистема) ЭП

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					<i>Руководство системного администратора</i>	Лист
						9
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>		

Модуль обеспечивает:

- проверка всех ЭП, содержащихся в электронных сообщениях и во вложениях: ЭП-СП, ЭП-ОВ, ЭП-СМЭВ;
- проверку наличия ЭП-СП и ЭП-ОВ в электронных сообщениях;
- контроль целостности передаваемых электронных сообщений;
- проверку аутентичности отправителя электронного сообщения;
- проверку срока действия сертификата ЭП;
- проверку сертификата ЭП на отозванность;
- возможность простановки ЭП-ОВ в электронных сообщениях.

Модуль (подсистема) журналирования

Модуль журналирования обеспечивает централизованный сбор информации о событиях в системе, в том числе о движении МВ сообщений по ЖЦ.

Модуль администрирования и управления

Модуль администрирования осуществляет, в том числе:

- регистрацию сведений в реестре сведений, разработанных в соответствии с МР версии 3;
- осуществление настроек опроса статуса по сведениям;
- управление доступом к сведениям (настройка матрицы доступа);
- отображение процессов/событий в реальном масштабе времени;
- поиск, отбор и анализ информации о работе системы и прохождению электронных сообщений, имеющейся в модуле хранения данных;
- формирование статистики по информации, имеющейся в модуле хранения данных.

Модуль хранения данных

Модуль хранения данных обеспечивает доступ (запись, чтение,

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					Руководство системного администратора	Лист
Изм.	Лист	№ документа	Подпись	Дата		10

модификация, удаление данных) к БД Системы, журналирование состояния Системы, всех событий в Системе, всех событий жизненного цикла электронного сообщения, результаты выполнения модулями Системы функций по обработке электронных сообщений, регистрацию всех действий администратора, просмотр состояния всех событий в режиме реального времени, а также обеспечивать механизм формирования статистики по передаваемым электронным сообщениям, включающий в себя следующие функции:

- парсинг электронных сообщений и сохранение значимой информации;
- просмотр журнала событий;
- формирование статистики по жизненному циклу электронных сообщений (соответствие запросов и ответов, количество циклов опроса очереди, успешность/не успешность доставки электронных сообщений с учетом кодов ошибок);
- хранение экземпляров электронных сообщений (XML файлов) в файловом хранилище,
- хранение файлов вложений электронных сообщений, в том числе и файлов ЭП.

Име. № подл.	
Подпись и дата	
Взам. инв. №	
Име. № дубл.	
Подпись и дата	

					<i>Руководство системного администратора</i>	<i>Лист</i>
						11
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>		

3. Установка

3.1. Порядок установки системы

Установка программного обеспечения на сервера должна проходить в следующем порядке:

1. СУБД Postgres Pro Standard;
2. Сервер приложений Tomcat;
3. RabbitMQ.

3.2. Установка СУБД Postgres Pro Standard

Установка сервера баз данных производится на операционную систему Centos 6 - x86-64.

Находясь под учётной записью суперпользователя (*root*) в консоли *shell*, нужно установить пакет, добавляющий в *yum* - менеджер RPM-пакетов - репозиторий, содержащий самые свежие версии Postgres Pro Standard

После этого можно использовать *yum* для установки и обновления Postgres Pro Standard.

В процессе установки возможна автоматическая загрузка дополнительного ПО, требуемого для работы Postgres Pro Standard.

После установки сервера БД необходимо запустить процесс первичной инициализации структуры каталогов для хранения файлов баз данных.

Далее нужно настроить автоматический запуск сервера Postgres Pro Standard при старте операционной системы.

Управление сервером (запуск/остановка/перечитывание конфигурационных файлов и т.п.) производится штатными средствами ОС:

service <service_name> start/stop/restart/reload/ ... ,

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					Руководство системного администратора	Лист
						13
Изм.	Лист	№ документа	Подпись	Дата		

команда *service <service_name>* выводит список доступных управляющих команд.

