ЕДИНАЯ ЗАЩИЩЕННАЯ МОБИЛЬНАЯ ПЛАТФОРМА: ЦЕНТР МОБИЛЬНЫХ СЕРВИСОВ

ОБЩЕЕ ОПИСАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Тюмень, 2016г.

Оглавление

Список терминов и сокращений

№	Термин или сокращение	Определение
1	ЕЗМП, ЕЗМП: ЦМС	Программный комплекс «Единая защищенная мобильная платформа: центр мобильных сервисов»
2	СПО	Свободно распространяемое программное обеспечение
3	ИС	Информационная система
4	БД	База данных
5	ПО	Программное обеспечение
6	СМЭВ	Система межведомственного электронного взаимодействия
7	ЕСИА	Единая система идентификации и аутентификации
8	SOAP	Протокол обмена структурированными сообщениями в распределённой вычислительной среде
9	REST	Архитектурный стиль взаимодействия компонентов распределённого приложения в сети
10	USSD	стандартный сервис в сетях GSM, позволяющий организовать интерактивное взаимодействие между абонентом сети и сервисным приложением в режиме передачи коротких сообщений

Назначение документа

Настоящий документ описывает назначение, функциональные характеристики и архитектуру программного комплекса ЕЗМП:ЦМС (Единая защищенная мобильная платформа: центр мобильных сервисов), а также информацию, необходимую для установки и эксплуатации.

Документ содержит описание модулей системы ЕЗМП и схемы взаимодействия модулей.

Общее описание и функциональные характеристики ПО

ЕЗМП представляет собой программный комплекс, построенный на базе свободно распространяемого программного обеспечения и обладающий следующими функциональными характеристиками:

1. Подключение к платформе сторонних отраслевых информационных систем (веб-сервисов), в том числе систем с ограниченным доступом, и их публикация во внешнюю сеть;
2. Разработка прикладных информационных систем (ИС) на базе Платформы:
   - единая технологическая платформа для разработки серверных компонентов различных мобильных приложений;
   - возможность интеграции со сторонними информационными системами;
3. Подключение к платформе стороннего программного обеспечения (ПО), являющегося потребителем для опубликованных веб-сервисов: ретрансляция коммуникаций между клиентским ПО и сторонней прикладной информационной системой. В качестве клиентского ПО могут выступать мобильные приложения, веб-приложения, сторонние информационные системы;

4. Технологическая независимость подключаемых веб-сервисов и клиентского ПО от архитектуры самой платформы. Для подключенных компонентов (веб-сервисов и клиентского ПО), а так же разработанных на базе ЕЗМП прикладных ИС сохраняется возможность их модификации и взаимной адаптации при:
   - изменении состава автоматизируемых функций прикладной ИС и внешнего интегрированного сервиса;
   - изменении требований к безопасности прикладной ИС и внешнего интегрированного сервиса;
   - изменении количества поставщиков информации для прикладной ИС.
5. Возможность создания единого личного кабинета для множества прикладных ИС и мобильных приложений. Платформой обеспечиваются следующие механизмы:
   - единая регистрация и аутентификация пользователей;
   - рассылка и восстановление паролей через СМС;
   - ведение единой базы учетных записей и ролей, предоставление механизмов управления ими;
   - единый инструментарий для оповещения пользователей клиентского ПО и обратной связи;
6. Встроенные механизмы администрирования для каждого компонента Платформы;
7. Журналирование коммуникаций между клиентским ПО и подключенными веб-сервисами;
8. Контроль доступа для клиентского ПО и управление правами пользователей;
9. Онлайн мониторинг состояния системы;

ЕЗМП позволяет объединить в единое информационное пространство существующие информационные системы (ИС) и базы данных (БД). Что может обеспечить:

- Снижение стоимость разработки и сопровождения ИС за счет использования ранее разработанных модулей и стандартизации процессов разработки программного обеспечения (ПО);
- Создать благоприятный климат для разработчиков ПО за счет возможности безопасного доступа к государственным сервисам;
- Увеличить объем услуг, оказываемых в электронном виде за счет повышения уровня сервиса и использования современных технологий мотивации (акции, бонусы, геймификация и т.п.)

Архитектура системы

Основными субъектами систем, построенных на базе ЕЗМП являются:

- Поставщик услуги — произвольная информационная система, имеющая внешний интерфейс в виде веб-сервиса SOAP либо REST API;
- Потребитель услуги (клиентское ПО) — любое программное обеспечение, реализующее клиентский интерфейс для взаимодействия с веб-сервисом поставщика услуги;
- Платформа ЕЗМП — специализированное программное обеспечение, организующее трансляцию запросов и контроль взаимодействия потребителя и поставщика услуги.

Схематично архитектура решений на базе ЕЗМП представлена на рисунке 1. На верхнем уровне решений, построенных на базе ЕЗМП, находятся поставщики и потребители услуг:

- Веб-порталы и приложения (в т.ч. мобильные).
- Отраслевые информационные системы и базы данных.
- Сервисы СМЭВ (ЕСИА и др.)
- SMS-, USSD-, платежные шлюзы и т.п.

