

Сервер аутентификации Blitz Identity Provider

Версия 5.0

РУКОВОДСТВО АДМИНИСТРАТОРА

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
1. ПОДГОТОВКА К УСТАНОВКЕ	7
1.1. МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К РАЗВЕРТЫВАНИЮ	7
1.2. РЕКОМЕНДУЕМЫЕ ТРЕБОВАНИЯ К РАЗВЕРТЫВАНИЮ В КЛАСТЕРЕ	8
2. УСТАНОВКА	12
2.1. УСТАНОВКА JDK	12
2.2. УСТАНОВКА MEMCACHED	13
2.3. УСТАНОВКА И НАСТРОЙКА СУБД	14
2.3.1. <i>Установка и настройка Couchbase Server</i>	14
2.3.2. <i>Установка и настройка PostgreSQL</i>	16
2.4. УСТАНОВКА И НАСТРОЙКА СЕРВЕРА ОЧЕРЕДЕЙ RABBITMQ	16
2.5. УСТАНОВКА ПРИЛОЖЕНИЙ BLITZ IDENTITY PROVIDER	17
2.6. НАСТРОЙКА синхронизации файлов конфигурации	21
2.7. НАСТРОЙКА ВЕБ-СЕРВЕРА	22
2.8. УСТАНОВКА И НАСТРОЙКА LDAP-КАТАЛОГА	23
2.9. ВХОД В КОНСОЛЬ УПРАВЛЕНИЯ	25
2.10. УСТАНОВКА ЛИЦЕНЗИОННОГО КЛЮЧА	26
2.11. УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ АДМИНИСТРАТОРОВ	27
2.12. ПЕРЕЗАПУСК ПРИЛОЖЕНИЙ BLITZ IDENTITY PROVIDER	28
3. НАСТРОЙКА АТРИБУТОВ УЧЕТНЫХ ЗАПИСЕЙ	29
3.1. КОНФИГУРИРОВАНИЕ ДОСТУПНЫХ АТРИБУТОВ	29
3.1.1. <i>Настройка хранимых атрибутов</i>	29
3.1.2. <i>Настройка вычисляемых атрибутов</i>	31
3.1.3. <i>Настройка правил преобразования входных значений</i>	32
3.1.4. <i>Настройка правил преобразования выходных значений</i>	33
3.1.5. <i>Настройка назначения атрибутов</i>	33
3.2. ПОДКЛЮЧЕНИЕ ХРАНИЛИЩ АТРИБУТОВ	34
3.2.1. <i>Типы хранилищ</i>	34
3.2.2. <i>Подключение хранилища по протоколу LDAP</i>	36
3.2.3. <i>Подключение к хранилищу по REST</i>	39
3.2.4. <i>Настройка внутреннего хранилища</i>	46
4. НАСТРОЙКА СПОСОБОВ АУТЕНТИФИКАЦИИ	47
4.1. НАСТРОЙКА ВХОДА ПО ЛОГИНУ И ПАРОЛЮ	48
4.2. НАСТРОЙКА ВХОДА С ПОМОЩЬЮ СРЕДСТВА ЭЛЕКТРОННОЙ ПОДПИСИ	52
4.2.1. <i>Настройка метода аутентификации в консоли управления</i>	52
4.2.2. <i>Использование и обновление плагина</i>	54
4.3. НАСТРОЙКА ВХОДА ЧЕРЕЗ ВНЕШНИЕ СЕРВИСЫ ИДЕНТИФИКАЦИИ	54
4.4. НАСТРОЙКА ВХОДА С ПОМОЩЬЮ ПРОКСИ-АУТЕНТИФИКАЦИИ	55
4.5. НАСТРОЙКА ВХОДА С ПОМОЩЬЮ СЕАНСА ОПЕРАЦИОННОЙ СИСТЕМЫ	56
4.5.1. <i>Настройки контроллера домена (Kerberos-сервера)</i>	57
4.5.2. <i>Настройки в консоли управления Blitz Identity Provider</i>	59
4.5.3. <i>Настройки браузеров пользователей</i>	61
4.5.4. <i>Настройки запуска приложений Blitz Identity Provider</i>	63
4.5.5. <i>Настройки веб-сервера</i>	63
4.6. НАСТРОЙКА ВХОДА С ПОМОЩЬЮ КОДОВ ПОДТВЕРЖДЕНИЯ	63
4.7. НАСТРОЙКА ВХОДА С ИЗВЕСТНОГО УСТРОЙСТВА	66

4.8.	ПОДТВЕРЖДЕНИЕ ВХОДА РАЗОВЫМ ПАРОЛЕМ НА ОСНОВЕ СОСТОЯНИЯ (НОТР)	66
4.9.	ПОДТВЕРЖДЕНИЕ ВХОДА РАЗОВЫМ ПАРОЛЕМ ОСНОВЕ ВРЕМЕНИ (ТОТР)	67
4.10.	ПРИВЯЗКА УСТРОЙСТВ К УЧЕТНЫМ ЗАПИСЯМ ПОЛЬЗОВАТЕЛЕЙ	69
4.10.1.	Привязка аппаратных брелоков.....	69
4.10.2.	Привязка мобильного приложения.....	71
4.11.	Коды ПОДТВЕРЖДЕНИЯ, ОТПРАВЛЯЕМЫЕ В SMS И PUSH-УВЕДОМЛЕНИЯХ	71
4.12.	Коды ПОДТВЕРЖДЕНИЯ, ОТПРАВЛЯЕМЫЕ ПО ЭЛЕКТРОННОЙ ПОЧТЕ.....	74
4.13.	ПОДТВЕРЖДЕНИЕ ВХОДА С ПОМОЩЬЮ DUO MOBILE.....	75
4.14.	НАСТРОЙКА ВНЕШНЕГО МЕТОДА АУТЕНТИФИКАЦИИ.....	78
5.	РЕГИСТРАЦИЯ ПРИЛОЖЕНИЙ.....	80
5.1.	СОЗДАНИЕ УЧЕТНОЙ ЗАПИСИ НОВОГО ПРИЛОЖЕНИЯ	80
5.2.	НАСТРОЙКА SAML И WS-FEDERATION	83
5.2.1.	Подключение по SAML 1.0/1.1/2.0	83
5.2.2.	Подключение по WS-Federation	84
5.2.3.	Настройка SAML-атрибутов	85
5.3.	НАСТРОЙКА OAUTH 2.0 И OPENID CONNECT 1.0.....	87
5.3.1.	Настройка приложения.....	87
5.3.2.	Общие настройки OAuth 2.0.....	91
5.3.3.	Добавление атрибутов в маркер идентификации	93
5.3.4.	Настройка динамической регистрации клиентов OAuth 2.0.....	96
5.4.	НАСТРОЙКА КЛИЕНТА REST-СЕРВИСОВ BLITZ IDENTITY PROVIDER	98
6.	НАСТРОЙКА ПРОЦЕДУР ВХОДА В ПРИЛОЖЕНИЯ	99
6.1.	СОЗДАНИЕ ПРОЦЕДУР ВХОДА	99
6.2.	ПРИМЕРЫ ПРОЦЕДУР ВХОДА	101
6.2.1.	Принудительная двухфакторная аутентификация в приложение	102
6.2.2.	Ограничение перечня доступных методов первого фактора.....	102
6.2.3.	Разрешить вход в приложение только при определенном значении атрибута у пользователя	103
7.	НАСТРОЙКА СЕРВИСОВ САМООБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ	105
7.1.	ОБЩИЕ НАСТРОЙКИ	105
7.2.	ЛИЧНЫЙ КАБИНЕТ	107
7.2.1.	Отображение атрибутов пользователя	107
7.2.2.	Дополнительные параметры.....	109
7.3.	РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ	109
7.3.1.	Форма регистрации.....	109
7.3.2.	Настройки сервиса регистрации	111
7.3.3.	Процедура регистрации.....	112
7.3.4.	Изменение текста условий использования	112
7.3.5.	Восстановление доступа	113
8.	ВХОД ЧЕРЕЗ ВНЕШНИЕ ПОСТАВЩИКИ ИДЕНТИФИКАЦИИ	114
8.1.	ВХОД ЧЕРЕЗ GOOGLE	114
8.2.	ВХОД ЧЕРЕЗ ЯНДЕКС	119
8.3.	ВХОД ЧЕРЕЗ FACEBOOK	122
8.4.	ВХОД ЧЕРЕЗ ВКОНТАКТЕ	126
8.5.	ВХОД ЧЕРЕЗ ОДНОКЛАССНИКИ	130
8.6.	ВХОД ЧЕРЕЗ MAIL ID	133
8.7.	ВХОД ЧЕРЕЗ ЕДИНУЮ СИСТЕМУ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ (ЕСИА)	136
8.8.	ВХОД ЧЕРЕЗ СИСТЕМУ ИДЕНТИФИКАЦИИ СБЕРБАНКА (СБЕР ID)	142

8.9.	ВХОД ЧЕРЕЗ СИСТЕМУ ИДЕНТИФИКАЦИИ MOS ID (СУДИР)	146
8.10.	ВХОД ЧЕРЕЗ ДРУГУЮ УСТАНОВКУ BLITZ IDENTITY PROVIDER	149
9.	УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЕЙ	153
9.1.	ПОИСК УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ	154
9.2.	ДОБАВЛЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ	154
9.3.	ПРОСМОТР И ИЗМЕНЕНИЕ АТТРИБУТОВ ПОЛЬЗОВАТЕЛЕЙ	155
9.3.1.	<i>Редактирование атрибутов пользователя</i>	<i>156</i>
9.3.2.	<i>Смена пароля пользователя</i>	<i>156</i>
9.3.3.	<i>Просмотр и отвязка аккаунтов социальных сетей</i>	<i>157</i>
9.3.4.	<i>Привязка устройств для проведения двухфакторной аутентификации по разовому паролю</i>	<i>157</i>
9.3.5.	<i>Привязка мобильного приложения Duo Mobile</i>	<i>158</i>
9.3.6.	<i>Просмотр групп, в которые включен пользователь</i>	<i>159</i>
9.3.7.	<i>Просмотр прав</i>	<i>159</i>
9.3.8.	<i>Просмотр и удаление выданных приложениям разрешений</i>	<i>160</i>
10.	ПРОСМОТР ГРУПП ПОЛЬЗОВАТЕЛЕЙ	161
11.	ПРОСМОТР СОБЫТИЙ БЕЗОПАСНОСТИ	162
12.	НАСТРОЙКА УВЕДОМЛЕНИЙ И ОТПРАВКИ СООБЩЕНИЙ	163
12.1.	НАСТРОЙКА ПОДКЛЮЧЕНИЯ К SMS-ШЛЮЗУ	164
12.2.	НАСТРОЙКА ПОДКЛЮЧЕНИЯ К СЕРВИСУ ОТПРАВКИ PUSH-УВЕДОМЛЕНИЙ	166
12.3.	НАСТРОЙКА ПОДКЛЮЧЕНИЯ К SMTP-ШЛЮЗУ	168
13.	НАСТРОЙКА ВНЕШНЕГО ВИДА СТРАНИЦЫ ВХОДА	169
13.1.	РЕДАКТИРОВАНИЕ ШАБЛОНА ПО УМОЛЧАНИЮ	169
13.2.	СОЗДАНИЕ И ИЗМЕНЕНИЕ НОВЫХ ШАБЛОНОВ С ПОМОЩЬЮ КОНСТРУКТОРА	172
13.3.	СОЗДАНИЕ И ИЗМЕНЕНИЕ НОВЫХ ШАБЛОНОВ В РУЧНОМ РЕЖИМЕ	173
14.	НАСТРОЙКИ ШЛЮЗА БЕЗОПАСНОСТИ	177
14.1.	НАСТРОЙКА BLITZ-KEEPER	178
14.2.	СОЗДАНИЕ ПРАВИЛ ДОСТУПА К СЕРВИСАМ	180
14.3.	НАСТРОЙКА ПРАВИЛ ОБМЕНА МАРКЕРОВ ДОСТУПА	183
15.	НАСТРОЙКИ КОНФИГУРАЦИОННЫХ ФАЙЛОВ	184
15.1.	ФАЙЛ НАСТРОЕК BLITZ.CONF	184
15.1.1.	<i>Настройка парольных политик</i>	<i>185</i>
15.1.2.	<i>Ограничение количества одновременных проверок пароля пользователя</i>	<i>186</i>
15.1.3.	<i>Настройка времени отображения экрана логина</i>	<i>187</i>
15.1.4.	<i>Настройка вызова внешнего сервиса проверки электронной подписи</i>	<i>187</i>
15.1.5.	<i>Настройка CAPTCHA</i>	<i>187</i>
15.1.6.	<i>Настройка отправки событий в сервер очередей</i>	<i>189</i>
15.1.7.	<i>Запрос проверочного атрибута при восстановлении пароля</i>	<i>191</i>
15.1.8.	<i>Настройка хранения объектов в Couchbase Server</i>	<i>191</i>
15.1.9.	<i>Настройка домена Blitz Identity Provider</i>	<i>192</i>
15.1.10.	<i>Настройка справочника прав доступа</i>	<i>192</i>
15.1.11.	<i>Расширенные настройки подключения к хранилищам</i>	<i>193</i>
15.1.12.	<i>Блокирование неактивных пользователей</i>	<i>195</i>
15.1.13.	<i>Запрет повторного использования идентификатора удаленного пользователя</i>	<i>195</i>
15.1.14.	<i>Настройка групп пользователей</i>	<i>195</i>
15.1.15.	<i>Вход через ЕСИА в режиме выбора сотрудника организации</i>	<i>196</i>
15.2.	НАСТРОЙКИ ТЕКСТОВ ИНТЕРФЕЙСА	200

15.2.1.	Мультиязычность	200
15.2.2.	Модификация текстовых сообщений веб-интерфейса.....	201
15.2.3.	Модификация шаблонов писем и SMS-сообщений.....	202
15.2.4.	Модификация сообщений для разных приложений	206
15.3.	Файлы НАСТРОЕК КОНСОЛИ УПРАВЛЕНИЯ.....	207
15.3.1.	Настройка входа в консоль управления через SSO.....	207
15.3.2.	Ограничение сессий	209
15.3.3.	Настройка ролей и прав доступа в консоль управления.....	210
16.	РЕШЕНИЕ ПРОБЛЕМ	212
	ПРИЛОЖЕНИЕ 1. ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ BLITZ IDENTITY PROVIDER.....	214
	ПРИЛОЖЕНИЕ 2. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ МЕР ЗАЩИТЫ ИНФОРМАЦИИ СОГЛАСНО ТРЕБОВАНИЯМ ФСТЭК.....	218

ВВЕДЕНИЕ

Сервер аутентификации Blitz Identity Provider защищает пользовательские учетные записи — предоставляет готовые, гибко настраиваемые и реализованные с учетом лучших практик функции защиты учетных записей.

Основные¹ функции Blitz Identity Provider:

1. обеспечение единого сквозного входа пользователя в приложения (Single Sign-On);
2. двухфакторная аутентификация;
3. конфигурируемый пользовательский интерфейс страниц входа, регистрации, восстановления доступа, управления учетной записью;
4. вход с использованием сторонних поставщиков идентификации: вход с помощью аккаунтов социальных сетей, Единой системы идентификации и аутентификации (ЕСИА, Госуслуги), федеративный вход пользователей с использованием внешних поставщиков идентификации;
5. проверка прав доступа пользователей при входе в приложения;
6. проверка прав доступа пользователей и приложений при использовании REST-сервисов;
7. протоколирование событий доступа и действий с учетными записями.

Blitz Identity Provider обеспечивает доступ пользователей Интернет к веб-сайтам и мобильным приложениям компании, а также доступ сотрудников к внутренним ресурсам компании и облачным сервисам.

Blitz Identity Provider используется как интеграционная платформа для подключения приложений компании к LDAP-каталогам и контроллерам домена. Если компания использует домен, то Blitz Identity Provider обеспечит сквозной доступ сотрудников к приложениям компании таким образом, что сотрудник будет проходить аутентификацию однократно, при входе в сетевой домен.

¹ Подробная функциональная спецификация Blitz Identity Provider приведена в Приложении 1.

1. Подготовка к установке

При разворачивании Blitz Identity Provider нужно установить и настроить:

1. Веб-сервер. Можно использовать существующий веб-сервер компании для балансировки нагрузки и снятия SSL-шифрования с входящего трафика.
2. Приложения Blitz Identity Provider – сервис аутентификации, приложение регистрации, приложение восстановления доступа, шлюз безопасности, консоль управления. Приложения регистрации, восстановления доступа, шлюз безопасности можно не устанавливать, если связанные с ними функции не планируется использовать.
3. СУБД. Можно использовать Couchbase Server или PostgreSQL.
4. Хранилище учетных записей и паролей. Можно использовать LDAP-сервер, Microsoft Active Directory или любую (потребуется разработать коннектор) существующую систему хранения учетных записей и паролей.

Развертывание возможно в конфигурации с минимальными ресурсами либо в кластерной конфигурации.

1.1. Минимальные требования к разворачиванию

Рекомендуется применять при подготовке сред тестирования и для продуктивных контуров при внедрениях со средними требованиями к обеспечению доступности и производительности.

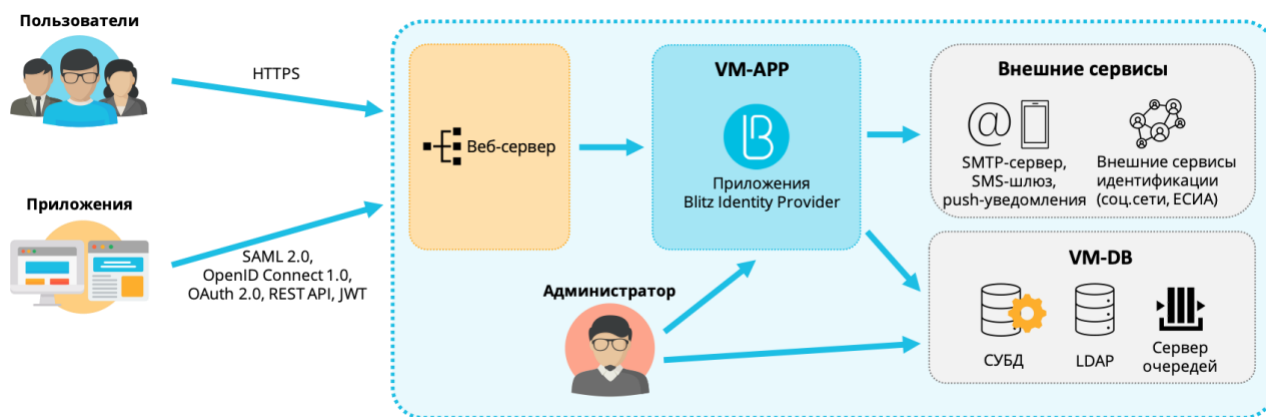


Рисунок 1 – Развертывание в минимальной конфигурации

Минимально для разворачивания необходимо использовать 2 виртуальные машины (далее – VM) со следующими характеристиками и ролями.

Минимальные требования к серверам для развертывания

Описание	ОС	Технические характеристики	Программное обеспечение
ВМ для приложений (VM-APP)	CentOS 7, RHEL 7 или Astra Linux	4 ядра ЦПУ, 8 ГБ ОЗУ, 50 ГБ НЖМД (HDD)	Blitz Identity Provider (blitz-idp, blitz-console, blitz-registration, blitz-recovery, blitz-keeper), JDK, nginx, memcached
ВМ для базы данных (VM-DB)	SE 1.6	8 ядер ЦПУ, 16 ГБ ОЗУ, 100 ГБ НЖМД (HDD)	Couchbase Server Community Edition 6.0 или PostgreSQL 9.6, 389 Directory Server или FreeIPA, RabbitMQ

Требования к сетевой связности:

- VM-APP должна быть доступна по 80, 443 (HTTP/HTTPS) из сетей пользователей;
- с VM-APP должен быть доступ:
 - к VM-DB по 8091, 8092, 8093, 11209, 11210, 11211, 4369, 21100-21199, 11214, 11215, 18091, 18092 (стандартные порты Couchbase Server), 5432 (стандартный порт PostgreSQL), 389, 636 (стандартные порты LDAP), 5672 (стандартный порт RabbitMQ);
 - к сервисам внешних поставщиков идентификации по 443:

Социальные сети	https://accounts.google.com https://graph.facebook.com https://oauth.yandex.ru https://oauth.vk.com https://account.mail.ru https://api.ok.ru
ЕСИА	https://esia-portal1.test.gosuslugi.ru https://esia.gosuslugi.ru
Сбер ID	https://online.sberbank.ru
СУДИР	https://login.mos.ru https://login-tech.mos.ru https://sudir.mos.ru https://sudir-test.mos.ru

- к SMS-шлюзу (при его использовании);
- к SMTP (при его использовании);
- к сервису push-уведомлений (при его использовании).

Для VM-APP нужно завести публичное DNS-имя (например, auth.domain.ru) и выпустить TLS-сертификат на auth.domain.ru или *.domain.ru.

1.2. Рекомендуемые требования к развертыванию в кластере

Схема развертывания в кластерной конфигурации приведена на рисунке 2. Рекомендуется использовать при построении продуктивных контуров систем аутентификации с высокими требованиями к доступности и пиковой производительности.

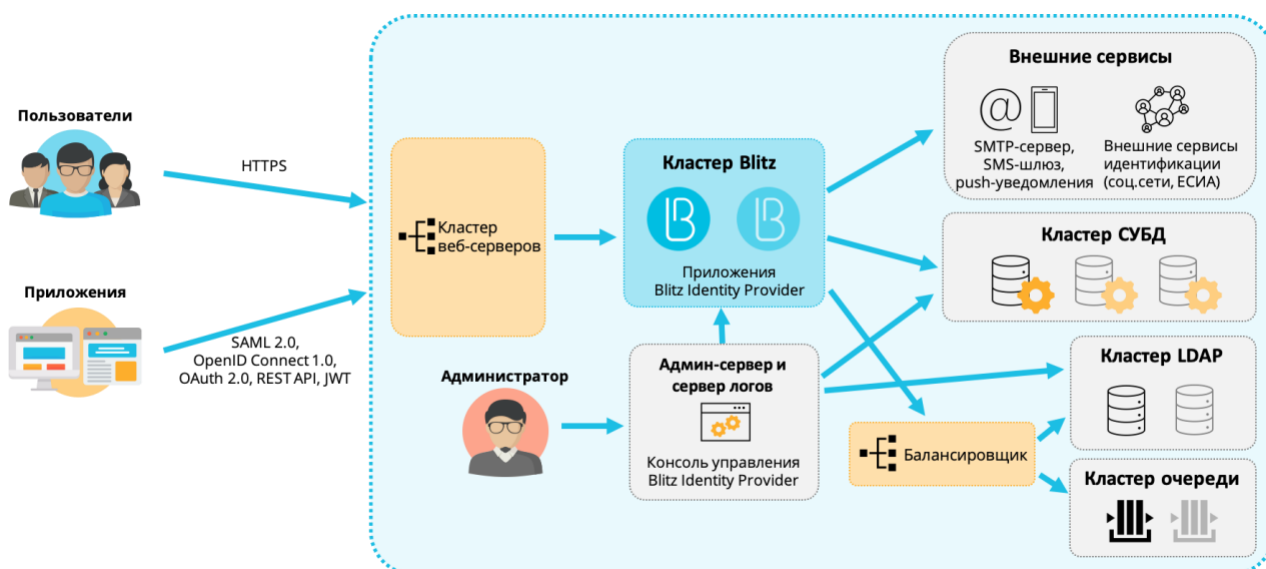


Рисунок 2 – Развертывание в кластерной конфигурации

Для развертывания в кластерной конфигурации рекомендуется использовать виртуальные машины (далее – VM) со характеристиками и ролями, указанными в таблице ниже.

Таблица 2

Рекомендуемые требования к серверам для развертывания в кластере

Описание	Кол-во	ОС	Технические характеристики	Программное обеспечение	Комментарий
VM веб-серверов (VM-WEB)	1-2	CentOS 7, RHEL 7 или Astra Linux SE 1.6	4 ядра ЦПУ, 4 ГБ ОЗУ, 50 ГБ НЖМД (HDD)	nginx	Можно использовать существующий веб-сервер для балансировки нагрузки и снятия TLS с входящего трафика
VM приложений Blitz Identity Provider (VM-APP)	2		4 ядра ЦПУ, 8 ГБ ОЗУ, 50 ГБ НЖМД (HDD)	Blitz Identity Provider (blitz-idp, blitz-registration, blitz-recovery, blitz-keeper), memcached, JDK	При высокой нагрузке рекомендуется развертывать каждое приложение Blitz Identity Provider в своем кластере на отдельных серверах
VM для консоли администрирования (VM-ADM)	1		2 ядра ЦПУ, 4 ГБ ОЗУ, 100 ГБ НЖМД (HDD)	Blitz Identity Provider (blitz-console), memcached, JDK	На этот сервер рекомендуется настроить сбор логов с различных серверов кластера Blitz Identity Provider

Описание	Кол-во	ОС	Технические характеристики	Программное обеспечение	Комментарий
ВМ для СУБД (VM-DB):	2-3		8 ядер ЦПУ, 16 ГБ ОЗУ, 500 ГБ НЖМД (HDD) (данные), 100 ГБ SSD (индексы) ²	Couchbase Server Community Edition 6.0 ³ или PostgreSQL 9.6	Для Couchbase Server рекомендуется минимум ⁴ 3 ВМ. Для PostgreSQL рекомендуется выделить один физический сервер под основной экземпляр и один под резерв (standby)
ВМ для LDAP (VM-LDAP)	2		4 ядра ЦПУ, 8 ГБ ОЗУ, 100 ГБ НЖМД (HDD)	389 Directory Server	В качестве хранилища можно использовать существующее хранилище на основе LDAP, Microsoft Active Directory, FreeIPA, либо иную систему хранения учетных записей и паролей (подключение через REST-коннектор)
ВМ для сервера очередей (VM-MQ)	1-2		4 ядра ЦПУ, 8 ГБ ОЗУ, 50 ГБ НЖМД (HDD)	RabbitMQ версии 3.7.9	Сервер очередей можно не использовать в случае применения Couchbase Server в качестве СУБД
ВМ для балансировщика (VM-NLB)	1-2		2 ядра ЦПУ, 4 ГБ ОЗУ, 50 ГБ НЖМД (HDD)	HAProxy, keepalived	Внутренний балансировщик нужен в случае кластеризации LDAP и сервера очередей

Требуемые версии системного ПО:

- OpenJDK 8, Liberica JDK 8 или Oracle JDK 8;
- Менеджер памяти Memcached версии 1.4.15 или выше.

Требования к сетевой связности:

- VM-WEB должна быть доступна по 80, 443 (HTTP/HTTPS) из сетей пользователей;
- с VM-WEB должен быть доступ к VM-APP по 9000 (blitz-idp), 9002 (blitz-registration), 9003 (blitz-recovery), 9012 (blitz-keeper) и VM-ADM по 9001 (blitz-console);
- с VM-APP должен быть доступ:

² См.: <https://docs.couchbase.com/server/6.0/install/install-linux.html>

³ Версии Couchbase Server 6.5, 6.6 и 7.0 временно не поддерживаются

⁴ См.: <https://docs.couchbase.com/server/current/install/deployment-considerations-lt-3nodes.html>

- к другим VM-APP и VM-ADM по 11211 (memcached);
- к VM-DB по 8091, 8092, 8093, 11209, 11210, 11211, 4369, 21100-21199, 11214, 11215, 18091, 18092 (стандартные порты Couchbase Server) или 5432 (стандартный порт PostgreSQL);
- к VM-LDAP (VM-NLB) по 389, 636 (стандартные порты LDAP);
- к VM-MQ (VM-NLB) по 5672 (стандартный порт RabbitMQ);
- к сервисам внешних поставщиков идентификации по 443:

Социальные сети <https://accounts.google.com>
<https://graph.facebook.com>
<https://oauth.yandex.ru>
<https://oauth.vk.com>
<https://account.mail.ru>
<https://api.ok.ru>

ЕСИА <https://esia-portal1.test.gosuslugi.ru>
<https://esia.gosuslugi.ru>

Сбер ID <https://online.sberbank.ru>

СУДИР <https://login.mos.ru>
<https://login-tech.mos.ru>
<https://sudir.mos.ru>
<https://sudir-test.mos.ru>

- к SMS-шлюзу (при его использовании);
 - к SMTP (при его использовании);
 - к сервису push-уведомлений (при его использовании).
- с VM-ADM должен быть доступ:
 - к VM-DB по 8091, 8092, 8093, 11209, 11210, 11211, 4369, 21100-21199, 11214, 11215, 18091, 18092 (стандартные порты Couchbase Server) или 5432 (стандартный порт PostgreSQL);
 - к VM-LDAP (VM_NLB) по 389, 636 (стандартные порты LDAP);
 - к VM-APP по 22 (ssh), 514 (rsyslog), 11211 (memcached);
 - к VM-MQ (VM-NLB) по 5672 (стандартный порт RabbitMQ);
 - с VM-DB должен быть доступ до других VM-DB по 8091, 8092, 8093, 11209, 11210, 11211, 4369, 21100-21199, 11214, 11215, 18091, 18092 (порты Couchbase Server) или 5432 (порт PostgreSQL);
 - с VM-LDAP должен быть доступ до других VM-LDAP по 389, 636 (порты LDAP);
 - с VM-MQ должен быть доступ до других VM-MQ по 4369, 35197, 5672.

Для VM-APP нужно завести публичное DNS-имя (например, auth.domain.ru) и выпустить TLS-сертификат на auth.domain.ru или *.domain.ru.

2. Установка

Для установки Blitz Identity Provider необходимо:

1. Установить JDK.
2. Установить менеджер памяти memcached.
3. Установить и настроить СУБД.
4. Установить и настроить сервер очередей RabbitMQ.
5. Установить консоль управления Blitz Console.
6. Установить приложения Blitz Identity Provider.
7. Установить шлюз безопасности Blitz Keeper (опционально).
8. Настроить синхронизацию конфигурационных файлов.
9. Настроить веб-сервер.
10. Настроить внешнее хранилище учетных записей (опционально).

2.1. Установка JDK

На серверах, предназначенных для установки ПО сервера Blitz Identity Provider и административной консоли Blitz Identity Provider, необходимо установить и настроить JDK 8.

В качестве JDK рекомендуется использовать один из следующих:

- OpenJDK 8;
- Liberica JDK 8;
- Oracle JDK 8.

Инструкция по установке OpenJDK 8 в CentOS и RHEL:

- Выполнить команду:

```
sudo yum install java-1.8.0-openjdk-devel
```

Инструкция по установке Liberica JDK 8 в Astra Linux Special Edition:

- загрузить дистрибутив Liberica JDK 8 с сайта производителя;
- выполнить команду:

```
pkg -i bellsoft-jdk8u252+9-linux-amd64.deb
```

- открыть на редактирование файл `java.security` в директории `/usr/lib/jvm/bellsoft-java8-amd64/jre/lib/security`;
- раскомментировать (или добавить) строку:

```
crypto.policy=unlimited
```

Инструкция по установке и настройке Oracle JDK 8:

- загрузить дистрибутив Oracle JDK 8 в виде архива tar⁵;
- скопировать загруженный дистрибутив на сервера (например, в директорию `/tmp`);

⁵ См.: <https://www.oracle.com/java/technologies/javase/javase-jdk8-downloads.html>

- создать директорию под установку Oracle JDK 8:

```
mkdir -p /opt/oracle/jdk/
```

- распаковать в созданную директорию дистрибутив Oracle JDK 1.8:

```
tar xf /tmp/jdk-8uXXX-linux-x64.tar.gz -C /opt/oracle/jdk/
```

Если версия Oracle JDK 1.8.0_151 и выше:

- открыть на редактирование файл `java.security` в директории `/opt/oracle/jdk/jdk1.8.0_XXX/jre/lib/security;`
- раскомментировать (или добавить) строку:

```
crypto.policy=unlimited
```

Если версия Oracle JDK 1.8.0_144 и ниже:

- загрузить дистрибутив Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8⁶;
- скопировать загруженный дистрибутив на сервера (например, в директорию `/tmp`);
- распаковать архив и скопировать содержимое в директорию с установленным Oracle JDK 8:

```
cd /tmp
unzip jce_policy-8.zip
cp UnlimitedJCEPolicyJDK8/*.jar /opt/oracle/jdk/jdk1.8.0_XXX/jre/lib/security/
```

2.2. Установка memcached

Версия memcached должна быть 1.4.15 или выше. Сервис memcached должен быть установлен на серверах, предназначенных для установки приложений Blitz Identity Provider: `blitz-console`, `blitz-idp`, `blitz-registration`, `blitz-recovery`. Для приложения `blitz-keeper` сервис memcached не нужен.

Для установки memcached в CentOS и RHEL:

- выполнить команду:

```
yum install memcached
```

- после завершения установки добавить сервис memcached в автозапуск и запустить сервис:

```
systemctl enable memcached
systemctl start memcached
```

Для установки memcached в Astra Linux Special Edition:

- выполнить команду:

```
apt-get install memcached
```

- после завершения установки добавить сервис memcached в автозапуск и запустить сервис:

```
systemctl enable memcached
systemctl start memcached
```

⁶ См.: <https://www.oracle.com/java/technologies/javase-jce8-downloads.html>

Сервис memcached запускается на порту 11211. Нужно убедиться, что этот порт открыт на межсетевых экранах и может быть использован для соединения между серверами с приложениями Blitz Identity Provider.

2.3. Установка и настройка СУБД

Сервер аутентификации Blitz Identity Provider поддерживает для работы использование следующих СУБД:

- СУБД Couchbase Server – рекомендуется при создании систем аутентификации с пиковой нагрузкой более 1000 запросов в секунду, количеством аутентификаций в сутки более 1 млн и с высокими требованиями к отказоустойчивости.
- СУБД PostgreSQL (или иная реляционная СУБД, поддерживающая работу по JDBC) – рекомендуется при создании систем аутентификации с умеренной нагрузкой и средними требованиями к отказоустойчивости, а также при использовании Astra Linux Special Edition.

2.3.1. Установка и настройка Couchbase Server

Инструкция по установке Couchbase Server приводится для CentOS 7 и RHEL 7. В случае развертывания под Astra Linux Special Edition в качестве СУБД рекомендуется использовать PostgreSQL.

Необходимо установить Couchbase Server на каждый из выделенных под установку СУБД серверов согласно инструкции:

<https://developer.couchbase.com/documentation/server/6.0/install/install-linux.html>

Дистрибутив Couchbase Server можно загрузить здесь:

<https://www.couchbase.com/downloads>

Примечание: В DEV/TEST-средах допустимо Couchbase Server устанавливать на существующие сервера с Blitz Identity Provider, но в этом случае нужно учесть, что в Couchbase Server используется своя встроенная Memcached-служба, и во избежание конфликта необходимо скорректировать используемые Memcached порты в Blitz Identity Provider и Couchbase Server.

После завершения установки добавить сервис Couchbase Server в автозапуск и запустить сервис:

```
systemctl enable couchbase-server  
systemctl start couchbase-server
```

Проверить работоспособность сервиса, выполнив команду:

```
systemctl status couchbase-server
```

Далее необходимо:

- инициализировать на каждом сервере кластер Couchbase Server согласно инструкции⁷ (на первом сервере инициализируется кластер, остальные сервера включаются в кластер). Все настройки можно задать как предложено по умолчанию, только нужно для каждого сервера в `hostname` задать полное имя сервера. В качестве имени сервера не рекомендуется использовать его IP-адрес;
- на одном любом сервере кластера Couchbase Server выполнить скрипт по подготовке Couchbase Server к использованию Blitz Identity Provider:
 - скрипт находится в директории `couchbase` в архиве `resources.zip` в составе дистрибутива Blitz Identity Provider;
 - скрипт нужно скопировать на любой сервер кластера Couchbase Server;
 - далее перейти в директорию и выполнить скрипт создания buckets для хранения информации Blitz Identity Provider и индексов для выполнения поисковых запросов Blitz Identity Provider в БД:

```
./cb_init.sh
```

- в процессе выполнения скрипта понадобится ввести:
 - имя URL сервера Couchbase Server – ввести строку вида `http://<hostname>:8091`, где в качестве `hostname` указать имя хоста сервера, с которого выполняется скрипт;
 - логин учетной записи администратора Couchbase Server – задается при инициализации кластера при выполнении предыдущего пункта инструкции;
 - пароль учетной записи администратора Couchbase Server – задается при инициализации кластера при выполнении предыдущего пункта инструкции;
 - логин учетной записи Couchbase Server, которая создается в процессе выполнения этого скрипта для подключения приложений Blitz Identity Provider;
 - пароль учетной записи Couchbase Server для подключения приложений Blitz Identity Provider.
- после выполнения скрипта произвести следующие настройки:
 - в консоли администрирования Couchbase Server отредактировать настройки количества копий данных на различных экземплярах Couchbase. Для этого в меню «Buckets» поочередно выбрать каждый bucket, нажать на нем «Edit» и задать значение настройки «Enable» в блоке «Replicas» и установить число реплик. Для кластера из 3 серверов рекомендуется задать в настройке значение **1** для числа реплик. Затем в меню «Settings» рекомендуется включить настройку «Enable auto-

⁷ См.: <https://docs.couchbase.com/server/6.0/install/init-setup.html>

failover» и задать значение «Timeout» в 30 секунд (auto-failover будет работать, только если в кластере СУБД не менее 3 серверов и настроена репликация для bucket).

- настроить резервное копирование БД, используя инструкцию⁸.

2.3.2. Установка и настройка PostgreSQL

Версия PostgreSQL должна быть 9.6.

В случае CentOS и RHEL необходимо установить PostgreSQL согласно инструкции:

<https://www.postgresql.org/download/linux/redhat/>.

В случае Astra Linux Special Edition для установки PostgreSQL необходимо:

- выполнить команду:

```
apt-get install postgresql
```

- после завершения установки запустить сервис:

```
systemctl start postgresql
```

После завершения установки PostgreSQL в выбранной ОС необходимо выполнить скрипт по подготовке PostgreSQL к использованию Blitz Identity Provider:

- скрипты находятся в директории `postgres` в архиве `resources.zip` в составе дистрибутива Blitz Identity Provider;
- скрипты нужно скопировать на сервер PostgreSQL;
- далее перейти в директорию и по очереди выполнить команды:

```
sudo -u postgres createdb blitzdb

su - postgres
psql
CREATE USER blitz WITH ENCRYPTED PASSWORD 'set-your-pwd';
GRANT ALL PRIVILEGES ON DATABASE blitzdb TO blitz;
GRANT ALL ON ALL TABLES IN SCHEMA public TO blitz;

sudo -u postgres psql -d blitzdb -f 001-init-database.sql
sudo -u postgres psql -d blitzdb -f 002-new_pp_columns.sql
```

вместо `set-your-pwd` нужно вставить пароль, который будет использоваться для подключения к PostgreSQL.

- настроить резервное копирование БД, используя инструкцию⁹.

2.4. Установка и настройка сервера очередей RabbitMQ

Сервер очередей RabbitMQ необходим в случае использования в качестве СУБД PostgreSQL. Если в качестве СУБД используется Couchbase Server, то использование RabbitMQ опционально.

В случае CentOS и RHEL необходимо установить RabbitMQ согласно инструкции:

<https://www.rabbitmq.com/install-rpm.html>.

⁸ См.: <https://docs.couchbase.com/server/6.0/backup-restore/backup-restore.html>

⁹ См.: <https://postgrespro.ru/docs/postgresql/9.6/backup-dump#backup-dump-all>

В случае Astra Linux Special Edition для установки RabbitMQ необходимо:

- выполнить команду:

```
apt-get install rabbitmq-server
```

- после завершения установки запустить сервис:

```
systemctl start rabbitmq-server
```

После завершения установки RabbitMQ в выбранной ОС необходимо войти в консоль RabbitMQ (обычно, `http://hostname:15672/`) и выполнить следующие настройки:

- создать `queue` с именем `blitz-tasks` (в меню «Queues» консоли);
- создать `exchange` с именем `blitz-tasks-exh` (в меню «Exchanges» консоли) и настроить `binding` на очередь `blitz-tasks` с `routing_key` с именем `blitz-tasks`;
- создать пользователя `blitz` (в меню «Admin» консоли) и назначить ему права на созданную очередь.

2.5. Установка приложений Blitz Identity Provider

Blitz Identity Provider состоит из следующих приложений:

- `blitz-console` – консоль управления;
- `blitz-idp` – сервис аутентификации и веб-приложение «личный кабинет»;
- `blitz-registration` – сервис регистрации;
- `blitz-recovery` – сервис восстановления пароля;
- `blitz-keeper` – шлюз безопасности.

Для установки приложений `blitz-console`, `blitz-idp`, `blitz-registration`, `blitz-recovery` используется единый установщик `blitz-5.X.X.bin`.

Для установки приложения `blitz-keeper` используется свой установщик `blitz-keeper-5.X.X.bin`.

При установке сертифицированной версии Blitz Identity Provider дополнительно используются файлы `blitz-idp-thirdparty-5.X.X.tar.gz` и `blitz-keeper-thirdparty-5.X.X.tar.gz`, содержащие архивы с используемыми Blitz Identity Provider сторонними библиотеками.

Установку консоли управления можно провести на любой сервер, где установлен сервер Blitz Identity Provider, но рекомендуется выделить под установку консоли управления отдельный административный сервер. На сервере предварительно должны быть установлены JDK (см. п. 2.1) и `memcached` (см. п. 2.2).