При установке Postgres Pro Standard автоматически создается пользователь системы с именем *postgres*. Домашний каталог пользователя *postgres* находится в */var/lib/pgsql*. В этом каталоге по умолчанию хранятся конфигурационные файлы сервера Postgres Pro Standard, файлы БД, содержащие данные, файлы журналов.

После установки сервер принимает соединения только с локальных адресов. Чтобы сервер мог принимать внешние соединения на всех интерфейсах, необходимо изменить параметр *listen_addresses* в файле */var/lib/pgsql/.../data/postgresql.conf*:

```
listen_addresses = '*'
```

Для того, чтобы сервер Postgres Pro Standard воспринял данную настройку, его необходимо перезапустить:

```
service <service_name> restart
```

По умолчанию Postgres Pro Standard резервирует малый объем памяти для операций сортировки и группировки данных и переходит к использованию временных файлов даже при незначительном увеличении количества обрабатываемых записей. Это приводит к серьезному увеличению нагрузки на дисковую подсистему и снижению быстродействия. Чтобы увеличить объем резервируемой памяти, нужно в файле */var/lib/pgsql/.../data/postgresql.conf* найти строку с параметром *work_mem = 1MB*, раскомментировать ее и увеличить значение до 32 МБ:

```
work_mem = 32MB
```

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					Руководство системного администратора	Лист
						14
Изм.	Лист	№ документа	Подпись	Дата		

Чтобы применить данные изменения нужно выполнить команду подгрузки конфигурационных файлов:

```
service <service_name> reload
```

Настройку объема используемой памяти можно совместить с изменением настройки адресов для приема соединений. В этом случае для применения настроек нужно выполнить перезапуск сервера Postgres Pro Standard командой *service <service_name> restart*, а команду подгрузки файлов конфигурации *service <service_name> reload* выполнять не нужно.

Для дальнейшего развёртывания базы данных нужно дать разрешение на подключение к СУБД с локального адреса с аутентификацией по логину/паролю.

Разрешение/запрещение доступа пользователей к БД настраивается путём редактирования файла */var/lib/pgsql/.../data/pg_hba.conf*.

Необходимо изменить метод аутентификации с *ident* на *md5* в двух строках, отвечающих за доступ с локальных адресов:

```
host all all 127.0.0.1/32 ident
host all all ::1/128 ident
```

нужно изменить на:

```
host all all 127.0.0.1/32 md5
host all all ::1/128 md5
```

Чтобы применить данные изменения нужно выполнить команду:

```
service <service_name> reload
```

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	Руководство системного администратора	Лист
						15

Пользователю *postgres*, созданному в процессе установки Postgres Pro Standard, автоматически назначаются права суперпользователя БД.

Один из способов воспользоваться этими правами - зайти под учётной записью администратора системы *root* и переключиться на пользователя *postgres* командой:

```
su - postgres
```

После этого нужно распаковать архив, соответствующий модулю системы, *smev_<имя_модуля>_db_deploy.tgz* с файлами скриптов, содержащими команды:

- создания пользователя БД, под которым будет работать Система;
- создания полной структуры таблиц БД;
- команды для наполнения данными таблиц настроек, таблиц словарей и справочников.

После разархивирования всех файлов командой:

```
tar -xvzfsmev_<имя_модуля>_db_deploy.tgz
```

нужно запустить shell-скрипт *smev_db_deploy.sh*, который создаст пользователя БД, полную начальную структуру БД и заведет в Системе пользователя с правами Системного Администратора.

3.3. Установка Tomcat

Для настройки Tomcat необходимо создать каталог */usr/java*:

```
# mkdir /usr/java
```

1. Перейти в каталог */usr/java*:

```
# cd /usr/java
```

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					Руководство системного администратора	Лист
						16
Изм.	Лист	№ документа	Подпись	Дата		

2. Скопировать файл с JDK в каталог */usr/java*:

```
# cp ~/jdk-8u66-linux-x64.tar.gz ./
```

3. Распаковать содержимое архива сJDK в каталог */usr/java*

```
# tar -xvzfjdk-8u66-linux-x64.tar.gz
```

4. Скачать разрешительные политики криптографии для Java) и установить в */usr/java/jdk-8u66-linux-x64/jre/lib/security/*

5. Скачать Tomcat 8 с сайта Tomcat в формате *tar.gz* в домашний каталог:
<http://tomcat.apache.org/download-80.cgi>.