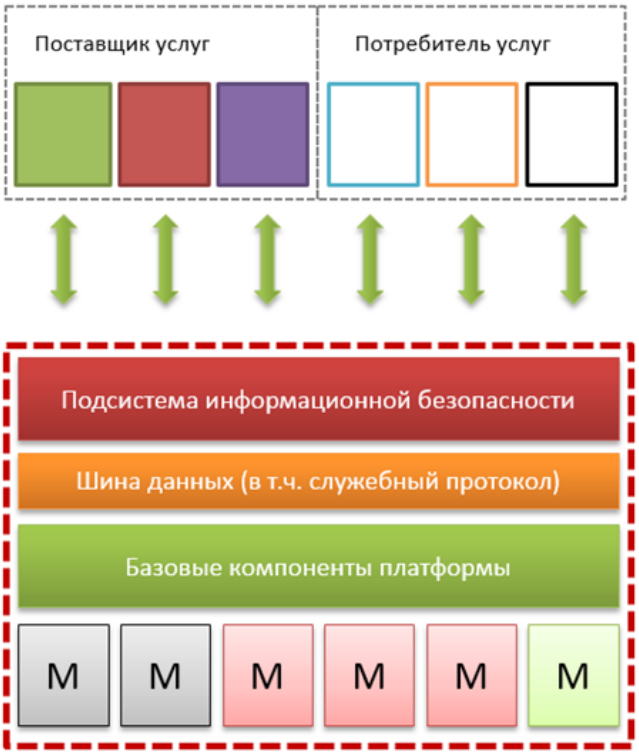


Рисунок 1. Архитектура решений на базе ЕЗМП

Взаимодействие потребителей и поставщиков осуществляется посредством веб-сервисов через посредника — ЕЗМП.

Компоненты, входящие в состав ядра платформы ЕЗМП, обеспечивают организацию безопасного взаимодействия веб-сервисов, предоставляемых отраслевыми информационными системами с внешними потребителями (мобильными и веб-приложениями, сторонними информационными системами).

В ядро платформы ЕЗМП входит:

- **Подсистема обмена данными** (интеграционная шина). Реализует возможность информационного взаимодействия между участниками.
- **Подсистема безопасности**. Реализует дискреционную и мандатную модель разграничения доступа потребителей услуг к веб-сервисам поставщиков, отслеживает доступность сервисов.

В состав **подсистемы базовых компонент** входит набор общих сервисов, реализующих типовой функционал для клиентских приложений:

- Веб-сервис «ЕЗМП.Паспорт» — предоставляет механизмы аутентификации и управления пользователями, группами, ролями;

- Веб-сервис «ЕЗМП.Лог» — предоставляет механизм журналирования событий;
- Веб-сервис «ЕЗМП.Обратная связь» — предоставляет механизм сбора сообщений обратной связи от конечных пользователей.

Подсистемы информационной безопасности, обмена данными и базовых компонент носят закрытый характер. Это исключает возможность внесения изменений в штатный режим работы. Подсистема функциональных модулей свободно расширяема. Функциональные модули могут создаваться, как владельцем ЕЗМП, так и сторонними разработчиками.

Схема информационного взаимодействия

Информационное взаимодействие между потребителем и поставщиком, осуществляется путем трансляции HTTP-запросов от клиентского ПО к веб-сервису поставщика через ядро ЕЗМП.

При этом возможны следующие варианты интеграции клиентских приложений с поставщиками услуг, приведенные на рис. 2.