Для установки приложений `blitz-console`, `blitz-idp`, `blitz-registration`, `blitz-recovery` необходимо:

- на предназначенные для установки сервера скопировать (например, в директорию `/tmp`) из дистрибутива Blitz Identity Provider файлы `blitz-5.X.X.bin` и `blitz-idp-thirdparty-5.X.X.tar.gz` (только в случае установки сертифицированной версии);

- запустить установщик `blitz-5.X.X.bin`:

```
cd /tmp
chmod +x blitz-5.X.X.bin
./blitz-5.X.X.bin
```

- в ответ на запросы установщика задать:
 - список устанавливаемых приложений, разделенных через пробел (в случае установки всех приложений указать all);
 - значение `JAVA_HOME` – задать директорию, в которую на сервере установлен JDK (например, `/usr/lib/jvm/bellsoft-java8-amd64` для Liberica JDK, `/usr/lib/jvm/java-1.8.0-openjdk` для OpenJDK 8, `/opt/oracle/jdk` для Oracle JDK 8);
 - путь к файлу `blitz-idp-thirdparty-5.X.X.tar.gz` (только в случае установки сертифицированной версии);
 - внешнее имя домена, на котором будет функционировать Blitz Identity Provider;
 - URL-путь, на котором будет функционировать Blitz Identity Provider (по умолчанию, `/blitz`);
 - пароль к хранилищу ключей Blitz Identity Provider. Хранилище ключей будет сгенерировано в процессе установки, и доступ к хранилищу будет закрыт заданным паролем.
- дождаться окончания установки приложений. Установка будет произведена в директорию `/usr/share/identityblitz`. В случае установки приложения `blitz_console` будет сгенерирован и показан логин/пароль администратора Blitz Identity Provider;

```
Your Blitz Identity Provider configured on domain: blitz-cert.loc
Your Blitz Identity Provider Console available on addresses:
  http://localhost:9001/blitz/console
  http://localhost:9001/blitz/console

Administration user credentials of Blitz Console:
  username - admin
  password - 50c2E6298B
Your can change user credentials at file - /usr/share/identityblitz/blitz-config/credentials
```

- отредактировать файл настроек `/usr/share/identityblitz/blitz-config/blitz.conf`:
 - в случае использования в качестве СУБД Couchbase Server в блоке настроек `blitz.prod.local.idp.internal-store-cb` в `[CB_NODES]` перечислить имена каждого сервера БД Couchbase Server в виде FQDN имени сервера (например, `"node1.blitz.loc"`). Указать логин (`user`) и пароль (`password`) учетной записи администратора Couchbase Server. Пароль следует указать в открытом виде, после запуска Blitz Identity Provider он будет зашифрован:

```
"internal-store-cb" : {
  "nodes" : [ CB_NODES ],
  "user" : "CB_USERNAME",
  "password" : "CB_PASSWORD"
}
```

- в случае использования в качестве СУБД PostgreSQL в блоке настроек `blitz.prod.local.idp.internal-store-jdbc` скорректировать параметры подключения к

БД: `PG_HOSTNAME` – имя хоста, `PG_DBNAME` – имя БД для Blitz Identity Provider (например, `blitzdb`), `PG_USERNAME` и `PG_USERPASSWORD` – имя и пароль пользователя для Blitz Identity Provider в БД. Пароль указывается в открытом виде и будет зашифрован в конфигурационном файле при запуске Blitz Identity Provider). Также в настройке `pool` скорректировать при необходимости параметры пула коннектов:

```
"internal-store-jdbc" : {
  "conn_url" :
"jdbc:postgresql://PG_HOSTNAME:5432/PG_DBNAME?user=PG_USERNAME&password=${pswd}&loggerLevel=DEBUG",
  "db_name" : "PG_DBNAME",
  "keyAlias" : "jdbc",
  "enc_params" : {
    "pswd" : "PG_USERPASSWORD"
  },
  "pool" : {
    "max_idle_conn" : 5,
    "max_total_conn" : 20,
    "max_wait_conn ms" : 30000,
    "min_idle_conn" : 1
  }
}
```

- отредактировать блок `blitz.prod.local.idp.tasks` (только при использовании СУБД PostgreSQL, в случае Couchbase Server не редактировать):

```
"tasks" : {
  "broker-rmq" : {
    "consumer" : {
      "poolSize" : 2
    },
    "exchange" : "RMQ_EXCH_NAME",
    "publisher" : {
      "ackTimeout" : 15,
      "channelsSize" : 8,
      "poolSize" : 2
    },
    "server" : {
      "host" : "RMQ_HOST",
      "port" : 5672
    },
    "user" : {
      "password" : "RMQ_PASSWORD",
      "username" : "RMQ_USERNAME"
    }
  },
  "executionRules" : [
    {
      "maxAttempts" : 2,
      "queue" : "default",
      "redeliveryDelayInSec" : 60
    }
  ],
  "queues" : [
    {
      "dequeueBatchSize" : 10,
      "dequeuePeriodInSec" : 30,
      "executorPoolSize" : 5,
      "name" : "default"
    }
  ]
}
```

Нужно раскомментировать блок настроек `broker-rmq`, переименовав его в `broker_rmq`, а также задать параметры подключения к очереди (вместо `RMQ_EXCH_NAME` – имя созданной `exchange`, вместо `RMQ_HOST` – адрес сервера очередей, вместо `RMQ_PASSWORD` и `RMQ_USERNAME` – имя и пароль

созданного пользователя на сервере очередей. Пароль следует указать в открытом виде, после запуска Blitz Identity Provider он будет зашифрован).

- отредактировать блок `blitz.prod.local.idp.net`, добавив в настройку `trustedServers` адреса подсетей серверов приложений Blitz Identity Provider:

```
"net" : {
  "domain" : "blitz-domain.com",
  "trustedServers" : [
    "192.168.1.0/24"
  ]
}
```

- отредактировать файл настроек `/usr/share/identityblitz/blitz-config/play.conf`:
 - отредактировать блок `memcached`:

```
"memcached" : {
  "servers" : [
    "[MEMCACHED]"
  ]
}
```

`[MEMCACHED]` – указать хост и порт службы memcached (например, `"ld-s-blitz1-dev.ao.company:11211"`).

- в случае использования PostgreSQL в качестве СУБД нужно скорректировать `modules` следующим образом:

```
"modules" : {
  "enabled" : ${play.modules.enabled}[
    "modules.JDBCModule",
    "modules.JDBCInternalStoreModule",
    "modules.JDBCAuditStoreModule",
    "modules.RmqTaskModule"
  ]
}
```

В случае использования Couchbase Server в качестве СУБД нужно оставить блок `modules` без изменений, а именно в следующем виде:

```
"modules" : {
  "enabled" : ${play.modules.enabled}[
    "modules.CouchbaseModule",
    "modules.CouchbaseInternalStoreModule",
    "modules.CBTaskModule",
    "modules.CBAuditStoreModule"
  ]
}
```

- если планируется использовать функцию защиты REST-сервисов с помощью Blitz Identity Provider, то скопировать на предназначенные для установки шлюза безопасности сервера (например, в директорию `/tmp`) из дистрибутива Blitz Identity Provider файлы `blitz-keeper-5.X.X.bin` и `blitz-keeper-thirdparty-5.X.X.tar.gz` (только в случае установки сертифицированной версии);
- запустить установщик `blitz-keeper-5.X.X.bin`:

```
cd /tmp
chmod +x blitz-keeper-5.X.X.bin
./blitz-keeper-5.X.X.bin
```

- в ответ на запросы установщика задать:
 - значение `JAVA_HOME` – задать директорию, в которую на сервере установлен JDK (например, `/usr/lib/jvm/bellsoft-java8-amd64` для Liberica JDK,

- `/usr/lib/jvm/java-1.8.0-openjdk` для OpenJDK 8, `/opt/oracle/jdk` для Oracle JDK 8);
- путь к файлу `blitz-keeper-thirdparty-5.X.X.tar.gz` (только в случае установки сертифицированной версии).
- дождаться окончания установки приложения. Установка будет произведена в директорию `/usr/share/identityblitz`.
- добавить приложения в автозапуск на соответствующих им серверах и запустить их:

```
systemctl enable blitz-console
systemctl start blitz-console
systemctl enable blitz-idp
systemctl start blitz-idp
systemctl enable blitz-registration
systemctl start blitz-registration
systemctl enable blitz-recovery
systemctl start blitz-recovery
systemctl enable blitz-keeper
systemctl start blitz-keeper
```

2.6. Настройка синхронизации файлов конфигурации

При развертывании Blitz Identity Provider в кластере необходимо настроить синхронизацию конфигурации Blitz Identity Provider между серверами кластера Blitz:

1. На сервере с консолью управления Blitz Console:

- установить `rsync` и `incron`:

```
sudo yum install rsync incron
```

или (для Astra Linux Special Edition)

```
sudo apt install rsync incron
```

- переключиться на пользователя `blitz`

```
sudo su - blitz
```

- сгенерировать `ssh` ключ командой (на все задаваемые утилитой вопросы рекомендуется выбрать ответы по умолчанию):

```
ssh-keygen
```

- прочитать и сохранить для дальнейшего использования публичный `ssh` ключ:

```
cat /usr/share/identityblitz/.ssh/id_rsa.pub
```

- открыть настройки `incrontab`:

```
incrontab -e
```

- в открывшемся окне редактора вставить следующее:

```
/usr/share/identityblitz/blitz-config IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE /usr/share/identityblitz/scripts/config_sync.sh ./ $# $%
```

- создать файл `/usr/share/identityblitz/scripts/config_sync.sh` и вставить в него скрипт:

```
#!/bin/bash
```

```
app_dir=/usr/share/identityblitz/blitz-config
```

```
node_list="NODES_LIST"
```

```
for node in $(echo "${node_list}"); do
  rsync -r -a --delete ${app_dir}/${1} ${USER}@${node}:${app_dir};
done
```

- в качестве значения `node_list`, вместо `NODES_LIST`, необходимо прописать список `hostname` нод кластера Blitz (кроме ноды консоли управления Blitz Console).
- сделать файл `/usr/share/identityblitz/scripts/config_sync.sh` исполняемым:

```
chmod +x /usr/share/identityblitz/scripts/config_sync.sh
```

- запустить `incrontab`, выполнив под пользователем `root` команду:

```
systemctl enable incron  
systemctl start incron
```

2. На остальных серверах приложений Blitz Identity Provider:

- установить `rsync`:

```
sudo yum install rsync
```

или (для Astra Linux Special Edition)

```
sudo apt install rsync
```

- переключиться в пользователя `blitz`:

```
sudo su - blitz
```

- выполнить следующий скрипт:

```
mkdir .ssh  
touch .ssh/authorized_keys  
chmod 700 .ssh  
chmod 640 .ssh/authorized_keys
```

- открыть файл `.ssh/authorized_keys` любым редактором, например `vim`, и вставить публичный `ssh` ключ, полученный ранее на сервере консоли управления Blitz Console.

2.7. Настройка веб-сервера

В качестве веб-сервера рекомендуется использовать `nginx`. Пример настроечного файла для `nginx` включен в дистрибутив Blitz Identity Provider – это файл `blitz-idp.conf` из директории `nginx` в архиве `resources.zip`. Нужно скорректировать следующие блоки настроек, после чего загрузить файл на сервер с `nginx` (каталог `/etc/nginx/conf.d`):

1. Скорректировать блок настроек балансировки:

```
upstream blitz-idp {  
    server [BLITZ-IDP-NODE-01]:9000 max_fails=3 fail_timeout=120;  
    server [BLITZ-IDP-NODE-02]:9000 max_fails=3 fail_timeout=120;  
}  
upstream blitz-reg {  
    server [BLITZ-REG-NODE-01]:9002 max_fails=3 fail_timeout=120;  
    server [BLITZ-REG-NODE-02]:9002 max_fails=3 fail_timeout=120;  
}  
upstream blitz-rec {  
    server [BLITZ-REC-NODE-01]:9003 max_fails=3 fail_timeout=120;  
    server [BLITZ-REC-NODE-02]:9003 max_fails=3 fail_timeout=120;  
}  
upstream blitz-keeper {  
    server [BLITZ-KPR-NODE-01]:9012 max_fails=3 fail_timeout=120;  
    server [BLITZ-KPR-NODE-02]:9012 max_fails=3 fail_timeout=120;  
}  
upstream blitz-console {  
    server [BLITZ-CONSOLE-NODE-01]:9001 max_fails=3 fail_timeout=120;  
}
```

Параметры имеют следующие назначения:

- `[BLITZ-%%-NODE-XX]` – имена (`hostname`) серверов с приложениями Blitz Identity Provider (`blitz-idp`, `blitz-registration`, `blitz-recovery`, `blitz-keeper`);
- `[BLITZ-CONSOLE-NODE-01]` – имя (`hostname`) сервера с Blitz Console.

2. Скорректировать блок настроек снятия TLS:

```
ssl_certificate [BLITZ-SSL-CERT-FILE];  
ssl_certificate_key [BLITZ-SSL-PRIVATEKEY-FILE];
```

Параметры имеют следующие назначения:

- `[BLITZ-SSL-CERT-FILE]` – путь (полное имя) к файлу с TLS-сертификатом сервера;
- `[BLITZ-IDP-CONSOLE-NODE-01]` – путь (полное имя) к файлу с TLS-ключом сервера.

3. Следует учесть, что Blitz Identity Provider игнорирует заголовок `X-Forwarded-Proto https`, если в nginx `X-Forwarded-For` содержит более одного IP-адреса, например:

```
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
```

В этом случае рекомендуется использовать следующее значение директивы:

```
proxy_set_header X-Forwarded-For $remote_addr;
```

Скопировать на сервер nginx в папку `/usr/share/nginx/html` папку `static_errors` с файлами страниц отображения ошибок сервера. Файлы с примерами оформления страниц ошибок можно взять в дистрибутиве Blitz Identity Provider – это папка `static_errors` в архиве `resources.zip`.

2.8. Установка и настройка LDAP-каталога

В качестве хранилища учетных записей можно использовать как существующее, так и специально развернутое в организации хранилище учетных записей.

Поддерживаются:

- LDAP-совместимые хранилища. Это может быть любой сервер, поддерживающий протокол LDAP, а также Microsoft Active Directory, Samba4, FreeIPA;
- иные типы хранилищ, для подключения Blitz Identity Provider к ним необходимо разработать специальные REST-сервисы.

В случае необходимости развертывания нового LDAP-каталога рекомендуется в качестве LDAP-каталога использовать 389 Directory Server, который входит в состав ОС CentOS, RHEL, Astra Linux Special Edition.

Для установки 389 Directory Server в CentOS и RHEL:

- выполнить команды установки:

```
yum install 389-ds-base 389-adminutil 389-admin 389-admin-console 389-console 389-ds-console  
yum install xauth
```

- установить `limits` в соответствии с рекомендациями 389 Directory Server:

```
echo "fs.file-max = 64000" >> /etc/sysctl.conf  
echo "* soft nfile 8192" >> /etc/security/limits.conf  
echo "* hard nfile 8192" >> /etc/security/limits.conf  
echo "ulimit -n 8192" >> /etc/profile
```

- инициализировать LDAP-каталог. Ответить на вопросы установщика.

```
setup-ds-admin.pl
```

- после завершения установки добавить LDAP-каталог в автозапуск и запустить сервис:

```
systemctl enable dirsrv.target  
systemctl start dirsrv.target
```

Для установки в Astra Linux Special Edition:

- выполнить команду установки и скрипт инициализации каталога:

```
apt-get install 389-ds-base
setup-ds
```

- после завершения установки добавить LDAP-каталог в автозапуск и запустить сервис:

```
systemctl enable dirsrv.target
systemctl start dirsrv.target
```

После установки 389 Directory Server выполнить его настройку для подготовки использования совместно с Blitz Identity Provider. Для этого:

- Скопировать на LDAP-сервер конфигурационные скрипты LDAP из состава дистрибутива Blitz Identity Provider (это папка `ldap` в архиве `resources.zip`).
- Выполнить скрипт первоначальной настройки `ldap_init.sh` – скрипт создаст ветку `sub` для хранения пользователей, сервисного пользователя `reader`, настроит права доступа пользователя и его парольную политику (бессрочный пароль для сервисного пользователя), создаст класс `blitz-schema` с атрибутами `uid`, `mail`, `mobile`, `sn`, `name`:

```
chmod +x ldap_init.sh
./ldap_init.sh
```

- Выполнить скрипт настройки TLS на сервере LDAP (скрипт создает копию текущей `NSS DB`, затем создает новую `NSS DB`, сертификаты и файл `pin.txt` для запуска сервера без ввода пароля):

```
chmod +x ldap_ssl.sh
./ldap_ssl.sh
```

- После выполнения скрипта перезапустить LDAP-каталог:

```
systemctl restart dirsrv.target
```

- Если требуется настроить и включить глобальные парольные политики в LDAP, то скорректировать и выполнить скрипт `ldap_pwdpolicy.sh`:

```
chmod +x ldap_pwdpolicy.sh
./ldap_pwdpolicy.sh
```

- Если требуется создать дополнительные атрибуты:
 - подготовить текстовый файл, в котором на каждой строке привести имя создаваемого атрибута (т.е. текстовый файл со столбцом создаваемых атрибутов);
 - выполнить скрипт создания дополнительных атрибутов, ответить на его вопросы:

```
chmod +x ldap_add_attr.sh
./ldap_add_attr.sh
```

- отредактировать текстовый файл по адресу `/etc/dirsrv/slapd-название инстанса/schema/99user.ldif`, добавить новые атрибуты в `objectclass` с именем `blitz-schema` в раздел `MAY`;
- перезапустить LDAP-каталог, чтобы применить изменения схемы каталога:

```
systemctl restart dirsrv.target
```


2.9. Вход в консоль управления

После установки Blitz Identity Provider основная настройка системы осуществляется в консоли управления, которая доступна по ссылке, обозначенной в результатах установки продукта. Для первого входа в консоль управления нужно использовать логин и пароль, сгенерированные в момент установки консоли управления (см. п. 2.5).

Обычно ссылка имеет вид `https://<blitz_domain>/blitz/console` или `http://<blitz_console_host>:9001/blitz/console`.

Стандартный вид экрана входа в консоль управления приведен на рисунке 3:

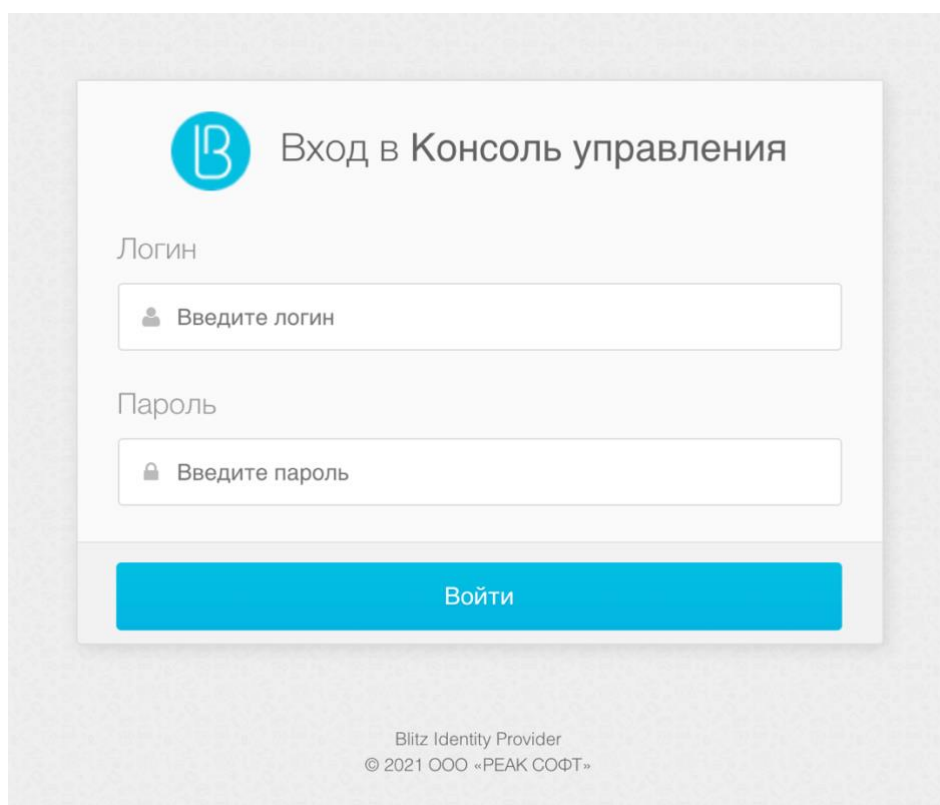


Рисунок 3 – Стандартный вид экрана входа в консоль управления

После успешного входа откроется главная страница консоли управления, вид которой приведен на рисунке 4. Навигация между различными настройками Blitz Identity Provider осуществляется с помощью меню, расположенного в левой части экрана.

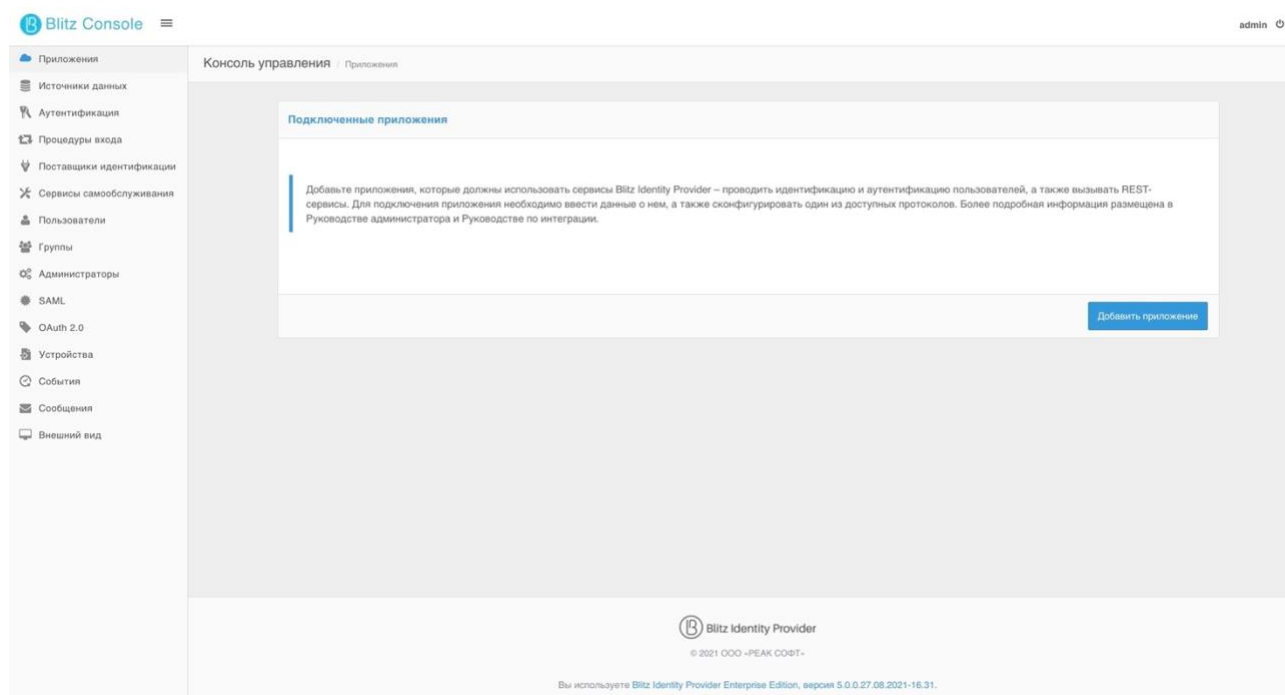


Рисунок 4 – Вид главного экрана консоли управления

2.10. Установка лицензионного ключа

Если нажать на ссылке «Вы используете Blitz Identity Provider ..., версия ...» в футере любой страницы консоли управления Blitz Identity Provider, то будет отображен экран, приведенный на рисунке 5.

На этом экране можно ознакомиться с номером версии текущей установки Blitz Identity Provider, перейти на сайт документации ПО и форму обратной связи.

В блоке «Информация о лицензии» можно посмотреть срок окончания лицензии и предельно разрешенное лицензией количество подключаемых приложений. При нажатии кнопки «Изменить лицензию» можно ввести новый лицензионный ключ.

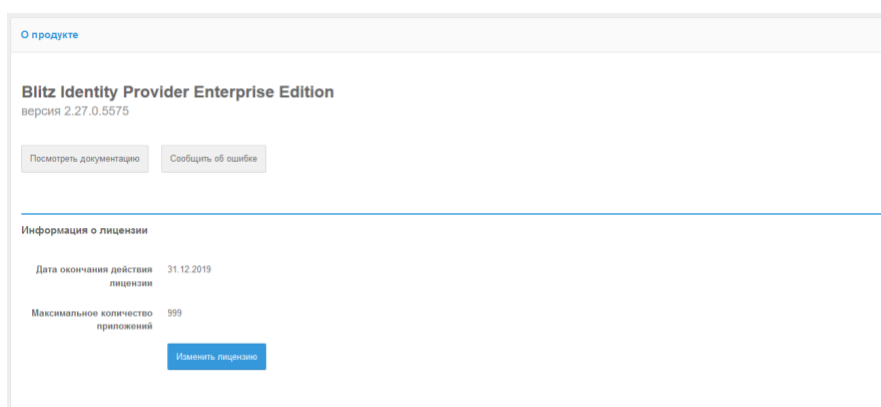


Рисунок 5 – Просмотр информации о лицензии

После установки нового лицензионного ключа рекомендуется перезапустить приложения Blitz Identity Provider.

В случае использования сертифицированной версии Blitz Identity Provider задать лицензионный ключ нужно через редактирование конфигурационного файла `blitz.conf` в каталоге `/usr/share/identityblitz/blitz-config`. Нужно найти блок настроек `blitz.prod.local.idp.license` и скорректировать его следующим образом (задать лицензионный ключ в параметре `key`):

```
"license" : {
  "key" : "MEQC...U"
}
```

2.11. Управление учетными записями администраторов

После установки Blitz Identity Provider рекомендуется создать дополнительные учетные записи администраторов, назначить им пароли и административные роли. Управление учетными записями администраторов доступно в разделе «Администраторы» (Рисунок 6).

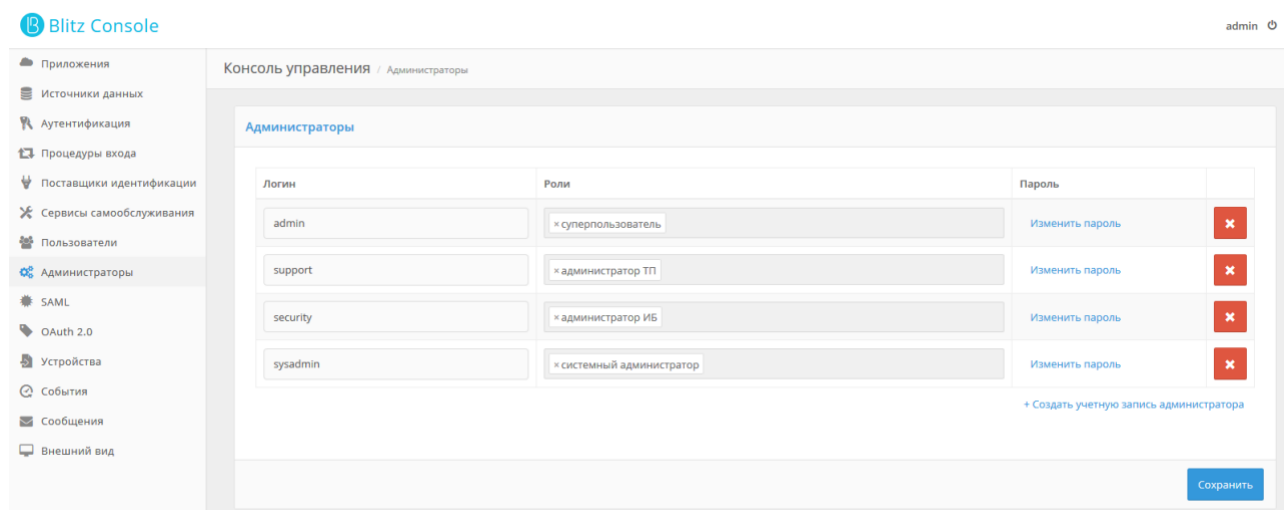


Рисунок 6 – Управление администраторами

В разделе «Администраторы» доступны следующие действия:

- создание и удаление учетных записей администраторов;
- изменение паролей учетных записей администраторов;
- назначение и отзыв ролей администраторов.

По умолчанию в Blitz Identity Provider доступны роли, приведенные в таблице 3. Можно перенастроить существующие роли или создать новые через настройки конфигурационного файла `credentials` (см. п. 15.3.3).

Таблица 3

Стандартные роли администраторов в Blitz Identity Provider

Роль	Доступные разделы консоли управления
суперпользователь (<code>root</code>)	Доступно все
администратор ИБ (<code>security</code>)	«Администраторы», «События»
системный администратор (<code>sysadmin</code>)	«Источники данных», «Аутентификация», «Процедуры входа», «Поставщики идентификации», «SAML»,

	«OAuth 2.0», «Устройства», «Сообщения»
администратор приложений (app_admin)	«Приложения»
Администратор интерфейса (ui_admin)	«Сервисы самообслуживания», «Внешний вид»
администратор ТП (support)	«Пользователи», «Группы», «События»

Дополнительно к стандартной идентификации и аутентификации администраторов по логину и паролю при входе в консоль управления можно настроить использование идентификации и аутентификации пользователей в консоль управления с использованием сервера аутентификации Blitz Identity Provider. Настройки выполняются через конфигурационный файл `console.conf` (см. п. 15.3.1).

2.12. Перезапуск приложений Blitz Identity Provider

Для перезапуска приложений Blitz Identity Provider необходимо использовать команду:

```
systemctl restart APP_NAME
```

Вместо `APP_NAME` нужно указать имя перезапускаемого приложения: `blitz-console`, `blitz-idp`, `blitz-registration`, `blitz-recovery`, `blitz-keeper`.

Пример команды для перезапуска приложения сервиса аутентификации:

```
systemctl restart blitz-idp
```

3. Настройка атрибутов учетных записей

3.1. Конфигурирование доступных атрибутов

Учетная запись пользователя описывается набором атрибутов. Значения атрибутов формируются следующими способами:

- считываются из подключенных хранилищ атрибутов (см. подробнее в п. 3.2.2–3.2.4);
- считываются из базы данных Blitz Identity Provider – чтение и сохранение атрибута в базе данных осуществляется в случае, если для атрибута не настроена связка с атрибутом в подключенном хранилище атрибутов;
- вычисляются из других атрибутов или заполняются константными значениями. Например, можно вычислять атрибут «домен пользователя» из адреса электронной почты или создать композитный атрибут «ФИО» из отдельных атрибутов с фамилией, именем и отчеством пользователя.

Конфигурирование атрибутов состоит из:

- настройки хранимых атрибутов, т.е. тех, которые ведутся в подключенных хранилищах или в базе данных Blitz Identity Provider;
- настройки вычисляемых атрибутов, т.е. тех, которые должны принимать константное значение или которые вычисляются по правилам.
- настройки правил преобразования входных значений, позволяющих преобразовывать значения атрибутов при изменении (например, при редактировании пользователем или при вызове соответствующих API);
- настройки правил преобразования выходных значений, позволяющих провести дополнительные преобразования с вычисляемыми атрибутами;
- настройки назначения атрибутов – определение идентификатора в системе и атрибутов, отвечающих за номер мобильного телефона, адрес электронной почты.

Для корректной работы Blitz Identity Provider как минимум должны быть выполнены следующие настройки:

- сконфигурированы атрибуты;
- один из атрибутов определен в качестве идентификатора.

3.1.1. Настройка хранимых атрибутов

Необходимо в разделе «Источники данных» перейти в блок «Хранимые атрибуты» и выполнить следующие шаги:

- добавить новый атрибут, нажав на ссылку «+Добавить атрибут»;

- указать наименование атрибута, которое будет использоваться в Blitz Identity Provider; Наименование атрибута может отличаться от его имени во внешнем хранилище – в таком случае необходимо указать правило преобразования в настройках этого хранилища (см. 3.2.2);
- указать тип значения атрибута – формат данных (String, Number, Boolean, Bytes, Array of Strings);
- определить параметры атрибута:
 - возможно ли производить по нему поиск (колонка «Поиск»)¹⁰;
 - является ли атрибут обязательным (колонка «Обяз.»);
 - должно ли значение атрибута быть уникальным в системе (колонка «Уник.»).

После добавления атрибута недопустимо менять его имя. При необходимости переименования атрибута следует удалить атрибут и создать новый.

При создании нового атрибута автоматически также создается маппинг нового атрибута во всех подключенных хранилищах атрибутов на атрибут с таким же названием. После создания новых атрибутов необходимо проверить и отредактировать настройки маппинга в подключенных хранилищах. Если атрибут не предполагается считывать из хранилища, то нужно удалить строку маппинга – в таком случае атрибут будет вестись в базе данных Blitz Identity Provider. Если в качестве СУБД используется PostgreSQL, то необходимо создать колонку в таблице `USR_ATR`. Имя колонки должно соответствовать имени добавляемого атрибута. Тип колонки должен быть выбран в зависимости от типа значения атрибута:

- колонка с типом `text` для атрибутов с типом `String` и `Bytes` (в этом случае значение будет сохранено в Base64);
- колонка с типом `text[]` для атрибута с типом `Array of strings`;
- колонка с подходящим числовым типом (`bigint`, `integer`, `smallint`) для атрибутов с типом `Number`;
- колонка с типом `bool` для атрибута с типом `Boolean`.

После добавления атрибутов необходимо перезапустить приложения с Blitz Identity Provider для вступления изменений в силу.

¹⁰ Если это атрибут из подключенного хранилища, то в целях производительности рекомендуется создать по нему поисковый индекс.

Хранимые атрибуты

Определите атрибуты учетной записи пользователя. Для этого задайте *название* – уникальное имя атрибута в системе. Название атрибута может отличаться от его имени во внешнем хранилище, в таком случае укажите правило преобразования в настройках этого хранилища.

Также выберите *тип значения* – тип данных атрибута.

Укажите, какие атрибуты являются:

- *поисковыми (Поиск)* - эти атрибуты будут учтены при поиске учетной записи в разделе «Пользователи», при использовании внешнего хранилища по этим атрибутам следует предусмотреть индекс;
- *обязательными (Обяз.)* - эти атрибуты должны быть заданы при регистрации пользователя и не могут быть удалены в дальнейшем.
- *уникальными (Уник.)* - значения этих атрибутов должны быть уникальны в системе.

Наименование атрибута	Тип значения	Поиск	Обяз.	Уник.	
uid	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
surname	String	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
name	String	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mail	String	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
mobile	String	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[+ Добавить атрибут](#)

Рисунок 7 – Пример настройки хранимых атрибутов

3.1.2. Настройка вычисляемых атрибутов

Для настройки вычисляемых атрибутов в блоке «Вычисляемые атрибуты» необходимо совершить следующие действия:

- добавить новый атрибут, нажав на ссылку «+Добавить атрибут»;
- указать наименование вычисляемого атрибута;
- указать тип значения данных – формат данных;
- указать правило вычисления атрибута на основе других атрибутов или присвоения ему константного значения.

Примеры правил:

- чтобы создать атрибут «Имя и фамилия» из хранимых атрибутов `firstname` и `lastname` необходимо определить хранимые атрибуты `firstname` и `lastname`, а далее задать вычисляемый атрибут `fullname` с правилом вычисления – `${firstname} ${lastname}`;
- чтобы создать атрибут «домен электронной почты» из хранимого атрибута `mail` необходимо определить хранимый атрибут `mail`, а далее задать вычисляемый атрибут `domain` и определить его правило вычисления `${mail##*@}`¹¹.

¹¹ Справку по поддерживаемым параметрам строк подстановки можно посмотреть здесь: <http://tldp.org/LDP/abs/html/parameter-substitution.html>

Вычисляемые атрибуты

При необходимости определите вычисляемые атрибуты – укажите их *наименование*, *тип значения*, а также настройте *правило вычисления* на основе хранимых атрибутов. Вычисляемому атрибуту может быть присвоено константное значение.

Примеры настройки

- Создать атрибут «Имя и фамилия» из хранимых атрибутов *firstname* и *lastname*: сначала определите хранимые атрибуты *firstname* и *lastname*. Далее задайте вычисляемый атрибут *fullname* с правилом вычисления – `${firstname} ${lastname}`.
- Создать атрибут «домен электронной почты» из хранимого атрибута *mail*: определите хранимый атрибут *mail*. Далее задайте вычисляемый атрибут *domain* и определите его правило вычисления `${mail##*@}`.

Справку по поддерживаемым параметрам строк подстановки можно посмотреть [здесь](#).

Наименование атрибута	Тип значения	Правило вычисления	
test	String	1	✖
adGroup	Array of strings	\$(memberOf)	✖

+ Добавить атрибут

Рисунок 8 – Пример настройки вычисляемых атрибутов

3.1.3. Настройка правил преобразования входных значений

Правила преобразования входных значений позволяют проверять корректность формата ввода данных и обеспечивают сохранение данных в корректном формате. Правила задаются с помощью регулярных выражений. Каждое правило включает в себя регулярное выражение, позволяющее провести декомпозицию (разбиения на части) введенного значения, и правило сохранения полученных частей (компоновка).

Пример решаемых задач:

- для проверки, что атрибут **mail** содержит знак **@**, необходимо указать выражение декомпозиции `^(.+)(@)(.+)$` и выражение компоновки `}${0-}`;
- для проверки формата мобильного телефона (**mobile**) и сохранения его в формате `+7(999)1234567`, необходимо указать выражение декомпозиции `^\(+?\)([78])? ?\(?([0-9]{3})\)? ?([0-9]{3})[-]?([0-9]{2})[-]?([0-9]{2})$` и выражение компоновки `+7(}${3-}`
`}${4-}${5-}${6-}`.

Правила преобразования входных значений

Эти правила позволяют проверять корректность формата ввода данных и обеспечивают сохранение данных в корректном формате. Правила задаются с помощью регулярных выражений.

Примеры настройки

Наименование атрибута	Декомпозиция	Компоновка	
mail	^(.+)(@)(.+)\$	}\${0}	✖
mobile	^\(+?\)([78])? ?\(?([0-9]{3})\)? ?([0-9]{3})[-]?([0-9]{2})[-]?([0-9]{2})\$	+7(}\${3-} <code>}\${4-}\${5-}\${6-}</code>	✖

+ Добавить правило

Рисунок 9 – Пример настройки правил преобразования входных значений

3.1.4. Настройка правил преобразования выходных значений

Эти правила позволяют совершить дополнительные преобразования с вычисляемыми атрибутами. Например, из атрибута с массивом ролей могут быть извлечены только необходимые роли. Пример настройки такого правила преобразования представлен на рисунке ниже.

Наименование атрибута	Декомпозиция	Компоновка
adGroup	^(CN=395U-ABCD-)(?!(TEST- DEV-).*)\$	\$(0-)

+ Добавить правило

Рисунок 10 – Пример настройки правил преобразования выходных значений

3.1.5. Настройка назначения атрибутов

Необходимо указать, какой атрибут будет идентификатором в системе. Идентификатор должен быть уникальным и не меняться со временем.

Не рекомендуется в будущем менять базовый идентификатор, т.к. к нему привязываются все пользовательские настройки. При изменении базового идентификатора будут потеряны настройки двухфакторной аутентификации, зарегистрированные события безопасности, запомненные списки устройств пользователей, связи с внешними учетными записями, хранимые в базе данных Blitz Identity Provider атрибуты пользователей.

Также нужно указать, какие атрибуты используются для специальных целей:

1. Атрибут, используемый в качестве признака блокировки учетной записи. Этот атрибут должен иметь тип значения **Boolean**. Blitz Identity Provider поддерживает блокировку пользователей, хранимых в LDAP-каталоге. Для использования этой функции также требуется настроить соответствующий атрибут в настройках LDAP-каталога (см. п. 3.2.2).
2. Выражение, определяющее имя пользователя в консоли. Например, выражение `${surname} ${name} ${middlename-}` позволяет отобразить у учетной записи (например, в разделе «Пользователи») фамилию, имя и отчество (если есть).
3. Атрибуты, используемые для хранения адресов электронной почты.
4. Атрибуты, используемые для хранения номеров мобильных телефонов.

В качестве электронной почты и мобильного телефона могут быть указаны несколько атрибутов (например, для личного и рабочего адреса электронной почты).

Назначение атрибутов

Укажите, какой атрибут будет идентификатором в системе. Идентификатор должен быть уникальным и не меняться со временем.

Также можно указать, какие атрибуты используются:

- для определения заблокированных учетных записей. Этот атрибут должен быть булевым (Boolean);
- в качестве адреса электронной почты;
- в качестве номера мобильного телефона

Можно также указать правило, по которому будет формироваться имя пользователя для отображения в консоли

Идентификатор: uid

Признак блокировки: [dropdown]

Имя пользователя в консоли: \${surname} \${name} \${middlename-}

Электронная почта: × mail

Мобильный телефон: × mobile

Сохранить

Рисунок 11 – Конфигурирование назначения атрибутов

3.2. Подключение хранилищ атрибутов

3.2.1. Типы хранилищ

В качестве хранилищ атрибутов пользователей Blitz Identity Provider позволяет использовать:

1. Внешнее (подключенное) хранилище. В качестве такого может выступать:
 - LDAP-хранилище – это может быть любой сервер, поддерживающий протокол LDAP (389 Directory Server, OpenLDAP, FreeIPA и другие), а также Microsoft Active Directory или Samba4;
 - иное хранилище, для подключения которого к Blitz Identity Provider необходимо разработать специальные REST-сервисы (см. п. 3.2.3).
2. Внутреннее хранилище. Все атрибуты пользователей хранятся в базе данных Blitz Identity Provider. В случае если в качестве СУБД используется Couchbase Server, то базу данных Blitz Identity Provider можно использовать для хранения небольшого числа учетных записей. В случае если в качестве СУБД используется PostgreSQL, то можно хранить любое число учетных записей.

Для корректной работы Blitz Identity Provider требуется настройка хотя бы одного хранилища и конфигурирование атрибутов (см. п. 3.1). По умолчанию настроено внутреннее хранилище и добавлен ряд атрибутов.

Каждая учетная запись пользователя хранится в каком-то одном определенном хранилище. Blitz Identity Provider допускает конфигурирование и подключение нескольких хранилищ, однако рекомендуется использовать одно основное хранилище для работы. Решение об использовании второго хранилища должно быть принято с учетом применяемой модели

данных. Например, в подключенном корпоративном Active Directory могут храниться данные сотрудников организации, а в дополнительном LDAP-хранилище – данные специально зарегистрированных «внешних» пользователей (сотрудники партнерских организаций, фрилансеры и пр.).

Выбор и настройка используемого хранилища осуществляется после настройки атрибутов в разделе «Источники данных» в разделе «Хранилища атрибутов». По умолчанию настроено внутреннее хранилище. Для добавления внешнего хранилища следует нажать на кнопку «Добавить новое хранилище», после чего указать тип внешнего хранилища и настроить параметры взаимодействия с ним. Хранилища после создания создаются выключенными – их нужно включить с помощью тумблера в разделе «Хранилища атрибутов».