6. Перейти в каталог */usr/share*:

```
# cd /usr/share
```

7. Скопировать архив с Tomcat в каталог */usr/share*:

```
# cp ~/apache-tomcat-8.0.28.tar.gz ./
```

8. Распаковать содержимое архива с Tomcat в каталог */usr/share*:

```
# tar -xvzf apache-tomcat-8.0.28.tar.gz
```

9. Перейти в каталог */etc/init.d*:

```
# cd /etc/init.d
```

10. Создать файл *tomcat* в каталоге */etc/init.d*:

Ине. № подл.	Подпись и дата
Взам. инв. №	Ине. № дубл.
Подпись и дата	

Изм.	Лист	№ документа	Подпись	Дата	Руководство системного администратора	Лист
						17

vim tomcat

11. В файл /etc/init.d/tomcat записать конфигурацию:

#!/bin/bash

description: Tomcat Start Stop Restart

processname: tomcat

chkconfig: 234 20 80

JAVA_HOME=/usr/java/jdk1.8.0_66

export JAVA_HOME

PATH=\$JAVA_HOME/bin:\$PATH

export PATH

CATALINA_HOME=/usr/share/apache-tomcat-8.0.32

case \$1 in

start)

sh \$CATALINA_HOME/bin/startup.sh

;;

stop)

sh \$CATALINA_HOME/bin/shutdown.sh

;;

restart)

sh \$CATALINA_HOME/bin/shutdown.sh

sh \$CATALINA_HOME/bin/startup.sh

;;

esac

exit 0

12. Изменить порты по умолчанию для Tomcat:

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	Подпись и дата
Изм.	Лист
№ документа	Подпись
Дата	Дата

4. Установить RabbitMQ командой «rpm -Uvh rabbitmq-server-3.6.10-1.noarch.rpm»
5. Запустить RabbitMQ : service rabbitmq-server start

3.5. Сервер приложений и WEB-сервер Системы

Дистрибутивы сервера приложений и WEB-сервера Системы представляют из себя архивы (файлы .war), которые копируются в каталог */usr/share/apache-tomcat-8.0.32/webapps* и разворачиваются автоматически при запуске Системы.

В случае если архив приложения больше 50MB необходимо в файле */usr/share/apache-tomcat-8.0.32/webapps/manager/WEB-INF/web.xml* модифицировать значение переменных *max-file-size* and *max-request-size*.

Для того чтобы проверить работоспособность Системы необходимо открыв в браузере страницу:

http://имя_сервера/remote_dis/ws/stub/RegionalMessageExchangeService?wsdl

при этом должно загрузиться описание функций Системы в формате wsd1.

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	<i>Руководство системного администратора</i>	Лист
						20

4. Операции по обслуживанию

4.1. Процедура останова Системы

Для останова Системы необходимо выполнить последовательно следующие действия:

1. Остановить WEB-сервер.
2. Остановить сервер приложений
3. Остановить СУБД.

Остановка WEB-сервера Системы.

1) Войти в консоль ОС сервера, на котором расположен WEB-сервер Системы с помощью ssh-клиента (например, Putty).