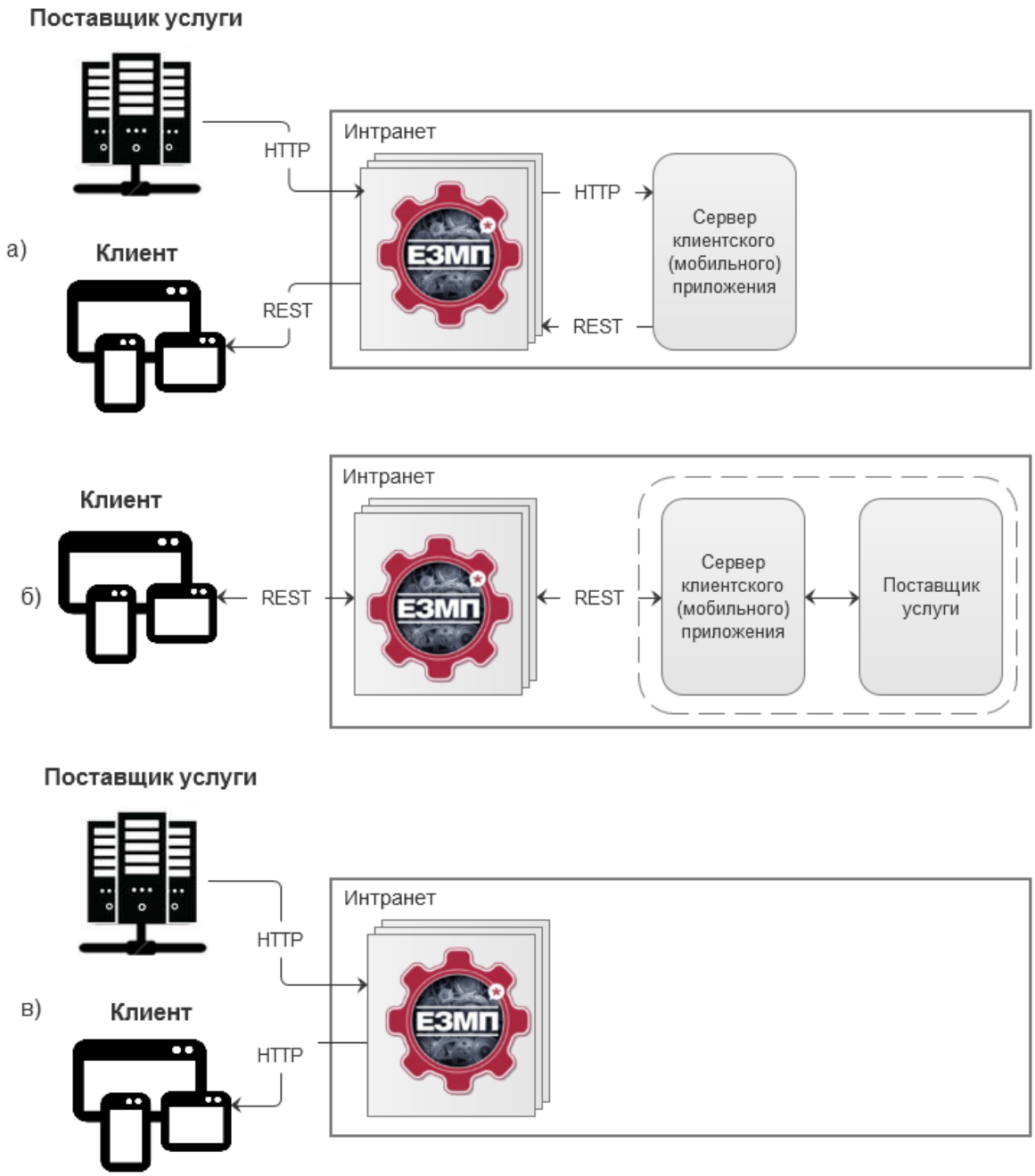


Рисунок 2. Сценарии взаимодействия с поставщиком услуг

Здесь, поставщик услуг, изображенный за пределами сети интранет, представляется как внешняя информационная система предоставляющая услугу (веб-сервис) «как есть». Это подразумевает, что какая либо адаптация или доработка такой системы не представляется возможной или не желательной. В случае необходимости интеграции с подобной системой, рекомендуется использовать сценарий «а».

Кроме трансляции запросов к поставщику, платформа ЕЗМП задействует подсистемы безопасности и базовых компонент, обеспечивающие выполнение таких типовых функций, как управление сеансами, авторизация пользователей, журналирование потоков данных и событий в клиентском ПО, контроль привилегий, контроль доступности сервисов и т.п.

Общая схема взаимодействия клиентского ПО с поставщиком выглядит следующим образом.

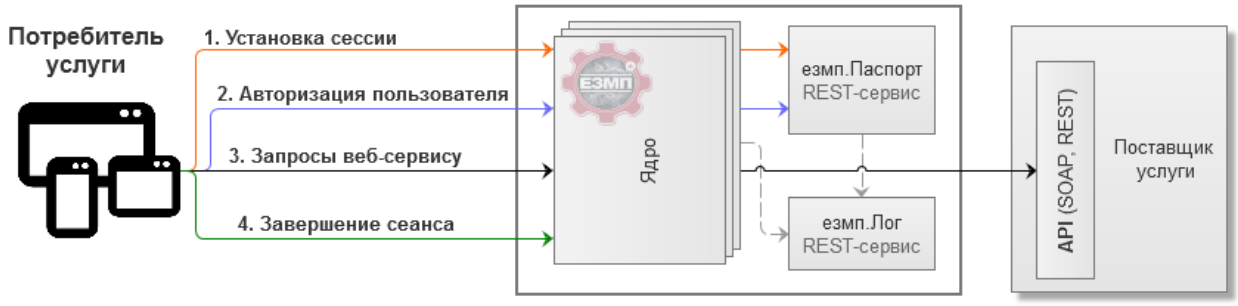


Рисунок 3. Общая схема работы клиентского приложения - потребителя услуги

Типовая схема взаимодействия компонентов системы в процессе отработки запросов между клиентом и поставщиком представлена на следующем рисунке.