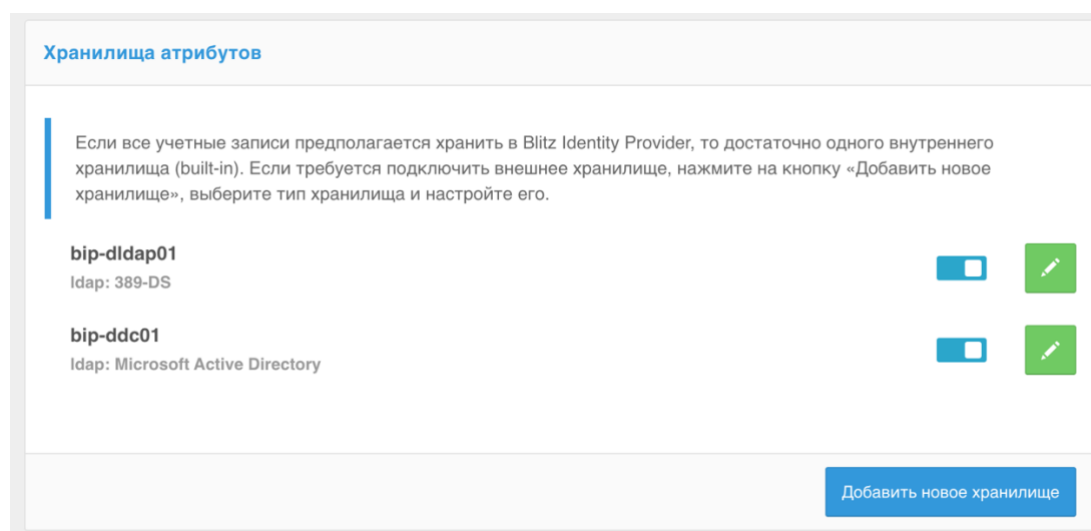


Рисунок 12 – Хранилища атрибутов

Допустимо удалить внутреннее хранилище, если его не планируется использовать. Для этого необходимо перейти в свойства соответствующего внешнего хранилища и нажать на кнопку «Удалить».

Использование нескольких хранилищ может решить задачу входа пользователей, хранящихся в разных LDAP-каталогах или в разных ветках одного каталога. Например, в результате объединения двух компаний можно подключить два каталога к Blitz Identity Provider и обеспечить вход пользователей, не прибегая к настройкам доверия, построению метакаталога и пр.

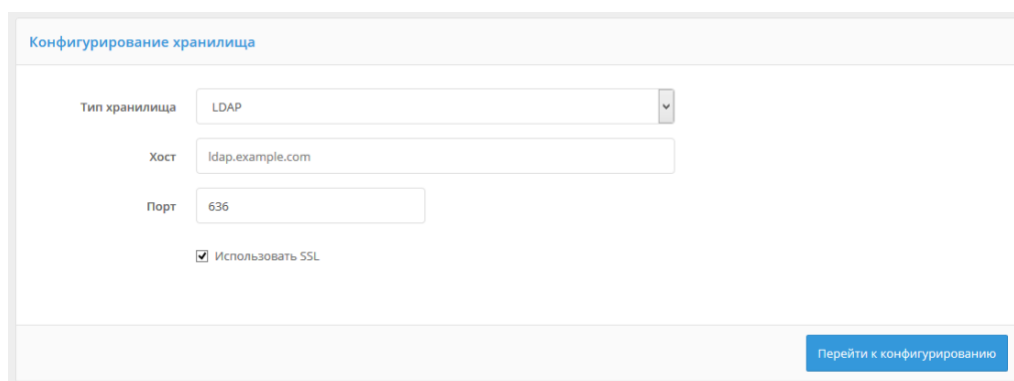


Рисунок 13 – Экран добавления хранилища учетных записей

3.2.2. Подключение хранилища по протоколу LDAP

Если в качестве источника учетных записей пользователей используется LDAP-хранилище, развернутое в организации, для его настройки необходимо воспользоваться разделом «Источники данных» консоли управления и выполнить следующие шаги:

- добавить новое хранилище, указать следующие данные:
 - тип добавляемого хранилища – выбрать **LDAP**;
 - адрес хранилища;
 - порт;
 - отметить галочку «Использовать SSL», если должно использоваться защищенное соединение;
- сконфигурировать LDAP-хранилище, настроив следующие параметры:
 - описание хранилища (опционально);
 - использует ли хранилище только для чтения данных или возможна запись в него;
 - необходимость использования SSL-соединения;
 - необходимость DNS-балансировки¹² вызовов к LDAP-хранилищу – для этого нажать кнопку «DNS-балансировка» и задать параметры «Доменное имя», «Порт», «Использовать SSL», «Режим работы», «Время хранения в кэше, мс»;
 - настройки пула соединений;
- указать логин и пароль пользователя, от имени которого будет осуществляться работа с LDAP-хранилищем (у этого пользователя должны быть права на чтение и на запись данных¹³), а также базовый DN – раздел каталога с учетными записями пользователей;

¹² При DNS-балансировке Blitz Identity Provider запрашивает у DNS-сервера по заданному доменному имени LDAP-каталога все адреса подключения. Если в DNS прописано более одного адреса, то в зависимости от выбранного режима работы Blitz устанавливает подключение к первому доступному серверу (режим работы FAILOVER), к случайному серверу (режим работы RANDOM) или к каждому серверу по очереди (режим работы ROUND_ROBIN). Полученный от DNS список серверов хранится в кэше Blitz Identity Provider в течение времени, заданного в настройке «Время хранения в кэше, мс».

¹³ Допустимо указать пользователя только с правами на чтение, если хранилище используется только для чтения.

- указать настройки поиска – глубину поиска и максимальное число возвращаемых учетных записей (это влияет на число пользователей, отображаемых в разделе «Пользователи» консоли управления).

Параметры подключения к LDAP хранилищу

Идентификатор:

Описание:

Только для чтения:

Настройка соединения Без балансировки DNS-балансировка

Хост:

Порт:

Использовать SSL

Настройка пула соединений

Таймаут соединения, мс	<input type="text" value="3000"/>	Начальное количество соединений	<input type="text" value="10"/>
Таймаут ответа, мс	<input type="text" value="3000"/>	Максимальное количество соединений	<input type="text" value="10"/>

Учетная запись для работы с хранилищем

Для корректной работы должна быть указана учетная запись с правами на чтение данных из хранилища. Если планируется изменение/добавление данных средствами Blitz Identity Provider, то необходимы права на запись

Пользователь(DN):

Пароль: [Изменить значение](#)

Базовый DN:

Настройки поиска

Глубина поиска:

Максимальное количество записей, возвращаемых при поиске:

Рисунок 14 – Настройка подключения к LDAP-хранилищу данных (фрагмент)

Настроить правила сопоставления атрибутов и указать правила разбиения и правила преобразования значений атрибутов. Это позволяет:

- дать атрибуту в системе другое название, не совпадающее с его именем в LDAP-каталоге. Например, если в LDAP-каталоге атрибут задан как `sn`, а в Blitz Identity Provider необходимо его использовать как `surname`, то выберите атрибут `surname` и укажите `sn` в качестве его названия в LDAP. Пример такой настройки приведен на рисунке ниже;

- использовать специальные правила записи атрибутов в данный LDAP-каталог. Например, если вы хотите сохранять мобильный телефон в формате `+7(999)1234567` в LDAP-каталог без скобок, то для записи задайте правило разбиения `^\+7\([0-9]{3})\([0-9]{7})$` и правило преобразования `+7${1-}$2-`.
- использовать специальные правила чтения атрибутов из данного LDAP-каталога. Например, если в LDAP-каталоге атрибут с номером мобильного телефона задан в формате `+79991234567`, а в Blitz Identity Provider используется формат `+7(999)1234567`, то для чтения из каталога можно использовать правило разбиения `^\+7\([0-9]{3})\([0-9]{7})$` и правило преобразования `+7($1-)$2-`.

Правила сопоставления атрибутов

Настройте правила сопоставления, если названия или форматы атрибутов в Blitz Identity Provider не совпадают с тем, как эти атрибуты определены в LDAP-каталоге. И для чтения, и для записи можно указать правила разбиения и правила преобразования значений атрибутов. Это позволяет:

- дать атрибуту в системе другое название, не совпадающее с его именем в LDAP-каталоге. Например, если в LDAP-каталоге атрибут задан как `sn`, а в Blitz Identity Provider необходимо его использовать как `surname`, то выберите атрибут `surname` и укажите `sn` в качестве его названия в LDAP;
- использовать специальные правила записи атрибутов в данный LDAP-каталог. Например, если вы хотите сохранять мобильный телефон в формате `+7(999)1234567` в LDAP-каталог без скобок, то для записи задайте правило разбиения `^\+7\([0-9]{3})\([0-9]{7})$` и правило преобразования `+7${1-}$2-`;
- использовать специальные правила чтения атрибутов из данного LDAP-каталога. Например, если в LDAP-каталоге атрибут с номером мобильного телефона задан в формате `+79991234567`, а в Blitz Identity Provider используется формат `+7(999)1234567`, то для чтения из каталога можно использовать правило разбиения `^\+7\([0-9]{3})\([0-9]{7})$` и правило преобразования `+7($1-)$2-`;

Атрибут	Название в LDAP	Запись		Чтение		
		Правило разбиения	Правило преобразования	Правило разбиения	Правило преобразования	
uid	userPrincipalName					✕
surname	sn					✕
name	givenName					✕
mail	mail					✕
mobile	telephoneNumber					✕

[+ Добавить атрибут](#)

Рисунок 15 – Настройка правил сопоставления атрибутов (фрагмент)

Если хранение созданного ранее (см. п. 3.1) атрибута в данном хранилище не предполагается, то можно просто удалить атрибут, используя кнопку удаления. В этом случае значение удаленного атрибута будет сохраняться при создании/редактировании учетной записи не в подключаемом внешнем хранилище, а в базе данных Blitz Identity Provider.

Если планируется использовать возможность блокировки учетной записи, то необходимо удалить атрибут, определенный в разделе «Источники данных» в качестве признака блокировки, из таблицы с правилами сопоставления атрибутов.

Если Blitz Identity используется для регистрации пользователей, причем запись осуществляется в данный каталог, то необходимо указать параметры создания новых пользователей – DN родительского контейнера, внутри которого будут создаваться пользователи, и системные атрибуты, связанные со спецификой хранилища¹⁴.

Параметры создания новых пользователей

Для корректной работы создания пользователя необходимо указать специфичные для LDAP хранилища параметры. При формировании значений параметров можно использовать строки подстановки из атрибутов пользователя. Списочное значение можно задать через запятую.

DN пользователей

Например, CN=\${mail},CN=users,DC=domain,DC=com

Первоначальные атрибуты	Название	Формат	Значение	
Например: objectclass.	objectClass	Array of strings	top,blitz-schema	<input type="button" value="✕"/>

[+ Добавить атрибут](#)

Рисунок 16 – Настройка параметров создания новых пользователей

3.2.3. Подключение к хранилищу по REST

Если в качестве источника учетных записей пользователей используется внешняя база данных (не LDAP-хранилище), то для подключения к ней нужно разработать коннектор. Коннектор обеспечивает чтение (или изменение) необходимых данных из базы данных и предоставляет данные в корректном формате в виде REST-сервисов для Blitz Identity Provider.

Для настройки взаимодействия с REST-сервисами коннектора необходимо выполнить следующие шаги:

- добавить новое хранилище – указать тип добавляемого хранилища **REST**;
- указать описание хранилища (опционально);
- указать, используется ли хранилище только для чтения данных или возможна запись в него;
- указать максимальное количество записей, возвращаемых при поиске;
- указать перечень доступных через REST-сервисы атрибутов;
- указать URL следующих сервисов:
 - сервис поиска пользователей;
 - сервис получения данных пользователя;
 - сервис проверки логина и пароля;

¹⁴ Например, objectclass, определяющий тип создаваемой учетной записи в LDAP. Для Microsoft Active Directory objectclass должен иметь формат Array of string и значение - top, person.

- сервис смены пароля пользователем;
- сервис добавления нового пользователя;
- сервис изменения данных пользователя;
- сервис удаления пользователя.

Скриншот страницы с настройками подключения к хранилищу с использованием REST-сервисов представлен на рис. 17.

Параметры REST-сервисов

Идентификатор: rest_test

Описание:

Только для чтения: Да

Максимальное количество записей, возвращаемых при поиске: 100

Перечень доступных атрибутов: uid, surname, name, mail, mobile, objectGUID, logon_name, objectSID, memberOf, mobile_test, passport

Атрибуты пользователя, которые доступны в запросах к REST-сервисам

Адреса REST-сервисов

URL сервиса поиска пользователей: http://172.25.0.142:3000/search
HTTP метод запроса: GET. Параметр запроса: rql — запрос в формате Resource Query Language (RQL).
Формат ответа: 200 OK, список пользователей в формате JSON Array в кодировке UTF-8.
Пример листинга

URL сервиса получения данных пользователя: http://172.25.0.142:3000/user/\${id}
При указании URL необходимо использовать строку подстановки для идентификатора пользователя – \${id}.
HTTP метод запроса: GET.
Формат ответа: 200 OK, данные пользователя в формате JSON в кодировке UTF-8.
Если пользователь не найден: 400 Bad Request, код ошибки USER_NOT_FOUND в формате text/plain; charset=utf-8.
Пример листинга

Рисунок 17 – Настройка подключения к хранилищу с использованием REST (фрагмент)

В следующих подразделах описаны требования к разработке REST-сервисов, предоставляющих необходимый Blitz Identity Provider доступ к хранилищу учетных записей.

3.2.3.1. Сервис поиска пользователей

Сервис поиска пользователей должен обрабатывать запросы методом **GET**, где в качестве параметра **rql** указывается поисковый запрос. Запрос имеет формат Resource Query Language (RQL)¹⁵ и должен поддерживать следующие операции:

- **limit** – количество возвращаемых записей;
- **and** – одновременное выполнение поисковых условий;

¹⁵ <https://github.com/kriszyp/rql>

- **or** – альтернативное выполнение поисковых условий (например, поиск по разным атрибутам в качестве логина);
- **eq** – проверка условия равенства с возможностью поиска по маске (например, с использованием звезды (*)).

Например, если в качестве логина в разделе «Аутентификация» настроен только поиск по атрибуту **mail**, то передаваемый при аутентификации RQL-параметр будет иметь вид (где **test@mail.ru** – данные, введенные пользователем в качестве логина):

```
rql=and(eq(mail,test@mail.ru),limit(10))
```

Если в качестве логина настроен поиск по атрибуту **mail** ИЛИ **uid**, то передаваемый RQL-параметр будет иметь вид:

```
rql=and(or(eq(uid,test@mail.ru),eq(mail,test@mail.ru)),limit(10))
```

Сервис должен возвращать список пользователей и их данные в формате JSON в кодировке UTF-8. По каждому пользователю должны быть возвращены атрибуты:

- **id** – идентификатор пользователя в подключенной базе данных. Предполагается, что этот идентификатор будет неизменным для данного пользователя;
- **attrs** – объект с перечнем возвращаемых данных пользователя. Необходимо возвращать те атрибуты, которые предполагается использовать в системе и которые сконфигурированы в разделе «Источники данных».

Пример запроса:

```
GET /users/search?rql=and(eq(uid,BIP*),limit(10)) HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
[
  {
    "id": "ID123",
    "attrs": {
      "uid": "BIP123",
      "name": "Ivan",
      "surname": "Ivanov",
      "mail": "ivanov@test.org",
      "mobile": "+79991234567"
    }
  },
  {
    "id": "ID456",
    "attrs": {
      "uid": "BIP456",
      "name": "Elena",
      "surname": "Ivanova",
      "mail": "ivanova@test.org",
      "mobile": "+79997654321"
    }
  }
]
```

3.2.3.2. Сервис получения данных пользователя

В ряде случаев Blitz Identity Provider запрашивает данные конкретного пользователя. Сервис получения данных пользователя должен обрабатывать запросы методом **GET**, в котором в URL указывается атрибут **id** – внутренний идентификатор пользователя в

подключенной базе данных. При задании URL этого сервиса необходимо использовать строку подстановки для идентификатора пользователя – `{id}`, например:

```
http://idstore.identityblitz.com/users/{id}
```

Если пользователь найден, то сервис должен отвечать **200 OK** и возвращать данные пользователя в формате JSON в кодировке UTF-8. Если пользователь не найден: **400 Bad Request**, код ошибки **USER_NOT_FOUND** в формате `text/plain; charset=utf-8`.

Пример запроса:

```
GET /users/ID123 HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа, если пользователь найден:

```
HTTP/1.1 200 OK
Date: Mon, 18 Jul 2016 12:28:59 GMT
Content-Type: application/json; charset=utf-8

{
  "id": "ID123",
  "attrs": {
    "uid": "BIP123",
    "name": "Ivan",
    "surname": "Ivanov",
    "mail": "ivanov@test.org",
    "mobile": "+79991234567"
  }
}
```

Ответ для случая, если пользователь не найден:

```
HTTP/1.1 400 Bad Request
Date: Mon, 18 Jul 2016 12:28:59 GMT
Content-Type: text/plain; charset=utf-8

USER_NOT_FOUND
```

3.2.3.3. Сервис проверки логина и пароля

Сервис проверки логина и пароля должен обрабатывать запросы методом **POST**, в теле которых указаны следующие параметры (в формате `application/x-www-form-urlencoded`):

- **id** – внутренний идентификатор пользователя в подключенной базе данных;
- **password** – пароль.

В случае успеха сервис должен вернуть ответ **200 OK**.

При невозможности провести аутентификацию сервис должен вернуть **400 Bad Request** с одной из следующих ошибок:

- **INVALID_CREDENTIALS** – неверный логин или пароль пользователя;
- **UNWILLING_TO_PERFORM** – пользователь заблокирован;
- **INAPPROPRIATE_AUTHENTICATION** — пользователь не может быть аутентифицирован по паролю;
- **PASSWORD_EXPIRED** — пароль пользователя устарел.

Пример запроса:

```
POST /users/bind HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/x-www-form-urlencoded
```

```
Cache-Control: no-cache
```

```
id=ivanov&password=12345678
```

Пример ответа (успешная проверка логина и пароля):

```
HTTP/1.1 200 OK
```

```
Date: Mon, 18 Jul 2016 12:38:53 GMT
```

```
Content-Type: application/json; charset=utf-8
```

Пример ответа (неверный логин и/или пароль):

```
HTTP/1.1 400 Bad Request
```

```
Date: Mon, 18 Jul 2016 12:38:53 GMT
```

```
Content-Type: text/plain; charset=utf-8
```

```
INVALID_CREDENTIALS
```

3.2.3.4. Сервис смены пароля пользователем

Сервис смены пароля пользователем должен обрабатывать запросы методом **POST**, в теле которых указаны следующие параметры (в формате **application/x-www-form-urlencoded**):

- **id** – идентификатор пользователя, полученный по результату операции проверки пароля пользователя;
- **old_password** – старый пароль;
- **new_password** – новый пароль.

В случае успеха сервис должен вернуть ответ **200 OK**.

В случае ошибки сервис должен вернуть **400 Bad Request** с одной из следующих ошибок:

- **INVALID_CREDENTIALS** — пользователь с данным идентификатором и паролем не найден;
- **UNWILLING_TO_PERFORM** — пользователь заблокирован;
- **CONSTRAINT_VIOLATION** — новый пароль не соответствует политикам безопасности.

Остальные возвращаемые ошибки должны быть аналогичны операции по проверке логина и пароля.

Пример запроса:

```
POST /users/changePassword HTTP/1.1
```

```
Host: idstore.identityblitz.com
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Cache-Control: no-cache
```

```
id=ivanov&old_password=12345678&new_password=0987654321
```

Пример ответа:

```
HTTP/1.1 400 Bad Request
```

```
Date: Mon, 18 Jul 2016 12:43:23 GMT
```

```
Content-Type: text/plain; charset=utf-8
```

```
CONSTRAINT_VIOLATION
```

3.2.3.5. Сервис добавления нового пользователя

Сервис добавления нового пользователя должен обрабатывать запросы методом **PUT**, в теле которых указаны следующие параметры (в формате **application/json**):

- `password` – пароль пользователя (опционально);
- `attrs` – атрибуты пользователя.

В случае успеха сервис должен вернуть данные пользователя в формате JSON в кодировке UTF-8.

Если пароль не удовлетворяет политикам безопасности, сервис должен вернуть `400 Bad Request` с ошибкой `CONSTRAINT_VIOLATION`.

Если такой пользователь уже существует, сервис должен вернуть `400 Bad Request` с ошибкой `USER_ALREADY_EXISTS` и уточнением, что пользователь с данным идентификатором уже существует.

Пример запроса:

```
PUT /users HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/json
Cache-Control: no-cache

{
  "password":"*****",
  "attrs": {
    "uid": "ivanov@test.org"
    "mail": "ivanov@test.org"
  }
}
```

Пример ответа (пользователь создан):

```
HTTP/1.1 200 OK
Date: Mon, 18 Jul 2016 12:28:53 GMT
Content-Type: application/json; charset=utf-8

{
  "id": "ID678",
  "attrs": {
    "uid": "ivanov@test.org",
    "mail": "ivanov@test.org"
  }
}
```

Пример ответа (учетная запись уже зарегистрирована):

```
HTTP/1.1 400 Bad Request
Date: Mon, 18 Jul 2016 12:43:23 GMT
Content-Type: text/plain; charset=utf-8

USER_ALREADY_EXISTS:ivanov@test.org
```

3.2.3.6. Сервис изменения данных пользователя

Сервис изменения данных пользователя должен обрабатывать запросы методом `POST`, в URL вызываемого сервиса указывается атрибут `id` – внутренний идентификатор пользователя в подключенной базе данных. При задании URL этого сервиса необходимо использовать строку подстановки для идентификатора пользователя – `${id}`, например:

```
http://idstore.identityblitz.com/users/${id}
```

В теле запроса на изменение данных указаны следующие параметры (в формате `application/json`):

- `password` – новое значение пароля пользователя (если пароль не передан, то он не должен измениться);

- **replaced** – новые значения атрибутов пользователя, которые нужно заменить или добавить;
- **deleted** – список названий удаляемых атрибутов.

В случае успеха сервис должен вернуть данные пользователя в формате JSON в кодировке UTF-8.

Если новый пароль не удовлетворяет политикам безопасности, сервис должен вернуть **400 Bad Request** с ошибкой **CONSTRAINT_VIOLATION**.

Если такой пользователь не существует, сервис должен вернуть **400 Bad Request** с ошибкой **USER_NOT_FOUND**.

Пример запроса:

```
POST /users/ID123 HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/json
Cache-Control: no-cache

{
  "replaced": {
    "mail": "ivanov@domain.org"
  },
  "deleted": ["surname"],
  "password": "#####"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Date: Mon, 18 Jul 2016 12:38:53 GMT
Content-Type: application/json; charset=utf-8

{
  "id": "ID123",
  "attrs": [
    "uid": "BIP123",
    "name": "Ivan",
    "email": "ivanov@domain.org"
  ]
}
```

3.2.3.7. Сервис удаления пользователя

Сервис удаления учетной записи пользователя должен обрабатывать запросы методом **DELETE**, в URL вызываемого сервиса указывается атрибут **id** – внутренний идентификатор пользователя в подключенной базе данных. При указании URL этого сервиса необходимо использовать строку подстановки для идентификатора пользователя – **#{id}**, например:

```
http://idstore.identityblitz.com/users/#{id}
```

В случае успеха сервис должен вернуть статус **200 OK**.

Если пользователь не существует, сервис должен вернуть **400 Bad Request** с ошибкой **USER_NOT_FOUND**.

Пример запроса:

```
DELETE /users/ID123 HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

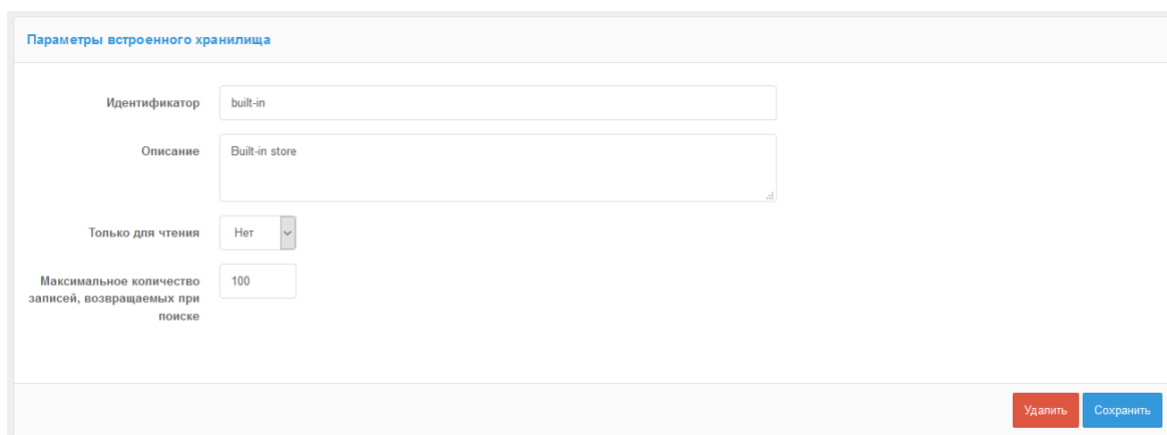
```
HTTP/1.1 200 OK
```

Date: Mon, 18 Jul 2016 12:28:53 GMT
Content-Type: application/json; charset=utf-8

3.2.4. Настройка внутреннего хранилища

Если в качестве источника учетных записей пользователей используется база данных Blitz Identity Provider, то необходимо выполнить следующие шаги:

- добавить новое хранилище, указав тип добавляемого хранилища – **BUILT-IN**;
- указать идентификатор хранилища;
- дать описание хранилища;
- определить, используется ли хранилище только для чтения или нет;
- указать максимальное число возвращаемых учетных записей при поиске.



The screenshot shows a web form titled "Параметры встроенного хранилища" (Parameters of built-in storage). It contains the following fields and controls:

- Идентификатор** (Identifier): A text input field containing "built-in".
- Описание** (Description): A text area containing "Built-in store".
- Только для чтения** (Read-only): A dropdown menu with "Нет" (No) selected.
- Максимальное количество записей, возвращаемых при поиске** (Maximum number of records returned during search): A text input field containing "100".

At the bottom right of the form, there are two buttons: "Удалить" (Delete) in red and "Сохранить" (Save) in blue.

Рисунок 18 – Настройка внутреннего хранилища

В случае если в качестве СУБД используется Couchbase Server, то внутреннее хранилище можно использовать для хранения небольшого числа учетных записей. В случае если в качестве СУБД используется PostgreSQL, то можно хранить любое число учетных записей.

4. Настройка способов аутентификации

Способы аутентификации настраиваются в разделе «Аутентификация» консоли управления (Рисунок 19). Методы аутентификации сгруппированы к первому, либо ко второму фактору (второй фактор используется для «усиления» первого фактора, например, пользователю в дополнение к паролю требуется ввести специальный код, сгенерированный мобильным приложением). Чтобы включить метод аутентификации, его нужно сначала настроить. Для перехода к настройкам метода нужно нажать кнопку «Перейти к конфигурации метода» (при первичной настройке метода) либо ссылку «Перейти к настройкам» (для корректировки текущих заданных настроек). Руководства по настройкам каждого метода приведены в подразделах.

The screenshot displays the 'Аутентификация' (Authentication) configuration page, divided into two main sections: 'Первый фактор' (First factor) and 'Второй фактор' (Second factor). Each section contains several authentication methods with their respective status toggles and configuration options.

Первый фактор (First factor):

- Вход по сеансу операционной системы (OS session login):** Тoggled off. Description: При входе будет использоваться текущий сеанс операционной системы. Action: [Перейти к конфигурации метода](#).
- Средство электронной подписи (Electronic signature):** Тoggled off. Description: При входе в систему пользователю необходимо использовать средство электронной подписи или смарт-карту. Action: [Перейти к конфигурации метода](#).
- Вход по разовой ссылке (One-time link login):** Toggled on. Description: Вход в систему осуществляется по специальной ссылке. Ссылка действует однократно в течение ограниченного периода времени. Action: [Перейти к настройкам](#).
- Подтверждение с помощью кода (Code verification):** Тoggled off. Description: После успешного первого входа пользователю нужно ввести код из сообщения, переданного на номер мобильного телефона. Action: [Перейти к настройкам](#).
- Логин и пароль (Login and password):** Toggled on. Description: При входе в систему пользователю необходимо ввести логин и пароль. Action: [Перейти к настройкам](#).
- Вход через внешние сервисы идентификации (External identity services):** Toggled on. Description: Для входа пользователь будет перенаправлен на внешний сервис идентификации. Пользователю потребуется дать согласие на передачу данных своей учетной записи в Blitz Identity Provider. Action: [Перейти к настройкам](#).
- Вход с известного устройства (Known device login):** Тoggled off. Description: После успешного входа устройство запоминается. В течение определенного периода вход в систему осуществляется автоматически. Action: [Сконфигурируйте метод для использования](#).

Второй фактор (Second factor):

- Разовый пароль на основе секрета (НОТП) (One-time password based on secret):** Тoggled off. Description: После успешного первого входа пользователю нужно ввести код, сгенерированный специальным устройством - генератором одноразовых паролей. Action: [Перейти к настройкам](#).
- Разовый пароль на основе времени (ТОТП) (One-time password based on time):** Toggled on. Description: После успешного первого входа пользователю нужно ввести код, сгенерированный мобильным приложением или устройством. Action: [Перейти к настройкам](#).
- Duo push-аутентификация (Duo push authentication):** Тoggled off. Description: Подтверждение входа с помощью мобильного приложения Duo Mobile - необходимо ответить на риз-уведомление. Action: [Перейти к конфигурации метода](#).
- Вход с известного устройства (Known device login):** Toggled on. Description: Позволяет не требовать усиленную аутентификацию (второй фактор) при входе с известного устройства.
- Подтверждение с помощью кода (Code verification):** Тoggled off. Description: После успешного первого входа пользователю нужно ввести код из сообщения, переданного на номер мобильного телефона. Action: [Перейти к настройкам](#).

At the bottom of each section, there is a link: [Добавить внешний метод аутентификации](#) (Add external authentication method).

Рисунок 19 – Настройка способов аутентификации (фрагмент)

В главном разделе «Аутентификация» можно управлять следующими настройками (Рисунок 20):

- перечень используемых методов аутентификации – для включения или отключения метода аутентификации установите переключатель в требуемое положение;
- требуемый уровень аутентификации по умолчанию – укажите **Первый фактор**, чтобы у пользователей запрашивалась только проверка первого фактора аутентификации (кроме пользователей, в настройках которых включена необходимость проверки второго фактора). Укажите **Первый и второй фактор**, чтобы для пользователей дополнительно к первому фактору требовалась проверка второго фактора аутентификации;
- параметры продолжительности сессии:
 - продолжительность сессии при бездействии пользователя;
 - максимальная продолжительность сессии.
- отображаемое имя пользователя – имя пользователя, которое отображается на странице входа. Задается в виде регулярного выражения, например: `${mail-$mobile}`. Такое регулярное выражение позволяет отображать один из контактов, сохраненных в атрибутах `mail` или `mobile` (если имеются оба, то отображается `mail`).

Общие настройки

Уровень аутентификации по умолчанию: Первый фактор

Продолжительность сессии при бездействии пользователя: 3600

Максимальная продолжительность сессии: 10800

Отображаемое имя пользователя: \${mail-\$mobile}

Сохранить

Рисунок 20 – Общие настройки аутентификации

4.1. Настройка входа по логину и паролю

Для использования входа по логину и паролю необходимо задать правила соответствия – каким образом определять, как введенный логин соотносится с пользователями в хранилище данных.

Для создания правила используется строка подстановки: `${login}` – это строка, введенная пользователем в поле «логин». В результате, например, правило `mail=${login}`

означает, что строка, введенная пользователем, будет сравниваться с атрибутом **mail** в хранилище данных (пример настройки см. рисунок 21);

Вход по логину и паролю

Для корректной работы входа по паролю укажите, каким образом должен формироваться логин и какому атрибуту в источнике данных он соответствует. Вы можете создать несколько альтернативных правил определения логина. Ввод логина не чувствителен к регистру.

Для создания правила используйте строки подстановки. Например, правило `cn=${login}` означает, что строка, введенная пользователем, будет сравниваться с атрибутом `cn` в хранилище данных.

[Посмотреть строки подстановки](#)

sAMAccountName = \${login} ✖ [+ добавить условие](#)

OR

mail = \${login} ✖ [+ добавить условие](#)

[+ добавить альтернативное правило](#)

[Отмена](#) [Сохранить](#)

Рисунок 21 – Настройка входа по логину и паролю

В настройках входа по логину и пароля можно включить проверку на соответствие пароля парольной политике (см. п. 15.1.1). Вводимый пользователем пароль будет в момент входа проверяться на соответствие парольной политике. В случае несоответствия пароля требованиям политики пользователь сможет задать новый пароль или пропустить этот шаг.

Для настройки проверки на соответствие пароля парольной политике при входе необходимо (Рисунок 22):

- выбрать опцию «Всегда проверять текущий пароль пользователя на соответствие парольной политике» или вписать имя некоторого заголовка в поле «Проверять при наличии HTTP заголовка» (в этом случае, если HTTP-запрос будет содержать указанный заголовок со значением **true**, то текущий пароль пользователя будет проверен на соответствие парольной политике);
- указать количество неудачных попыток для временной блокировки. После указанного количества неудачных попыток будет установлена временная блокировка пользователю на использование данного метода аутентификации;
- длительность временной блокировки (в минутах).

Соответствие пароля парольной политике

Всегда проверять текущий пароль пользователя на соответствие парольной политике

Проверять при наличии HTTP заголовка

Если HTTP-запрос будет содержать указанный заголовок со значением true, то текущий пароль пользователя будет проверен на соответствие парольной политике

Кол-во неудачных попыток для временной блокировки

После указанного кол-ва неудачных попыток будет установлена временная блокировка пользователю на использование данного метода аутентификации

Длительность временной блокировки

Определяет длительность временной блокировки в минутах по истечению которых пользователь снова сможет использовать данный метод аутентификации

Рисунок 22 – Настройка проверки на соответствие пароля парольной политике при входе

В настройках входа по логину и пароля можно управлять защитой от перебора пароля. При включенной защите замедляется проверка пароля. После ввода пароля пользователь будет ожидать проверки в течение заданного периода «Время задержки» (в секундах).

Администратор в настройке «Защита» может выбрать следующие режимы защиты:

- **Автоматический режим на уровне системы и пользователей** – защита включится для всех пользователей, если доля неуспешных аутентификаций превысит «Порог включения системной защиты, и выключится, если доля неуспешных аутентификаций станет ниже «Порог выключения системной защиты»;
- **Автоматический режим на уровне пользователей** – защита сработает в отношении пользователей, по которым будет превышено число неуспешных проверок пароля, заданное настройкой «Порог включения пользовательской защиты»;
- **Задержка аутентификации для всех пользователей** – защита будет включена для всех пользователей;
- **Отключена** – защита будет выключена.

Параметры «Порог включения системной защиты» и «Порог выключения системной защиты» задаются в процентах, соответствующих доле неуспешных аутентификаций в общем числе попыток аутентификации.

Пример настройки защиты от подбора пароля представлен ниже (Рисунок 23).

Рисунок 23 – Настройка защиты от подбора пароля

По умолчанию поиск пользователей для аутентификации происходит во всех активных хранилищах атрибутов. В блоке «Правила выбора хранилища атрибутов» можно настроить правила, при выполнении которых поиск пользователя будет осуществляться только в указанном хранилище. Можно задать несколько альтернативных правил выбора хранилища. Это позволит аутентифицировать одних пользователей через одно хранилище, а других – через другое. Для создания правила используются строки подстановки.

Например, на скриншоте ниже выполнена настройка, что при запросе входа приложением с идентификатором `test_app` логин и пароль пользователя будет проверяться по хранилищу `test_db`. Вход во все иные приложения будет производиться через хранилище `main`.

Хранилище атрибутов	Правило соответствия
main	<input type="checkbox"/> not \$[_rpld_] ^{ }\$
test_db	<input type="checkbox"/> not \$[_rpld_] test_app

Рисунок 24 – Настройка правил выбора хранилища атрибутов

4.2. Настройка входа с помощью средства электронной подписи

4.2.1. Настройка метода аутентификации в консоли управления

При использовании для аутентификации средств электронной подписи необходимо:

- в блоке настроек «Сертификаты» загрузить сертификаты удостоверяющих центров, подтверждающих подлинность сертификатов ключей электронной подписи или настроить взаимодействие с внешним сервисом проверки электронной подписи (см. п. 15.1.2);
- настроить в блоке «Правила соответствия» параметры сопоставления учетной записи пользователя в хранилище по его атрибутам из сертификата электронной подписи. В правилах сопоставления используются строки подстановки. Например, правило `cn=${SUBJECT.CN}` означает, что атрибут `SUBJECT.CN` сертификата будет сравниваться с атрибутом `cn` в хранилище данных. Возможно указание нескольких условий одновременно, а также указание альтернативных правил.

При конфигурировании входа по электронной подписи можно также указать:

- следует ли этот метод использовать в качестве первого и второго фактора. Если да, то пользователь, прошедший аутентификацию по электронной подписи, будет считаться прошедшим двухфакторную аутентификацию (пример настройки см. рисунок 25).
- следует ли проверять действительность сертификата. В этом случае Blitz Identity Provider, используя указанную в сертификате точку распределения списка отзыва (CRL), будет проверять, не был ли сертификат отозван. Для активации этой возможности следует отметить чекбокс «Проверять, что сертификат пользователя не отозван»;
- следует ли создавать (регистрировать) учетную запись при первом входе по электронной подписи. В этом случае, если пользователь не найден по определенным правилам соответствия, то ему будет предложено зарегистрировать учетную запись. Чтобы включить эту функцию, следует отметить чекбокс «Создавать учетную запись, если пользователь не найден по сертификату электронной подписи» и настроить правила регистрации пользователя – каким образом заполнять атрибуты в хранилище из атрибутов сертификата. Для задания правил следует использовать строки подстановки. Например, правило `mail=${SUBJECT.E}` означает, что в атрибут `mail` будет сохранена электронная почта из сертификата электронной подписи пользователя;

Общие настройки

Приравнять использование этого метода к применению первого и второго фактора. Если опция включена, то вход по электронной подписи будет означать, что пользователь прошел двухфакторную аутентификацию

Проверять, что сертификат пользователя не отозван

Правила соответствия

Для корректной работы входа по электронной подписи укажите, какие поля должны считываться из сертификата и каким атрибутам в источнике данных они соответствуют. Вы можете создать несколько альтернативных правил.

Для обозначения считываемых из сертификата атрибутов используйте **строки подстановки**. Например, правило `CN=${SUBJECT.CN}` означает, что атрибут `SUBJECT.CN` сертификата будет сравниваться с атрибутом CN в хранилище данных.

[Посмотреть строки подстановки](#)

mail = \$(SUBJECT.E) ✖

+ добавить условие

+ добавить альтернативное правило

Создание учетной записи

Если при входе по электронной подписи пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите, как атрибуты Blitz Identity Provider должны формироваться из атрибутов сертификата. Используйте **строки подстановки**. Например, правило `mail=${SUBJECT.E}` означает, что в атрибут mail будет сохранена электронная почта из сертификата.

[Посмотреть строки подстановки](#)

Создавать учетную запись, если пользователь не найден по сертификату электронной подписи

Атрибут	=	Правило	
mail	=	\$(SUBJECT.E)	✖
uid	=	\$(SUBJECT.E)	✖

+ Добавить атрибут

Сертификаты

Загрузите сертификаты удостоверяющих центров (CA), подтверждающих подлинность ключей электронной подписи пользователей.

Укажите путь к сертификату для загрузки

Серийный номер	Кому выдан	Кем выдан	Период действия	
4895289539783411785911423731610500995	CN=Тестовый УЦ РТК (РТЛабс), OU=Удостоверяющий центр, O=ОАО Ростелеком, L=Москва, ST=77 Москва, C=RU, EMAILADDRESS=ca@rt.ru, STREET=Сущевский вал д. 26, OID.1.2.643.3.131.1.1=#120C303031323334353637383930, OID.1.2.643.100.1=#120D31323334353637383930313233	CN=Тестовый УЦ РТК (РТЛабс), OU=Удостоверяющий центр, O=ОАО Ростелеком, L=Москва, ST=77 Москва, C=RU, EMAILADDRESS=ca@rt.ru, STREET=Сущевский вал д. 26, OID.1.2.643.3.131.1.1=#120C303031323334353637383930, OID.1.2.643.100.1=#120D31323334353637383930313233	from 11/19/13 to 11/19/18	✖

Рисунок 25 – Настройка входа по электронной подписи

4.2.2. Использование и обновление плагина

Для корректной работы входа по электронной подписи на компьютерах пользователей используется специальный плагин – Blitz Smart Card Plugin. При первом входе по электронной подписи пользователю будет предложено установить плагин. После загрузки файла и его запуска пользователю следует пройти все шаги установки плагина. При повторном входе с данного устройства не потребуется устанавливать плагин заново.

Blitz Identity Provider поставляется вместе с версией плагина, позволяющей работать со средством электронной подписи в качестве метода аутентификации.

При необходимости обновить версию Blitz Smart Card Plugin следует заменить дистрибутивы плагина – они размещены в директории `assets` с установкой Blitz Identity Provider, в архиве `assets.zip`. Структура архива имеет следующий вид:

```
plugins/sc/deb/BlitzScPlugin.deb
plugins/sc/rpm/BlitzScPlugin.rpm
plugins/sc/win/BlitzScPlugin.msi
plugins/sc/mac/BlitzScPlugin.pkg
plugins/sc/mac/BlitzScPlugin-10.14.pkg
...
```

Необходимо распаковать архив `assets.zip`, заменить файлы с дистрибутивом плагина и заархивировать обратно файлы в `assets.zip`.