2) Остановить Tomcat: выполнить в консоли следующую команду:

servicetomcatstop

3) Проверить, корректно ли остановлен сервер:

psaux | grepjava

Если в выводе команды будет запись вида

```
root 20151 0.0 11.2 5608164 1855448 ? Sl Dec18 2:19 /usr/bin/java -
Djava.util.logging.config.file=/usr/share/apache-tomcat-
7.0.47/conf/logging.properties -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -
Dfile.encoding=UTF8 -Djava.endorsed.dirs=/usr/share/apache-tomcat-
7.0.47/endorsed -classpath /usr/share/apache-tomcat-
7.0.47/bin/bootstrap.jar:/usr/share/apache-tomcat-7.0.47/bin/tomcat-juli.jar -
Dcatalina.base=/usr/share/apache-tomcat-7.0.47 -
Dcatalina.home=/usr/share/apache-tomcat-7.0.47 -
Djava.io.tmpdir=/usr/share/apache-tomcat-7.0.47/temp
org.apache.catalina.startup.Bootstrap start
```

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

Изм.	Лист	№ документа	Подпись	Дата
------	------	-------------	---------	------

Руководство системного администратора

Лист

21

то остановить процесс командой kill:

kill 20151

где вместо 20151 подставить PID процесса (второе значение в выводе записи о процессе)

Остановка Сервера приложений Системы.

1) Войти в консоль ОС сервера, на котором расположен сервер приложений Системы, с помощью ssh-клиента (например, Putty).

2) Остановить Tomcat: выполнить в консоли следующую команду:

servicetomcatstop

3) Проверить, корректно ли остановлен сервер:

psaux | grepjava

Если в выводе команды будет запись вида

```
root 20151 0.0 11.2 5608164 1855448 ? Sl Dec18 2:19 /usr/bin/java -
Djava.util.logging.config.file=/usr/share/apache-tomcat-
7.0.47/conf/logging.properties -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -
Dfile.encoding=UTF8 -Djava.endorsed.dirs=/usr/share/apache-tomcat-
7.0.47/endorsed -classpath /usr/share/apache-tomcat-
7.0.47/bin/bootstrap.jar:/usr/share/apache-tomcat-7.0.47/bin/tomcat-juli.jar -
Dcatalina.base=/usr/share/apache-tomcat-7.0.47 -
Dcatalina.home=/usr/share/apache-tomcat-7.0.47 -
Djava.io.tmpdir=/usr/share/apache-tomcat-7.0.47/temp
org.apache.catalina.startup.Bootstrap start
```

то остановить процесс командой kill:

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

Изм.	Лист	№ документа	Подпись	Дата

Руководство системного администратора

Лист

22

kill 20151

где вместо 20151 подставить PID процесса (второе значение в выводе записи о процессе)

Остановка сервера СУБД

1. Войти в консоль ОС сервера, на котором расположен сервер СУБД Системы с помощью ssh-клиента (например, Putty).
2. Остановка Postgres Pro Standard:
Service <service_name> stop

4.2 Порядок запуска Системы

Порядок запуска Системы определен следующей последовательностью:

1. Запустить СУБД.
2. Запустить Сервер приложений Системы.
3. Запустить WEB-сервер Системы.

Запуск СУБД Системы.

1. Войти в консоль ОС сервера, на котором расположен сервер СУБД Системы, с помощью ssh-клиента (например, Putty).
2. Остановка Postgres Pro Standard:
Service <service_name> start

Запуск Сервера приложений Системы.

- 1) Войти в консоль ОС сервера, на котором расположен сервер приложений Системы с помощью ssh-клиента (например, Putty).
- 2) Запустить Tomcat: выполнить в консоли следующую команду
Service tomcat start

Запуск WEB-сервера Системы.

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					<i>Руководство системного администратора</i>	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>		23

- 1) Войти в консоль ОС сервера, на котором расположен сервер приложений Системы с помощью ssh-клиента (например, Putty).
- 2) Запустить Tomcat: выполнить в консоли следующую команду:
Service tomcat start

4.3. Обслуживание

Обслуживание включает в себя процесс мониторинга и диагностирования состояния Системы. При диагностировании могут помочь следующие файлы:

1. На всех серверах вывод сообщений для отладки и исключений производится в файл java.log.html
2. На серверах, работающих с БД (ЖЦ, контроль, словари и справочники, лог, модуль подписи) работа с БД описывается файлом jdbc.log.txt
3. На серверах с модулем взаимодействия с внешними системами логирование входящих/исходящих сообщений ведется в файле network.log.html

Все вышеперечисленные логи находятся в папке logs расположения Tomcat. Ротация файлов происходит раз в сутки.