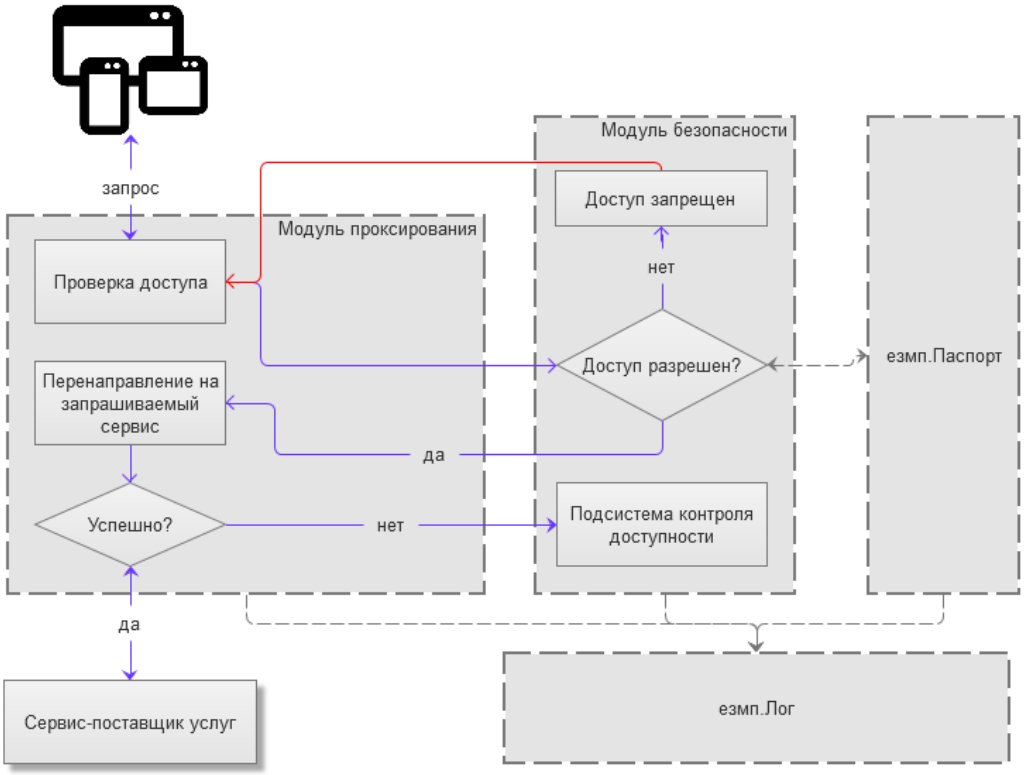


Рисунок 4. Типовая схема взаимодействия компонентов системы

Сервис аутентификации и управления пользователями «ЕЗМП.Паспорт»

ЕЗМП-Паспорт - единый сервис регистрации и авторизации для всех пользователей и программных клиентов.

К функциям ЕЗМП-Паспорта относятся:

- Осуществление аутентификации и авторизации программных клиентов и их пользователей.

- Управление политиками доступа программных клиентов и их пользователей.

Порядок развертывания и первоначальной настройки ПО

Используемое программное обеспечение

Для функционирования Системы, необходим следующий набор вспомогательного программного обеспечения:

1. Компилятор c++11;
2. СУБД MySQL\MariaDB версии не ниже 5;
3. СУБД Redis версии не ниже 3;
4. Веб-сервер с поддержкой FastCGI (например, Nginx);
5. СУБД PostgreSQL версии не ниже 9.3;
6. Сервер приложений Apache Tomcat версии не ниже 7;
7. Java SE Development Kit версии не ниже 8.

Системные требования

Система может функционировать как на операционных системах (ОС) семейства Linux (рекомендуется Debian Linux; протестировано на Debian 7.8, Ubuntu 14.04, Ubuntu 15.x), так и на ОС Windows.

Для функционирования Системы, используются следующие TCP-порты:

1. 80 — для веб-приложения;
2. 443 — для веб-приложения по защищенному протоколу SSL;
3. 5432 — для СУБД PostgreSQL;
4. 8081 — для Apache Tomcat7 JDK 8.

Установка Системы

Установка подсистемы обмена данными (ЕЗМП.Прокси)

Пакет дистрибутива модуля ЕЗМП.Прокси предварительно распаковать во временный каталог, перейти в данный каталог.

Установка предкомпилированной версии осуществляется путем запуска скрипта «install.sh».

sudo ./install.sh

Данный скрипт скопирует все требуемые файлы, и создаст каталоги, если необходимо.

По умолчанию, программа копируется в /opt/ezmp и пути к библиотекам при запуске программы прописаны как /opt/ezmp/libs.

- /var/log/ezmp/ezmp.log — основной файл лога ЕЗМП.Прокси;
- /var/log/ezmp/error.log — лог ошибок ЕЗМП.Прокси.

Для запуска, остановки и перезапуска демона используются следующие команды:

sudo systemctl start ezmp

sudo systemctl restart ezmp

sudo systemctl stop ezmp

Удаление осуществляется путем запуска скрипта «unistall.sh».

sudo ./uninstall.sh

Данный скрипт удалит все ранее скопированные файлы.

Пример установки для ОС Debian Jessie

Если была установлена минимальная версия системы, то понадобится установить стандартные пакеты.

sudo aptitude install make linux-headers-amd64 gcc

sudo aptitude install mysql-server

sudo mysql_secure_installation

sudo aptitude install redis-server

sudo aptitude install nginx

Если дистрибутив ЕЗМП.Прокси находится в каталоге «/tmp/dist»

cd /tmp/dist

sudo ./install.sh

При установке так же создается структура базы данных (БД) для ЕЗМП.Прокси, однако можно импортировать БД и вручную. SQL файл для импорта, а так же все дополнительные файлы лежат в каталоге «dist/extras».

После установки ЕЗМП.Прокси нужно отредактировать все конфигурационные файлы (redis, mysql, nginx, ezmp), если это не было сделано ранее.

Рекомендуется использовать подключение к БД и сервису «езмп» через Unix domain socket.

Подключение базы данных

Данные для подключения находятся в файле «/etc/ezmp/ezmp.ini».

Настройки MySQL осуществляются в блоке *[MySql]*, настройки Redis осуществляются в блоке *[Redis]*. Параметры настройки данных блоков были описаны выше.

База данных Redis может работать через сокет. Для этого нужно отредактировать конфигурационный файл «/etc/redis/redis.conf».

Добавить:

unixsocket /var/run/redis/redis.sock

unixsocketperm 777

Выставляем права 777 на сокет для того что бы пользователь www-data мог читать и писать в сокет.