4.3. Настройка входа через внешние сервисы идентификации

Возможен вход с использованием следующих внешних сервисов идентификации:

- поставщика идентификации социальной сети Facebook;
- поставщика идентификации социальной сети ВКонтакте;
- поставщика идентификации Яндекс;
- поставщика идентификации Google;
- поставщика идентификации социальной сети Одноклассники;
- поставщика идентификации Mail.ru (Mail ID);
- единой системы идентификации и аутентификации (ЕСИА) сайта gosuslugi.ru;
- поставщика идентификации Сбер ID;
- поставщика идентификации Mos ID (СУДИР);
- поставщика идентификации, работающего по OpenID Connect.

Подключения к внешним сервисам идентификации должны быть предварительно сконфигурированы в консоли управления в разделе «Поставщики идентификации» (см. п. 7 документа).

В разделе настроек «Вход через внешние сервисы идентификации» необходимо выбрать, какие из настроенных поставщиков идентификации должны использоваться при входе (см. Рисунок 26).

Название поставщика	Уникальное название	Тип поставщика	
Google	google_1	google	<input checked="" type="checkbox"/>
Яндекс	yandex_1	yandex	<input checked="" type="checkbox"/>
Facebook	facebook_1	facebook	<input checked="" type="checkbox"/>
VK	vk_1	vk	<input checked="" type="checkbox"/>
Одноклассники	ok_1	ok	<input checked="" type="checkbox"/>
Blitz	blitz_1	blitz	<input type="checkbox"/>
ESIA	esia_1	esia	<input checked="" type="checkbox"/>
Сбербанк ID	sbrf_1	sbrf	<input checked="" type="checkbox"/>

Рисунок 26 – Включение необходимых внешних сервисов идентификации

4.4. Настройка входа с помощью прокси-аутентификации

Прокси-аутентификация (аутентификация с помощью прокси-сервера) производится по данным, передаваемым в HTTP-заголовках.

При включенной прокси-аутентификации Blitz Identity Provider производит только идентификацию пользователя, тогда как аутентификацию (в результате проверки сертификата) осуществляет прокси-сервер. Включение данного метода аутентификации допустимо в тех случаях, когда все пользователи обращаются к Blitz Identity Provider через прокси-сервер.

Для корректной работы метода необходимо указать:

- требуемые HTTP-заголовки – перечень HTTP-заголовков, которые должны присутствовать в запросе для прохождения прокси-аутентификации пользователя;
- HTTP-заголовок с сертификатом пользователя (опциональный параметр) – заголовок, содержащий x.509 сертификат пользователя;
- соответствие значений HTTP-заголовков и идентификационных данных пользователя в хранилище атрибутов.

Возможна настройка маппинга атрибутов сертификата, передаваемого в HTTP-заголовке, и данных пользователя в хранилище.

Пример настроек входа с помощью прокси-аутентификации представлен на рисунке 27.

Прокси-аутентификация

Чтобы использовать данный метод аутентификации, обязательно должен быть настроен прокси-сервер, передающий в HTTP-заголовках идентификационную информацию пользователя. Метод применяется автоматически, если в HTTP-заголовках получены необходимые для идентификации пользователя данные. Если заголовки не обнаружены, то будут использованы другие методы аутентификации.

HTTP-заголовки

Требуемые HTTP-заголовки

- X-SSL-Client-CERT
- X-SSL-Client-Serial
- X-SSL-Client-S-DN
- X-SSL-Client-Mail

Для добавления HTTP-заголовка введите его и нажмите Enter

Укажите названия HTTP-заголовков, которые должны присутствовать для проведения аутентификации пользователя. Если заголовки не указаны, то аутентификация будет возможна при любом наборе заголовков

HTTP-заголовок с сертификатом пользователя

X-SSL-Client-CERT

Заголовок, в котором передается сертификат пользователя. Если указан, то возможна идентификация пользователя по атрибутам сертификата

Правила соответствия

Для корректной работы прокси-аутентификации укажите, какие HTTP-заголовки соответствуют каким атрибутам в источнике данных. Вы можете создать несколько альтернативных правил.

Для обозначения заголовков используйте строки подстановки. Например, правило `cn=$(HTTP_X_SSL_CLIENT_CN)` означает, что заголовок `HTTP_X_SSL_CLIENT_CN` будет сравниваться с атрибутом `cn` в хранилище данных.

Если настроено считывание сертификата из определенного заголовка, то можно настроить правила соответствия полей сертификата и атрибутов в хранилище данных, используя строки подстановки.

[Посмотреть строки подстановки для X509 сертификата.](#)

mail = X-SSL-Client-Mail

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Отмена Сохранить

Рисунок 27 – Настройка входа с помощью прокси-аутентификации

4.5. Настройка входа с помощью сеанса операционной системы

Способ входа с использованием сеанса операционной системы позволяет пользователям не проходить дополнительно идентификацию и аутентификацию в Blitz Identity Provider, если они ранее вошли со своего ПК в сеть организации и прошли идентификацию и аутентификацию в операционной системе (вошли в сетевой домен). Такие пользователи получают возможность сквозной идентификации при доступе ко всем приложениям, подключенным к Blitz Identity Provider.

Для входа с помощью сеанса операционной системы в организации должен быть развернут Kerberos-сервер (отдельно или в составе контроллера домена организации) и выполнены следующие настройки (см. описания далее в подразделах):

1. Настройки контроллера домена (Kerberos-сервера).
2. Настройки в консоли управления Blitz Identity Provider.
3. Настройки браузеров пользователей.
4. Настройки запуска приложений Blitz Identity Provider.
5. Настройки веб-сервера.

4.5.1. Настройки контроллера домена (Kerberos-сервера)

На контролере домена необходимо зарегистрировать учетную запись для сервера Blitz Identity Provider. Для созданной учетной записи нужно на странице «Account» в блоке «Account options» оснастки контроллера домена включить настройки «User cannot change password» и «Password never expires». Также отметить опции «This account supports Kerberos AES 256 bit encryption» и «Do not require Kerberos preauthentication» (Рисунок 28).

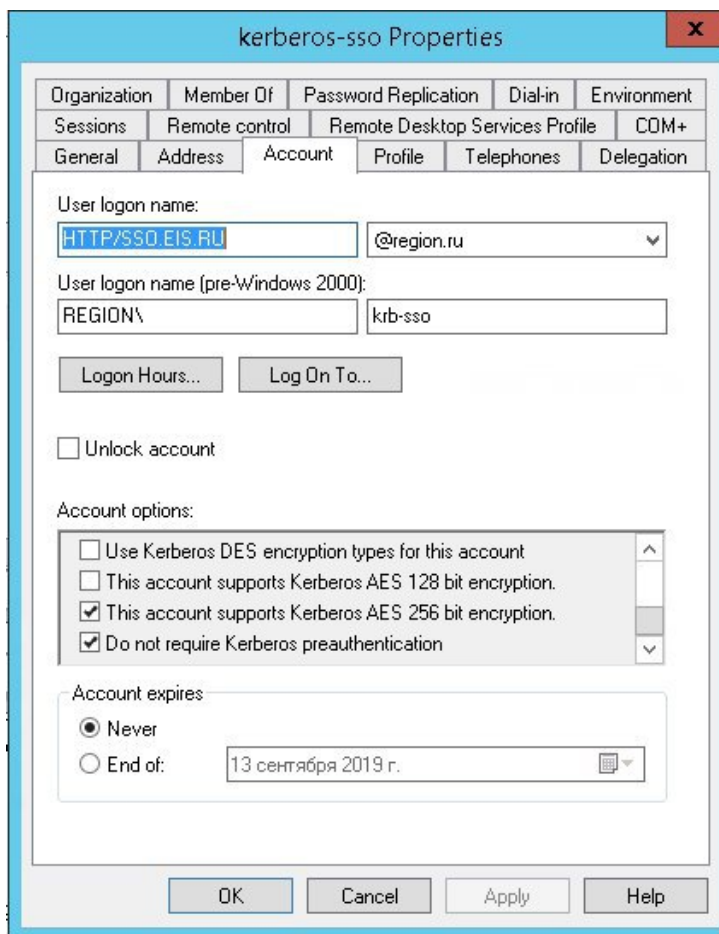


Рисунок 28 – Свойства Kerberos

В оснастке управления групповыми политиками следует настроить политику «Configure encryption types allowed for Kerberos», указав следующие возможные значения: RC4_HMAC_MD5, AES128_HMAC_SHA1 и AES256_HMAC_SHA1.

Пример настройки:

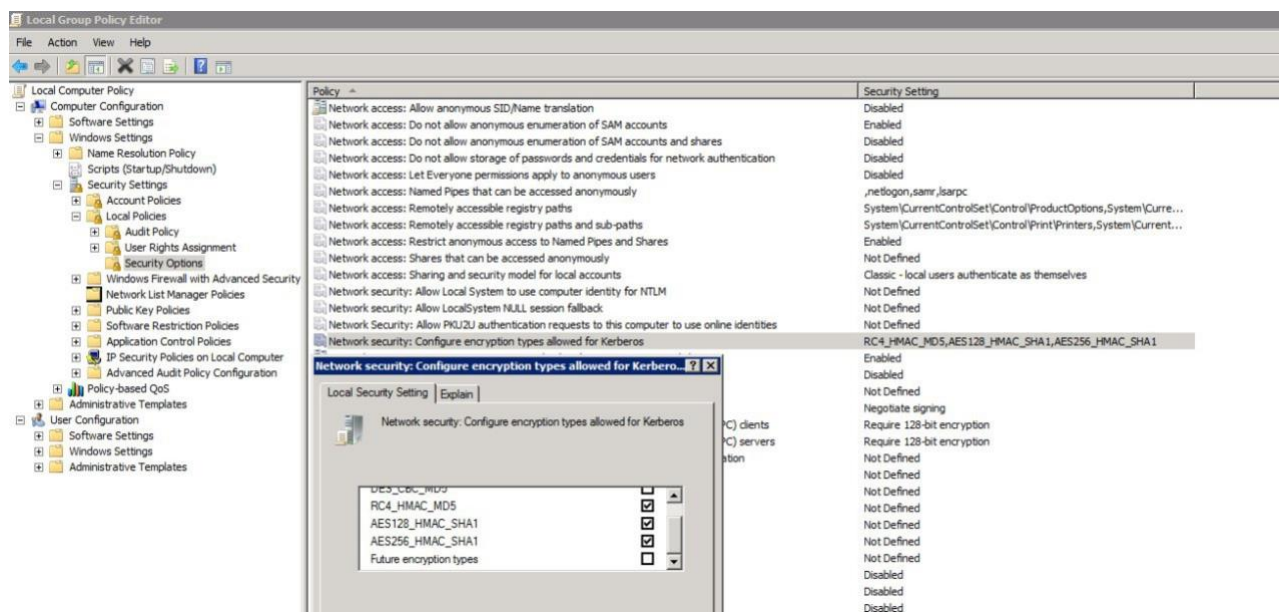


Рисунок 29 – Настройка политик шифрования

Далее необходимо создать Service Principal Name (SPN) для идентификации сервера Blitz Identity Provider сервером Kerberos. Это выполняется с помощью следующей команды:

```
ktpass -princ HTTP/idp.company.ru@DOMAIN.LOC -mapuser DOMAIN\blitzidpsrv -out
C:\temp\spnego_spn.keytab -mapOp set -crypto ALL -ptype KRB5_NT_PRINCIPAL /pass SecretPassword
```

Параметры команды ktpass:

- значение параметра mapuser – имя созданной в домене учетной записи сервера Blitz Identity Provider, например, DOMAIN\blitzidpsrv;
- значение параметра princ – имя SPN сервера с Blitz Identity Provider для идентификации в среде Kerberos. Это имя состоит из имени хоста сервера с Blitz Identity Provider, имени Kerberos Realm в верхнем регистре (обычно совпадает с именем домена) и используемого транспортного протокола (HTTP). Пример значения SPN – HTTP/idp.company.ru@DOMAIN.LOC. Важно, чтобы HTTP/ в начале имени SPN указывалось именно большими буквами, как в примере.
- параметр mapOp – если задан в значение add, то новый SPN будет добавлен к существующим. Если задано значение set, то SPN будет перезаписан.
- параметр out – задает путь к генерируемому keytab-файлу. Например, C:\temp\spnego_spn.keytab.
- параметр /pass – значение пароля от учетной записи сервера Blitz Identity Provider в домене.
- параметры crypto и ptype задают ограничения на используемые алгоритмы и тип генерируемой Kerberos-службы. Рекомендуется задать параметры как в указанном примере -crypto ALL -ptype KRB5_NT_PRINCIPAL.

Сгенерированный keytab-файл необходимо сохранить. Он будет необходим для последующей настройки в консоли управления Blitz Identity Provider.

4.5.2. Настройки в консоли управления Blitz Identity Provider

Необходимо перейти в консоли управления в разделе «Аутентификация» к настройкам способа входа «Вход по сеансу операционной системы». В открывшемся окне необходимо загрузить сгенерированный ранее keytab-файл. Имя SPN при этом будет задано автоматически в соответствии с загруженным файлом.

По результатам загрузки keytab-файла будет отображаться информация о Kerberos-службе (см. рисунок 30).

При необходимости можно:

- удалить загруженный keytab-файл;
- загрузить еще keytab-файлы, в случае подключения Blitz Identity Provider к нескольким контроллерам домена.

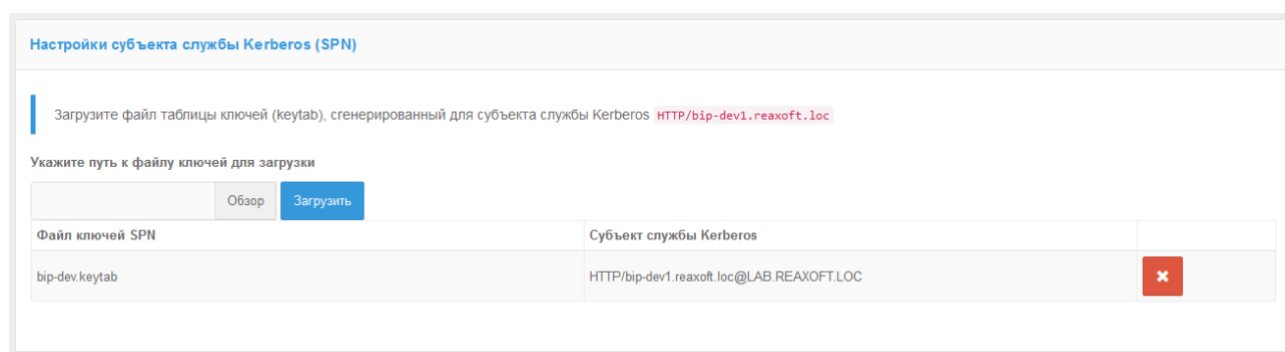


Рисунок 30 – Keytab-файл успешно загружен

Далее необходимо определить параметры соответствия Kerberos-токена (TGS) и учетной записи в Blitz Identity Provider (Рисунок 31).

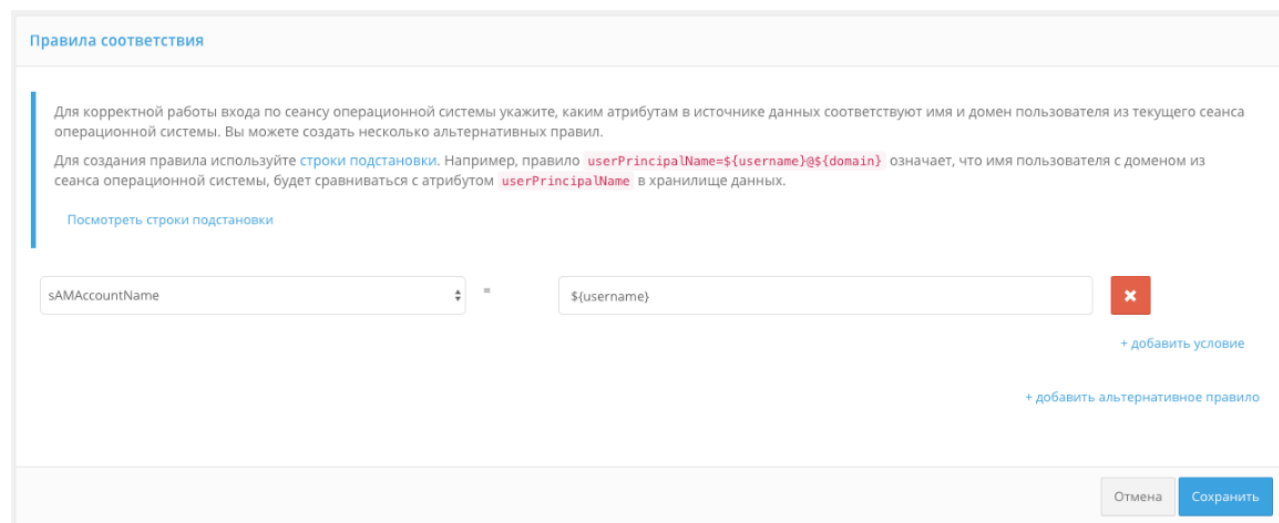


Рисунок 31 – Настройка соответствия Kerberos-идентификатора пользователя и его учетной записи в хранилище

Например, можно задать соответствие, что получаемый из Kerberos-токена идентификатор пользователя (username) должен соответствовать атрибуту `sAMAccountName` учетной записи, получаемому из LDAP-каталога (Microsoft Active Directory).

Далее необходимо установить параметры задержек при использовании метода входа с использованием сеанса операционной системы (Рисунок 32).

Дополнительные настройки

Время задержки перед запуском метода	<input type="text" value="5"/>	Количество секунд, в течение которых пользователь может переключиться на другой метод аутентификации
Время ожидания получения токена	<input type="text" value="5"/>	Количество секунд ожидания получения токена. По окончании периода возвращается сообщение об ошибке

Отмена Сохранить

Рисунок 32 – Дополнительные настройки

Blitz Identity Provider предоставляет два возможных сценария использования входа по сеансу операционной системы:

Основной сценарий. Пользователи входят в операционную систему, и после этого должны сквозным образом входить во все приложения, подключенные к Blitz Identity Provider. Предоставлять пользователям возможность войти в приложения под другой учетной записью не требуется. В этом случае нужно установить «Время задержки перед запуском метода», равное **0** секунд. При обращении к приложению сразу будет произведена попытка сквозного входа по сеансу операционной системы.

Дополнительный сценарий. Пользователи не всегда имеют возможность войти в домен операционной системы, либо пользователям в некоторых случаях необходима возможность войти в приложения под другой учетной записью чем та, что они использовали для входа в домен. В этом случае нужно установить «Время задержки перед запуском метода» такое, чтобы пользователю хватило времени для возможности отменить автоматический вход с использованием сеанса операционной системы.

«Время ожидания получения токена» нужно установить достаточным, чтобы Kerberos-сервер успевал предоставить ответ Blitz Identity Provider. Обычно достаточно установить 5 секунд.

Как и в случае входа по логину и паролю, по умолчанию поиск пользователей для аутентификации происходит во всех активных хранилищах. В блоке «Правила выбора хранилища атрибутов» можно настроить правила, при выполнении которых поиск пользователя будет осуществляться в определенном хранилище (подробнее см. п. 4.1).

4.5.3. Настройки браузеров пользователей

В зависимости от используемого пользователем браузера может потребоваться его дополнительная настройка для поддержки Kerberos-идентификации.

Для Google Chrome в Windows и Apple Safari в macOS отдельная настройка не требуется.

Для Google Chrome в macOS и в Linux нужно осуществлять запуск Google Chrome специальным образом:

```
"/Applications/Google Chrome.app/Contents/MacOS/Google Chrome" --args --auth-server-whitelist="idp.domain.ru" --auth-negotiate-delegate-whitelist="idp.domain.ru"
```

Где в качестве `idp.domain.ru` нужно указать URL сайта Blitz Identity Provider.

Для Microsoft Internet Explorer нужно задать следующие настройки:

- в меню «Сервис → Свойства обозревателя → Безопасность → Местная интрасеть» нажать кнопку «Сайты». В открывшемся окне нажать кнопку «Дополнительно» и внести сайт с Blitz Identity Provider в список сайтов «Местная интрасеть» (см. рис. 33).
- в меню «Сервис → Свойства обозревателя → Безопасность → Местная интрасеть» нажать кнопку «Другой...». В открывшемся окне найти настройку «Проверка подлинности пользователя → Вход». Установить ее в значение «Автоматический вход в сеть только в зоне интрасети» (см. рис. 34).
- перезапустить браузер.

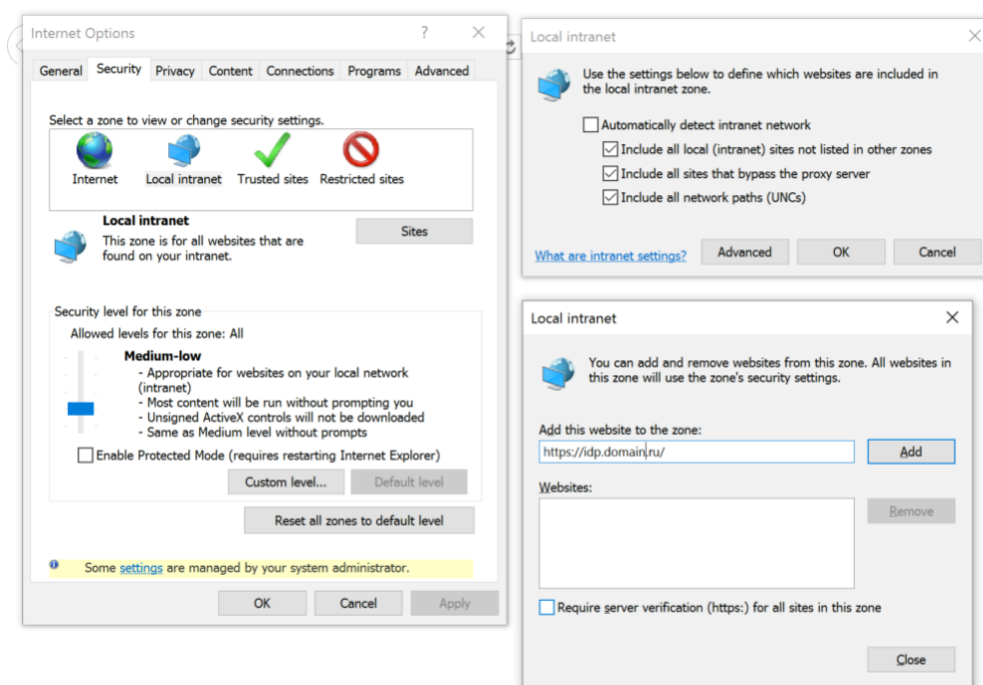


Рисунок 33 – Настройки Internet Explorer для Kerberos – включение Blitz Identity Provider в ресурсы Локальной вычислительной сети

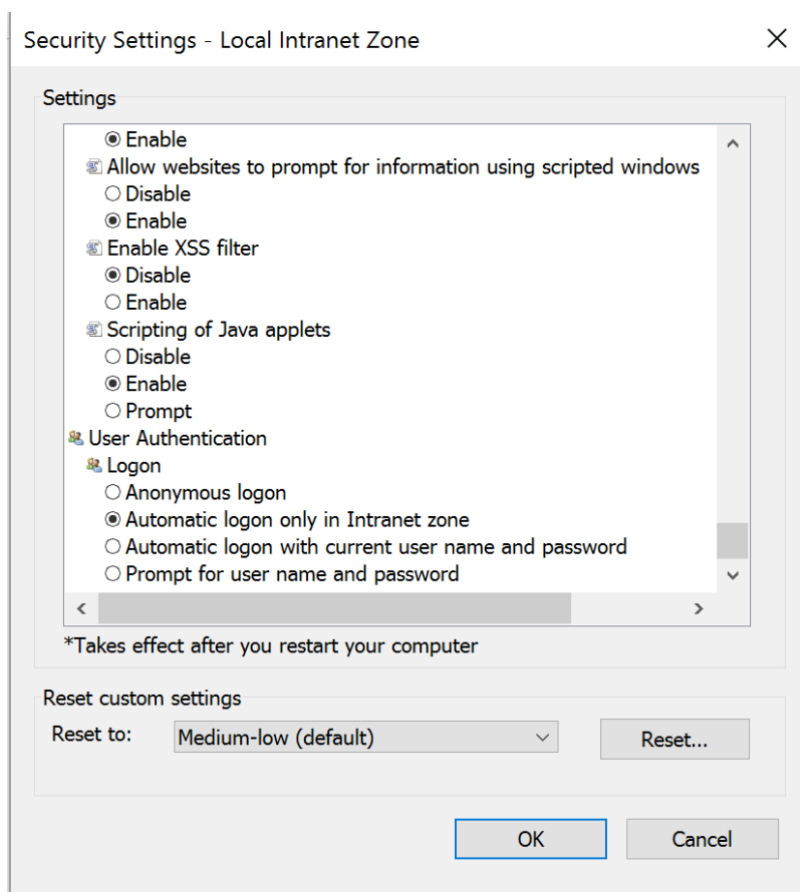


Рисунок 34 – Настройки Internet Explorer для Kerberos – включение
встроенной идентификации

Для Mozilla Firefox нужно задать следующие настройки:

- в адресной строке браузера ввести `about:config` и нажать «Enter». В следующем окне ввести `network.nego` в поле «Фильтры». Дважды нажать на найденной записи «`network.negotiate-auth.trusted-uris`» и установить в ней значение URL сайта с Blitz Identity Provider, например, `idp.domain.ru`. При указании адресов можно использовать звезду (*) и указать несколько URL через запятую, например: `https://*.idp.domain.ru,http://*.idp.domain.ru`. Закрыть всплывающее окно кнопкой «OK»;
- дважды нажать на найденной записи «`network.negotiate-auth.delegation-uris`» и установить в ней значение URL сайта с Blitz Identity Provider, например, `idp.domain.ru`. При указании адресов можно использовать звезду (*) и указать несколько URL через запятую, например: `https://*.idp.domain.ru,http://*.idp.domain.ru`. Закрыть всплывающее окно кнопкой «OK»;
- открыть параметр «`network.auth-sspi`», установить его значение в `true`;
- перезапустить браузер.

4.5.4. Настройки запуска приложений Blitz Identity Provider

У пользователей могут возникнуть проблемы при входе по сеансу операционной системы, если они используют браузер Internet Explorer, и если в домене их учетная запись включена во многие группы безопасности, либо если DN учетной записи достаточно длинный. Чтобы избежать такой ситуации, необходимо при запуске приложения сервиса аутентификации blitz-idp задать специальный JAVA-параметр, определяющий большой допустимый размер HTTP-заголовка. Для этого необходимо отредактировать файл `/etc/default/blitz-idp`. В параметр `JAVA_OPTS` добавить ключ:

```
-Dakka.http.parsing.max-header-value-length=16K
```

4.5.5. Настройки веб-сервера

У пользователей могут возникнуть проблемы при входе по сеансу операционной системы, если они используют браузер Internet Explorer, и если в домене их учетная запись включена во многие группы безопасности, либо если DN учетной записи достаточно длинный. Чтобы избежать такой ситуации, необходимо скорректировать настройки веб-сервера, определяющие допустимый размер буферов заголовков.

Рекомендуемые значения буферов для nginx приведены ниже:

```
proxy_buffer_size 16k;  
proxy_buffers 4 16k;  
proxy_busy_buffers_size 16k;  
client_body_buffer_size 16K;  
client_header_buffer_size 16k;  
client_max_body_size 8m;  
large_client_header_buffers 2 16k;
```

4.6. Настройка входа с помощью кодов подтверждения

Можно использовать отправляемые в мобильное приложение push-уведомления или SMS-сообщения для проверки:

- первого фактора аутентификации;
- второго фактора аутентификации (см. п. 4.11).

Для использования кодов подтверждения необходимо:

- настроить и включить метод аутентификации «Подтверждение с помощью кода» (Рисунок 35). Необходимо настроить:
 - способ идентификации учетной записи – задать регулярное выражение. Например, правило `mobile=${login}` означает, что введенный пользователем логин в форме входа будет сопоставлен с атрибутом `mobile`;
 - длину кода подтверждения;
 - время действия кода подтверждения;
 - количество попыток ввода кода подтверждения;

- сконфигурировать способы отправки кода:
 - отправлять push-уведомление – нужно указать атрибут с номером мобильного телефона или иным необходимым сервису идентификатором пользователя, например, `{mobile}`;
 - отправлять SMS – указать атрибут с номером мобильного телефона пользователя, например, `{mobile}`;
- настроить подключение Blitz Identity Provider к SMS-шлюзу и сервису отправки push-уведомления (см. п. 12.1).

Если у пользователя не задан номер мобильного телефона, то он не сможет использовать способ подтверждения входа с помощью кода подтверждения, отправляемого по SMS.

По умолчанию используются единые настройки для кодов подтверждения, отправляемых для проверки первого и второго фактора. Для разделения настроек необходимо перейти по ссылке «Сконфигурировать профиль для каждого фактора» в блоке «Профили настройки метода». Тогда настройки будут разведены и можно будет переключаться между первым и вторым фактором.

При необходимости перейти к единым настройкам следует перейти по ссылке «Преобразовать в единый профиль» в блоке «Профили настройки метода».

Подтверждение с помощью кода

Первый фактор
Второй фактор

Для корректной идентификации пользователя укажите, каким образом должен формироваться логин и какому атрибуту в источнике данных он соответствует. Вы можете создать несколько альтернативных правил определения логина. Ввод логина не чувствителен к регистру.

Для создания правила используйте [строки подстановки](#). Например, правило `CN=${login}` означает, что строка, введенная пользователем, будет сравниваться с атрибутом `CN` в хранилище данных.

[Посмотреть строки подстановки](#)

mobile

=

\${login}

✕

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Параметры кодов подтверждения

Длина

6

Количество символов в коде подтверждения

Время действия

120

Количество секунд, после которого код подтверждения перестает действовать. Необходима отправка нового кода

Количество попыток

3

Количество неудачных попыток ввода кода подтверждения. Если количество попыток превышено, требуется отправка нового кода

[+ Добавить способ отправки](#)
Отмена
Сохранить

Рисунок 35 – Настройки входа с помощью кода подтверждения

4.7. Настройка входа с известного устройства

Вход с известного устройства позволяет не запрашивать идентификацию и аутентификацию пользователя (метод первого фактора), если пользователь, в течение определенного времени, уже осуществлял вход с данного устройства и браузера. Иными словами, пользователь может входить без аутентификации после перезапуска браузера.

Настройка метода включает в себя указание длительности запоминания устройства. Также можно установить, что при входе с запомненного устройства не будет требоваться двухфакторная аутентификация (опция «Приравнять использование этого метода к применению первого и второго фактора»). Если эта опция включена, то вход с известного устройства будет означать, что пользователь прошел двухфакторную аутентификацию (Рисунок 36).

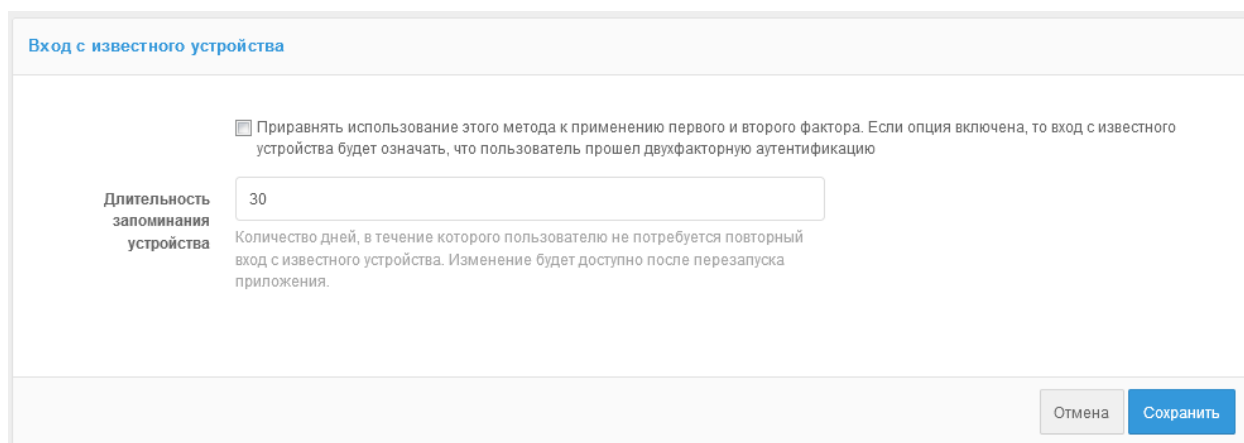


Рисунок 36 – Настройка входа с известного устройства

4.8. Подтверждение входа разовым паролем на основе состояния (НОТР)

Для проверки второго фактора аутентификации с использованием метода аутентификации «Разовый пароль на основе секрета (НОТР)» можно использовать любой аппаратный брелок, совместимый со стандартом RFC4226 «НОТР: An HMAC-Based One-Time Password Algorithm»¹⁶.

Для использования НОТР необходимо:

- настроить и включить метод аутентификации (см. Рисунок 37);
- загрузить в Blitz Identity Provider файл с описаниями НОТР-устройств. Файл с описаниями предоставляет поставщик НОТР-устройств. Для загрузки файла с описанием используется раздел меню «Устройства» в консоли управления Blitz Identity Provider;

¹⁶ См.: <https://tools.ietf.org/html/rfc4226>

- привязать НОТР-устройство к учетной записи пользователя и выдать НОТР-устройство пользователю. Привязку можно выполнить двумя способами – либо администратор привязывает устройство по серийному номеру к учетной записи пользователя в консоли управления в меню «Пользователи», либо пользователь привязывает устройство к своей учетной записи самостоятельно с использованием веб-приложения «Личный кабинет» (см. п. 7.2).

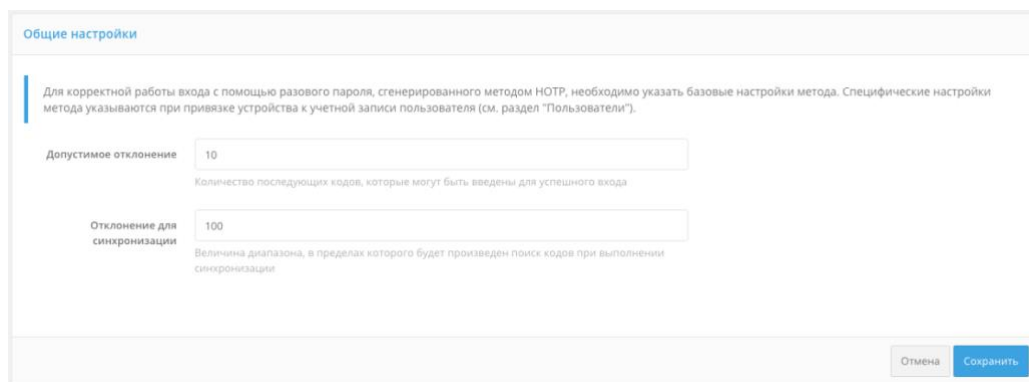


Рисунок 37 – Настройки НОТР-аутентификации

Для настройки метода аутентификации «Разовый пароль на основе секрета (НОТР)» необходимо задать максимальное допустимое отклонение при проверке кода — количество последующих кодов (например, если пользователь случайно нажал кнопку генерирования нового пароля и не использовал его в процессе аутентификации), при котором аутентификация пройдет успешно. При этом при вводе пользователем правильного кода Blitz Identity Provider автоматически восстановит синхронизацию с устройством.

Если пользователь многократно будет нажимать на устройстве кнопку выработки кода и не будет использовать код для подтверждения входа, то устройство перестанет быть синхронизированным с сервером. В этом случае при очередном входе пользователя в Blitz Identity Provider ему на странице входа будет предложено пройти процедуру сверки устройства. Для этого пользователь введет три последовательно выработанных устройством кода подтверждения. Далее в соответствии с заданной настройкой «Отклонение для синхронизации» Blitz Identity Provider проверит, встречается ли введенная пользователем последовательность кодов, и восстановит синхронизацию с устройством в случае успеха.

4.9. Подтверждение входа разовым паролем основе времени (ТОТР)

Для проверки второго фактора аутентификации с использованием метода аутентификации «Разовый пароль на основе времени (ТОТР)» можно использовать любые устройства и программы, совместимые со стандартом RFC6238 «TOTP: Time-Based One-Time

Password Algorithm»¹⁷. В качестве таковых могут быть:

- аппаратные брелоки (генераторы разовых паролей) на основе времени;
- мобильные приложения¹⁸.

В настройках метода аутентификации «Разовый пароль на основе времени (TOTP)» необходимо указать:

1. Допустимое отклонение при проверке кода (количество предыдущих / последующих кодов). По умолчанию оба значения равны 1: пользователь при входе может ввести как текущий код подтверждения, так и следующий или предыдущий (т.е. сгенерированный в соседних временных интервалах). Такая необходимость может возникнуть, например, для компенсации возможной незначительной рассинхронизации серверного времени и времени на TOTP-устройствах пользователей.
2. Настройка отображения генераторов разовых паролей, которая включает в себя «Атрибут с именем пользователя» и «Название единой системы входа». Эти параметры будут отображаться в мобильном приложении после привязки учетной записи пользователя.
3. Ссылки на приложения-генераторы разовых паролей. Следует указать ссылки на приложения, которые рекомендуется использовать пользователям. Эти ссылки будут предложены пользователю в веб-приложении «Личный кабинет».

¹⁷ См.: <https://tools.ietf.org/html/rfc6238>

¹⁸ Наиболее известные приложения для выработки TOTP-кодов: Google Authenticator, Twilio Authy, FreeOTP Authenticator, Microsoft Authenticator, Яндекс.Ключ.

Разовый пароль на основе времени (TOTP)

Для корректной работы входа с помощью разового пароля, сгенерированного методом TOTP, необходимо указать базовые настройки метода. Некоторые настройки метода указываются при привязке устройства к учетной записи пользователя (см. раздел "Пользователи").

Допустимое отклонение (вперед)
Количество последующих по времени кодов, которые могут быть введены для успешного входа

Допустимое отклонение (назад)
Количество предыдущих по времени кодов, которые могут быть введены для успешного входа

Настройка отображения генераторов разовых паролей

Атрибут с именем пользователя
Имя пользователя будет отображаться в генераторе разовых паролей после привязки

Название единой системы входа
Название системы будет отображаться в генераторе разовых паролей после привязки

Ссылки на приложения - генераторы разовых паролей

Укажите для каждой ОС, какие мобильные приложения рекомендуется использовать для генерации разовых паролей. Если ссылка не указана, то пользователям не будет предложено загрузить приложение для данной ОС.

iOS	<input type="text" value="http://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8"/>
Android	<input type="text" value="https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2"/>
Windows Mobile	<input type="text" value="https://www.microsoft.com/ru-ru/store/apps/authenticator/9wzdncrfj3rj"/>

Рисунок 38 – Общие настройки TOTP-аутентификации

4.10. Привязка устройств к учетным записям пользователей

Привязка HOTP и TOTP устройств через консоль управления отличается в зависимости от того, используются аппаратные брелоки или мобильные приложения.

4.10.1. Привязка аппаратных брелоков

Для возможности использования аппаратных HOTP и TOTP устройств в качестве средств аутентификации администратор должен предварительно загрузить в консоли управления в меню «Устройства» (Рисунок 39) файл с описаниями партии устройств, полученной от их поставщика. Файл содержит сведения о серийном номере устройства, векторе инициализации и ряд других настроек. Blitz Identity Provider поддерживает загрузку файлов распространенных форматов (специализированные XML-файлы, CSV-файлы) файлов с описаниями устройств от различных производителей устройств.

Рисунок 39 – Загрузка файлов с описаниями устройств генерации кодов

Для выполнения загрузки файла нужно задать имя для загружаемых генераторов (это может быть, например, имя устройства), формат данных, а также путь к файлу с описаниями устройств. По нажатии кнопки «Загрузить» Blitz Identity Provider сообщит, сколько записей устройств было загружено или отброшено (если их описание в файле было некорректно, либо запись об устройстве уже присутствует в системе).

В разделе «Устройства» также можно выполнить поиск устройства по серийному номеру, посмотреть, было ли привязано и к какой учетной записи найденное устройство.

После загрузки файла следует:

- перейти к учетной записи пользователя (меню «Пользователи», см п. 9.3.3 документа);
- найти раздел «Генератор паролей на основе времени (TOTP)» или «Генератор паролей на основе секрета (HOTP)»;
- выбрать «Другой тип»;
- ввести серийный номер необходимого устройства и текущий код подтверждения.

Рисунок 40 – Привязка аппаратного TOTP-генератора

4.10.2. Привязка мобильного приложения

Для привязки мобильного приложения следует:

- перейти к учетной записи пользователя, которому необходимо привязать мобильное приложение (меню «Пользователи», см. п. 9.3.3 документа);
- найти раздел «Генератор паролей на основе времени (TOTP)»;
- выбрать «GoogleAuthenticator»;
- при необходимости отредактировать название мобильного приложения;
- с помощью мобильного приложения сфотографировать отображаемый QR-код или ввести в приложение строчку-секрет.

Также пользователь может самостоятельно привязать мобильное приложение, генерирующее TOTP-коды, в веб-приложении «Личный кабинет».

Генератор паролей на основе времени (TOTP)

Название генератора: GoogleAuthenticator

Алгоритм шифрования: SHA1

Длина пароля: 6
Число символов, из которых будет состоять разовый пароль

Время обновления пароля: 30
Время (в секундах), в течение которого будет обновляться разовый пароль

Секрет: NAWGF7K7DXV7SDH25FCMBOS8UPWJ2CQG
Секрет закодирован в Base32 кодировке

Сохранить

Рисунок 41 – Привязка мобильного приложения, генерирующего TOTP-коды

4.11. Коды подтверждения, отправляемые в SMS и push-уведомлениях

Можно использовать отправляемые в мобильное приложение push-уведомления или SMS-сообщения для подтверждения входа (второго фактора аутентификации).

Для этого необходимо:

- настроить и включить метод аутентификации «Подтверждение с помощью кода».

Необходимо задать:

- длину кода подтверждения;
- время его действия;
- количество допустимых попыток;

- сконфигурировать способы отправки кода:
 - отправлять push-уведомление – нужно указать атрибут с номером мобильного телефона или иным необходимым сервису идентификатором пользователя, например, `{mobile}`;
 - отправлять SMS – указать атрибут с номером мобильного телефона пользователя, например, `{mobile}`;
- настроить подключение Blitz Identity Provider к SMS-шлюзу и сервису отправки push-уведомления (см. п. 12.1).