4.4. Резервное копирование

Для обеспечения сохранности данных Системы требуется осуществлять резервное копирование баз данных сервера СУБД.

Для резервного копирования данных используется программа pg_dumpall, входящая в состав дистрибутива Postgres Pro Standard. pg_dumpall выполняет резервную копию всех баз данных сервера, включая роли (пользователей БД) и табличные пространства.

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					<i>Руководство системного администратора</i>	<i>Лист</i>
						24
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>		

Запуск программы `pg_dumpall` можно осуществлять как из командной строки консоли сервера, так и из командной строки удаленной рабочей станции, способной подключиться к серверу БД по протоколу TCP/IP.

Для запуска `pg_dumpall` из командной строки на сервере нужно зайти в операционную систему сервера под учётной записью пользователя `postgres` и в командной строке выполнить следующую команду:

`pg_dumpall > path_to_dump_file_name_N`

где `path_to_dump_file_name_N` – полный путь к файлу, в который будет записан дамп (N – номер дня недели от 1 до 7: 1 – понедельник, 7 – воскресенье).

Для возможности запуска `pg_dumpall` с рабочей станции необходимо разрешить доступ пользователю `postgres` ко всем базам данных при подключении к серверу БД с рабочей станции.

Доступ обеспечивается добавлением строки в файл `/var/lib/pgsql/9.4/data/pg_hba.conf` на сервере БД:

`host all postgres xxx.xxx.xxx.xxx/32 md5`

где `xxx.xxx.xxx.xxx` – ip-адрес рабочей станции.

На рабочей станции должен быть установлен дистрибутив Postgres Pro Standard версии не ниже той, что установлена на сервере БД.

Запуск программы `pg_dumpall` на рабочей станции осуществляется из командной строки следующей командой:

`pg_dumpall -h xxx.xxx.xxx.xxx -U postgres > path_to_dump_file_name_N`

где `xxx.xxx.xxx.xxx` – ip-адрес или доменное имя сервера БД, `postgres` – имя пользователя, имеющего доступ ко всем объектам всех баз данных (суперпользователь), `path_to_dump_file_name_N` – полный путь к файлу на рабочей станции, в который будет записан дамп (N – номер дня недели от 1 до 7: 1 – понедельник, 7 – воскресенье).

Во время работы `pg_dumpall` будет запрашивать пароль пользователя `postgres` отдельно для каждой базы данных, имеющейся на сервере. Чтобы

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					Руководство системного администратора	Лист
						25
Изм.	Лист	№ документа	Подпись	Дата		

автоматизировать ввод пароля, нужно в файл `~/.pgpass` (`%appdata%\postgresql\pgpass.conf` в ОС семейства MS Windows), находящийся в домашнем каталоге пользователя, под которым произведен вход в операционную систему рабочей станции, добавить строку:

```
xxx.xxx.xxx.xxx:5432:*:postgres:<password>
```

где `xxx.xxx.xxx.xxx` – ip-адрес или доменное имя сервера БД, `postgres`– имя пользователя, имеющего доступ ко всем объектам всех баз данных (суперпользователь), `<password>`– пароль пользователя postgres сервера Postgres Pro Standard.

Данные сохраняются в виде текстовых файлов, содержащих команды SQL и пригодных для последующего чтения программой `psql`.