Подключение Web-интерфейса на примере Nginx

Необходимо добавить в конфигурационный файл веб-сервера следующую настройку:

```
location / {
        include ezmp.conf;
        fastcgi_pass unix:/tmp/ezmp.sock;
}
```

Например, итоговая конфигурация может выглядеть следующим образом:

```
server {
        listen 9090 ;
        listen [::]:9090 ;
        root /var/www/html;
        index index.html index.htm index.nginx-debian.html;
        server_name _;

location / {
 fastcgi_buffers 8 4k;
 fastcgi_buffer_size 2k;
 include ezmp.conf;

 fastcgi_pass unix:/tmp/ezmp.sock;
 }
}
```

Установка базовых компонент для операционных систем семейства Linux (на примере Debian)

В процессе установки подсистемы базовых компонент (ЕЗМП.Паспорт, ЕЗМП.Лог), потребуется доступ к сети Интернет для установки необходимых пакетов.

Архив с дистрибутивом пакета базовых компонент и вспомогательным ПО необходимо предварительно поместить в папку «~/files» (папка files в домашнем каталоге текущего пользователя).

Далее необходимо выполнить следующие шаги:

1. распаковать необходимые для установки файлы в папку ~/files;
2. перейти в каталог «files» (cd ~/files);
3. Прописать следующие команды в файл install.sh.

```
#!/bin/sh
#var
ROOT_PASSWORD='cerTypul'
SCRIPT=$(readlink -f "$0")
```

```
SCRIPTPATH=$(dirname "$SCRIPT")

JDKPATH='/usr/lib/jvm'

#init

export DEBIAN_FRONTEND=noninteractive

debconf-set-selections <<< 'oracle-java8-installer shared/accepted-oracle-license-v1-1 select true'


echo "deb http://ppa.launchpad.net/webupd8team/java/ubuntu trusty main" | tee /etc/apt/sources.list.d/webupd8team-java.list

echo "deb-src http://ppa.launchpad.net/webupd8team/java/ubuntu trusty main" | tee -a /etc/apt/sources.list.d/webupd8team-java.list

apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys EEA14886

apt-get update


#install

apt-get --assume-yes install oracle-java8-installer oracle-java8-set-default \

        tomcat7 tomcat7-user \

        postgresql-9.4 postgresql-contrib pgadmin3


#configire

cp -R $SCRIPTPATH/tools/jdk1.7.0_05 $JDKPATH/

chown -R root:root $JDKPATH/jdk1.7.0_05

chmod -R 0755 $JDKPATH/jdk1.7.0_0


service tomcat7 stop

update-rc.d -f tomcat7 remove

tomcat7-instance-create -p 8081 -c 8006 /opt/tomcat7_jdk8

chown tomcat7:tomcat7 /opt/tomcat7_jdk*


ln -s /etc/tomcat7/policy.d/ /opt/tomcat7_jdk8/policy.d

ln -s /var/lib/tomcat7/conf/policy.d /opt/tomcat7_jdk8/conf/policy.d

rm /opt/tomcat7_jdk8/conf/server.xml

cp $SCRIPTPATH/conf/tomcat7_jdk8/server.xml /opt/tomcat7_jdk8/conf/

cp $SCRIPTPATH/conf/tomcat7_jdk8/tomcat7_jdk8_default /etc/default/tomcat7_jdk8
```

```
cp $SCRIPTPATH/conf/tomcat7_jdk8/tomcat7_jdk8_initd /etc/init.d/tomcat7_jdk8

cp $SCRIPTPATH/backend/passport* /opt/tomcat7_jdk8/webapps/
cp $SCRIPTPATH/backend/logservice* /opt/tomcat7_jdk8/webapps/

chmod 0755 /etc/init.d/tomcat7*
update-rc.d tomcat7_jdk8 defaults
chown -R tomcat7:tomcat7 /opt/tomcat7_jdk*

sudo -u postgres psql << EOF
CREATE DATABASE ezmppassport;
CREATE DATABASE logservice;
EOF
sudo -u postgres psql -d ezmppassport  << EOF
\i $SCRIPTPATH/conf/db_scripts/passport_init.sql
EOF
sudo -u postgres psql -d logservice  << EOF
\i $SCRIPTPATH/conf/db_scripts/logservice_init.sql
EOF
sudo -u postgres psql << EOF
alter user postgres password '$ROOT_PASSWORD';
EOF

#start

sudo service apache2 restart
sudo service tomcat7_jdk8 restart
```

4. Выполнить скрипт install.sh с помощью команды «*sudo sh install.sh*»;
5. После успешного выполнения скрипта, необходимо дождаться запуска всех сервисов (примерно 5 минут), прежде чем выполнять вход в Систему.

Настройка Системы

Для конфигурирования Системы необходимо изменить конфигурационные файлы.