Если у пользователя не задан номер мобильного телефона, то он не сможет использовать способ подтверждения входа с помощью кода подтверждения, отправляемого по SMS.

По умолчанию используются единые настройки для кодов подтверждения, отправляемых для проверки первого и второго фактора (см. п. 4.6). Для разделения настроек необходимо перейти по ссылке «Сконфигурировать профиль для каждого фактора» в блоке «Профили настройки метода». Тогда настройки будут разведены и можно будет переключаться между первым и вторым фактором.

При необходимости перейти к единым настройкам следует перейти по ссылке «Преобразовать в единый профиль» в блоке «Профили настройки метода».

Подтверждение с помощью кода

Первый фактор
Второй фактор

Параметры кодов подтверждения

Длина

Количество символов в коде подтверждения

Время действия

Количество секунд, после которого код подтверждения перестает действовать. Необходима отправка нового кода

Количество попыток

Количество неудачных попыток ввода кода подтверждения. Если количество попыток превышено, требуется отправка нового кода

Способы отправки кода

Настройте способы отправки кодов подтверждения. Если будет выбрано более одного способа, то первый будет рассматриваться как основной, а остальные как резервные.

Отправлять	Атрибут с контактом	
Push-уведомление ▼	<input style="width: 90%;" type="text" value="\${mobile}\${guid}"/>	✕
SMS ▼	<input style="width: 90%;" type="text" value="\${mobile-}"/>	✕

[+ Добавить способ отправки](#)

Отмена
Сохранить

Профили настройки метода

Для каждого фактора используется свой профиль. В результате преобразования настройки текущего профиля будут использованы для единого профиля.

[Преобразовать в единый профиль](#)

Рисунок 42 – Настройки кодов подтверждения для двухфакторной аутентификации

4.12. Коды подтверждения, отправляемые по электронной почте

Можно использовать отправляемые по электронной почте коды подтверждения для подтверждения входа (второго фактора аутентификации).

Для этого необходимо:

- настроить и включить этот метод аутентификации. Для корректной работы метода необходимо определить:
 - длину кода подтверждения;
 - время его действия;
 - количество допустимых попыток;
 - сконфигурировать способ отправки: указать атрибут, в которых сохранен адрес электронной почты пользователя, например, `#{email}`;
- настроить подключение Blitz Identity Provider к SMTP-сервису (см. п. 12.3).

Следует помнить, что если у пользователя не задан адрес электронной почты, то он не сможет использовать метод подтверждения входа с помощью кодов, отправляемых на электронную почту.

The screenshot shows a configuration page titled "Подтверждение с помощью электронной почты". It is divided into two main sections: "Параметры кодов подтверждения" and "Параметры отправки".

Параметры кодов подтверждения

- Длина:** Input field with value "6". Description: "Количество символов в коде подтверждения".
- Время действия:** Input field with value "300". Description: "Количество секунд, после которого код подтверждения перестает действовать. Необходима отправка нового кода".
- Количество попыток:** Input field with value "10". Description: "Количество неудачных попыток ввода кода подтверждения. Если количество попыток превышено, требуется отправка нового кода".

Параметры отправки

- Атрибут с контактом:** Input field with value "\${mail-}". Description: "Выражение, по которому будет формироваться адрес электронной почты для отправки кода подтверждения".

At the bottom right, there are two buttons: "Отмена" (grey) and "Сохранить" (blue).

Рисунок 43 – Настройки кодов подтверждения, отправляемых по электронной почте

4.13. Подтверждение входа с помощью Duo Mobile

Можно использовать мобильное приложение Duo Mobile¹⁹ (компания Cisco) для подтверждения входа (второго фактора аутентификации).

Для этого необходимо выполнить настройки на стороне сервиса Duo Security:

- зарегистрировать учетную запись на сайте Duo²⁰;
- войти в панель администратора²¹ и перейти в раздел «Applications»;
- нажать на «Protect an Application», среди приложений найти «Auth API». После этого нажать на «Protect this Application», чтобы получить свой интеграционный и секретный ключ, а также имя хоста.

После этого нужно провести настройки в консоли управления Blitz Identity Provider:

- сконфигурировать метод аутентификации «Duo push-аутентификация» (см. рис. 44).

Необходимо указать:

- параметры учетной записи Duo (имя хоста, интеграционный и секретный ключ);
 - параметры взаимодействия:
 - имя пользователя (задается с помощью строки подстановки) – это имя будет отображено в Duo Mobile в качестве имени учетной записи;
 - время действия кода активации (в секундах) – время, в течение которого действителен код привязки (QR-код);
 - данные для отображения в приложении – информация, отображаемая пользователю в Duo Mobile в виде «ключ: значение». Здесь можно передать значение пользовательского атрибута или какое-то фиксированное значение. В качестве значения также можно указать строку `${app}` – это позволит отобразить имя приложения, куда пользователь входит;
 - ссылки на загрузку приложения Duo Mobile.
- включить метод «Duo push-аутентификации» в разделе «Аутентификация».

¹⁹ См.: <https://duo.com/product/multi-factor-authentication-mfa/duo-mobile-app>

²⁰ См.: <https://signup.duo.com/>

²¹ См.: <https://admin.duosecurity.com/>

Настройки Duo push-аутентификации

Для использования push-аутентификации от Duo Security необходимо:

- зарегистрировать учетную запись на [сайте Duo](#);
- войти в [панель администратора](#) и перейти в раздел Applications;
- нажать на Protect an Application, среди приложений найти Auth API. После этого нажать на Protect this Application, чтобы получить свой интеграционный и секретный ключ, а также имя хоста.

Учетная запись

Имя хоста (API hostname)

Интеграционный ключ (integration key)

Секретный ключ (secret key)

Параметры взаимодействия

Шаблон имени пользователя
Строка подстановки, определяющая имя пользователя в запросе на вход. Например, "\$ {mail}"

Время действия кода активации
Время (в секундах), в течение которого действителен код привязки (штрихкод)

Данные для отображения в приложении

При аутентификации может быть передана информация, которая будет отображена в мобильном приложении в виде "ключ: значение". Задайте необходимые ключи и их значения, используя строки подстановки. Например, `Имя = $ {name} $ {surname}` позволит передать ключ `Имя` со значением из атрибутов `name` и `surname`.

[Посмотреть строки подстановки](#)

Имя пользователя	=	\$ {name}	✕
Вход в:	=	Blitz IDP PROD	✕

[+ Добавить](#)

Ссылки на приложения - Duo Mobile

Укажите для каждой ОС, какие мобильные приложения рекомендуется использовать для push-аутентификации. Если ссылка не указана, то пользователям не будет предложено загрузить приложение для данной ОС.

iOS	https://itunes.apple.com/ru/app/duo-mobile/id422663827
Android	https://play.google.com/store/apps/details?id=com.duosecurity
Windows Mobile	https://www.microsoft.com/ru-ru/store/p/duo-mobile/9nblgg08rr

Отмена
Сохранить

Рисунок 44 – Настройки Duo push-аутентификации

Привязка приложения Duo Mobile к учетной записи пользователя возможна следующими способами:

- пользователем самостоятельно через веб-приложение «Личный кабинет»;
- администратором через консоль управления.

В веб-приложении «Личный кабинет» пользователь должен перейти в раздел «Безопасность / Подтверждение входа» и выполнить следующие шаги:

1. Выбрать способ подтверждения входа – «Подтверждение с помощью мобильного приложения Duo Mobile».
2. Установить на смартфон приложение Duo Mobile и отсканировать QR-код, а также нажать «Подтвердить».
3. После проверки этот метод аутентификации будет добавлен пользователю.

В консоли управления администратор должен:

1. Найти необходимого пользователя.
2. Перейти к блоку «Приложение Duo Mobile (QR-код)» и нажать на кнопку «Привязать Duo Mobile».
3. Попросить пользователя отсканировать QR-код с помощью мобильного приложения Duo Mobile.

На рисунках приведен пример внешнего вида страницы входа при подтверждении входа с помощью push-уведомления в приложении Duo Mobile.

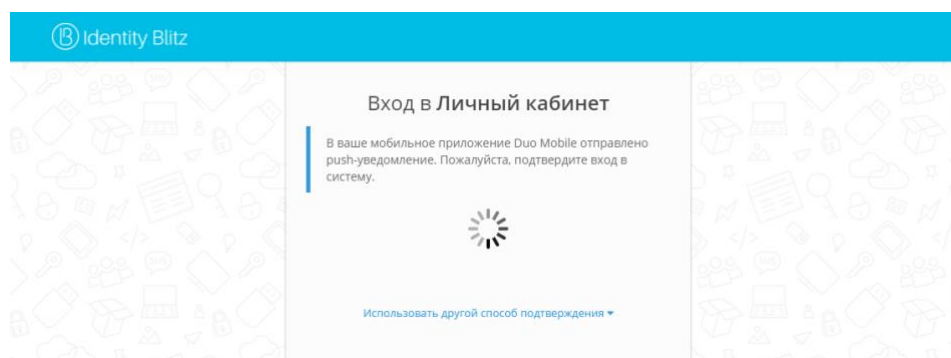


Рисунок 45 – Инициирование push-аутентификации



Рисунок 46 – Запрос push-аутентификации на смартфоне (приложение Duo Mobile)

4.14. Настройка внешнего метода аутентификации

Blitz Identity Provider позволяет разработчикам при внедрении добавить поддержку своего собственного метода аутентификации. Для этого нужно разработать приложение, реализующее логику аутентификации, и подключить этого приложение к Blitz Identity Provider. В Blitz Identity Provider для этого конфигурируется метод аутентификации «Внешний метод аутентификации». Можно реализовать внешний метод аутентификации для работы как в качестве первого, так и в качестве второго фактора аутентификации.

Для настройки использования Blitz Identity Provider внешнего метода аутентификации необходимо:

1. Сконфигурировать новый «внешний» метод первого или второго фактора аутентификации, нажав на ссылку «Добавить внешний метод аутентификации».

Указать параметры этого метода аутентификации:

- идентификатор метода – карточка с названием метода будет отображаться среди методов аутентификации, к методу с данным идентификатором можно будет обращаться из процедуры входа;
- URL внешнего сервиса;
- названия утверждений – перечень утверждений, которые внешний метод может установить пользователю
- передаваемые cookie – перечень названий cookies, которые будут пробрасываться при вызове внешнего метода;
- передаваемые заголовки – перечень заголовков, которые будут пробрасываться при вызове внешнего метода;
- URL сервиса определения применимости – адрес опционального сервиса метода. Если указан, то данный URL будет вызываться перед вызовом

основного сервиса, чтобы определить применимость данного метода аутентификации. Если URL не указан, то считается, что метод применим всегда;

- cookie безопасности – название cookie, в которой будет передаваться идентификатор сессии из внешнего метода.

2. На стороне внешнего метода необходимо предусмотреть обработку запросов на аутентификацию и определение применимости согласно документу «Руководству по интеграции».

Добавление внешнего метода аутентификации

Идентификатор	<input type="text" value="first"/>	Уникальное название (идентификатор) внешнего метода аутентификации. Будет использоваться в том числе и в аудите
URL сервиса	<input type="text" value="https://extmethod.test.net"/>	Адрес основного сервиса внешнего метода аутентификации. Принимает на вход текущую информацию о процессе аутентификации и возвращает HTTP-ответ, который отображается пользователю
Названия утверждений	<input type="text"/>	Названия утверждений, которые сервис может установить пользователю
Передаваемые cookie	<input type="text"/>	Названия cookies, которые будут пробрасываться при вызове сервиса метода
Передаваемые заголовки	<input type="text"/>	Названия заголовков, которые будут пробрасываться при вызове сервиса метода
URL сервиса определения применимости	<input type="text"/>	Адрес опционального сервиса метода. Если указан, то данный URL будет вызываться перед вызовом основного сервиса, чтобы определить применимость данного метода аутентификации. Если URL не указан, то считается, что метод применим всегда
Cookie безопасности	<input type="text" value="Bmr"/>	Название cookie, в которой будет передаваться идентификатор сессии из внешнего метода

Рисунок 47 – Пример настройки внешнего метода

5. Регистрация приложений

Регистрация приложений в Blitz Identity Provider необходима для того, чтобы приложения могли использовать предоставляемые Blitz Identity Provider сервисы:

- запрашивать идентификацию и аутентификацию пользователей;
- вызывать REST-сервисы Blitz Identity Provider.

Управление приложениями осуществляется в разделе «Приложения» консоли управления (Рисунок 48).

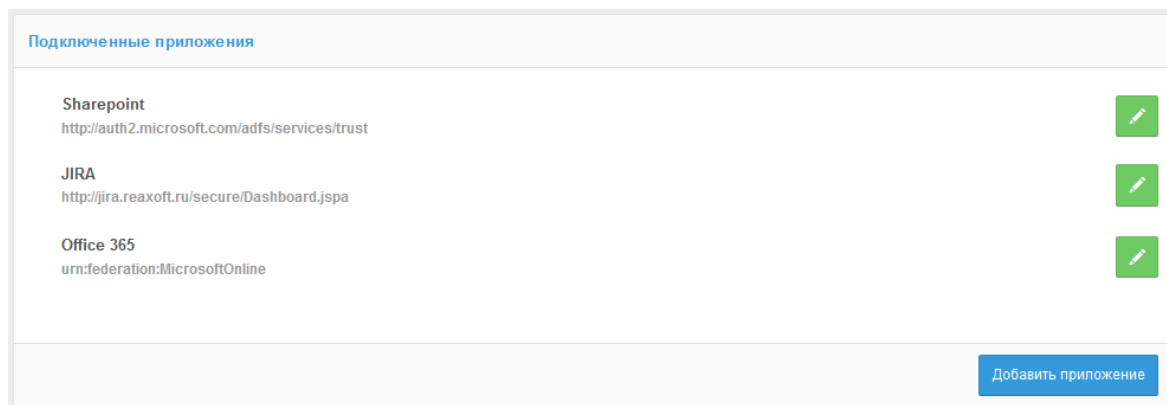


Рисунок 48 – Главный экран настройки приложений

5.1. Создание учетной записи нового приложения

Для подключения нового веб-приложения необходимо перейти в раздел «Приложения» консоли и выбрать пункт «Добавить приложение». Это действие запустит мастер подключения нового приложения, работа которого включает в себя следующие шаги:

Шаг 1. Базовые настройки. Требуется указать идентификатор подключаемого приложения (при подключении по протоколу SAML идентификатор соответствует entityID, при подключении по OAuth 2.0 – client_id, при задании идентификатора для OAuth 2.0 **недопустимо** использовать двоеточие), его название и домен, т.е. URL, по которому доступно данное приложение (рис. 49).

Название приложения используется в дальнейшем в Blitz Identity Provider при отображении на странице входа в случае инициирования приложением запроса на идентификацию пользователя.

Домен приложения используется при необходимости перенаправления пользователя в приложение из веб-страниц Blitz Identity Provider. Перенаправление осуществляется на указанный домен или на переданный в процессе взаимодействия с Blitz Identity Provider специализированный redirect_url, но при этом выполняется сверка, что redirect_url соответствует заданному в настройке приложения домену.

Новое приложение

Идентификатор (entityID, client_id)
Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth (соответствует client_id).

Название
Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider.

Домен

Рисунок 49 – Базовые настройки приложения

Шаг 2. Выбор шаблона страницы входа и настройка логота (Рисунок 50). В списке «Шаблон страниц» необходимо выбрать, на основе какого шаблона должна отображаться страница входа при попытке доступа пользователя в данное приложение. Инструкция по созданию нового шаблона входа приведена в п. 13.

При необходимости можно указать ключ шифрования идентификаторов («домен приватности»). Создание домена приватности обеспечивает уникальность идентификатора пользователя, полученного приложением по результатам аутентификации, т.е. этот идентификатор будет уникальным, но специфичным для данного приложения. Иными словами, если запрос на получение данных пользователя будет инициировать приложение из другого домена приватности, то оно будет получать другое значение идентификатора пользователя. При нажатии на поле будут отображены сконфигурированные ранее ключи шифрования, с возможностью задать новый. Приложения, имеющие общий ключ шифрования, будут получать идентичный идентификатор пользователя.

В настройке «Префиксы ссылок возврата при выходе» нужно задать допустимые URL страниц перенаправления пользователя после инициирования приложением логота. Настройку следует задавать только в случае, если в приложении реализована функция логота. Допустимо задать один или несколько префиксов ссылок возврата.

Параметры приложения

Идентификатор (entityID или client_id)
Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).

Название
Отображаемое пользователями имя приложения. Используется только внутри Blitz Identity Provider

Домен
Ссылка на стартовую страницу приложения, например, http://testdomain.ru/. При TLS-аутентификации приложения проверяется, что в сертификате приложения указан именно этот домен

Ключ шифрования идентификаторов
Если ключ задан, то идентификатор пользователя для приложения будет зашифрован с использованием данного ключа. Значение ключа можно выбрать из списка. Также можно назначить новый ключ, для этого введите его в строке поиска и нажмите Enter

Шаблон страниц
Шаблон страниц определяет внешний вид страниц входа. Если шаблон не указан, то используется шаблон по умолчанию.

Префиксы ссылок возврата при выходе
Список URL используется для проверки ссылок возврата (post_logout_redirect_uri). Если в запросе на выход указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в выходе будет отказано

[Удалить приложение](#) [Сохранить](#)

Рисунок 50 – Выбор шаблона страницы входа и настройка логгута

Шаг 3. Настройки протоколов подключения (Рисунок 51). Необходимо настроить один или несколько протоколов подключения приложения к Blitz Identity Provider.

Протоколы

[SAML](#) [OAuth 2.0](#) [Simple](#) [REST](#)

Протокол SAML не сконфигурирован. [Сконфигурировать](#)

Рисунок 51 – Настройка протоколов подключения

Поддерживаются следующие протоколы подключения:

- SAML – для подключения приложений по SAML 1.0, 1.1, 2.0 и WS-Federation для идентификации и аутентификации пользователей;
- OAuth 2.0 – для подключения приложений по OAuth 2.0, OpenID Connect 1.0 (OIDC) для идентификации и аутентификации пользователей. В рамках этого протокола возможно конфигурирование динамической регистрации клиентов;
- Simple – для подключения веб-приложений для осуществления идентификации и аутентификации с помощью подстановки в приложение логина и пароля с проxy-сервера, если приложение не поддерживает возможности подключения по SAML/OIDC;
- REST – для подключения приложений, использующих REST-сервисы Blitz Identity Provider по регистрации/изменению учетных записей, управлению устройствами аутентификации пользователей.

Если организация планирует разработку или доработку собственных приложений для

подключения их к Blitz Identity Provider, то разработчикам необходимо ознакомиться с документом «Руководство по интеграции».

Если организация планирует подключить к Blitz Identity Provider приложения, имеющие штатную поддержку подключения по SAML 1.0, SAML 1.1, SAML 2.0, WS-Federation или OIDC (OpenID Connect 1.0, OAuth 2.0), то в последующих подразделах, описываются общие настройки на стороне Blitz Identity Provider подключения произвольного приложения с поддержкой SAML/OIDC.

5.2. Настройка SAML и WS-Federation

5.2.1. Подключение по SAML 1.0/1.1/2.0

При подключении приложения по SAML необходимо задать следующие настройки (Рисунок 52):

- загрузить SAML-метаданные подключаемого приложения;
- убедиться, что переключатель SAML-профиля стоит в режиме «SAML 2.0 Web SSO Profile»;
- в блоке «SAML-профиль» нажать «Сконфигурировать». В появившихся полях указать:
 - указать, нужно ли подписывать SAML-атрибуты (SAML Assertions) в ответах Blitz Identity Provider;
 - указать, нужно ли шифровать SAML-атрибуты в ответах Blitz Identity Provider;
 - указать, нужно ли шифровать SAML-идентификаторы (SAML NameIds) в ответах Blitz Identity Provider;
 - указать, нужно ли включать в ответ перечень утверждений с атрибутами пользователей;
- указать, какие SAML-атрибуты пользователя из Blitz Identity Provider передавать в приложение. SAML-атрибуты должны быть предварительно сконфигурированы в разделе «SAML» консоли управления (см. п. 5.2.3).

Протоколы

SAML OAuth 2.0 Simple REST

Метаданные Открыть с файловой системы

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
3     xmlns:blitz="urn:blitz:shibboleth:2.0:mdext"
4     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
5     entityID="https://bip-dev1.reaxoft.loc/saml-app02">
6   <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
7     <md:KeyDescriptor use="signing">
8       <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
9         <ds:X509Data>
10          <ds:X509Certificate>
11            MIICfzCCAegCCQDUzgTYycEA+TANBgkqhkiG9w0BAQUFADCBgzELMAkGA1UEBhMC
12            U1UxDzANBgNVBAgMBk1vc2NvdzEPMANBA1UEBwwGTW9zY293MRwwDgYDVQKDA5
13            ZWF4b2Z2OMREwDwYDVQQLEDAhZemF5dHN1dGJlEQMA4GA1UEAwwHdGVzZC1zcDEbMBkG
14            CSqGS1b3DQEJARyMdgVzdEB0ZXN0LnJ1b3R4XDEOMTIyMzEOMTEONVcoXDTIOMTIy
15            MzEOMTEONVcoXDTIOMTIyMzEOMTEONVcoXDTIOMTIyMzEOMTEONVcoXDTIOMTIy

```

SAML профиль SAML 2.0 Web SSO Profile WS-Federation Passive Requestor Profile

Подписывать утверждения: always
Правило подписи SAML-утверждений (Sign assertions)

Шифровать утверждения: never
Правило шифрования SAML-утверждений (Encrypt assertions)

Шифровать идентификаторы (NameIDs): never
Правило шифрования идентификаторов (Encrypt NameIDs)

Включить передачу SAML-утверждений о пользователе в специальном блоке Attribute Statement

Атрибуты пользователя
Определите, какие атрибуты пользователя должны передаваться в приложения и с какими названиями

SAML-атрибут	Передавать	
LogonName	<input checked="" type="checkbox"/>	✘
transientId	<input checked="" type="checkbox"/>	✘

[+ Добавить](#)

[Сохранить](#)

Рисунок 52 – Настройки протокола SAML для приложения

5.2.2. Подключение по WS-Federation

При подключении приложения по WS-Federation необходимо задать следующие настройки (Рисунок 53):

- загрузить метаданные подключаемого приложения;
- переключатель SAML-профиля установить в режим «WS-Federation Passive Requestor Profile»;
- в блоке «SAML-профиль» нажать «Сконфигурировать». В появившихся полях указать:
 - указать, нужно ли подписывать утверждения (Assertions) в ответах Blitz Identity Provider;

- указать время жизни утверждений в ответе. Необходимо использовать формат ISO 8601 для указания продолжительности периода²², например, PT5M – 5 минут;
 - указать, нужно ли включать в ответ перечень утверждений с атрибутами пользователей;
- указать, какие атрибуты пользователя из Blitz Identity Provider передавать в приложение. Атрибуты должны быть предварительно сконфигурированы в разделе «SAML» консоли управления (см. п. 5.2.3).

Протоколы

SAML OAuth 2.0 Simple REST

Метаданные Открыть с файловой системы

```

1 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2 <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
3   xmlns:esia="urn:esia:shibboleth:2.0:mdeext"
4   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
5   entityID="https://lab-app.reaxoft.loc/owa/"
6   <md:SPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:wsf-prp:1.0:protocol">
7     <md:AssertionConsumerService Binding="urn:mace:shibboleth:1.0:bindings:HTTP-POST-wsigin"
8       Location="https://lab-app.reaxoft.loc/owa/"
9       index="1"/>
10  </md:SPSSODescriptor>
11 </md:EntityDescriptor>
    
```

SAML профиль SAML 2.0 Web SSO Profile WS-Federation Passive Requestor Profile

Подписывать утверждения: always
Правило подписи SAML-утверждений (Sign assertions)

Время жизни утверждений: PT5M
Время жизни утверждений в ответе в формате ISO 8601. Например, PT5M - 5 минут.

Включить передачу SAML-утверждений о пользователе в специальном блоке Attribute Statement

Атрибуты пользователя
Определите, какие атрибуты пользователя должны передаваться в приложения и с какими названиями

SAML-атрибут	Передавать	
transientid	<input type="checkbox"/>	✘
upn	<input checked="" type="checkbox"/>	✘

[+ Добавить](#)

[Сохранить](#)

Рисунок 53 – Настройки протокола WS-Federation для приложения

5.2.3. Настройка SAML-атрибутов

Для регистрации SAML-атрибутов пользователя в Blitz Identity Provider используется

²² См.: <http://www.ifap.ru/library/gost/86012001.pdf>

раздел «SAML» консоли управления (Рисунок 54).

Для добавления нового SAML-атрибута необходимо:

1. Нажать на ссылку «+ Добавить новый SAML-атрибут».
2. Ввести:
 - название SAML-атрибута (именно оно будет отображаться при подключении SAML-приложений);
 - источник атрибута (отображаются атрибуты, определенные в разделе «Источники данных»);
3. Нажать «Добавить». Атрибут будет добавлен.
4. Определить кодировщики атрибутов. Для этого необходимо:
 - нажать на ссылку «Добавить кодировщик»;
 - выбрать тип кодировщика; следует обратить внимание, что тип кодировщика зависит от версии протокола, с которой работает поставщик услуг (подключенное приложение);
 - название SAML-атрибута, которое будет передано поставщику услуг (в рамках данного типа кодировщика);
 - короткое название, которое будет передано поставщику услуг (в рамках данного типа кодировщика);
 - формат имени.

При необходимости можно определить несколько кодировщиков выбранного SAML-атрибута (для этого каждый кодировщик должен относиться к разным типам кодировщиков).

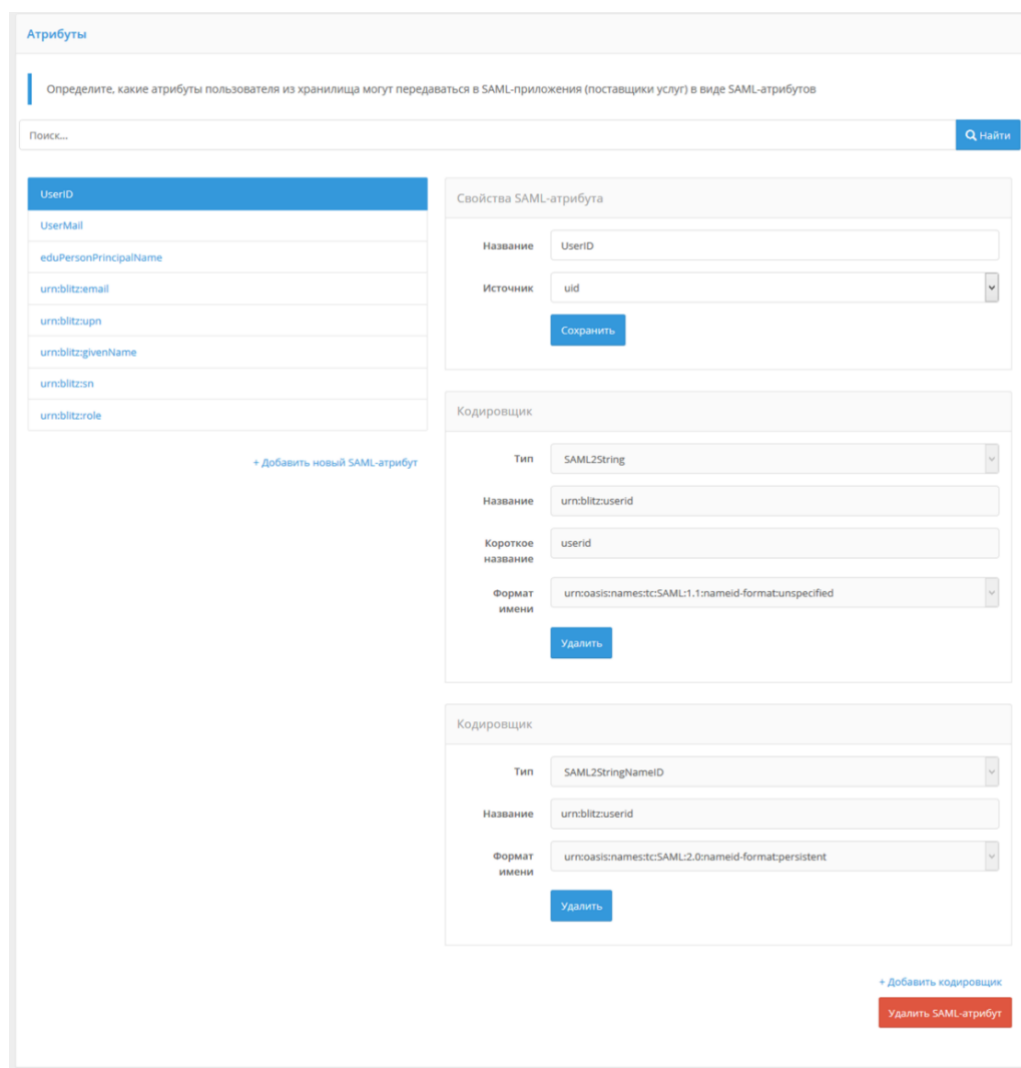


Рисунок 54 – Создание SAML-атрибутов

5.3. Настройка OAuth 2.0 и OpenID Connect 1.0

5.3.1. Настройка приложения

При подключении приложения по OAuth 2.0 или OpenID Connect 1.0 (OIDC) необходимо задать следующие настройки (Рисунок 55):

- указать секретный ключ (или использовать сгенерированный по умолчанию ключ) подключаемого приложения (`client_secret`), который должен использоваться подключенным приложением при обращении к Blitz Identity Provider (если не указан, то аутентификация приложения-клиента должна производиться иначе, например, с использованием проху TLS);
- указать дополнительный секретный ключ (`client_secret`) подключаемого приложения. Рекомендуется для случаев, когда нужно обеспечить плавную смену `client_secret` для данного приложения;
- указать предопределенную ссылку возврата (`redirect_uri`) – URL, на который по

- умолчанию будет переадресован пользователь после прохождения авторизации (`redirect_uri`);
- указать допустимые префиксы ссылок возврата – префикс используется для проверки ссылок возврата (`redirect_uri`), переданных в запросах на идентификацию от приложений. Если в запросе на аутентификацию указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в аутентификации будет отказано;
 - допустимые разрешения – разрешения (`scope`), которые имеет право запрашивать данное приложение;
 - разрешения по умолчанию – разрешения (`scope`), которые будут по умолчанию выданы приложению после аутентификации. Если не указаны, то в запросе на аутентификацию всегда должны быть явно прописаны требуемые разрешения;
 - отметить при необходимости опцию «Не требовать от пользователя согласие на предоставление доступа к данным о себе». Если она отмечена, то при первом входе пользователя в систему не будет отображена страница согласия на предоставление данных этой системе;
 - отметить при необходимости опцию «Обязательное использование Proof Key for Code Exchange (RFC 7636) для Authorization code grant type», если запросы на аутентификацию должны выполняться согласно RFC 7636;
 - выбрать при необходимости метод аутентификации при обращении к сервису выдачи маркеров. Указанные методы аутентификации должны использоваться при обращении к сервису выдачи маркеров (`token endpoint`). При пустом значении доступны все методы;
 - выбрать при необходимости допустимые `grant type`. Параметр определяет список `grant type`, которые будут доступны приложению. При пустом списке доступны все `grant type`;
 - выбрать при необходимости допустимые `response type`. Параметр определяет список `response type`, которые будут доступны приложению при обращении к URL авторизации (`authorization endpoint`). При пустом списке доступны все `response type`;
 - указать время жизни маркера доступа (в секундах). Если параметр не задан, то берется из общих настроек из раздела «OAuth 2.0».
 - указать время жизни маркера обновления (в секундах). Если параметр не задан, то берется из общих настроек из раздела «OAuth 2.0».

Настройки взаимодействия с приложением

Секрет (client_secret)

Секретный ключ подключаемого приложения (client_secret). Если указан, то именно этот секрет должен использоваться подключаемым приложением при обращении к Blitz Identity Provider.

Дополнительный секрет (client_secret)

Дополнительный секретный ключ подключаемого приложения (client_secret). Если указан, то может использоваться в качестве альтернативы к основному секрету.

Предопределенная ссылка возврата (redirect_uri)

URL, на который по умолчанию будет перенаправлен пользователь после проведения аутентификации (redirect_uri).

Префиксы ссылки возврата

Для добавления нового префикса введите его и нажмите Enter. Префикс используется для проверки ссылки возврата (redirect_uri). Если в запросе на аутентификацию указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в аутентификации будет отказано.

Допустимые разрешения bliz_change_password auto_data_update usr_grps bliz_group native bliz_user_rights openid profile bliz_rm_rights esia bliz_api_user_chg bliz_api_sys_users bliz_api_sys_users_chg bliz_api_user

Разрешения (scope), которые будут доступны приложению.

Разрешения по умолчанию openid profile

Разрешения (scope), которые будут по умолчанию выданы приложению после аутентификации. Если значения по умолчанию не указаны, то в запросе необходимо явно прописать требуемые разрешения.

Не требовать от пользователя согласие на предоставление доступа к данным о себе

Обязательное использование Proof Key for Code Exchange (RFC 7636) для Authorization code grant type

Метод аутентификации при обращении к сервису выдачи маркеров

Указанный метод аутентификации должен использоваться при обращении к сервису выдачи маркеров (token endpoint). При пустом значении доступны все методы.

Допустимые grant type urn:ietf:params:oauth:grant-type:device_code refresh_token client_credentials implicit authorization_code password

Список grant type, которые будут доступны приложению. При пустом списке доступны все grant type.

Допустимые response type code token id_token device_code

Список response type, которые будут доступны экземпляру приложения при обращении к URL авторизации (authorization endpoint). При пустом списке доступны все response type.

Время жизни маркера доступа

Задается количество секунд через которое код доступа будет не действителен. Если не задан, то берется из общих настроек.

Режим выдачи маркеров доступа по умолчанию

Режим выдачи маркеров доступа (access_token), если явно не указан в запросе. При offline-режиме не выдается маркер обновления (refresh_token).

Время жизни маркера обновления

Задается количество секунд через которое код обновления будет не действителен. Если не задан, то берется из общих настроек.

Добавленные в маркер идентификации (id_token) утверждения esia_email esia_lastname esia_firstname esia_mobile org_old esia_inn org_unit esia_snils org_title org_OGRNP org_state esia_passport org INN org_shortcode org_OGRN org_name esia_middlename esia_birthPlace org_email esia_gender org_fullName org_city org_type org_id esia_birthDate

Дополнительные утверждения (claims), которые будут добавлены в маркер идентификации (id_token).

Device Authorization Grant

Формат пользовательского кода

Формат указывается в виде шаблона на основе регулярного выражения, по которому происходит генерация пользовательского кода для привязки устройства. Например: [0-9]{2,3}-[0-9]{2,3}

Время жизни пользовательского кода

Задается количество секунд через которое пользовательский код будет не действителен. Если не задан, то берется из общих настроек.

Ссылка на страницу ввода пользовательского кода

Если ссылка не задана, то она формируется автоматически.

Добавить в URL пользовательский код

Рисунок 55 – Настройки протоколов OAuth 2.0 и OIDC для приложения

Возможно также изменение режима выдачи маркеров доступа по умолчанию. Blitz Identity Provider предусматривает два режима выдачи маркеров доступа (`access_token`):

- `offline`-режим – при запросе маркера доступа будет выдан также бессрочный маркер обновления (`refresh_token`), которые может быть использован для получения нового маркера доступа. Приложению рекомендуется использовать этот режим, если оно должно получать актуальные данные пользователя из Blitz Identity Provider за пределами времени действия пользовательской сессии. Например, если приложение делает почтовую рассылку и перед ее отправкой хочет получить актуальный адрес электронной почты из Blitz Identity Provider;
- `online`-режим – будет выдан только маркер доступа. Приложению рекомендуется использовать этот режим, если ему достаточно получать актуальные данные пользователя в момент входа (в течение активной сессии пользователя).

Режим выдачи маркеров доступа может быть явно указан в запросе на проведение идентификации; если он не указан, то используется режим по умолчанию.

Если необходимо взаимодействие по протоколу OIDC (OpenID Connect 1.0), то в качестве одного из разрешений (`scope`) необходимо указать `openid`. Тогда в обмен на код авторизации при вызове Token Endpoint будут выданы не только маркер доступа (`access token`) и маркер обновления (`refresh token`), но и маркер идентификации (`id_token`). В настройках приложения возможно указать необходимость добавления атрибутов пользователя в маркер идентификации (`id_token`). Возможно добавление как атрибутов, сконфигурированных в разделе «Источники данных», так и дополнительных сессионных атрибутов (подробнее см. п. 5.3.3).

Также можно настроить возможность использования приложением авторизации по спецификации Device Authorization Grant²³. Для этого в параметре «Допустимые response type» добавить вариант `device code`, а в параметре «Допустимые grant type» добавить вариант `urn:ietf:params:oauth:grant-type:device_code`. Дополнительно в блоке «Device Authorization Grant» можно настроить:

- формат пользовательского кода, для этого следует использовать регулярные выражения;
- время жизни пользовательского кода, например;
- ссылка на страницу ввода пользовательского кода.

При необходимости можно отметить галочку «Добавлять в URL пользовательский код». Если она отмечена, то Blitz Identity Provider при авторизации устройства будет

²³ См.: <https://tools.ietf.org/html/rfc8628>

возвращать не только ссылку на страницу ввода пользовательского кода (например, <https://test.ru/device>), но еще и ссылку с кодом в качестве параметра (например, <https://test.ru/device?uc=676-267-324>).

5.3.2. Общие настройки OAuth 2.0

Для задания общих настроек OAuth 2.0, а также для конфигурирования набора разрешений (scope) используется раздел «OAuth 2.0» консоли управления (Рисунок 56).

Свойства

URL с метаданными Blitz Identity Provider /sps/oauth/.well-known/openid-configuration
При подключении приложений по OpenID Connect в настройках этих приложений может потребоваться указать эту ссылку на файл с метаданными поставщика идентификации

URL для авторизации /sps/oauth/ae
На данный URL (authorization endpoint) должен быть направлен запрос на проведение авторизации пользователя

URL для получения и обновления маркера /sps/oauth/te
На данный URL (token endpoint) должен быть направлен запрос на получение или обновление маркера доступа

Время жизни маркера доступа, сек

Формат маркера доступа

Аутентификация систем-клиентов с использованием Proxy TLS. Для аутентификации систем по Proxy TLS должно быть настроено взаимодействие через прокси-сервер и обеспечено установление двустороннего TLS-соединения. В поле Common Name (CN) сертификата системы должен быть указан домен системы

Device Authorization Grant

Время жизни пользовательского кода в секундах

Минимально разрешенный интервал опроса статуса кода привязки устройства в секундах

Настройка scopes

Укажите разрешения (scope), которые могут быть запрошены системами (приложениями). При необходимости укажите, какие атрибуты пользователя из хранилища могут быть получены по этим разрешениям

Название разрешения	Описание	Атрибуты пользователя	Системный	
<input type="text" value="blitz_change_password"/>	Смена пароля	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="✖"/>
<input type="text" value="userinfo"/>	Основные данные профиля пользователя	<input type="text" value="x given_name x email x sub x name x family_name"/>	<input type="checkbox"/>	<input type="button" value="✖"/>
<input type="text" value="native"/>	Получение css-куки	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="✖"/>
<input type="text" value="blitz_api_user"/>	Получение всех атрибутов	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="✖"/>

+ Добавить scope

Рисунок 56 – Задание общих настроек OAuth 2.0 / OIDC

В разделе «OAuth 2.0» консоли управления можно посмотреть различные URL обработчиков Blitz Identity Provider, связанных с OAuth 2.0 и OIDC:

- «URL с метаданными Blitz Identity Provider» – по этой ссылке размещены динамически обновляемые настройки (метаданные) Blitz Identity Provider²⁴. Разработчики приложений могут не прописывать все указанные ниже URL в конфигурации своего приложения, а использовать в настройках единую ссылку на эти метаданные;
- «URL для авторизации» – адрес обработчика OAuth 2.0 Authorization Endpoint для запросов через браузер на получение кода авторизации;
- «URL для получения и обновления маркера» – адрес обработчика OAuth 2.0 Token Endpoint для получения маркеров безопасности (access_token, id_token, refresh_token).

При необходимости можно:

- изменить «Время жизни маркера доступа», используемое по умолчанию при выпуске маркеров для всех приложений;
- указать «Формат маркера доступа», используемый по умолчанию при выпуске маркеров для всех приложений: строка (opaque) или JWT;
- отметить опцию «Аутентификация систем-клиентов с использованием Proxy TLS». В этом случае должно быть настроено взаимодействие приложений с Blitz Identity Provider через прокси-сервер с установкой двустороннего TLS-соединения. В поле «Common Name (CN)» сертификата системы должен быть указан домен системы подключаемого приложения.

Для корректной работы взаимодействия с приложениями по протоколу OAuth 2.0 необходимо определить разрешения (scope). Для этого нужно указать:

- название разрешения;
- описание разрешения (оно будет отображаться пользователю на странице согласия на предоставление доступа);
- является ли разрешение системным – такие разрешения предоставляются приложениям только с использованием OAuth 2.0 Client Credentials Flow (не в контексте разрешения отдельного пользователя, а общие);
- атрибуты пользователя, которые будут предоставлены по данному разрешению (атрибуты должны быть определены в меню «Источники данных»).

Для корректной работы аутентификации по OpenID Connect 1.0 нужно убедиться, что разрешение с названием `openid` определено в этом разделе консоли. Также можно прописать

²⁴ Созданы в соответствие с: <https://tools.ietf.org/html/draft-ietf-oauth-discovery-10>

атрибуты, передаваемые по этому разрешению²⁵.

Также в этом разделе можно определить общие настройки для взаимодействия с приложениями по спецификации Device Authorization Grant. Здесь имеется возможность указать:

- время жизни пользовательского кода (в секундах);
- минимально разрешенный интервал опроса статуса кода привязки устройства в секундах. Если приложение опрашивает сервис Blitz Identity Provider чаще, чем указано в этом параметре, то будет возвращена ошибка.

При необходимости для каждого приложения можно указать индивидуальные настройки, связанные со спецификацией Device Authorization Grant (см. п. 5.3.1).

5.3.3. Добавление атрибутов в маркер идентификации

Приложения, подключенные по протоколу OpenID Connect 1.0, могут получать данные в маркере идентификации. Перечень атрибутов, которые будут переданы в маркере идентификации, должен быть задан в пункте «Добавляемые в маркер идентификации (id_token) утверждения» настроек протокола (см. Рисунок 55).

Помимо хранимых атрибутов, в маркер идентификации могут быть добавлены утверждения:

- полученные при входе пользователя по электронной подписи. Это могут быть данные о сертификате ключа электронной подписи, данные о физическом / юридическом лице из сертификата;
- полученные при входе через ЕСИА;
- определенные в процедуре входа.

Для получения утверждений из сертификата ключа электронной подписи необходимо отредактировать конфигурационный файл `blitz.conf`, добавив в блок настроек `blitz.prod.local.idp.login.methods.x509` добавить структуру следующего содержания:

```
"claims" : [  
  {  
    "name" : "attr_name",  
    "value" : "cert_attr_name"  
  }  
]
```

В этой структуре `attr_name` – имя атрибута, которое будет использовано в маркере идентификации, а `cert_attr_name` – обозначение атрибута в сертификате (примеры доступных значений приведены в таблице 4).

²⁵ В этом случае указанные данные могут быть получены по маркеру доступа (access token), выданному на разрешение openid.

Таблица 4

Пример данных, получаемых из сертификата ключа электронной подписи

Обозначение атрибута в сертификате	Описание
SUBJECT.OGRN	ОГРН организации
SUBJECT.OGRNIP	ОГРНИП индивидуального предпринимателя
SUBJECT.INN	ИНН организации
SUBJECT.E	Служебный email должностного лица
SUBJECT.O	Имя организации
SUBJECT.ST	Регион организации
SUBJECT.L	Населенный пункт организации
SUBJECT.STREET	Улица, дом, номер офиса организации
SUBJECT.O	Подразделение должностного лица
SUBJECT.T	Должность представителя
SUBJECT.<OID>	Значением из атрибута с указанным OID. Например, SUBJECT.1.2.643.100.5 позволяет обратиться к атрибуту с OID 1.2.643.100.5

Пример добавляемой в конфигурационный файл структуры:

```
"claims" : [
  {
    "name" : "org_OGRN",
    "value" : "SUBJECT.OGRN"
  },
  {
    "name" : "org_INN",
    "value" : "SUBJECT.INN"
  },
  {
    "name" : "org_email",
    "value" : "SUBJECT.E"
  },
  {
    "name" : "org_name",
    "value" : "SUBJECT.O"
  }
]
```

Чтобы утверждения из ЕСИА были доступны, необходимо отредактировать конфигурационный файл `blitz.conf`, добавив в блок настроек `blitz.prod.local.idp.federation.points.esia` добавить структуру следующего содержания:

```
"claims" : [
  {
    "name" : "attr name",
    "value" : "esia attr name"
  }
]
```

В этой структуре `attr_name` – имя атрибута, которое будет использовано в маркере идентификации, а `esia_attr_name` – обозначение атрибута при получении его из ЕСИА (Таблица 5).

Таблица 5

Пример данных, получаемых из ЕСИА

Обозначение атрибута, полученного из ЕСИА	Описание
oid	Уникальный идентификатор учетной записи ЕСИА
lastName	Фамилия

firstName	Имя
middleName	Отчество
birthDate	Дата рождения
gender	Пол
snils	СНИЛС
inn	ИНН
passport	Паспортные данные
birthPlace	Место рождения
email	Электронная почта
mobile	Моб. телефон

Пример добавляемой в конфигурационный файл структуры:

```
"claims" : [
  {
    "name" : "esia firstName",
    "value" : "firstName"
  },
  {
    "name" : "esia lastName",
    "value" : "lastName"
  },
  {
    "name" : "esia middleName",
    "value" : "middleName"
  },
  {
    "name" : "esia birthDate",
    "value" : "birthDate"
  },
  {
    "name" : "esia gender",
    "value" : "gender"
  },
  {
    "name" : "esia snils",
    "value" : "snils"
  },
  {
    "name" : "esia inn",
    "value" : "inn"
  },
  {
    "name" : "esia passport",
    "value" : "passport"
  },
  {
    "name" : "esia birthPlace",
    "value" : "birthPlace"
  },
  {
    "name" : "esia_email",
    "value" : "email"
  },
  {
    "name" : "esia mobile",
    "value" : "mobile"
  }
]
```

Чтобы иметь возможность определять сессионные утверждения в процедуре входа, соответствующие утверждения также должны быть определены в конфигурационном файле. Для этого в раздел `blitz.prod.local.idp.login` конфигурационного файла необходимо добавить атрибут `sessionClaims` с перечнем утверждений, которые могут быть определены в процедуре.

Например, следующая запись позволяет определить атрибут `custom_attr`:

```
"sessionClaims" : [
  "custom_attr"
]
```

5.3.4. Настройка динамической регистрации клиентов OAuth 2.0

Чтобы включить возможность динамической регистрации клиентов, необходимо выполнить следующие шаги:

- зарегистрировать приложение и настроить для него протокол подключения OAuth 2.0 согласно документации (см. п. 5.3.2);
- в настройках OAuth 2.0 для данного приложения перейти на закладку «Динамические клиенты» (Рисунок 57).

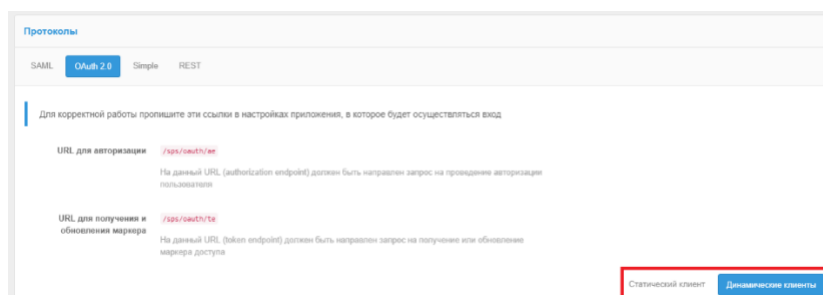


Рисунок 57 – Включение динамической регистрации клиентов

Указать базовые настройки динамической регистрации клиентов:

- разрешить динамическую регистрацию клиентов;
 - указать допустимые к прямой передаче утверждения. Эти утверждения допускается указывать в запросе на регистрацию экземпляра приложения. В случае их наличия в метаданных приложения (`software_statement`), приоритет будет отдан значению из метаданных. Рекомендуется разрешить передачу только типа устройства (`device_type`).
- Создать первичные маркеры для приложения. Первичные маркеры используются для авторизации экземпляров приложения при их регистрации.

Сгенерировать метаданные приложения (`software_statement`). Эти метаданные передаются в качестве утверждения в запросе на регистрацию экземпляра приложения. В качестве атрибутов метаданных можно указать:

- версию приложения (обязательный атрибут). Версия приложения должна соответствовать версии первичного маркера, используемого приложением;
- префиксы ссылок возврата. Префикс используется для проверки ссылок возврата (`redirect_uri`). Если в запросе на аутентификацию указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в аутентификации будет отказано;
- допустимые разрешения – разрешения (`scope`), которые будут доступны приложению;
- метод аутентификации при обращении к сервису выдачи маркеров. Указанный метод аутентификации должен использоваться экземпляром приложения при обращении к сервису выдачи маркеров (Token endpoint)
- допустимые значения `grant type`. Список `grant type`, которые будут доступны экземпляру

приложения;

- допустимые значения response type. Список response type, которые будут доступны экземпляру приложения при обращении к URL авторизации (Authorization endpoint).

Следует учесть, что указанные атрибуты метаданных должны соответствовать параметрам OAuth 2.0, определенным для приложения («Статический клиент»).

После подписания метаданных приложения их вместе с первичными маркерами следует передать разработчикам подключаемого приложения.

Пример настроек динамической регистрации клиента представлен на рисунке ниже (Рисунок 58).

Настройки динамической регистрации клиентов

Разрешить динамическую регистрацию клиентов

Идентификатор приложения (software_id)
Используется для регистрации динамических клиентов

Допустимые к прямой передаче утверждения
Эти утверждения допускаются указывать в запросе на регистрацию инстанса приложения

[Изменить](#)

Подписание метаданных приложения

Подпишите метаданные приложения (software_statement). Эти метаданные передаются в качестве утверждения в запросе на регистрацию инстанса приложения

Версия приложения
Версия приложения в метаданных должна соответствовать версии в первичном маркере

Префиксы ссылок возврата
Для добавления нового префикса введите его и нажмите Enter
Префикс используется для проверки ссылок возврата (redirect_uri). Если в запросе на аутентификацию указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в аутентификации будет отказано

Допустимые разрешения
Разрешения (scope), которые будут доступны приложению.

Метод аутентификации при обращении к сервису выдачи маркеров
Указанный метод аутентификации должен использоваться инстансом приложения при обращении к сервису выдачи маркеров (token endpoint)

Допустимые значения grant type
Список grant type, которые будут доступны инстансу приложения

Допустимые значения response type
Список response type, которые будут доступны инстансу приложения при обращении к URL авторизации (authorization endpoint)

[Сгенерировать](#)

Первичные маркеры

Первичные маркеры используются для авторизации инстансов приложения при их регистрации

Идентификатор	Дата создания	Версия ПО	
LP5fobJkub5PmzBew2qheePdwW5pA_Y2XsJd5ybNG4QBKF8xqW3epqpbzROE8-sSiHuXisPMWNB5a_gQ8jmg	04.06.2019 16:11:34	1	✖

Версия ПО [Выпустить](#)

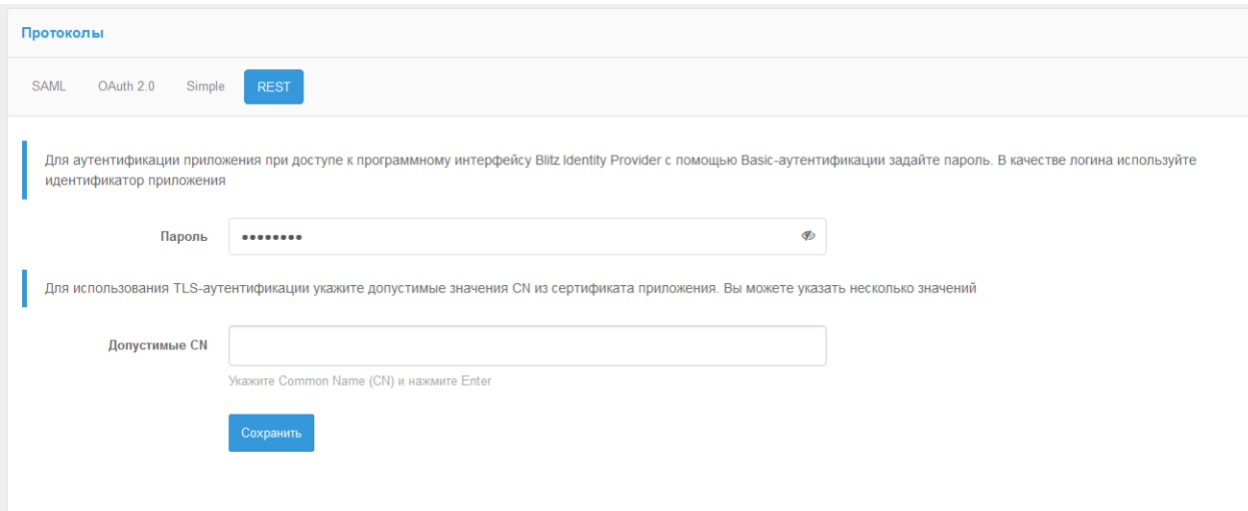
Рисунок 58 – Настройки динамической регистрации клиентов

5.4. Настройка клиента REST-сервисов Blitz Identity Provider

Для вызова REST-сервисов Blitz Identity Provider необходимо настроить приложение, которое будет выступать в качестве системы-клиента REST-сервисов. Для этого нужно зарегистрировать новое приложение в разделе «Приложения» (см. п. 5.1).

Далее перейти к настройкам приложения, в качестве протокола подключения указать REST и заполнить следующие данные (Рисунок 59):

- «Пароль» – будет использоваться при HTTP Basic авторизации. В качестве логина используется идентификатор приложения;
- «Допустимые CN» – перечень значений атрибута CN сертификата, используемого при TLS-аутентификация;



The screenshot shows a configuration page titled "Протоколы" (Protocols). At the top, there are tabs for "SAML", "OAuth 2.0", "Simple", and "REST", with "REST" being the active tab. Below the tabs, there are two sections of instructions and input fields. The first section says: "Для аутентификации приложения при доступе к программному интерфейсу Blitz Identity Provider с помощью Basic-аутентификации задайте пароль. В качестве логина используйте идентификатор приложения" (For application authentication when accessing the Blitz Identity Provider API using Basic authentication, set a password. Use the application identifier as the login). Below this is a "Пароль" (Password) input field with a masked password of seven dots and a visibility icon. The second section says: "Для использования TLS-аутентификации укажите допустимые значения CN из сертификата приложения. Вы можете указать несколько значений" (For using TLS authentication, specify allowed CN values from the application certificate. You can specify several values). Below this is a "Допустимые CN" (Allowed CNs) input field. Underneath the field, it says "Укажите Common Name (CN) и нажмите Enter" (Specify Common Name (CN) and press Enter). At the bottom of the form is a blue "Сохранить" (Save) button.

Рисунок 59 – Настройка приложения для работы с REST-сервисами

Если для приложения не заданы настройки протокола подключения REST, то приложение не сможет использовать REST API сервера Blitz Identity Provider, защищаемые с использованием HTTP Basic авторизации.

6. Настройка процедур входа в приложения

Процедуры входа применяются для настройки правил доступа пользователей к различным приложениям. С помощью процедур можно определить, например, какие приложения должны быть доступны каким пользователям, при каких условиях должна требоваться двухфакторная аутентификация и какие методы подтверждения входа может применять пользователь. Применение процедур входа позволяет организации исполнить принятые в ней политики контроля доступа к приложениям.

6.1. Создание процедур входа

Управление процедурами входа осуществляется в разделе «Процедуры входа» консоли управления Blitz Identity Provider (Рисунок 60).

Идентификатор	Приложения	Описание	Статус
AccessByAttribute v4		If the user attribute "applist" (as an array) contains entityID (or client_id) of the application, access will be granted	Не активирована
FFmethods v19		Limited list of first factor methods for application	Не активирована
Require2ndFactor v3		This procedures enables 2nd factor for the application	Не активирована

Создать новую процедуру входа

Рисунок 60 – Экран настроек процедур входа

Создание процедуры входа включает в себя следующие шаги:

1. Указание базовых параметров процедуры:
 - идентификатор процесса (процедуры);
 - описание процедуры;
 - приложения – перечень приложений, для которых будет применяться данная процедура.

Для каждого приложения может быть создана только одна процедура. Если для данного приложения не создано процедуры, к нему будет применяться стандартная процедура входа (процедура входа по умолчанию). Если процедура создана без указания приложений, то она заменит стандартную процедуру входа.

Создание новой процедуры входа

Идентификатор процесса: ProfileAccess
Идентификатор процесса должен быть корректным Java-идентификатором, Java-классом, описывающим процесс входа, будет иметь такое же название.

Описание: Процедура входа в Личный Кабинет
При необходимости укажите комментарий, описывающий особенности и назначение процесса.

Приложения: Личный кабинет
Список приложений, для которых будет применяться данная процедура входа. Если приложения не указаны, то процедура будет считаться глобальной, и применяться в тех случаях, когда нет процедуры для конкретного приложения. При этом одновременно активирована может быть только одна глобальная процедура, а также не должно быть коллизий при определении процедуры входа для определенного приложения.

Создать

Рисунок 61 – Экран создания новой процедуры входа

2. Написание исходного кода процедуры (Рисунок 62). Для успешной работы процедуры входа необходимо написать на языке Java класс, реализующий необходимый интерфейс **Strategy**. Вся контекстная информация о пользователе, о текущем состоянии процедуры аутентификации и т.д. доступна в объекте **Context**. Процедура состоит из двух блоков, которые определяют:
 - действия, предпринимаемые на начальном этапе процесса аутентификации. В этом блоке, например, можно определить, при каких случаях авторизовать пользователя в приложение в режиме SSO (если пользователь ранее был аутентифицирован);
 - действия, предпринимаемые после первичной аутентификации пользователя. В этом блоке, например, можно определить, какие методы двухфакторной аутентификации при каких условиях использовать.
3. После написания кода необходимо нажать на кнопку «Компилировать». При наличии ошибок некорректные фрагменты кода будут выделены цветом и подписаны ошибки.
4. Если компиляция прошла успешно, можно сохранить процедуру.
5. Сохраненную процедуру можно активировать – для этого следует нажать на кнопку «Активировать» в шапке соответствующей процедуры.
6. Можно редактировать как активированную, так и деактивированную процедуру. После редактирования следует компилировать процедуру, после чего – сохранить. Если процедура была активирована, то новая скомпилированная процедура заменит старую.

Если процедура активирована, то сохранить можно только ту процедуру, которую удастся скомпилировать. Иными словами, если при редактировании активированной процедуры была выявлена ошибка, то кнопка «Сохранить» работать не будет, а при перезагрузке страницы изменения будут утеряны.

Исходный код процедуры

Для успешной работы процедуры аутентификации необходимо написать на языке `Java` класс, реализующий интерфейс `Strategy`. Название класса должно совпадать с идентификатором процесса (`SecondFAforAll`). Класс должен иметь публичный `default` конструктор. В целях безопасности загрузка класса осуществляет отдельный `class loader` с ограниченным списком `imports`. Вся контекстная информация о пользователе, о текущем состоянии процедуры аутентификации и т.д. доступна в объекте `Context`.

Посмотреть интерфейс Strategy ▾ Посмотреть разрешенные imports ▾ Посмотреть описание Context ▾ Загрузить Blitz Development Kit

```

1 package com.identityblitz.idp.flow.dynamic;
2
3 import java.lang.*;
4 import java.util.*;
5 import java.math.*;
6 import org.slf4j.LoggerFactory;
7 import org.slf4j.Logger;
8 import com.identityblitz.idp.login.authn.flow.Context;
9 import com.identityblitz.idp.login.authn.flow.Strategy;
10 import com.identityblitz.idp.login.authn.flow.StrategyState;
11 import com.identityblitz.idp.login.authn.flow.StrategyBeginState;
12 import com.identityblitz.idp.login.authn.flow.LCookie;
13 import com.identityblitz.idp.flow.common.api.*;
14 import com.identityblitz.idp.flow.dynamic.*;
15 import java.lang.invoke.LambdaMetafactory;
16 import java.util.function.Consumer;
17
18 import static com.identityblitz.idp.login.authn.flow.StrategyState.*;
19
20 public class SecondFAforAll implements Strategy {
21
22     private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");
23
24     @Override public StrategyBeginState begin(final Context ctx) {
25         return StrategyState.LOGOUT_THEN_MORE(new String[] {});
26     }
27
28     @Override public StrategyState next(final Context ctx) {
29         if(ctx.justCompletedFactor() == 2)
30             return StrategyState.ENOUGH();
31         else
32             return StrategyState.MORE(new String[] {});
33     }
34 }

```

Компилировать Сохранить

Рисунок 62 – Экран редактирования исходного кода процедуры входа (фрагмент)

6.2. Примеры процедур входа

В поставку входят несколько готовых процедур, которые могут быть при необходимости изменены:

- принудительная двухфакторная аутентификация в приложение (`Require2ndFactor`);
- ограничение перечня доступных методов первого фактора при входе в приложение (`FFmethods`);
- предоставление доступа к приложению только при определенном значении атрибута (`AccessByAttribute`).

Далее приводятся листинги этих процедур. Для удобства отладки можно выводить информацию о состоянии аутентификации в лог, воспользовавшись функцией `logger.debug()`. Например, следующая команда выведет в лог заданный уровень аутентификации для пользователя:

```
logger.debug("requiredFactor="+ctx.userProps("requiredFactor"));
```

6.2.1. Принудительная двухфакторная аутентификация в приложение

Эта процедура требует двухфакторной аутентификации для доступа к приложению. Если пользователь переходит в приложение в рамках единой сессии, то при наличии одного пройденного фактора у него будет дополнительно проверен второй фактор, т.е. SSO в этом случае не работает.

```
@Override public StrategyState begin(final Context ctx) {
    if(ctx.claims("subjectId") != null) {
        // if the user is already authenticated, then we check the number of factors passed
        if (ctx.sessionTrack().split(",").length < 2)
            return StrategyState.MORE(new String[]{});
        else
            return StrategyState.ENOUGH();
    }
    // if he is not authenticated or passed less than 2 factors, then we require passing 2FA
    else
        return StrategyState.MORE(new String[]{});
}

@Override public StrategyState next(final Context ctx) {
    // if the user has passed one auth factor, then we require a second one; if more than one - we
    sign in to the application
    if(ctx.justCompletedFactor() == 1)
        return StrategyState.MORE(new String[]{});
    else
        return StrategyState.ENOUGH();
}
```

6.2.2. Ограничение перечня доступных методов первого фактора

Данная процедура позволяет при входе в приложение предлагать пользователю только определенные методы идентификации и аутентификации (аналогичную процедуру с иным перечнем методов, можно назначить другому приложению). Для обозначения методов аутентификации первого фактора в процедуре используются следующие идентификаторы:

- **password** – вход по логину и паролю;
- **x509** – вход по электронной подписи;
- **externalIdps** – вход через внешние поставщики идентификации (социальные сети, ЕСИА);
- **spnego** – вход по сеансу операционной системы;
- **sms** – вход по коду подтверждения из SMS-сообщения;
- **knownDevice** – вход по известному устройству.

```
@Override public StrategyState begin(final Context ctx) {
    if(ctx.claims("subjectId") != null)
        return StrategyState.ENOUGH();
    else
        return StrategyState.MORE(new String[]{"password","x509"});
}

@Override public StrategyState next(final Context ctx) {
    if(ctx.justCompletedFactor() == 1)
        return StrategyState.MORE(new String[]{});
    else {
        String reqFactor = ctx.userProps("requiredFactor");
        if(reqFactor == null)
            return StrategyState.ENOUGH();
        else {
            if(Integer.valueOf(reqFactor) < ctx.justCompletedFactor())
                return StrategyState.ENOUGH();
            else
                return StrategyState.MORE(new String[]{});
        }
    }
}
```

```

        return StrategyState.MORE(new String[]{});
    }
}

```

6.2.3. Разрешить вход в приложение только при определенном значении атрибута у пользователя

Приведенная ниже процедура использует атрибут `appList` для принятия решения о доступе пользователя к приложению. Для работы этой процедуры необходимо создать атрибут `appList` в виде массива (Array of strings). В качестве значений элементов этого массива следует использовать идентификаторы приложений. В результате доступ к приложению будет предоставлен, если среди значений `appList` у данного пользователя будет идентификатор этого приложения. Такая архитектура процедуры позволяет назначить ее сразу нескольким приложениям и регулировать доступ к ним при помощи одного атрибута.

```

@Override public StrategyState begin(final Context ctx) {
    if(ctx.claims("subjectId") != null){
        // if the user is already authenticated, then check his attribute access
        int appListIdx = 0;
        boolean hasAccess = false;
        while (appListIdx > -1) {
            String app = ctx.claims("appList.[" + appListIdx + "]");
            logger.debug("app [" + appListIdx + "] = " + app);
            if (app == null) {
                appListIdx = -1;
            }
            else if (app.equals(ctx.appId())) {
                appListIdx = -1;
                hasAccess = true;
            }
            else {
                appListIdx ++;
                logger.debug("AppList index = " + appListIdx);
            }
        }
        if(hasAccess)
            return StrategyState.ENOUGH();
        else
            return StrategyState.DENY;
    }
    // if user has not been authenticated, then we ask him to pass the first factor of authentication
    else
        return StrategyState.MORE(new String[]{});
}

@Override public StrategyState next(final Context ctx) {
    // after primary authentication, we check his attribute appList, if it is correct, then we analyze
    the requiredFactor parameter of the user (the required level of authentication) and depending on
    this require the second factor
    int appListIdx = 0;
    boolean hasAccess = false;
    while (appListIdx > -1) {
        String app = ctx.claims("appList.[" + appListIdx + "]");
        logger.debug("app [" + appListIdx + "] = " + app);
        if (app == null) {
            appListIdx = -1;
        }
        else if (app.equals(ctx.appId())) {
            appListIdx = -1;
            hasAccess = true;
        }
        else {
            appListIdx ++;
            logger.debug("AppList index = " + appListIdx);
        }
    }
    if(!hasAccess)
        return StrategyState.DENY;
}

```

```
String reqFactor = ctx.userProps("requiredFactor");
if(reqFactor == null)
    return StrategyState.ENOUGH();
else {
    if(Integer.valueOf(reqFactor) < ctx.justCompletedFactor())
        return StrategyState.ENOUGH();
    else
        return StrategyState.MORE(new String[]{});
}
```

Пример упрощенного варианта процедуры – допуск пользователя в приложение при условии, что адрес его электронной почты равен `ivanov@company.ru`:

```
@Override public StrategyState begin(final Context ctx) {
    if(ctx.claims("subjectId") != null){
        // if user has been authenticated, than check his email
        if("ivanov@company.ru".equals(ctx.claims("mail")))
            return StrategyState.ENOUGH();
        else
            return StrategyState.DENY;
    }
    else
        // if user has not been authenticated, than ask him to authenticate
        return StrategyState.MORE(new String[]{});
}

@Override public StrategyState next(final Context ctx) {
    // after attribute validation we should check is the 2FA required or not
    if(!"ivanov@reaxoft.ru".equals(ctx.claims("mail")))
        return StrategyState.DENY;
    String reqFactor = ctx.userProps("requiredFactor");
    if(reqFactor == null)
        return StrategyState.ENOUGH();
    else {
        if(Integer.valueOf(reqFactor) < ctx.justCompletedFactor())
            return StrategyState.ENOUGH();
        else
            return StrategyState.MORE(new String[]{});
    }
}
```


7. Настройка сервисов самообслуживания пользователей


Blitz Identity Provider предоставляет веб-приложения, с помощью которых пользователи самостоятельно могут выполнять ряд операций:

1. Веб-приложение «Личный кабинет» – позволяет выполнить ряд операций с учетной записью, например, посмотреть/изменить свои данные, настроить способы аутентификации, посмотреть последние события, сменить пароль. При включении доступно по адресу: <https://{hostname}/blitz/profile>.
2. Веб-приложение «Регистрация пользователей». При включении становится доступен переход со страницы входа на форму самостоятельной регистрации (ссылка «Нет аккаунта? Зарегистрироваться»).
3. Веб-приложение «Восстановление доступа». Позволяет пользователю сменить пароль от своей учетной записи после прохождения проверок. Если приложение включено, то пользователи смогут перейти со страницы входа (ссылка «Забыли пароль?») на форму восстановления доступа.

Настройка данных сервисов осуществляется в разделе «Сервисы самообслуживания» консоли управления.

Администратор консоли управления должен самостоятельно проверять корректность помещаемых на страницу входа JS-скриптов и содержимое страниц регистрации и личного кабинета на предмет возможных уязвимостей.

7.1. Общие настройки

На главной странице раздела «Сервисы самообслуживания» можно включить или выключить соответствующие приложения (сервисы), используя переключатель (). Следует при этом учесть, что переключатель лишь влияет на отображение ссылок (например, «Забыли пароль?»), тогда как наличие самого сервиса зависит от того, было ли соответствующее приложение установлено администратором: blitz-idp – веб-приложение «Личный кабинет», blitz-registration – веб-приложение «Регистрация пользователей», blitz-recovery – веб-приложение «Восстановление доступа».

Также на главной странице можно настроить параметры, применяемые во всех сервисах самообслуживания:

- параметры кода подтверждения, отправляемого в SMS – можно изменить длину кода и время его действия, а также количество попыток;
- параметры кода подтверждения, отправляемого по электронной почте – можно изменить длину кода и время его действия.

Сервисы самообслуживания

Регистрация <input checked="" type="checkbox"/>	Восстановление доступа <input checked="" type="checkbox"/>
Самостоятельная регистрация пользователей. Перейти к настройкам	Самостоятельное восстановление доступа посредством отправки ссылки на адрес электронной почты или кода подтверждения в SMS-сообщении. Перейти к настройкам
Личный кабинет <input checked="" type="checkbox"/>	
Возможность редактировать свои данные, включить усиленную аутентификацию, изменить настройки безопасности. Перейти к настройкам	

Общие настройки

Задайте параметры кодов подтверждения, отправляемых по SMS и электронной почте. Эти коды используются при регистрации пользователей, для восстановления доступа к учетной записи, а также при изменении номера мобильного телефона / адреса электронной почты через Личный кабинет.

Параметры кода подтверждения, отправляемого в SMS

Длина	<input type="text" value="6"/>	Число символов в коде подтверждения
Время действия	<input type="text" value="300"/>	Количество секунд, после которого код перестает действовать
Количество попыток	<input type="text" value="3"/>	Количество неудачных попыток ввода кода подтверждения. Если количество попыток превышено, требуется отправка нового кода

Параметры кода подтверждения, отправляемого по электронной почте

Длина	<input type="text" value="6"/>	Число символов в коде подтверждения
Время действия	<input type="text" value="3600"/>	Количество секунд, после которого код перестает действовать

Рисунок 63 – Сервисы самообслуживания и их общие настройки

В подразделах осуществляется настройка каждого сервиса самообслуживания в отдельности.

7.2. Личный кабинет

Личный кабинет – веб-приложение, в котором пользователь может выполнить следующие действия:

- посмотреть или изменить данные своей учетной записи;
- посмотреть и настроить способы подтверждения входа (двухфакторной аутентификации);
- посмотреть последние события безопасности (например, события входа);
- сменить пароль;
- посмотреть привязанные учетные записи социальных сетей, привязать новые «внешние» учетные записи, отвязать лишние учетные записи;
- посмотреть привязанные устройства доступа, отвязать лишние устройства;
- посмотреть и отозвать выданные приложениями разрешения на доступ к данным.

Настройка Личного кабинета включает в себя конфигурирование способа отображения атрибутов пользователя и изменение дополнительных параметров.

7.2.1. Отображение атрибутов пользователя

На основной странице Личного кабинета отображается блок с данными учетной записи.

Пример этого блока представлен на рис. 64.

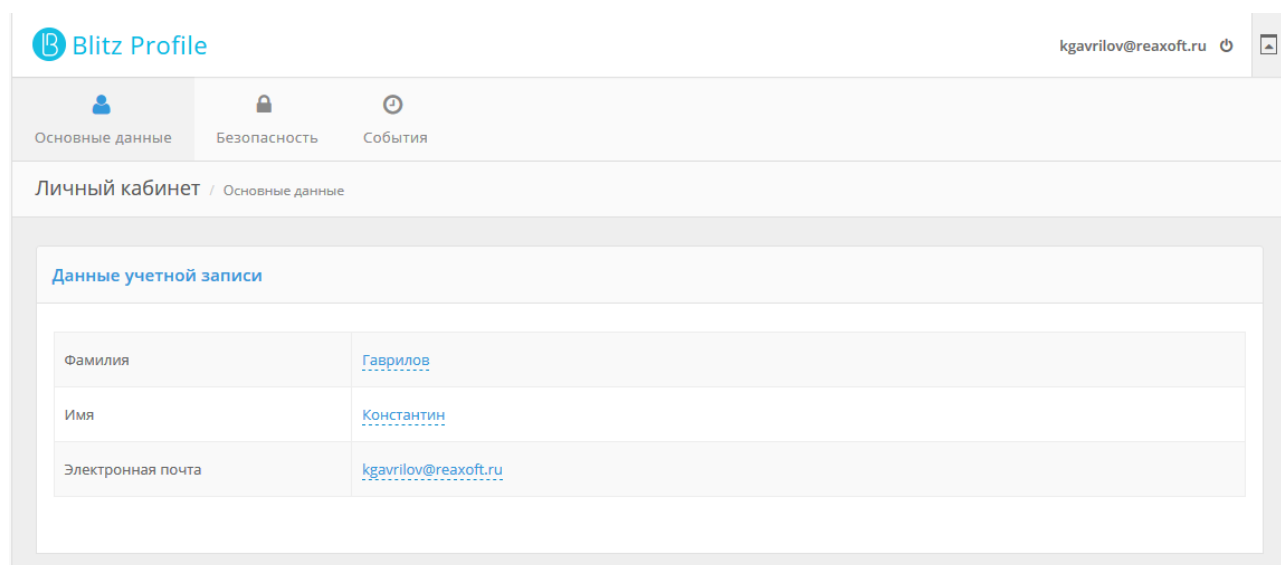


Рисунок 64 – Личный кабинет: данные учетной записи

Отображение данных пользователя определяется HTML-шаблоном. Шаблон представляет собой текстовый файл, который компилируется с помощью шаблонизатора Twirl²⁶. В шаблоне необходимо разместить функции, позволяющие пользователю в Личном

²⁶ См.: <https://github.com/playframework/twirl>

кабинете вводить и редактировать данные о себе.

В шаблоне доступны следующие функции:

- `@show(attrName)` – отображает значение атрибута;
- `@showStrings(attrName, values)` – отображает значение массива;
- `@editAsText(attrName, readableName, errorMsg)` – отображает значение атрибута и позволяет его изменить (параметр `errorMsg` необязательный);
- `@editAsBoolean(attrName, readableName)` – отображает значение логического типа (`true/false`) атрибута и позволяет его изменить;
- `@editAsStrings(attrName, readableName, values)` – отображает значение (массив) атрибута и позволяет его изменить.

В этих функциях используются следующие параметры:

- `attrName` – название атрибута, определенное в «Источники данных»;
- `readableName` – отображаемое в письме пользователю имя атрибута (можно задать как идентификатор из файла сообщений или как текст);
- `values` – значения, представляющие собой формат «ключ – описание», где ключ – значение массива, описание – читаемое значение ключа (например, `ListMap("a" -> "значение a", "c" -> "значение c")`), может задаваться как идентификатор из файла сообщений или как текст;
- `errorMsg` – описание ошибки, которое отображается в случае ошибочного ввода значения (можно задать как идентификатор из файла сообщений или как текст). Про файлы сообщений см. п. 15.2.2 документа. Рекомендуется использовать файлы сообщений при необходимости поддержки мультиязычности.

Примеры функций:

Отображение атрибута `mail`:

```
@editAsText("mail", "Электронная почта")
```

Отображение атрибута `mobile` с возможностью его редактировать:

```
@editAsText("mobile", "Мобильный телефон", "Ошибка")
```

Отображение булевого атрибута `info` с возможностью его редактировать:

```
@editAsBoolean("info", "Подписка")
```

Отображение массива строк `subscription_array` с возможностью его редактировать (выбор значений):

```
@editAsStrings("subscription_array", "Подписки", ListMap("a" -> "Акции и бонусные программы", "b" -> "Новости компании", "c" -> "Дайджест событий за месяц"))
```

Пример отображения массива строк в интерфейсе Личного кабинета представлен на рисунке 65.

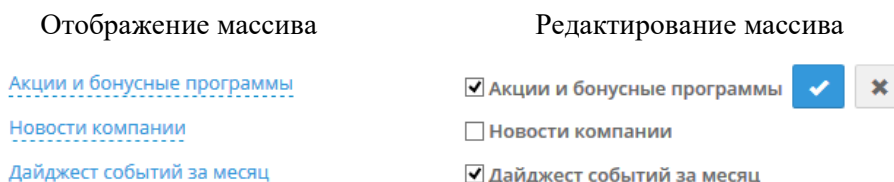


Рисунок 65 – Личный кабинет: массив строк (в режиме отображения и редактирования)

7.2.2. Дополнительные параметры

В качестве дополнительных параметров можно задать:

- шаблон приветствия – информацию, которая отображается в правом верхнем углу Личного кабинета. Допустимо использовать строки подстановки. Например, “ `${surname} ${surname}` ” позволит отобразить фамилию и имя пользователя;
- URL для перехода после успешного выхода из Личного кабинета;
- доступные пользователям функции, т.е. функции, которые могут быть задействованы пользователем из Личного кабинета. Возможно включить или выключить следующие функции:
 - смена пароля;
 - просмотр и привязка социальных сетей;
 - просмотр устройств доступа;
 - просмотр и отзыв разрешений
 - просмотр событий
 - привязка HOTP-генераторов;
 - привязка TOTP-генераторов;
 - настройка подтверждения входа по SMS-коду;
 - настройка push-аутентификации.

7.3. Регистрация пользователей

Регистрация пользователей – веб-приложение, позволяющее пользователю самостоятельно создать свою учетную запись. Настройка регистрации включает в себя конфигурирование формы регистрации, изменение параметров сервиса и создание процедуры регистрации (опционально).

7.3.1. Форма регистрации

Перечень запрашиваемых данных пользователя определяется HTML-шаблоном. Шаблон представляет собой текстовый файл, который компилируется с помощью шаблонизатора Twirl. В шаблоне необходимо разместить функции, позволяющие пользователю при регистрации вводить данные о себе.

Примеры функций, доступных в шаблоне:

- `@attrInput("email", msg("reg.email"), Map("placeholder" -> "mail@example.com", "error-messages" -> msg("reg.email.wrong")))` – отображает на странице поле для ввода атрибута `email`, описанного в системе. `msg("reg.email")` - это название атрибута, которое берется из файла сообщений в соответствии с текущими языковыми настройками. При пустом поле ввода в нем отображается `"mail@example.com"` в качестве подсказки, а при некорректном вводе – сообщение `msg("reg.email.wrong")` из файла сообщений;
- `@attrInput("surname", "Фамилия", Map("placeholder" -> "Фамилия", "error-messages" -> "Ошибка"))` – отображает на странице поле для ввода фамилии пользователя в переменную `surname`. Эту переменную далее можно использовать при исполнении процедуры регистрации.
- `@passwordsInput` - отображает на странице поля ввода пароля и его подтверждение;
- `@agreement` - отображает ссылку на условия использования;
- `@attrExpr` – функция, позволяющая создать вычисляемый атрибут (или присвоить атрибуту константное значение);
- `@submitButton` - отображает кнопку «Зарегистрироваться».

Пример шаблона для регистрации:

```
@attrInput("surname", "Фамилия", Map("placeholder" -> "Фамилия", "error-messages" -> "Ошибка"))
@attrInput("name", "Имя", Map("placeholder" -> "Имя", "error-messages" -> "Ошибка"))
@attrInput("mobile", "Номер мобильного телефона", Map("placeholder" -> "+7(999)9999999", "error-
messages" -> "reg.page.mobile.req.err.msg"))
@attrInput("mail", "Адрес электронной почты", Map("placeholder" -> "name@example.com", "error-
messages" -> "reg.page.email.req.err.msg"))
@passwordsInput
@agreement
@attrExpr("uid", "VIP-${&random(4)}")
@submitButton
```

Пример отображения указанного шаблона в интерфейсе веб-приложения «Регистрация пользователя» представлен на рис. 6б.

Identity Blitz

Регистрация в Личный кабинет

Фамилия
Фамилия

Имя
Имя

Номер мобильного телефона
+7(999)9999999

Адрес электронной почты
name@example.com

Придумайте пароль
Пароль

Повторите пароль, чтобы не ошибиться
Ваш пароль еще раз

Пароль должен состоять не менее чем из 8 символов. Рекомендуется, чтобы пароль состоял из прописных и строчных букв и имел хотя бы одну цифру. Не применяйте пароли, используемые для других сайтов, и пароли, которые можно легко подобрать.

Нажимая на кнопку «Зарегистрироваться» вы соглашаетесь с [условиями использования](#)

Зарегистрироваться

Рисунок 66 – Пример отображения регистрационной формы

7.3.2. Настройки сервиса регистрации

В качестве настроек можно задать:

- хранилище для учетной записи – нужно выбрать одно из сконфигурированных хранилищ (раздел «Источники данных») для сохранения учетной записи;
- необходимые для регистрации атрибуты пользователя – атрибуты, наличие которых необходимо для завершения процедуры регистрации. Обязательные атрибуты пользователя не нужно включать в данный список. Возможно добавление нескольких альтернативных правил. Если отмечен чекбокс «Использовать условия из процедуры регистрации», то настроенные условия игнорируются и применяются условия, определенные функцией `isEnough` из процедуры регистрации;
- URL внешнего сервиса регистрации. Если задать в качестве параметра этот URL, то по этому адресу будет направлен пользователь при переходе к процессу регистрации (вместо приложения регистрации Blitz Identity Provider).

Скриншот фрагмента страницы настроек регистрации представлен на рис. 67.

The screenshot shows the 'Настройки сервиса регистрации' (Registration Service Settings) page. It features several configuration fields:

- Хранилище для учетной записи** (Account storage): A dropdown menu with 'bip-dldap01' selected.
- Условия для успешной регистрации** (Registration conditions): A section with a red 'X' icon and a checkbox labeled 'Использовать условия из процедуры регистрации' (Use conditions from the registration procedure). Below it is a text input field and a '+ Добавить альтернативное условие' (+ Add alternative condition) button.
- URL внешнего сервиса регистрации** (External registration service URL): A text input field.

At the bottom right, there are two buttons: 'Отмена' (Cancel) and 'Сохранить' (Save).

Рисунок 67 – Скриншот настроек сервиса регистрации

7.3.3. Процедура регистрации

Процедура регистрации – Java-код, реализующий необходимые проверки после того, как пользователь заполнит форму регистрации. В ходе исполнения процедуры возможно выполнение следующих действий:

- выполнение дополнительных проверок введенных данных;
- выполнение преобразования введенных данных;
- сохранение значений атрибутов в хранилище;
- вызов внешних REST-сервисов.

При необходимости преобразовать данные, введенные пользователем, и далее сохранить их в виде атрибутов, в шаблоне страницы регистрации следует использовать функцию `@attrInput` вместо `@textInput`.

7.3.4. Изменение текста условий использования

На странице регистрации пользователя размещена ссылка на условия использования. Условия использования размещены в архиве `assets.zip`, расположенном в директории `assets` установки Blitz Identity Provider в заархивированном каталоге `documents\user_agreement`.

Для изменения правил использования следует распаковать архив `assets.zip`, заменить файлы `user_agreement_ru.pdf` (русская версия) и `user_agreement_en.pdf` (английская версия) на требуемые и заархивировать архив с сохранением исходной структуры.

Также возможно изменить ссылку на правила использования. Для этого следует отредактировать строку `reg.page.reg.action.agreement` и `setPswd.page.agreement` (см.п. 15.2.2). Такой способ рекомендуется применять, если правила использования размещены на внешнем ресурсе, например, в виде отдельной веб-страницы.

7.3.5. Восстановление доступа

Настройка сервиса восстановления доступа включает в себя указание атрибутов, по которым будет производиться поиск учетной записи, а также контактов (адреса электронной почты и/или номера мобильного телефона), которые будут использованы для восстановления доступа (рис. 68). Атрибуты с контактами должны быть определены в разделе «Источники данных» в качестве адреса электронной почты и номера мобильного телефона.

Также можно при необходимости отметить опцию «Проверять наличие пользователей, имеющих право менять пароль в найденной учетной записи». В этом случае, если у найденного пользователя имеется связанная («родительская») учетная запись, имеющая право менять пароль этому пользователю, то об этом будет выведено предупреждение.

Кроме того, можно включить дополнительную проверку для учетных записей с настроенной двухфакторной аутентификацией. Если опция включена, то для восстановления доступа к учетной записи, защищенной двухфакторной аутентификацией, потребуется пройти дополнительный способ подтверждения. Чтобы эта опция заработала, необходимо указать методы, которые могут быть использованы для дополнительной проверки. В результате систему можно настроить таким образом, что после подтверждения кода, полученного по электронной почте, также потребуется ввести код, отправленный в SMS.

The screenshot shows the 'Восстановление доступа' (Recovery) settings page. The page title is 'Восстановление доступа'. Under the heading 'Настройки сервиса восстановления' (Recovery service settings), there are three main sections:

- Возможные контакты восстановления доступа** (Possible recovery contacts): A text input field containing 'x mobile' and 'x mail'. Below it, a note says: 'Задайте список атрибутов пользователя, соответствующих возможным контактам пользователя' (Specify a list of user attributes corresponding to possible user contacts).
- Возможные атрибуты для поиска** (Possible search attributes): A text input field containing 'x mail', 'x mobile', 'x snils', and 'x login'. Below it, a note says: 'Задайте список атрибутов пользователя, по которым будет осуществляться поиск пользователя' (Specify a list of user attributes by which user search will be performed).
- Проверять наличие пользователей, имеющих право менять пароль в найденной учетной записи** (Check for users with the right to change the password in the found account): A checkbox that is checked.
- Включить дополнительную проверку для учетных записей с настроенной двухфакторной аутентификацией** (Enable additional verification for accounts with configured two-factor authentication): A checkbox that is checked.
- Список методов** (List of methods): A text input field containing 'x email', 'x totp', and 'x sms'. Below it, a note says: 'Задайте список методов, которые могут быть использованы для дополнительной проверки' (Specify a list of methods that can be used for additional verification).

At the bottom right of the form, there are two buttons: 'Отмена' (Cancel) and 'Сохранить' (Save).

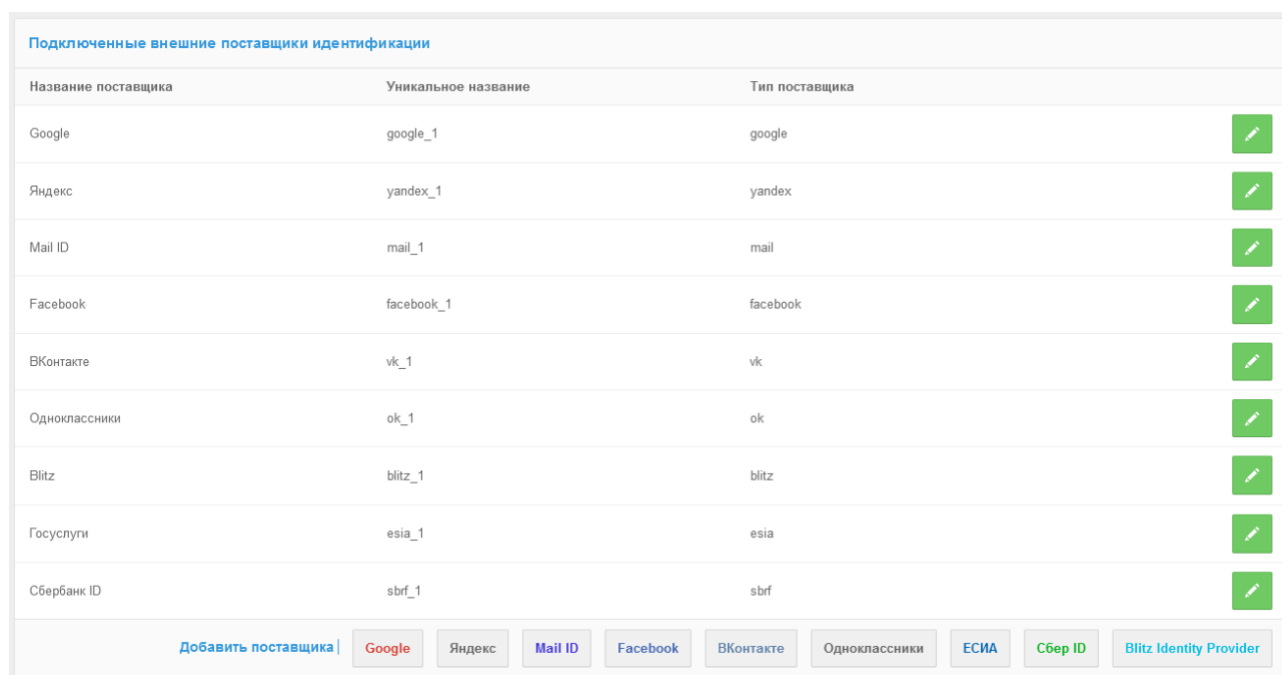
Рисунок 68 – Восстановление доступа










8. Вход через внешние поставщики идентификации

Настройка входа через внешние поставщики идентификации включает в себя следующие шаги:

1. Сконфигурировать конкретного поставщика идентификации в разделе «Поставщики идентификации» в консоли управления Blitz Identity Provider.
2. Сконфигурировать этого поставщика идентификации на стороне поставщика идентификации.
3. Включить возможность входа через данный поставщик идентификации в разделе «Аутентификации» (см. п. 4.3).

Для настройки используется раздел «Поставщики идентификации» в консоли управления. Начальный экран показывает уже настроенные поставщики идентификации и позволяет выбрать для настройки требуемый тип поставщика идентификации (Рисунок 69). Настройки поставщиков каждого из типов описаны далее в подразделах.



Название поставщика	Уникальное название	Тип поставщика	
Google	google_1	google	
Яндекс	yandex_1	yandex	
Mail ID	mail_1	mail	
Facebook	facebook_1	facebook	
ВКонтакте	vk_1	vk	
Одноклассники	ok_1	ok	
Blitz	blitz_1	blitz	
Госуслуги	esia_1	esia	
Сбербанк ID	sbrf_1	sbrf	

Добавить поставщика | [Google](#) | [Яндекс](#) | [Mail ID](#) | [Facebook](#) | [ВКонтакте](#) | [Одноклассники](#) | [ЕСИА](#) | [Сбep ID](#) | [Blitz Identity Provider](#)

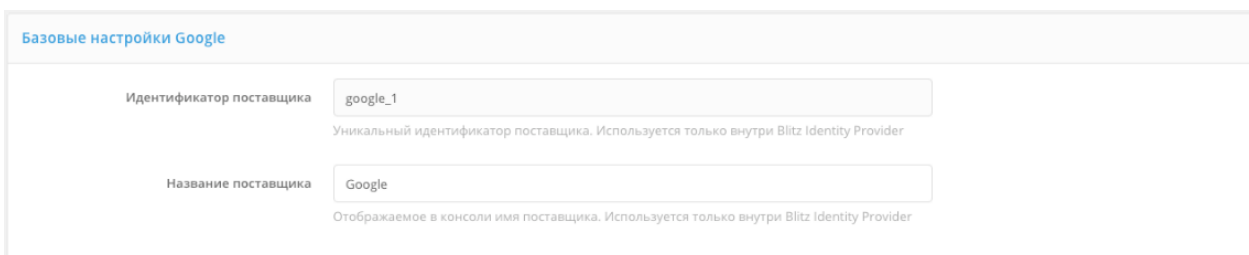
Рисунок 69 – Вид экрана настройки поставщиков идентификации

8.1. Вход через Google

Для конфигурирования входа через учетную запись Google следует выполнить следующие шаги в разделе «Поставщики идентификации» консоли управления:

1. Добавить поставщика, имеющего тип **Google**.
2. Ввести идентификатор поставщика (можно не менять предложенный системой идентификатор).

3. Ввести название поставщика. Именно это название будет отображаться на странице входа Blitz Identity Provider.



Базовые настройки Google

Идентификатор поставщика
Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика
Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider

Рисунок 70 – Базовые настройки поставщика идентификации Google

4. Перейти в «Диспетчер API Google» (Рисунок 71)²⁷, в котором выполнить следующие операции:
 - перейти в раздел «Учетные данные»;
 - создать проект и создать новые учетные данные типа «Идентификатор клиента OAuth»;
 - выбрать тип нового идентификатора клиента (например, веб-приложение) и дать ему название;
 - ограничения не задавать, они будут указаны позже;
 - Google сгенерирует идентификатор и секрет клиента, они потребуются для последующего ввода в консоли управления Blitz Identity Provider.

²⁷ См.: <https://console.developers.google.com>

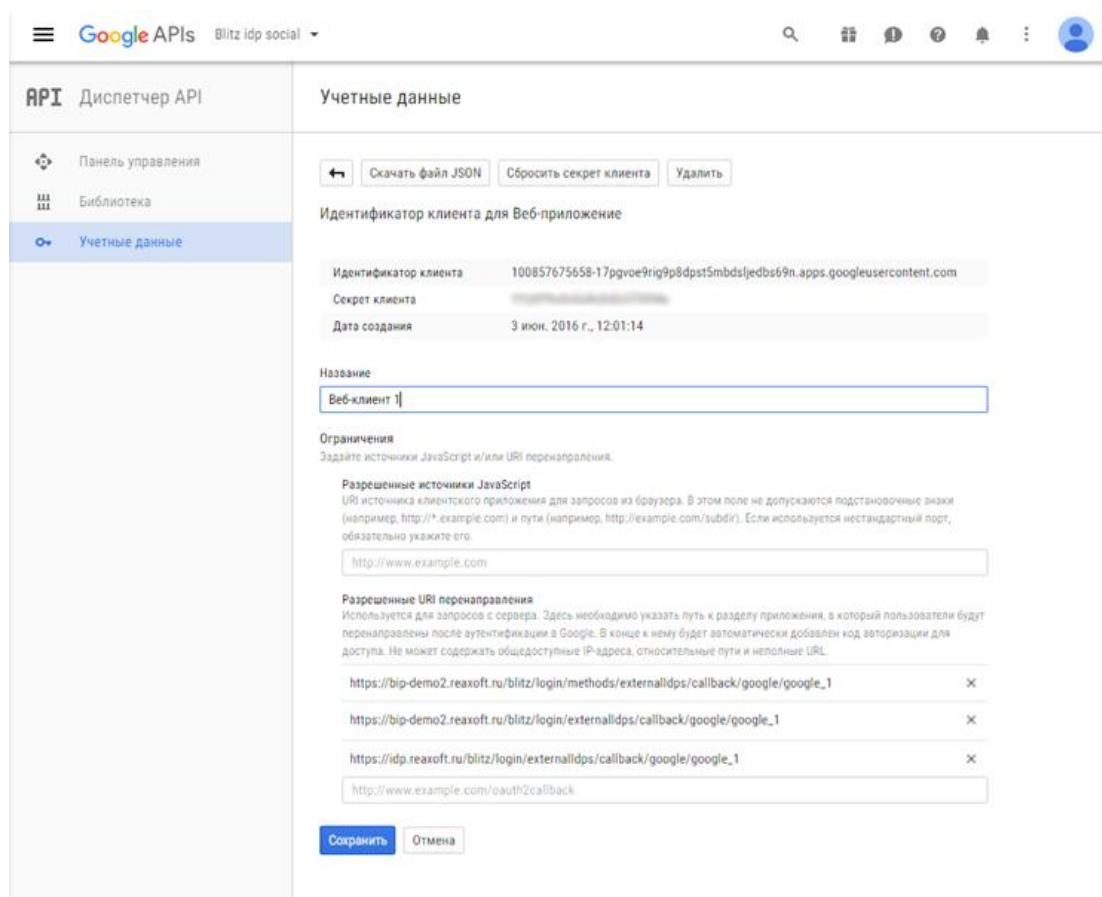


Рисунок 71 – Настройки в Диспетчере API Google

- Перейти в консоль управления Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 72), которые включают в себя:
 - идентификатор клиента (Client ID), полученный в Диспетчере API Google;
 - секрет клиента (Client secret), полученный в Диспетчере API Google;
 - запрашиваемые разрешения (scope), предусмотренные в Google²⁸;
 - правила, которые будут использоваться для идентификации учетной записи в Google и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Google. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов - `name` и `surname` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;

²⁸ См.: <https://developers.google.com/+/web/api/rest/oauth#authorization-scopes>

- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт Google, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
 - при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
 - правила сохранения атрибутов, полученных из Google, в Blitz Identity Provider. Например, правило `mail=${email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи Google (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через Google данный атрибут будет обновлен в хранилище Blitz Identity Provider.
6. Перейти в Диспетчер API Google и указать в качестве разрешенного URI перенаправления значение, указанное в параметре «URI перенаправления (Redirect URI)» консоли управления.
 7. Сохранить данные и в Blitz Identity Provider, и в Диспетчере API Google.
 8. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.3).

Настройки поставщика идентификации Google

Безопасность

Используйте раздел "Учетные данные" Диспетчера API Google для заполнения указанных ниже параметров. Не забудьте сохранить в "Учетных данных" указанные URI перенаправления.

URI перенаправления (Redirect URI)

Эти ссылки должны быть прописаны в настройках поставщика идентификации для корректной обработки результатов аутентификации пользователя. Используйте схему https, если вы используете защищенное соединение.

Идентификатор клиента (Client ID)

Секрет клиента (Client secret) [Изменить значение](#)

Разрешения

Запрашиваемые разрешения

Для добавления разрешения введите его имя и нажмите Enter

Укажите перечень разрешений (scope), которые должны быть получены при обращении к поставщику идентификации. [Перечень доступных разрешений Google](#)

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `${attr_name}`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

=

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `${attr_name}`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=VIP-${&random(4)}` позволит присвоить атрибуту `uid` значение `VIP-xxxxxx`, где `xxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Атрибут	Правило	Мастер
<input type="text" value="LastName"/>	<input style="width: 100%;" type="text" value="\${surname}"/>	<input type="checkbox"/> <input type="button" value="x"/>

[+ Добавить атрибут](#)

Рисунок 72 – Дополнительные настройки поставщика идентификации Google

8.2. Вход через Яндекс

Для конфигурирования входа через учетную запись Яндекс следует выполнить следующие шаги в разделе «Поставщики идентификации» консоли управления:

1. Добавить поставщика, имеющего тип **Яндекс**.
2. Ввести идентификатор поставщика (можно не менять предложенный системой идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице входа Blitz Identity Provider.

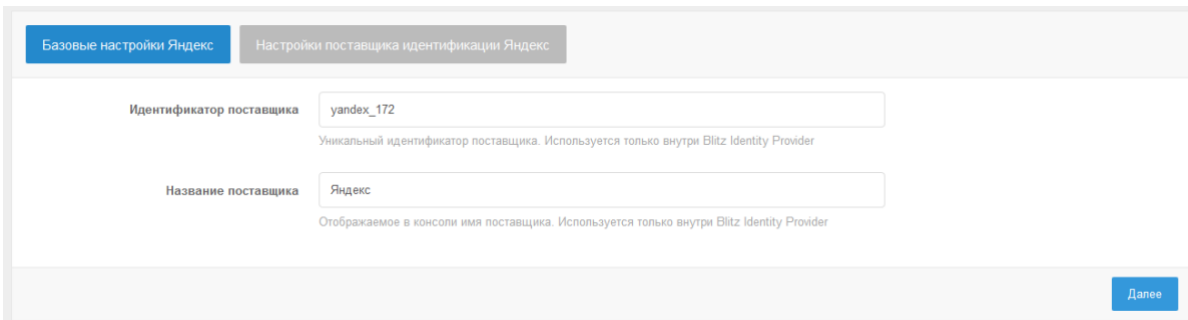


Рисунок 73 – Базовые настройки поставщика идентификации Яндекс

4. Перейти в приложение «Яндекс.ОAuth»²⁹, в котором выполнить следующие операции:
 - нажать на кнопку «Зарегистрировать новое приложение»;
 - ввести данные приложения, в том числе:
 - в настройках «Платформы» отметить «Веб-сервисы» и скопировать в поле «Callback URI» перечень URI перенаправления, предложенные в консоли Blitz Identity Provider;
 - в перечне доступов раскрыть «API Яндекс.Паспорта» и отметить «Доступ к адресу электронной почты», «Доступ к дате рождения» и «Доступ к логину, имени и фамилии, полу».
 - по результатам регистрации будет сгенерирован ID приложения и его пароль, они потребуются для последующего ввода в Blitz Identity Provider.
5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 72), которые включают в себя:
 - идентификатор клиента (ID приложения), полученный в приложении Яндекс.ОAuth;
 - пароль приложения, полученный в приложении Яндекс.ОAuth;
 - запрашиваемые разрешения (scope), предусмотренные в Яндекс.ОAuth – для

²⁹ См.: <https://oauth.yandex.ru/>

- указанных выше доступов следует указать `login:email`, `login:info` и `login:birthday`;
- правила, которые будут использоваться для идентификации учетной записи в Яндекс и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого из Яндекса. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${first_name} ${last_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов - `first_name` и `last_name` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило.
 - при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт Яндекс, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
 - при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
 - при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
 - правила сохранения атрибутов, полученных из Яндекс, в Blitz Identity Provider. Например, правило `mail=${default_email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `default_email` учетной записи Яндекс (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно

поставить опцию «Мастер». Если она отмечена, то при каждом входе через Яндекс данный атрибут будет обновлен в хранилище Blitz Identity Provider.

6. Сохранить данные и в Blitz Identity Provider.
7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.3).

Настройки поставщика идентификации Яндекс

Безопасность

Для заполнения используйте данные из приложения [Яндекс OAuth](#). Не забудьте сохранить в настройках приложения Яндекс OAuth указанные URI перенаправления, а также отметить в разделе [Доступы/API Яндекс.Паспорта](#) данные, которые необходимо получать от Яндекса.

URI перенаправления (Callback URI)

Эти ссылки должны быть прописаны в параметре Callback URI приложения Яндекс OAuth для корректной обработки результатов аутентификации пользователя. Используйте схему https, если вы используете защищенное соединение.

ID приложения

Пароль приложения [Изменить значение](#)

Разрешения

Запрашиваемые разрешения

Для добавления разрешения введите его имя и нажмите Enter

Укажите перечень разрешений (scope), которые должны быть получены при обращении к поставщику идентификации. Перечень доступных для приложения разрешений Яндекс

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `cn=$(name) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

=

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `cn=$(name) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=BITP-$(random(4))` позволит присвоить атрибуту `uid` значение `BITP-xxxxxxx`, где `xxxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Пример атрибутов для mappinga

Атрибут	Правило	Мастер	
<input type="text" value="mail"/>	= <input type="text" value="\$(default_email)"/>	<input type="checkbox"/>	<input type="button" value="✖"/>
<input type="text" value="FirstName"/>	= <input type="text" value="\$(first_name)"/>	<input type="checkbox"/>	<input type="button" value="✖"/>
<input type="text" value="LastName"/>	= <input type="text" value="\$(last_name)"/>	<input type="checkbox"/>	<input type="button" value="✖"/>

[+ Добавить атрибут](#)

Рисунок 74 – Дополнительные настройки поставщика идентификации Яндекс

8.3. Вход через Facebook

Для конфигурирования входа через учетную запись Facebook следует выполнить следующие шаги в разделе «Поставщики идентификации»:

1. Добавить поставщика, имеющего тип **Facebook**.
2. Ввести идентификатор поставщика (или не менять предложенный идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице аутентификации.

Базовые настройки Facebook

Идентификатор поставщика	<input type="text" value="facebook_1"/>
<small>Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider</small>	
Название поставщика	<input type="text" value="Facebook"/>
<small>Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider</small>	

Рисунок 75 – Базовые настройки поставщика идентификации Facebook

4. Перейти в панель «Facebook для разработчиков» (Рисунок 76)³⁰, в которой выполнить следующие операции:
 - войдите с помощью своей учетной записи Facebook и при необходимости зарегистрируйтесь в качестве разработчика;
 - добавьте новое приложение, указав его название, адрес электронной почты для связи и категорию приложения;
 - создайте идентификатор приложения;
 - перейдите в настройки приложения, раздел «Основное». В этом разделе указать параметр «Домены приложения» (должен соответствовать домену, на котором установлен Blitz Identity Provider) и добавить сайт с аналогичным URL.
 - Перейти в раздел «Проверка приложения» и активировать пункт «Сделать приложение «...» доступным для всех?»

³⁰ См.: <https://developers.facebook.com/apps/>

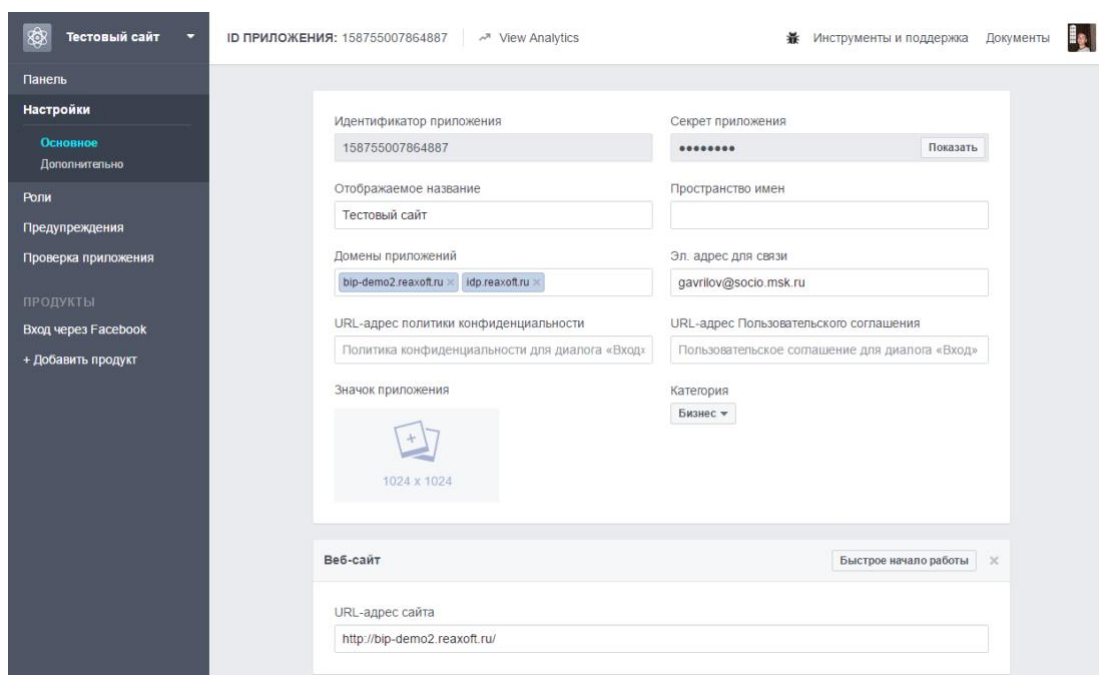


Рисунок 76 – Настройки в панели Facebook для разработчиков

5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 77), которые включают в себя:

- идентификатор приложения (App ID), полученный в панели Facebook для разработчиков;
- секрет приложения (App Secret), полученный в панели Facebook для разработчиков;
- запрашиваемые разрешения (scope), предусмотренные в Facebook³¹;
- запрашиваемые атрибуты, предусмотренные в Facebook; допустимо указывать только те атрибуты, которые предусмотрены выбранными разрешениями;
- правила, которые будут использоваться для идентификации учетной записи в Facebook и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Facebook. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `name` и `surname` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило.

³¹ См.: <https://developers.facebook.com/docs/facebook-login/permissions/>

- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт Facebook, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
 - при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
 - при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
 - правила сохранения атрибутов, полученных из Facebook, в Blitz Identity Provider. Например, правило `mail=${email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи Facebook (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через Facebook данный атрибут будет обновлен в хранилище Blitz Identity Provider.
6. Сохранить данные и в Blitz Identity Provider, и в панели Facebook для разработчиков.

Настройки поставщика идентификации Facebook

Безопасность

Для заполнения используйте панель [Facebook для разработчиков](#). Не забудьте сохранить в настройках приложения Facebook указанный домен приложения.

Домен приложения `sudir.reaxoft.ru`

URL-адреса для перенаправления
 OAuth `http(s)://sudir.reaxoft.ru/sps/login/externaldps/callback/facebook/facebook_1/false`
`http(s)://sudir.reaxoft.ru/sps/profile/social/externaldps/callbackPopup/facebook/facebook_1`

Эти ссылки должны быть прописаны в настройках поставщика идентификации для корректной обработки результатов аутентификации пользователя. Используйте схему `https`, если вы используете защищенное соединение.

Идентификатор приложения (App ID)

Секрет приложения (App Secret) [Изменить значение](#)

Разрешения и атрибуты

Запрашиваемые разрешения

Для добавления разрешения введите его имя и нажмите Enter
Укажите перечень разрешений (scope), которые должны быть получены при обращении к поставщику идентификации. [Перечень доступных разрешений Facebook](#)

Запрашиваемые атрибуты

Для добавления атрибута введите его имя и нажмите Enter. Укажите перечень атрибутов, которые должны быть получены при обращении к поставщику идентификации. Перечень доступных атрибутов зависит от того, какие разрешения запрашиваются.

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `${attr_name}`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

= ✕

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `${attr_name}`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=BIP-${&random(4)}` позволит присвоить атрибуту `uid` значение `BIP-xxxxxx`, где `xxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Атрибут	Правило	Мастер	
<input type="text" value="mail"/>	= <input type="text" value="\${email}"/>	<input type="checkbox"/>	✕

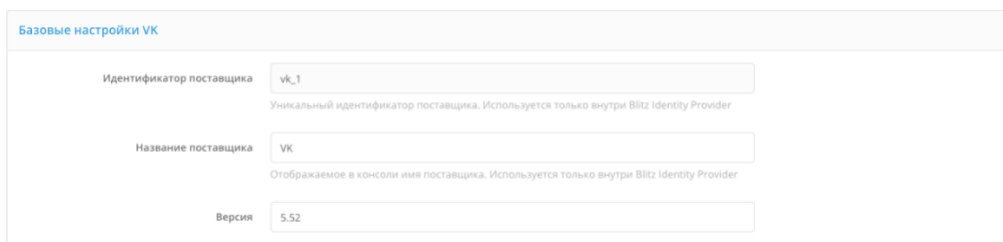
[+ Добавить атрибут](#)

Рисунок 77 – Дополнительные настройки поставщика идентификации Facebook

8.4. Вход через ВКонтакте

Для конфигурирования входа через учетную запись ВКонтакте следует выполнить следующие шаги в разделе «Поставщики идентификации»:

1. Добавить поставщика, имеющего тип **VK**.
2. Ввести идентификатор поставщика (или не менять предложенный идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице аутентификации.



Базовые настройки VK

Идентификатор поставщика	vk_1	Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider
Название поставщика	VK	Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider
Версия	5.52	

Рисунок 78 – Базовые настройки поставщика идентификации ВКонтакте

4. Перейти в «Панель VK для разработчиков» (Рисунок 79)³², в которой выполнить следующие операции:
 - войдите с помощью своей учетной записи ВКонтакте;
 - перейти в раздел «Мои приложения»;
 - выбрать пункт «Создать приложение»;
 - выбрать тип создаваемого приложения – «Веб-сайт», указать его название, адрес, и домен;
 - в появившемся окне настроек приложения прописать базовый домен приложения (должен совпадать с доменом, на котором установлен Blitz Identity Provider).

³² См.: <https://new.vk.com/dev>

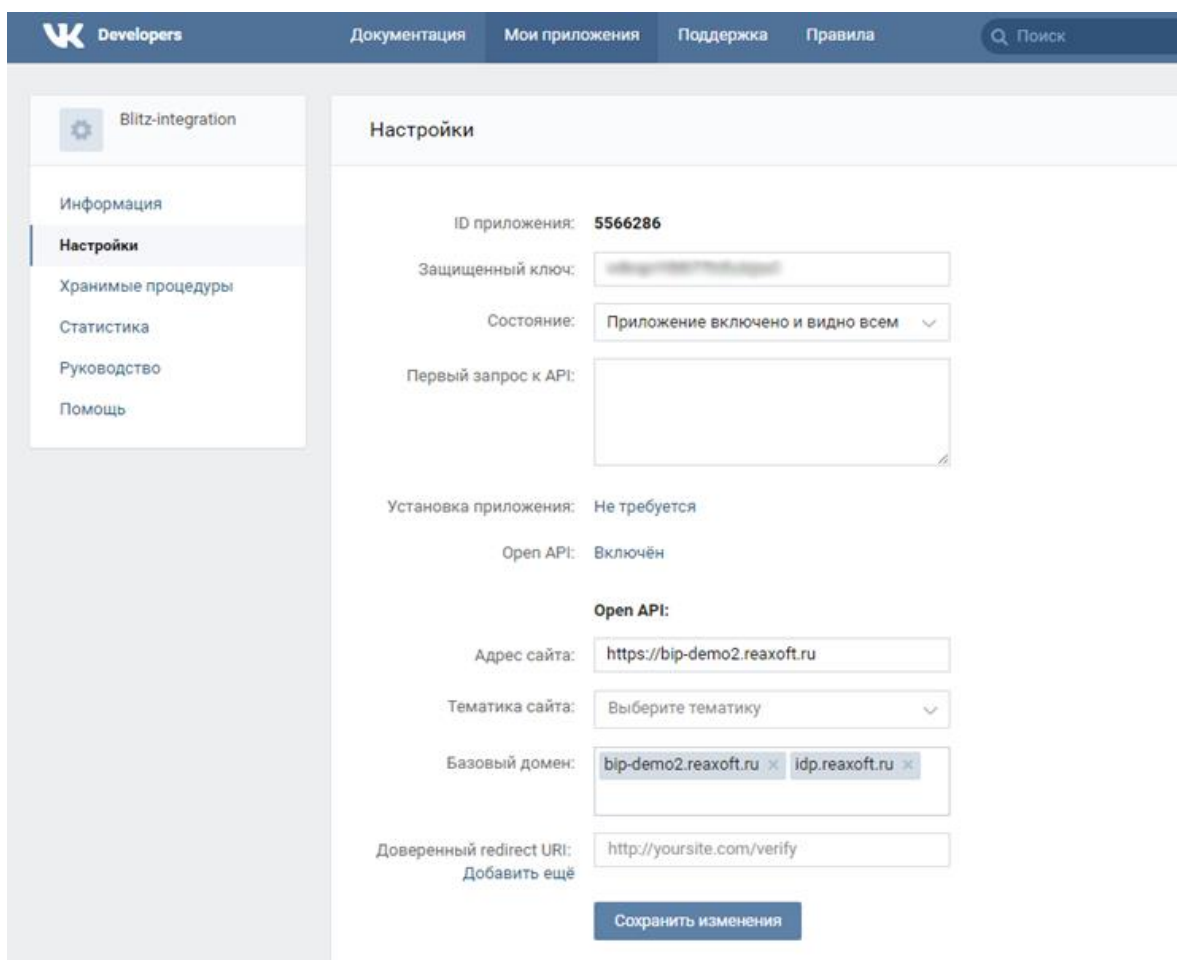


Рисунок 79 – Настройки в панели VK для разработчиков

5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 80), которые включают в себя:
 - ID приложения, полученный в панели VK для разработчиков;
 - защищенный ключ, полученный в панели VK для разработчиков;
 - запрашиваемые разрешения, предусмотренные в ВКонтакте³³;
 - правила, которые будут использоваться для идентификации учетной записи в ВКонтакте и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от ВКонтакте. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `name` и `surname` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;

³³ См.: <https://new.vk.com/dev/permissions>

- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт ВКонтакте, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
 - при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
 - при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
 - правила сохранения атрибутов, полученных из ВКонтакте, в Blitz Identity Provider. Например, правило `mail=${email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи ВКонтакте (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через ВКонтакте данный атрибут будет обновлен в хранилище Blitz Identity Provider.
6. Сохранить данные и в Blitz Identity Provider, и в панели VK для разработчиков.
7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п 4.3).

Настройки поставщика идентификации ВКонтакте

Безопасность

Используйте раздел "Мои приложения" панели VK для разработчиков для заполнения указанных ниже параметров. Не забудьте сохранить в панели ВКонтакте указанные URI перенаправления

Версия

Доверенные redirect URI

Эти ссылки должны быть прописаны в настройках поставщика идентификации для корректной обработки результатов аутентификации пользователя. Используйте схему https, если вы используете защищенное соединение.

ID приложения

Защищенный ключ [Изменить значение](#)

Разрешения

Запрашиваемые разрешения

Для добавления разрешения введите его имя и нажмите Enter

Укажите перечень разрешений (scope), которые должны быть получены при обращении к поставщику идентификации. [Перечень доступных разрешений ВКонтакте](#)

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `${attr_name}`, где attr_name - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - name и surname через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

=

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `${attr_name}`, где attr_name - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - name и surname через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=8IP-${&random(4)}` позволит присвоить атрибуту uid значение 8IP-xxxxxx, где xxxxxx - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Атрибут	Правило	Мастер	
<input type="text" value="mail"/>	= <input type="text" value="\${email}"/>	<input type="checkbox"/>	<input type="button" value="x"/>
<input type="text" value="FirstName"/>	= <input type="text" value="\${first_name}"/>	<input checked="" type="checkbox"/>	<input type="button" value="x"/>
<input type="text" value="LastName"/>	= <input type="text" value="\${last_name}"/>	<input checked="" type="checkbox"/>	<input type="button" value="x"/>

[+ Добавить атрибут](#)

Рисунок 80 – Дополнительные настройки поставщика идентификации ВКонтакте

8.5. Вход через Одноклассники

Для конфигурирования входа через учетную запись сети «Одноклассники» следует выполнить следующие шаги в разделе «Поставщики идентификации»:

1. Добавить поставщика, имеющего тип **Одноклассники**.
2. Ввести идентификатор поставщика (или не менять предложенный идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице аутентификации.

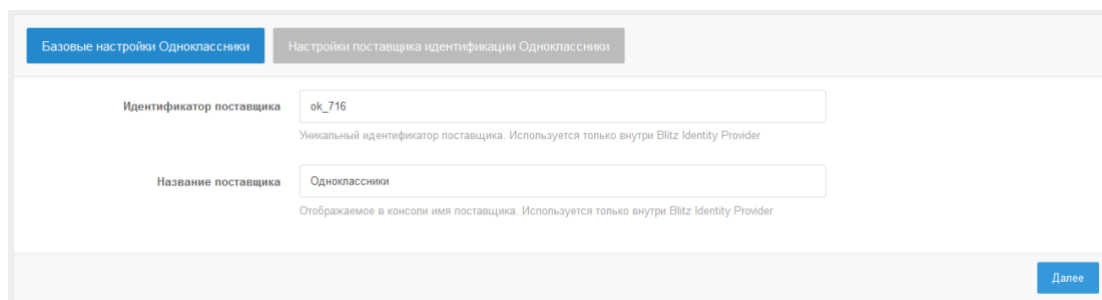


Рисунок 81 – Базовые настройки поставщика идентификации сети «Одноклассники»

4. Перейти на страницу «OAuth авторизация»³⁴, где выполнить следующие операции:
 - зарегистрироваться в сети Одноклассники и привязать к своему аккаунту email
 - на этот email будут приходить письма, содержащие регистрационные данные приложений;
 - получить права разработчика по ссылке <https://ok.ru/devaccess>;
 - зарегистрировать свое приложение и получить Application ID, публичный ключ приложения и секретный ключ приложения;
 - запросить следующие права для приложения: **VALUABLE_ACCESS**, **LONG_ACCESS_TOKEN**, **GET_EMAIL**;
 - прописать перечень разрешённых `redirect_uri`.
5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 82), которые включают в себя:
 - ввод регистрационных данных приложения, полученных ранее:
 - название приложения (Application ID);
 - секретный ключ приложения;
 - публичный ключ приложения;

³⁴ См.: <https://apiok.ru/ext/oauth/>

- правила, которые будут использоваться для идентификации учетной записи в сети Одноклассники и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого из Одноклассники. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${first_name} ${last_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `first_name` и `last_surname` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт сети Одноклассники, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из Одноклассники, в Blitz Identity Provider. Например, правило `mail=${email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи сети Одноклассники (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно

поставить опцию «Мастер». Если она отмечена, то при каждом входе через Одноклассники данный атрибут будет обновлен в хранилище Blitz Identity Provider.

6. Сохранить данные и в Blitz Identity Provider.

Настройки поставщика идентификации Одноклассники

Безопасность

Используйте раздел "Как начать использовать OAuth" страницы [OAuth авторизация](#) для заполнения указанных ниже параметров. Не забудьте сохранить в настройках приложения Одноклассники указанные ниже разрешенные `redirect_uri`

Разрешённые `redirect_uri` `http(s)://sudir.reaxoft.ru/sps/login/externaldps/callback/ok/ok_1/false`
`http(s)://sudir.reaxoft.ru/sps/profile/social/externaldps/callbackPopup/ok/ok_1`

Эти ссылки должны быть прописаны в Список разрешённых `redirect_uri` приложения Одноклассники для корректной обработки результатов аутентификации пользователя. Используйте схему `https`, если вы используете защищенное соединение.

Название приложения (Application ID)

Секретный ключ приложения [Изменить значение](#)

Публичный ключ приложения [Изменить значение](#)

Разрешения

Запрашиваемые разрешения VALUEABLE_ACCESS x GET_EMAIL x

Для добавления разрешения введите его имя и нажмите Enter

Укажите перечень разрешений (score), которые должны быть получены при обращении к поставщику идентификации. [Перечень доступных разрешений Одноклассники](#)

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `cn=$(name) ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

= ✖

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `cn=$(name) ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=81P-$(8*random(4))` позволит присвоить атрибуту `uid` значение `81P-xxxxxxx`, где `xxxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

[Пример атрибутов для маппинга](#)

Атрибут	Правило	Мастер	
<input type="text" value="mail"/>	= <input type="text" value="\$ {email}"/>	<input type="checkbox"/>	✖
<input type="text" value="FirstName"/>	= <input type="text" value="\$ {first_name}"/>	<input type="checkbox"/>	✖
<input type="text" value="LastName"/>	= <input type="text" value="\$ {last_name}"/>	<input type="checkbox"/>	✖

[+ Добавить атрибут](#)

Рисунок 82 – Дополнительные настройки поставщика идентификации сети Одноклассники

8.6. Вход через Mail ID

Для конфигурирования входа через учетную запись Mail ID следует выполнить следующие шаги в разделе «Поставщики идентификации» консоли управления:

1. Добавить поставщика, имеющего тип **Mail ID**.
2. Ввести идентификатор поставщика (можно не менять предложенный системой идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице входа Blitz Identity Provider.

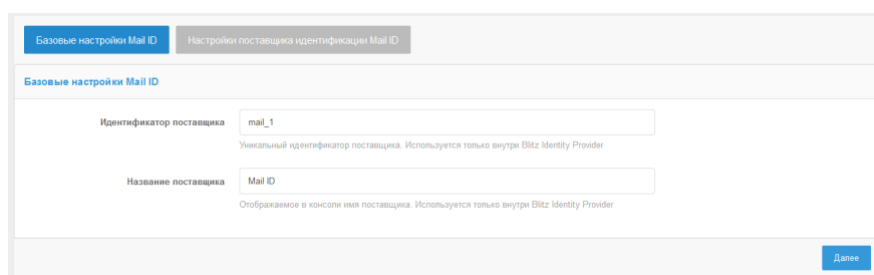


Рисунок 83 – Базовые настройки поставщика идентификации Mail ID

4. Перейти на странице «Создание приложения» Mail.ru³⁵, в котором выполнить следующие операции:
 - нажать на кнопку «Создать приложение»;
 - аутентифицировать под учетной записью Mail.ru;
 - ввести данные приложения, в том числе:
 - название приложения;
 - в поле «Все redirect_uri» указать перечень URI перенаправления, предложенные в консоли Blitz Identity Provider;
 - в блоке «Платформы» поставить галочку на Web;
 - по результатам регистрации будет сгенерирован ID Приложения и его секрет, они потребуются для последующего ввода в Blitz Identity Provider.
5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 72), которые включают в себя:
 - идентификатор клиента (ID приложения), полученный ранее;
 - секрет приложения, полученный ранее;
 - запрашиваемые разрешения (scope), например, **userinfo**;

³⁵ См.: <https://help.mail.ru/developers/oauth/app>

- правила, которые будут использоваться для идентификации учетной записи в Mail ID и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Mail ID. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${first_name} ${last_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов - `first_name` и `last_name` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило.
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт Mail ID, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из Mail ID, в Blitz Identity Provider. Например, правило `mail=${email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи Mail ID (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через Mail ID данный

атрибут будет обновлен в хранилище Blitz Identity Provider.

6. Сохранить данные и в Blitz Identity Provider.
7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.3).

Настройки поставщика идентификации Mail ID

Безопасность

Для заполнения используйте данные из приложения `oauth@mail.ru`. Не забудьте сохранить в настройках приложения OAUTH@MAIL.RU указанные URI перенаправления и в качестве используемой платформы выбрать Web.

URI перенаправления (`redirect_uri`) `http(s)://sudir.reaxoft.ru/sps/login/externalldps/callback/mail/mail_1/false`
`http(s)://sudir.reaxoft.ru/sps/profile/social/externalldps/callbackPopup/mail/mail_1`

Эти ссылки должны быть прописаны в параметре `redirect_uri` приложения `oauth@mail.ru` для корректной обработки результатов аутентификации пользователя. Используйте схему `https`, если вы используете защищенное соединение.

ID приложения:

Секрет приложения: [Изменить значение](#)

Разрешения

Запрашиваемые разрешения:

Для добавления разрешения введите его имя и нажмите Enter