Для настройки автоматического запуска процедуры резервного копирования на сервере БД можно использовать программу `cron`. Чтобы обеспечить запуск программы `pg_dumpall` ежедневно в 2 часа ночи от имени пользователя `postgres`, в файл `/etc/crontab` нужно добавить следующие строки:

```
0 2 * * 2 postgres pg_dumpall > path_to_dump_file_name_1
0 2 * * 3 postgres pg_dumpall > path_to_dump_file_name_2
0 2 * * 4 postgres pg_dumpall > path_to_dump_file_name_3
0 2 * * 5 postgres pg_dumpall > path_to_dump_file_name_4
0 2 * * 6 postgres pg_dumpall > path_to_dump_file_name_5
0 2 * * 0 postgres pg_dumpall > path_to_dump_file_name_6
0 2 * * 1 postgres pg_dumpall > path_to_dump_file_name_7
```

Требуется обеспечить восстановление состояния базы данных на любой момент времени за последнюю неделю. Этого можно добиться при ежедневном полном копировании всех баз данных. Потребуется хранить 7 последних копий.

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	Руководство системного администратора	Лист
						26

4.5 Восстановление данных из резервной копии

Для восстановления данных нужен сервер с развернутым дистрибутивом Postgres Pro Standard.

Для восстановления данных из резервной копии используется программа `psql`, входящая в состав дистрибутива Postgres Pro Standard.

Для запуска `psql` нужно зайти в операционную систему сервера под учётной записью пользователя `postgres` и в командной строке выполнить следующую команду:

```
psql -f path_to_dump_file_name_N postgres
```

где `postgres` – имя системной базы данных, которая создается автоматически при разворачивании сервера Postgres Pro Standard,
`path_to_dump_file_name_N`– полный путь к файлу, содержащему дамп, созданный программой `pg_dumpall`.

4.6. Обновление программного обеспечения

Обновление программного обеспечения выполняется для расширения функциональных возможностей Системы или устранения ошибок.

Обновление может выполняться в штатном и внеплановом (экстренном) режиме.

Перед проведением обновления в штатном режиме системному администратору необходимо:

1. Уведомить должностное лицо, ответственное за функционирование системы в целом (и, в частности, за принятие решения об останове системы и проведении ее обновления) и получить соответствующее разрешение.

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					Руководство системного администратора	Лист
						27
Изм.	Лист	№ документа	Подпись	Дата		

Уведомление должно включать следующие сведения (план обновления):

- Причина обновления
- Перечень изменений, вносимых в систему
- Интервал времени, в течение которого система будет недоступна.

Уведомление направляется по электронной почте не менее чем за 16 рабочих часов до планируемого обновления.

Разрешение или отказ в проведении обновления направляется должностным лицом системному администратору по электронной почте не менее чем за 8 рабочих часов до планируемого обновления.

Если в указанное время ответ должностного лица не получен, то это рассматривается в качестве положительного решения.

2. После согласования (получения разрешения) уведомить всех пользователей системы о планируемом обновлении.

Уведомление направляется пользователям посредством размещения новости в соответствующем модуле Системы не менее чем за 8 рабочих часов до планируемого обновления.

Уведомление пользователей должно включать сведения, указанные в п.1.

Перед проведением внепланового (экстренного) обновления системному администратору необходимо уведомить должностное лицо и получить соответствующее разрешение.

Уведомление должно включать следующие сведения (план обновления):

- Причина обновления
- Перечень изменений, вносимых в систему

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					<i>Руководство системного администратора</i>	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>		28

- Интервал времени, в течение которого система будет недоступна.

Уведомление и разрешение (либо отказ) могут быть направлены должностному лицу в произвольной форме (лично, телефон, почта и пр.) непосредственно перед обновлением.

Уведомление пользователей об обновлении не требуется.

После проведения обновления администратору системы необходимо:

1. Уведомить должностное лицо о завершении обновления. Уведомление должно включать следующие сведения:

- Перечень изменений, внесенных в систему
- Интервал времени, в течение которого система была недоступна
- Отклонения от плана обновления.

Уведомление направляется по электронной почте не позднее чем через 8 рабочих часов после обновления.

2. Уведомить всех пользователей системы об изменениях системы. Уведомление направляется пользователям посредством размещения новости в соответствующем модуле Системы не позднее чем через 8 рабочих часов после обновления. Уведомление пользователей должно включать информацию о перечне изменений.

Обновление в штатном режиме должно проводиться в нерабочее время.