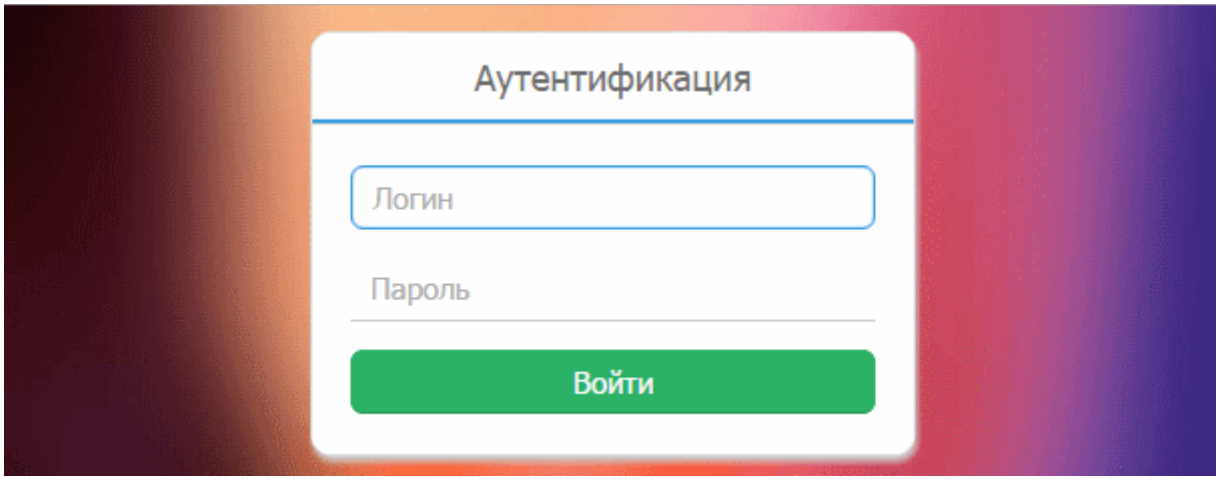
Для конфигурирования серверной части Системы, необходимо отредактировать конфигурационные файлы, находящиеся в следующих каталогах:

- /opt/tomcat7_jdk8/webapps/passport/WEB-INF/classes/config.ini
- /opt/tomcat7_jdk8/webapps/logservice/WEB-INF/classes/config.ini

Управление учетными записями пользователей

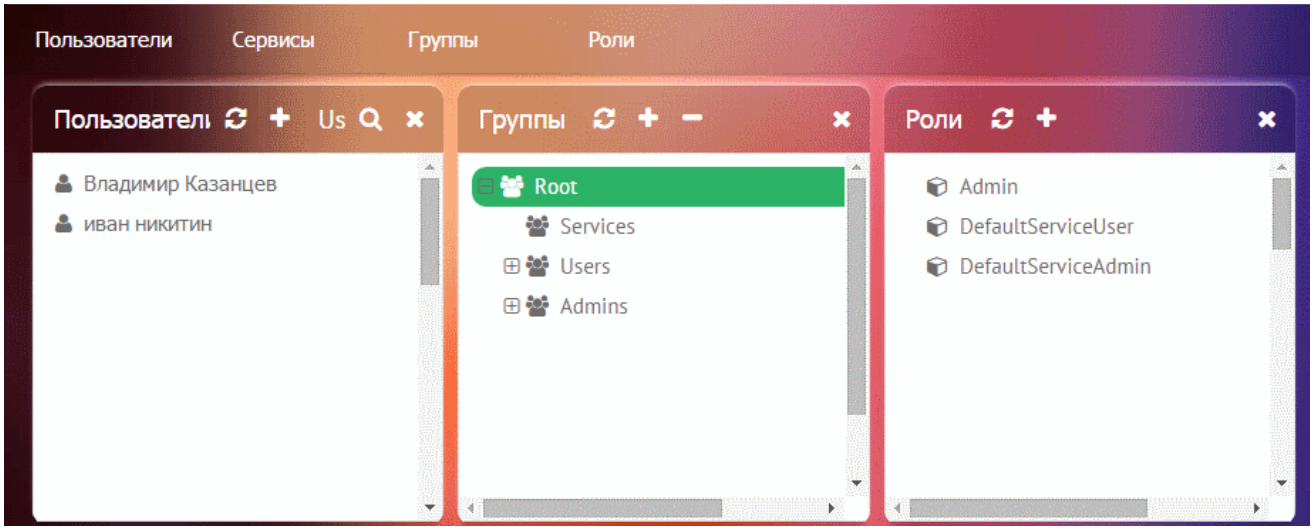
Управление пользователями, группами и ролями осуществляется через административный интерфейс подсистемы управления учетными записями (ЕЗМП.Паспорт).
Доступ к подсистеме осуществляется через веб-браузер, по адресу http://<ip-address>:8080/passport/admin.

Ниже приведена форма авторизации в административную консоль подсистемы управления пользователями.



Основной интерфейс административной консоли управления пользователями включает три модуля:

- Пользователи
- Группы
- Роли

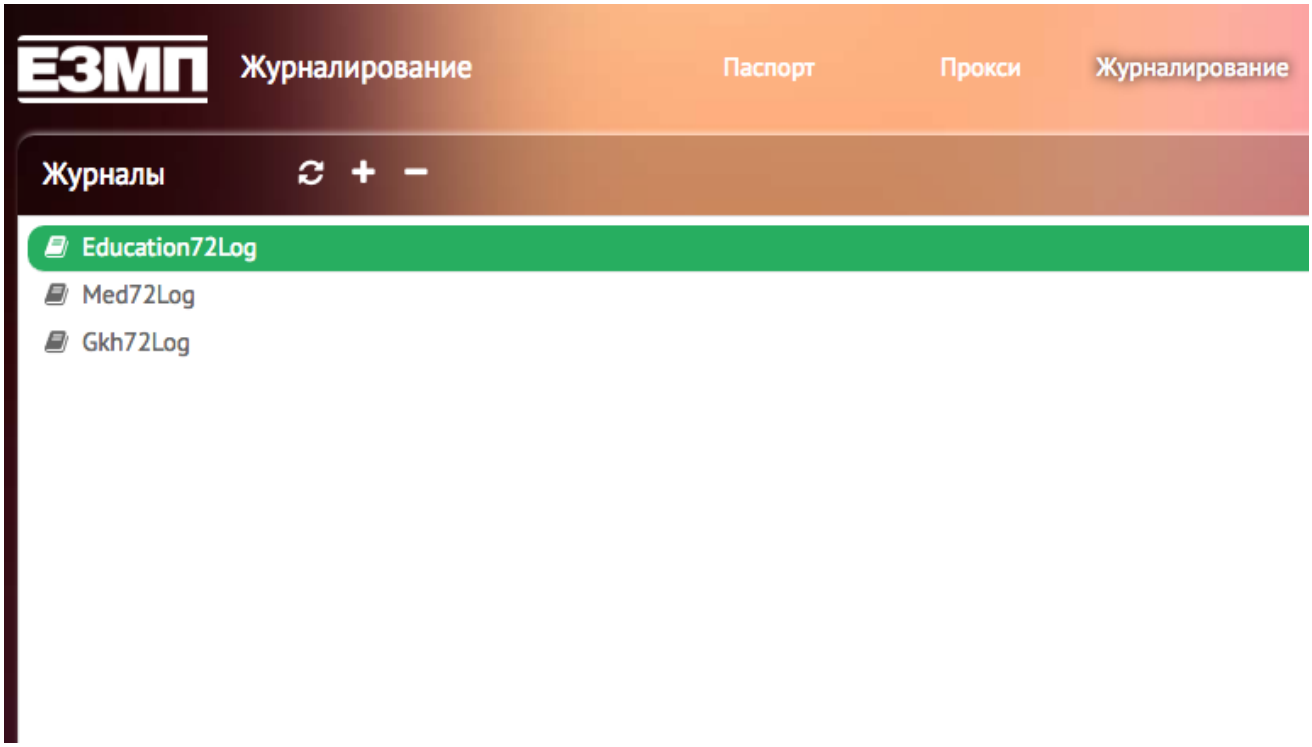


Работа с каждым из модулей осуществляется однотипно.
С помощью кнопки «+» добавляется новый элемент. С помощью кнопки «-» удаляется элемент.

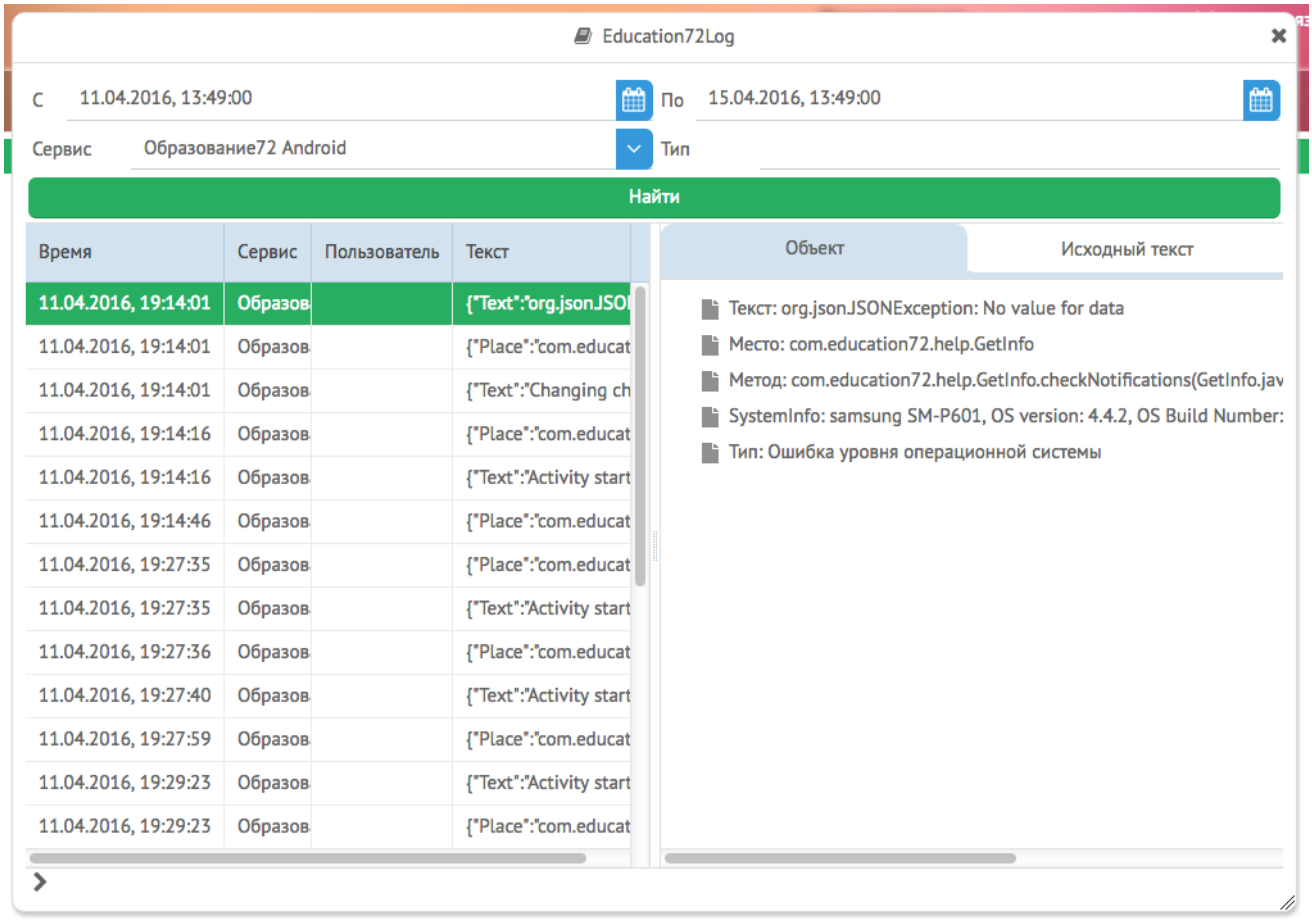
Назначение ролей осуществляется перетаскиванием мышью роли на пользователя или группу. Перемещение пользователя между группами осуществляется перетаскиванием мышью пользователя на группу.
Создание вложенных групп и ролей может быт так же выполнено при помощи перетаскивания мышью.