Под обновлением программного обеспечения подразумевается обновление следующих программных компонентов:

- Обновление сервера приложения системы
- Обновление WEB-сервера
- Обновление базы данных Системы

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	<i>Руководство системного администратора</i>	Лист
						29

4.7. Мониторинг работоспособности Системы

В Системе применяются следующие методы мониторинга работоспособности Системы:

- Автоматическое информирование уполномоченных лиц о состоянии Системы посредством подсистемы мониторинга.
- Использование интерфейса подсистемы мониторинга.
- Анализ лог-файлов Системы.

Регламент проведения процедуры мониторинга:

1. Ежедневное изучение показателей Системы с использованием интерфейса подсистемы мониторинга.
2. При обнаружении роста значений показателей Системы необходимо проинформировать разработчиков системы и согласовать процедуры улучшения работоспособности Системы.
3. Анализ лог-файла Системы, созданного за предыдущий рабочий день.
4. При наличии критических ошибок в лог файлах (приоритет записи ERROR, FATAL), необходимо проинформировать разработчиков системы, вылав по электронной почте соответствующий фрагмент лог-файла.

Интерфейс подсистемы мониторинга.

Подсистема мониторинга представляет собой решение распределенного мониторинга корпоративного класса с открытыми исходными кодами. Является программным обеспечением для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. Zabbix использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления, основанные на email, практически для любого события. Это позволяет быстро реагировать на проблемы с серверами. Система предлагает функции отчетности и визуализации данных, основанные на данных истории.

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					Руководство системного администратора	Лист
						30
Изм.	Лист	№ документа	Подпись	Дата		

Все отчеты и статистика, формируемые системой мониторинга, доступны через WEB-интерфейс.

Инструкция на русском языке представлена по адресу: <https://www.zabbix.com/documentation/ru/2.0>.

В частности, информацию по настройке оповещений в системе мониторинга можно найти по ссылке:

<https://www.zabbix.com/documentation/ru/2.0/manual/config/notifications>.

Подсистема логирования.

Подсистема логирования обеспечивает:

1. Создание и хранения информации о технологических ошибках, происходящих в Системе.
2. Логирование событий изменений настроек Системы и редактирования нормативно-справочной информации.
3. Формирование журнала событий, позволяющих идентифицировать их по дате и времени, отправителю, получателю, типу событий и пользователю.
4. Предоставление интерфейса взаимодействия с подсистемой мониторинга.

Лог системы

В Системе формируются лог-файлы, предназначенные для разработчиков системы и системного администратора.

В системных логах предусмотрено 6 уровней приоритета событий (по возрастанию приоритета):

- TRACE - наиболее полная информация, трассировка выполнения программы.
- DEBUG - детальная информация для отладки.
- INFO – информация о выполнении действий.

Подпись и дата
Инв. № дубл.
Взам. инв. №
Подпись и дата
Инв. № подл.

					<i>Руководство системного администратора</i>	Лист
Изм.	Лист	№ документа	Подпись	Дата		31

- WARN – предупреждение.
- ERROR - в программе произошла ошибка.
- FATAL - произошла фатальная ошибка.

Логирование ведется в формате HTML, при этом формируется общий лог для всех событий системы, уровень которых WARN и выше.

Логи формируются в режиме dailyrolling – каждый день создается новый файл лога, при этом файл за предыдущий день переименовывается следующим образом: к имени файла добавляется суффикс в формате ГГГГ-ММ-ДД.html, где ГГГГ – это год в четырехзначном формате, ММ – порядковый номер месяца, ДД – число в месяце.

В лог-файлах содержится следующая информация:

- Дата и время события
- Поток, в котором возникло данное событие
- Уровень события
- Java-пакет, в котором произошло данное событие
- Сообщение, описывающее событие.

Лог файлы расположены на сервере приложений Системы в каталоге:
/usr/share/apache

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	

Изм.	Лист	№ документа	Подпись	Дата	Руководство системного администратора	Лист
						32