Использование сервиса журналирования

Сервис «ЕЗМП.Лог» позволяет отслеживать события, происходящие в рамках работы с ЕЗМП.



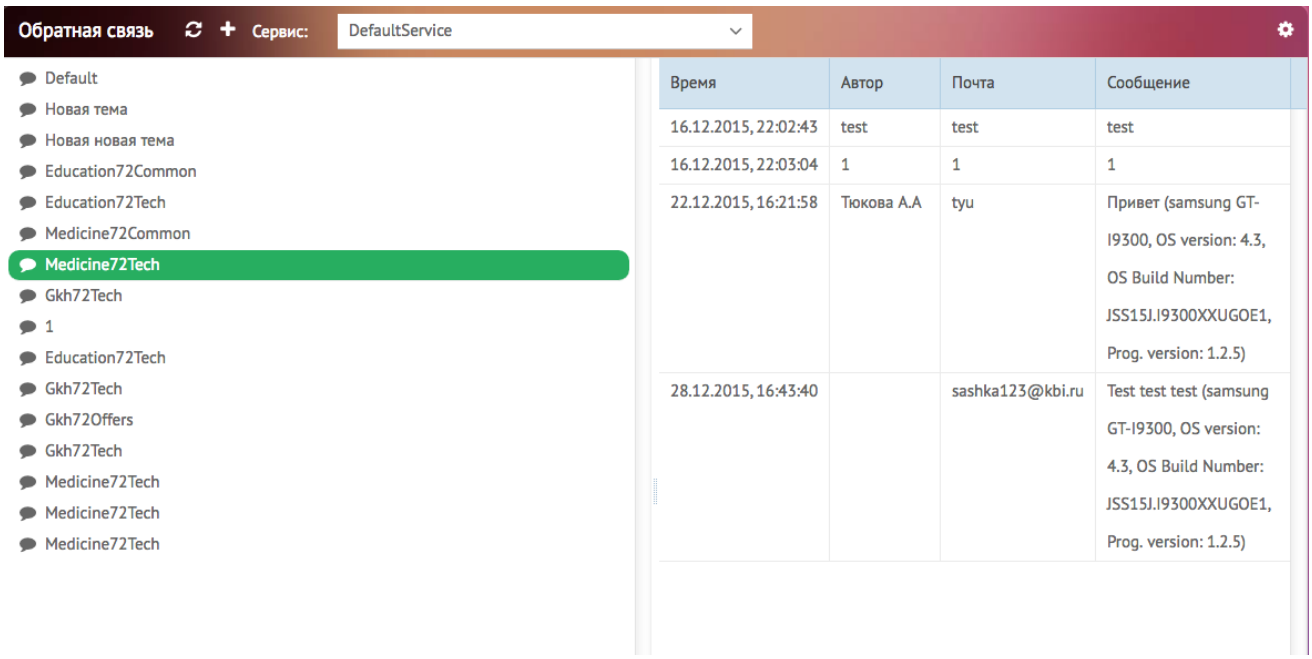
На главной странице сервиса находится список журналов событий. Есть возможность управления списком: с помощью кнопок «+» и «-» можно соответственно добавить либо удалить журнал.
Для работы с содержимым журнала необходимо дважды кликнуть по нему.



Окно просмотра содержимого журнала состоит из трёх частей. В левой половине окна приведён список записей журнала, а правая часть окна предназначена для вывода подробной информации по отдельно взятой записи. Выбрать запись для просмотра подробной информации по ней можно просто кликнув по записи в списке в левой половине окна.
Верхняя часть окна предназначена для фильтрации списка записей по дате внесения записи в журнал, сервису, к которому она относится, и типу. После выставления параметров запроса поиск по журналу осуществляется по нажатию на кнопку «Найти»

Просмотр обратной связи

Сервис «ЕЗМП.Обратная связь» позволяет организовать управление обратной связью из клиентских приложений для сервисов, подключенных к ЕЗМП.



Все сообщения обратной связи разбиты на темы, список тем можно увидеть в левой части главного экрана. Для добавления новой темы следует нажать на кнопку «+». Для просмотра сообщений темы на неё следует кликнуть, после чего откроется список сообщений в правой части окна. Будут выведены только сообщения, относящиеся к сервису, выбранному в верхней части окна.
При клике на значок шестерёнки в верхнем правом углу открывается окно настроек обратной связи.