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `${attr_name}`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

=

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `${attr_name}`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=BITP-${&random(4)}` позволит присвоить атрибуту `uid` значение `BITP-xxxxxxx`, где `xxxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

[Пример атрибутов для маппинга](#)

Атрибут	Правило	Мастер
<input type="text" value="mail"/>	= <input style="width: 100px;" type="text" value="\${email}"/>	<input checked="" type="checkbox"/> <input type="button" value="✖"/>

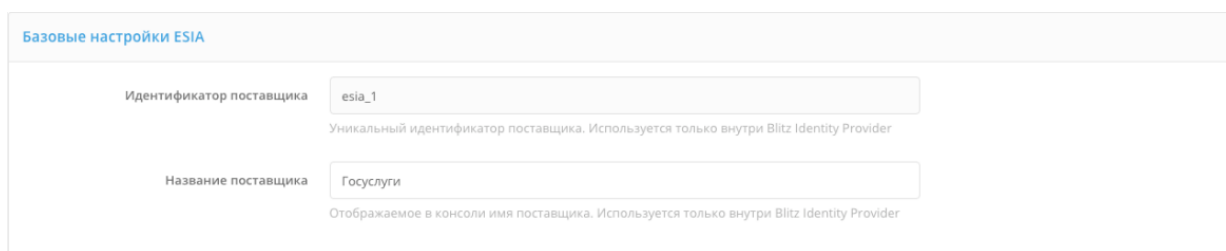
[+ Добавить атрибут](#)

Рисунок 84 – Дополнительные настройки поставщика идентификации Mail ID

8.7. Вход через Единую систему идентификации и аутентификации (ЕСИА)

Для конфигурирования входа через учетную запись ЕСИА следует выполнить следующие шаги в разделе «Поставщики идентификации»:

1. Добавить поставщика, имеющего тип **ЕСИА**.
2. Ввести идентификатор поставщика (или не менять предложенный идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице аутентификации.



Базовые настройки ESIA

Идентификатор поставщика
Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика
Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider

Рисунок 85 – Базовые настройки поставщика идентификации ЕСИА

4. Получить в удостоверяющем центре ключ электронной подписи для взаимодействия с ЕСИА и выгрузить сертификат открытого ключа. Произвести конвертацию ключа в формат, совместимый с Blitz Identity Provider.
5. Сертификат ключа необходимо зарегистрировать на Технологическом портале ЕСИА (см. следующий пункт).
6. Осуществить регистрацию информационной системы организации через Технологический портал ЕСИА³⁶, в котором выполнить следующие операции:
 - нажать на кнопку «Добавить систему»;
 - указать название системы, отображаемое название, мнемонику системы, список URL системы (задать домен развернутой системы Blitz Identity Provider, с указанием протокола https), алгоритм формирования электронной подписи и выбрать ответственного сотрудника (Рисунок 86);
 - сохранить данные и перейти к настройке сертификатов информационной системы;
 - загрузить сертификат для зарегистрированной информационной системы на Технологическом портале (Рисунок 87);

³⁶ См.: <https://esia.gosuslugi.ru/console/tech/> До регистрации ИС в ЕСИА необходимо зарегистрировать учетную запись организации в ЕСИА и дать одному из сотрудников доступ к Технологическому portalу.

Данные информационной системы

ОСНОВНЫЕ ДАННЫЕ СИСТЕМЫ

Название системы

Отображаемое название
Укажите название системы, которое будет отображаться пользователям Госуслуг и интегрированных систем. Рекомендуется указывать понятное для массового пользователя название, например, вместо «Единый портал государственных услуг (функций)» - «Госуслуги».

Мнемоника системы
Если система зарегистрирована в СМЭВ, то мнемоника в ЕСИА должна соответствовать мнемонике точки подключения в СМЭВ. Система, регистрируемая в ЕСИА с целью получения доступа к сервису ЕСИА в СМЭВ, должна быть предварительно зарегистрирована в СМЭВ

Информация о системе

URL системы
Введите список адресов (каждый в отдельном поле, с префиксом "https://"), которые могут быть указаны в ссылке для обратного перехода после аутентификации пользователя в ЕСИА.
Если система предполагает взаимодействие с ЕСИА только через СМЭВ (без аутентификации пользователя), то в качестве URL возможно указание https://esia.gosuslugi.ru
Если, при направлении пользователя для аутентификации в ЕСИА, в ссылке для обратного перехода будет указан адрес, не входящий в список доверенных URL, процесс аутентификации будет прерван. Допускается указывать имя домена или IP-адрес сервера в формате IPv4 / IPv6.

Алгоритм формирования электронной подписи
Выберите криптографический алгоритм формирования электронной подписи, который будет использоваться при выпуске маркеров доступа, маркеров идентификации, маркеров обновления, кода авторизации

URL для отправки push сообщений
Введите адрес (с префиксом "https://"), который будет использоваться ЕСИА для отправки в ИС сообщений - уведомлений (push-сообщений)

КАТЕГОРИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Категория информационной системы

Время жизни access token, мин
min: 10; max: 180

Время жизни refresh token, мин
min: 60; max: 1051200

ОТВЕТСТВЕННЫЙ ЗА ЭКСПЛУАТАЦИЮ СИСТЕМЫ

ФИО
Введите имя ответственного сотрудника вашей организации и выберите его из выпадающего списка. Пользователь должен быть присоединен к учетной записи вашей организации.

Адрес электронной почты

Номер телефона

Рисунок 86 – Добавление системы в Технологическом портале ЕСИА

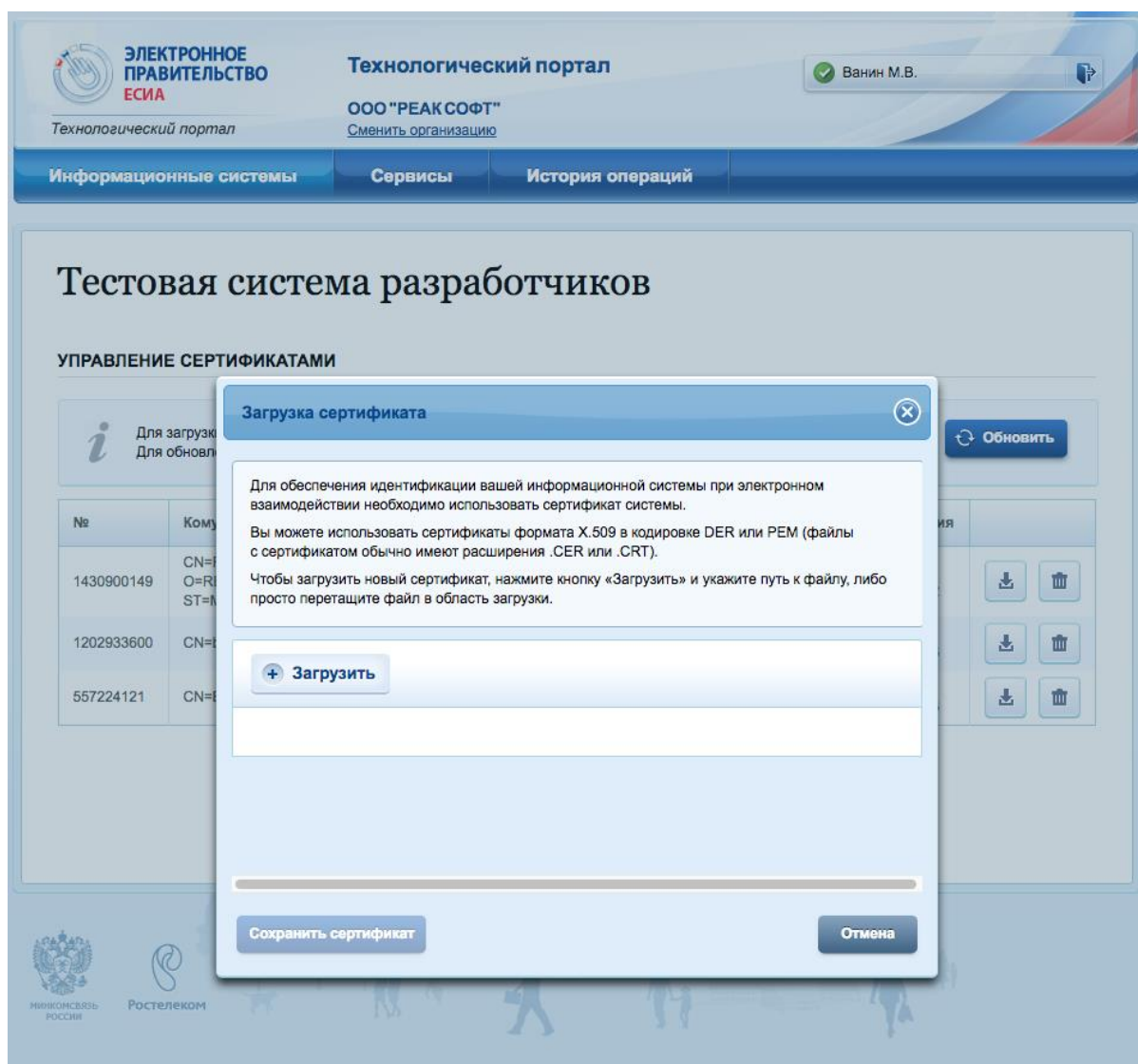


Рисунок 87 – Добавление сертификата системы в Технологическом портале ЕСИА

7. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 88), которые включают в себя:

- URI внешнего поставщика – домен среды ЕСИА, к которой производится подключение, например, <https://esia.gosuslugi.ru>;
- мнемоника системы, указанная ранее в Технологическом портале ЕСИА;
- идентификатор ключа электронной подписи (alias) – идентификатор ключа электронной подписи, загруженный в хранилище Blitz Identity Provider³⁷. Именно сертификат ключа этой электронной подписи должен быть загружен в Технологический портал ЕСИА;
- запрашиваемые разрешения – перечень запрашиваемых разрешений из ЕСИА;
- запрашиваемые данные пользователя – необходимо отметить те данные,

³⁷ Хранилище, указанное в разделе keystore конфигурационного файла Blitz Identity Provider.

- которые следует получать из ЕСИА; эти данные должны быть доступны по запрашиваемым разрешениям;
- правила, которые будут использоваться для идентификации учетной записи в ЕСИА и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от ЕСИА. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `name` и `surname` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
 - при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт ЕСИА, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
 - при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
 - при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети;
 - правила сохранения атрибутов, полученных из ЕСИА, в Blitz Identity Provider. Например, правило `mail=${email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи ЕСИА (для пользователей, воспользовавшихся этим поставщиком

идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через ЕСИА данный атрибут будет обновлен в хранилище Blitz Identity Provider.

8. Сохранить данные в Blitz Identity Provider.

Чтобы вход через ЕСИА заработал, необходимо получить официальное разрешение на проведение идентификации и аутентификации пользователей с помощью зарегистрированной системы и получить доступ к тестовой/промышленной среде ЕСИА³⁸.

³⁸ Подробнее см.: <https://identityblitz.ru/services/esia-integration>

Настройки поставщика идентификации ЕСИА

Безопасность

Заполните данные для корректного взаимодействия Blitz Identity Provider с ЕСИА.

URL для авторизации:

URL для получения и обновления маркера:

URL для получения данных:

Мнемоника системы (client_id):

Идентификатор ключа электронной подписи (alias):

Предварительно ключ электронной подписи должен быть загружен в хранилище, указанное в разделе keystore конфигурационного файла Blitz Identity Provider.

После заполнения этих данных не забудьте перейти в **Технологический портал ЕСИА**, где должна быть зарегистрирована информационная система с указанной мнемоникой и сертификатом ключа электронной подписи.

Разрешения и данные пользователя

Выберите разрешения из доступного списка

Доступные разрешения

Запрашиваемые разрешения:

Для добавления разрешения введите его имя и нажмите Enter

Укажите перечень разрешений (scope), которые должны быть получены при обращении к поставщику идентификации.

Запрашиваемые данные пользователя: Основные данные Документы Адреса Контакты

Отмеченные ранее разрешения (scope) должны позволять получать указанные данные.

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=$(name) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

=

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `CN=$(name) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=BTP-$(random(4))` позволит присвоить атрибуту uid значение `BTP-xxxxxx`, где `xxxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Доступные атрибуты для маппинга

Атрибут	Правило	Мастер	
esia_oid	=\$[oid]	<input type="checkbox"/>	<input type="button" value="✖"/>
surname	=\$(lastName)	<input checked="" type="checkbox"/>	<input type="button" value="✖"/>
name	=\$(firstName)	<input checked="" type="checkbox"/>	<input type="button" value="✖"/>
middlename	=\$(middleName)	<input checked="" type="checkbox"/>	<input type="button" value="✖"/>
trusted	=\$(trusted)	<input checked="" type="checkbox"/>	<input type="button" value="✖"/>
passport	=\$(passport)	<input checked="" type="checkbox"/>	<input type="button" value="✖"/>
passport_sn	=\$(passportSN)	<input checked="" type="checkbox"/>	<input type="button" value="✖"/>

[+ Добавить атрибут](#)

Рисунок 88 – Дополнительные настройки поставщика идентификации ЕСИА

8.8. Вход через систему идентификации Сбербанка (Сбер ID)

Для конфигурирования входа через учетную запись Сбер ID следует выполнить следующие шаги в разделе «Поставщики идентификации»:

1. Добавить поставщика, имеющего тип **Сбер ID**.
2. Ввести идентификатор поставщика (или не менять предложенный идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице аутентификации.

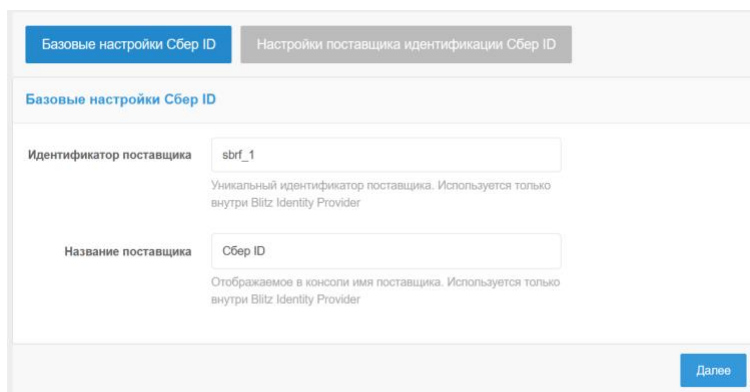


Рисунок 89 – Базовые настройки поставщика идентификации Сбер ID

4. Зарегистрировать приложение в системе Сбер ID. Для этого воспользоваться инструкцией, размещенной на официальном сайте этого поставщика идентификации³⁹. По результатам регистрации вы должны иметь:
 - идентификатор клиента (Client ID);
 - секрет клиента (Client Secret);
 - сертификат своей системы, подключенной к Сбер ID;
 - сертификат Сбер ID.
5. Настройте защищенный канал связи между организацией и банком с использованием сертификата, полученного от ПАО «Сбербанк».
6. Перейти в Blitz Identity Provider и заполнить настройки поставщика идентификации (Рисунок 90), которые включают в себя:
 - URL для авторизации – адрес, по которому должна инициироваться аутентификация, например: <https://online.sberbank.ru/CSAFront/oidc/authorize.do>;
 - URL для получения и обновления маркера – адрес, по которому происходит получение и обновление маркера доступа. Должен быть указан внутренний адрес сети, обращение через который обеспечит работу по защищенному каналу связи между организацией и банком;

³⁹ См.: <https://developer.sberbank.ru/doc/v1/sberbank-id/enrollsteps>

- URL для получения данных – адрес, по которому происходит получение данных пользователя. Должен быть указан внутренний адрес сети, обращение через который обеспечит работу по защищенному каналу связи между организацией и банком;
- идентификатор клиента (Client ID);
- секрет клиента (Client Secret);
- запрашиваемые группы данных – перечень запрашиваемых групп данных из Сбер ID;
- правила, которые будут использоваться для идентификации учетной записи в Сбер ID и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Сбер ID. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${first_name} ${last_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `first_name` и `last_name` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт Сбер ID, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;

- опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
 - правила сохранения атрибутов, полученных из Сбер ID, в Blitz Identity Provider. Например, правило `mail=${email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи Сбер ID (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через Сбер ID данный атрибут будет обновлен в хранилище Blitz Identity Provider.
7. Сохранить данные в Blitz Identity Provider.
 8. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.3).

Настройки поставщика идентификации Сбербанк ID

Безопасность

Для заполнения используйте данные, полученные при регистрации своей системы в Банке.

URI перенаправления (Redirect URI) http(s)://sudir.reasoft.ru/sp/login/externalidps/callback/sbrf_1/false
http(s)://sudir.reasoft.ru/sp/profile/social/externalidps/callback/Popup/sbrf/sbrf_1

Адрес страницы, на которую будет перенаправлен ответ после успешной аутентификации в системе Банка.

URL для авторизации

URL для получения и обновления маркера

URL для получения данных

Client ID

Client Secret [Изменить значение](#)

Группы данных

Запрашиваемые группы данных

name x	email x	address_req x	openid x
international_passport x	birthdate x	maandoc x	inn x
driving_license x	snbs x	gender x	address_of_actual_residence x

Для добавления группы данных введите ее имя и нажмите Enter

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `sn-$(name) $(surname)` означает, что атрибут SN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

=

[+ добавить условие](#)

OR

=

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `sn-$(name) $(surname)` означает, что атрибут SN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid-$(IP-$(random(4)))` позволит присвоить атрибуту `uid` значение `IP-xxxxxx`, где `xxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

[Пример атрибутов для шаблона](#)

Атрибут	Правило	Мастер
<input type="text" value="mail"/>	= <input type="text" value="\$(email)"/>	<input type="checkbox"/> ✕
<input type="text" value="mobile"/>	= <input type="text" value="\$(phone_number)"/>	<input type="checkbox"/> ✕
<input type="text" value="sbrfid"/>	= <input type="text" value="\$(sub)"/>	<input checked="" type="checkbox"/> ✕
<input type="text" value="FirstName"/>	= <input type="text" value="\$(given_name)"/>	<input type="checkbox"/> ✕
<input type="text" value="MiddleName"/>	= <input type="text" value="\$(middle_name)"/>	<input type="checkbox"/> ✕
<input type="text" value="LastName"/>	= <input type="text" value="\$(family_name)"/>	<input type="checkbox"/> ✕
<input type="text" value="birthDate"/>	= <input type="text" value="\$(birthdate)"/>	<input type="checkbox"/> ✕

[+ Добавить атрибут](#)

[Отмена](#) [Удалить](#) [Сохранить](#)

Рисунок 90 – Дополнительные настройки поставщика идентификации Сбер ID

8.9. Вход через систему идентификации Mos ID (СУДИР)

Для конфигурирования входа через учетную запись Mos ID (СУДИР) следует выполнить следующие шаги в разделе «Поставщики идентификации»:

1. Добавить поставщика, имеющего тип **Mos**.
2. Ввести идентификатор поставщика (или не менять предложенный идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице аутентификации.

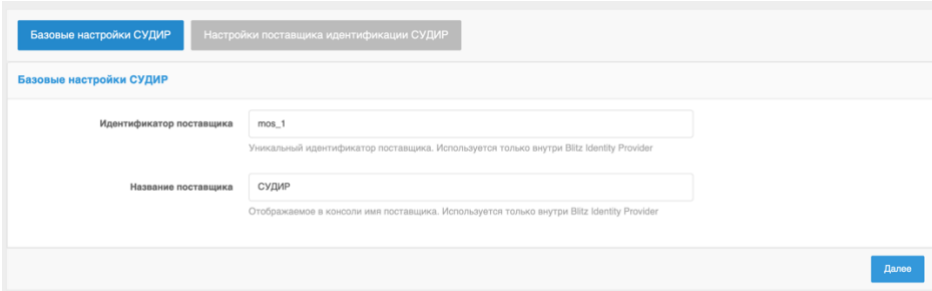


Рисунок 91 – Базовые настройки поставщика идентификации СУДИР

4. Зарегистрировать приложение в системе СУДИР. Для этого подать заявку согласно инструкции, размещенной на официальном сайте этого поставщика идентификации⁴⁰. По результатам регистрации вы должны иметь:
 - идентификатор (`client_id`);
 - секрет (`client_secret`).
5. Перейти в Blitz Identity Provider и заполнить настройки поставщика идентификации (Рисунок 92), которые включают в себя:
 - URL для авторизации – адрес, по которому должна инициироваться аутентификация, например: `https://login.mos.ru/sps/oauth/ae`;
 - URL для получения и обновления маркера – адрес, по которому происходит получение и обновление маркера доступа, например: `https://login.mos.ru/sps/oauth/te`;
 - URL для получения данных – адрес, по которому происходит получение данных пользователя, например: `https://login.mos.ru/sps/oauth/me`;
 - идентификатор (`client_id`);
 - секрет (`client_secret`);
 - запрашиваемые разрешения – перечень запрашиваемых разрешений, например, `openid` и `profile`;

⁴⁰ См.: <https://login.mos.ru/support> (внешний СУДИР) и <https://sudir.mos.ru/support> (внутренний СУДИР)

- идентификатор – укажите имя атрибута в СУДИР, который должен использоваться в качестве уникального идентификатора учетной записи. Для внешнего СУДИР это `guid`, для внутреннего СУДИР это `uid`.
- правила, которые будут использоваться для идентификации учетной записи в СУДИР и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от СУДИР. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${FirstName} ${LastName}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `FirstName` и `LastName` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт СУДИР, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту СУДИР;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту СУДИР.
- правила сохранения атрибутов, полученных из СУДИР, в Blitz Identity Provider. Например, правило `mail=${mail}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `mail` учетной записи

СУДИР (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через СУДИР данный атрибут будет обновлен в хранилище Blitz Identity Provider.

6. Сохранить данные в Blitz Identity Provider.
7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.3).

Настройки поставщика идентификации СУДИР

Безопасность

Заполните данные для корректного взаимодействия Blitz Identity Provider с системой управления доступом города Москвы. Подробнее о получении доступа и настройках подключения к порталу Москвы (mos.ru) можно посмотреть [здесь](#). Информация о работе с внутренним контуром СУДИР размещена [здесь](#).

Предопределенные ссылки возврата (redirect_uri) `http(s)://agumerov.identityblitz.ru/blitz/login/externalidpa/callback/mos/mos_1/false`
`http(s)://agumerov.identityblitz.ru/blitz/profile/social/externalidpa/callback/Popup/mos/mos_1`

Эти ссылки должны быть прописаны в настройках поставщика идентификации для корректной обработки результатов аутентификации пользователя. Используйте схему https, если вы используете защищенное соединение.

URL для авторизации

URL для получения и обновления маркера

URL для получения данных

Идентификатор (client_id)

Секрет (client_secret) [Изменить значение](#)

Разрешения

Запрашиваемые разрешения

Для добавления разрешения введите его имя и нажмите Enter

Укажите перечень разрешений (розрр), которые должны быть получены при обращении к поставщику идентификации. Обратитесь к администратору внешнего поставщика идентификации Blitz Identity Provider, чтобы получить перечень доступных разрешений

Идентификация учетных записей

Укажите уникальный атрибут внешнего поставщика идентификации, который будет использоваться для связи учетной записи в Blitz Identity Provider.

Идентификатор

Идентификация учетных записей

Укажите правила соответствия учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `$(attr_name)`, где attr_name - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `On$(name)$(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - name и surname через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

=

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `$(attr_name)`, где attr_name - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `On$(name)$(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - name и surname через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=BlP-$(&random(4))` позволит присвоить атрибуту uid значение BlP-XXXXXX, где XXXXXX - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Атрибут	Правило	Мастер
<input type="text" value="mail"/>	<input type="text" value="\$(mail)"/>	<input type="checkbox"/>

[+ Добавить атрибут](#)

[Отмена](#) [Удалить](#) [Сохранить](#)

Рисунок 92 – Дополнительные настройки поставщика идентификации СУДИР

8.10. Вход через другую установку Blitz Identity Provider

Для конфигурирования входа через учетную запись другого Blitz Identity Provider (например, установленного в другой организации, далее – «доверенный Blitz Identity Provider») следует выполнить следующие шаги в разделе Поставщики идентификации:

1. Добавить поставщика, имеющего тип **Blitz Identity Provider**.
2. Ввести идентификатор поставщика (или не менять предложенный идентификатор).
3. Ввести название поставщика. Именно это название будет отображаться на странице аутентификации.

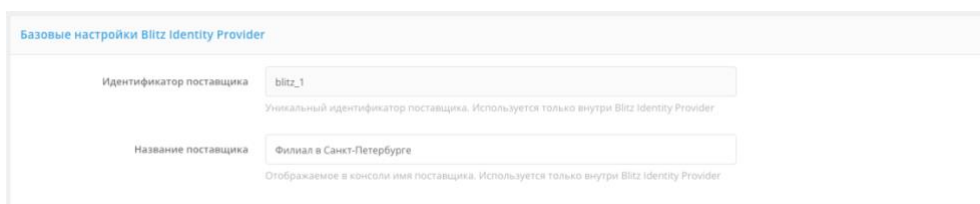


Рисунок 93 – Базовые настройки поставщика идентификации Blitz Identity Provider при настройке федеративного доступа

4. Открыть консоль управления доверенного Blitz Identity Provider (или попросить администратора другого Blitz Identity Provider это сделать) и выполнить следующие операции:
 - перейти в раздел «Приложения»;
 - нажать на кнопку «Добавить приложение»;
 - указать идентификатор приложения, название и домен приложения;
 - сохранить приложение и перейти к его настройке;
 - выбрать протокол подключения OAuth 2.0;
 - указать секрет (client_secret), либо оставить предзаполненный вариант;
 - указать префикс ссылки возврата, в качестве которой указать URL основной Blitz Identity Provider, в который будет осуществляться вход;
 - произвести настройку необходимых разрешений в разделе «OAuth 2.0».
5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 94), которые включают в себя:
 - URL для авторизации – адрес доверенного Blitz Identity Provider, по которому можно получить код авторизации;
 - URL для получения и обновления маркера – адрес доверенного Blitz Identity Provider, по которому можно получать маркеры доступа;
 - URL для получения данных – адрес доверенного Blitz Identity Provider, по которому можно получать данные пользователя;

- идентификатор (`client_id`), указанный в настройках доверенного Blitz Identity Provider;
- секрет (`client_secret`), указанный в настройках доверенного Blitz Identity Provider;
- запрашиваемые разрешения, данные разрешения должны быть определены в разделе «OAuth 2.0» доверенного Blitz Identity Provider;
- идентификатор – атрибут доверенного Blitz Identity Provider, который будет использоваться в качестве идентификатора пользователя (обеспечивает уникальность учетной записи даже при изменении атрибута, отвечающего за имя пользователя);
- правила, которые будут использоваться для идентификации учетной записи в доверенном Blitz Identity Provider и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от доверенного Blitz Identity Provider. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${name} ${surname}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `name` и `surname` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт доверенного Blitz Identity Provider, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если

учетная запись была идентифицирована»:

- опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из доверенного Blitz Identity Provider, в Blitz Identity Provider. Например, правило `mail=${email}` означает, что атрибут с именем `mail` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи доверенного Blitz Identity Provider (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через доверенного Blitz Identity Provider данный атрибут будет обновлен в хранилище Blitz Identity Provider.
6. Сохранить данные в Blitz Identity Provider.
 7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п 4.3).

Базовые настройки Blitz Identity Provider

Идентификатор поставщика:
Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика:
Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider

Настройки поставщика идентификации Blitz Identity Provider

Безопасность

Для заполнения указанных параметров обратитесь к администратору внешнего поставщика идентификации Blitz Identity Provider. Необходимая информация размещена в свойствах подключаемого приложения (по протоколу OAuth 2.0). Также передайте администратору приведенные ниже URI перенаправления.

Предопределенные ссылки возврата (redirect_uri):

Эти ссылки должны быть прописаны в настройках поставщика идентификации для корректной обработки результатов аутентификации пользователя. Используйте ссылку http, если вы используете заданное соединение.

URL для авторизации:

URL для получения и обновления маркера:

URL для получения данных:

Идентификатор (client_id):

Секрет (client_secret):

Разрешения

Запрашиваемые разрешения:
Для добавления разрешения введите его имя и нажмите Enter. Укажите перечень разрешений (scope), которые должны быть получены при обращении к поставщику идентификации. Обратитесь к администратору внешнего поставщика идентификации Blitz Identity Provider, чтобы получить перечень доступных разрешений.

Идентификация учетных записей

Укажите уникальный атрибут внешнего поставщика идентификации, который будет использоваться для связи учетной записи в Blitz Identity Provider.

Идентификатор:

Идентификация учетных записей

Укажите правила сопоставления учетных записей Blitz Identity Provider и поставщика идентификации. При первом входе пользователя через поставщика идентификации с помощью этих правил будет осуществляться поиск учетной записи в Blitz Identity Provider для ее последующего связывания с учетной записью поставщика идентификации.

Для создания правила используйте строки подстановки `{attr_name}`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `cn={name} {surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована

Для правила должна быть найдена только одна учетная запись по заданным правилам соответствия

Требовать ввод пароля, если учетная запись была идентифицирована

-

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, получаемых от поставщика идентификации. Для формирования каждого атрибута должно быть создано свое правило.

Для создания правила используйте обозначение `{attr_name}`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `cn={name} {surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел.

Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=ERP-{idnumber(4)}` позволит присвоить атрибуту `uid` значение `ERP-xxxxxx`, где `xxxxxx` - случайное сгенерированное величина (набор цифр и букв латинского алфавита).

Атрибут	Правило	Мастер
<input type="text" value="LastName"/>	<input style="width: 100%;" type="text" value="{LastName}"/>	<input type="checkbox"/> <input type="button" value="✖"/>

[+ Добавить атрибут](#)

Рисунок 94 – Настройки подключения к внешнему поставщику идентификации Blitz Identity Provider

9. Управление учетными записями пользователей

В разделе «Пользователи» консоли управления доступны следующие операции:

- поиск учетных записей пользователей;
- добавление учетных записей пользователей;
- просмотр и редактирование идентификационных данных пользователей;
- смена пароля учетной записи;
- просмотр и отвязка учетных записей внешних систем;
- задание значений дополнительных атрибутов пользователей;
- привязку устройств для проведения двухфакторной аутентификации;
- просмотр групп, в которые включен пользователь;
- просмотр прав;
- просмотр выданных приложениям разрешений на доступ к данным;
- удаление учетной записи.

Общий вид страницы управления данными пользователей представлен на рисунке 95.

The screenshot displays the 'Пользователи' (Users) management page. At the top, there is a search bar containing 'test@reaxoft.ru' and a 'Найти' (Find) button. Below the search bar, there is a link to 'Создать учетную запись пользователя...' (Create user account...). The main content area is titled 'Учетные записи пользователей' (User accounts) and features a blue sidebar with the user's details: 'built-in: BIP-JHAV7DQ' and 'Петров Иван'. The main panel, titled 'Данные пользователя' (User data), contains several input fields for user information: name (Иван), username (petrov), surname (Петров), mail* (test@reaxoft.ru), uid (BIP-JHAV7DQ), mobile (+7(910)4135615), and email (test@reaxoft.ru). A 'Сохранить' (Save) button is located at the bottom right of this section. Below the user data, there is a 'Смена пароля' (Change password) section with a 'Новый пароль' (New password) input field and a checked checkbox for 'Сгенерировать пароль' (Generate password). An 'Изменить' (Change) button is at the bottom right of this section.

Рисунок 95 – Вид страницы управления пользователями

9.1. Поиск учетных записей пользователей

Для поиска пользователей необходимо ввести идентификатор пользователя и нажать на кнопку «Найти». В качестве отображаемого идентификатора используется атрибут, определенный в разделе «Источники данных» в качестве базового идентификатора, а также атрибуты, отмеченные как поисковые.

Перечень найденных пользователей содержит:

- значение идентификатора найденного пользователя;
- хранилище, в котором найден пользователь;
- имя пользователя, сконфигурированное в разделе «Источники данных».

Нажатие на любую из найденных учетных записей открывает детальную информацию о пользователе.

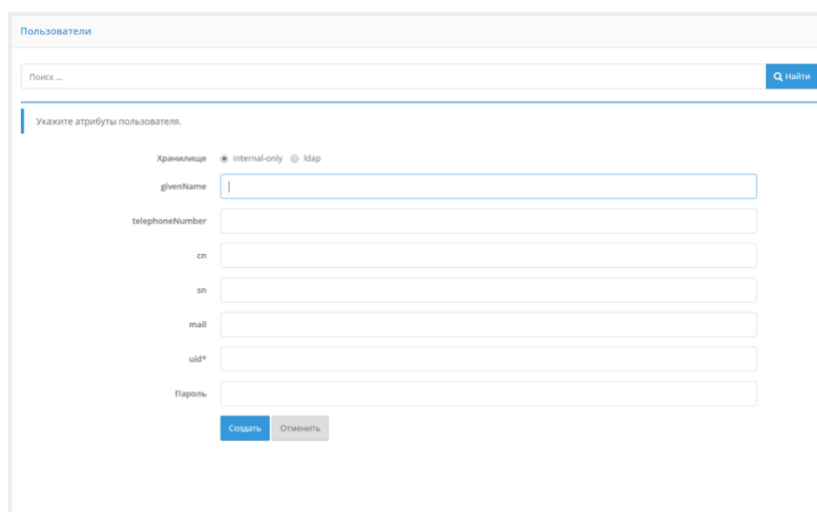
9.2. Добавление учетных записей пользователей

Для добавления новой учетной записи требуется нажать на ссылку «Создать учетную запись пользователя...». В отрывшемся окне:

- указать хранилище, в котором следует сохранить данные пользователя;
- задать все необходимые атрибуты;
- нажать на кнопку «Создать».

При создании учетной записи следует учитывать те ограничения, которые настроены для хранилища данных, в которое осуществляется запись. Например, если сохранение производится в LDAP-каталог, то должны быть заполнены все обязательные атрибуты, не нарушены ограничения на уникальность атрибутов и пр.

При этом с точки зрения Blitz Identity Provider обязательным является только идентификатор и обязательные атрибуты (соответствующие атрибуты отмечены знаком «звезда» (*)).



The screenshot shows a web interface for creating a user. At the top, there is a search bar with the text 'Поиск...' and a 'Найти' button. Below the search bar, the heading 'Пользователи' is visible. The main section is titled 'Укажите атрибуты пользователя.' and contains a form with the following fields: 'Хранилище' (with radio buttons for 'internal-only' and 'ldap'), 'givenName', 'telephoneNumber', 'cn', 'sn', 'mail', 'uid*' (marked with an asterisk), and 'Пароль'. At the bottom of the form are two buttons: 'Создать' and 'Отменить'.

Рисунок 96 – Создание учетной записи пользователя

9.3. Просмотр и изменение атрибутов пользователей

При нажатии на идентификатор любого найденного пользователя отображается информация о нем – карточка пользователя. Она содержит значения атрибутов, которые были определены в разделе «Источники данных», а также привязанные учетные записи внешних поставщиков идентификации, привязанные средства аутентификации и др.

The screenshot displays the 'Пользователи' (Users) management interface. At the top, there is a search bar with the email 'test@reaxoft.ru' and a 'Найти' (Find) button. Below the search bar, there is a link to 'Создать учетную запись пользователя...' (Create user account...). The main content area is titled 'Учетные записи пользователей' (User accounts) and features a blue sidebar with the user's identifier 'built-in: BIP-JHAV7DQ' and name 'Петров Иван'. The main panel is divided into several sections: 1. 'Данные пользователя' (User data) with fields for name (Иван), username (petrov), surname (Петров), mail* (test@reaxoft.ru), uid (BIP-JHAV7DQ), mobile (+7(910)4135615), and email (test@reaxoft.ru), with a 'Сохранить' (Save) button. 2. 'Смена пароля' (Change password) with a 'Новый пароль' (New password) field, a 'Сгенерировать пароль' (Generate password) checkbox, and an 'Изменить' (Change) button. 3. 'Привязанные учетные записи внешних систем' (Linked external system accounts) showing that no accounts are currently linked. 4. 'Требуемый уровень аутентификации' (Required authentication level) with a dropdown menu set to 'Первый и второй фактор' (First and second factor) and a 'Сохранить' (Save) button.

Рисунок 97 – Просмотр информации о пользователе (фрагмент)

На карточке пользователя можно совершать следующие операции:

- редактировать атрибуты пользователя;
- изменять пароль;
- просматривать перечень привязанных аккаунтов внешних поставщиков аутентификации;
- изменять требуемый уровень аутентификации для пользователя;
- привязывать устройства для проведения аутентификации: генераторы разовых паролей (см. п. 9.3.3) и мобильные приложения для получения push-уведомлений (см. п. 9.3.5);
- просматривать группы, в которые включен пользователь (см. п. 9.3.6);
- просматривать права пользователя и права, которые имеются в отношении данного пользователя (см. п. 9.3.7);
- просматривать и удалять выданные приложениям разрешения.

9.3.1. Редактирование атрибутов пользователя

При просмотре карточки выбранной учетной записи пользователя администратор может изменить любой атрибут пользователя. При редактировании учетной записи следует учитывать те ограничения, которые настроены для хранилища данных, в которое осуществляется запись.

Следует учитывать, что при изменении данных через интерфейс редактирования атрибутов не учитываются правила, используемые в процессе самостоятельной регистрации пользователя. Например, изменение адреса электронной почты или номера мобильного телефона не требует подтверждения.

9.3.2. Смена пароля пользователя

Для смены пароля используется блок «Смена пароля». Новый пароль можно ввести вручную, либо сгенерировать – для этого необходимо оставить чекбокс «Сгенерировать пароль». Новый пароль будет отображен в информационном блоке успешного выполнения операции.

При задании нового пароля вручную следует учитывать ограничения парольной политики для того хранилища, куда сохраняется пароль.

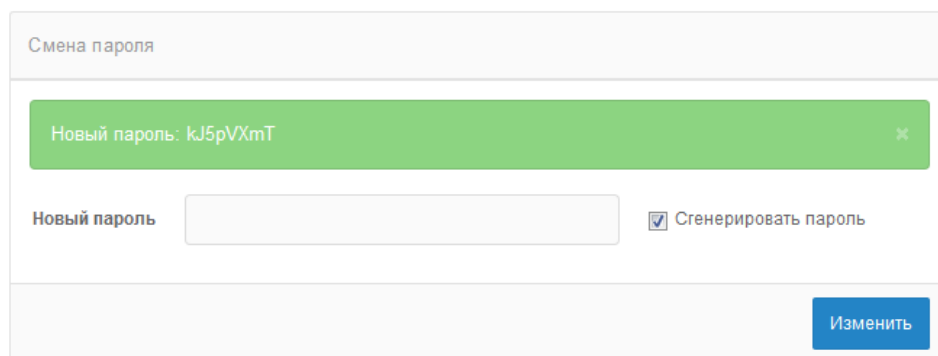


Рисунок 98 – Смена пароля

9.3.3. Просмотр и отвязка аккаунтов социальных сетей

В блоке «Привязанные учетные записи внешних систем» можно посмотреть перечень аккаунтов внешних поставщиков идентификации (социальных сетей, ЕСИА, Сбер ID), привязанных к учетной записи найденного пользователя. Каждая привязка характеризуется уникальным идентификатором, где последняя часть – это внутренний идентификатор аккаунта в соответствующем поставщике идентификации. Например, в записи `esia:esia_1:1000347601` последняя часть (`1000347601`) – это идентификатор аккаунта в ЕСИА. При необходимости можно удалить соответствующую привязку.

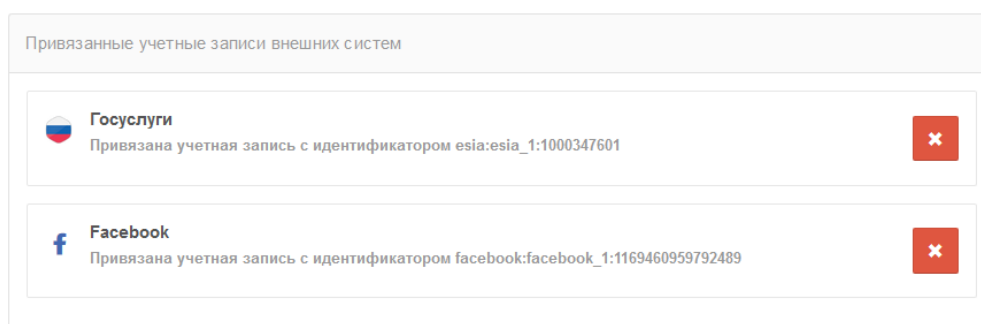


Рисунок 99 – Просмотр информации о пользователе:
привязанные аккаунты внешних поставщиков

9.3.4. Привязка устройств для проведения двухфакторной аутентификации по разовому паролю

Администратор может привязать к учетной записи выбранного пользователя средство для проведения двухфакторной аутентификации. Например, можно привязать аппаратный НОТР/ТОТР генератор по серийному номеру (Рисунок 100) либо привязать к учетной записи по QR-коду мобильное приложение, осуществляющее выработку ТОТР-кодов (Рисунок 101).

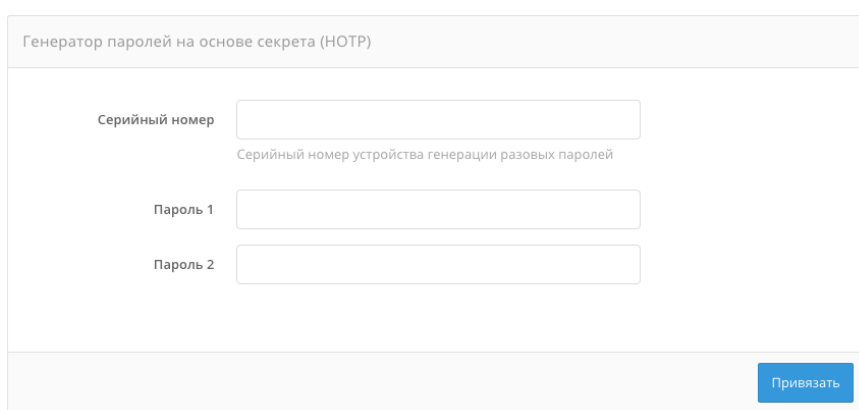


Рисунок 100 – Привязка HOTP-устройства по серийному номеру администратором

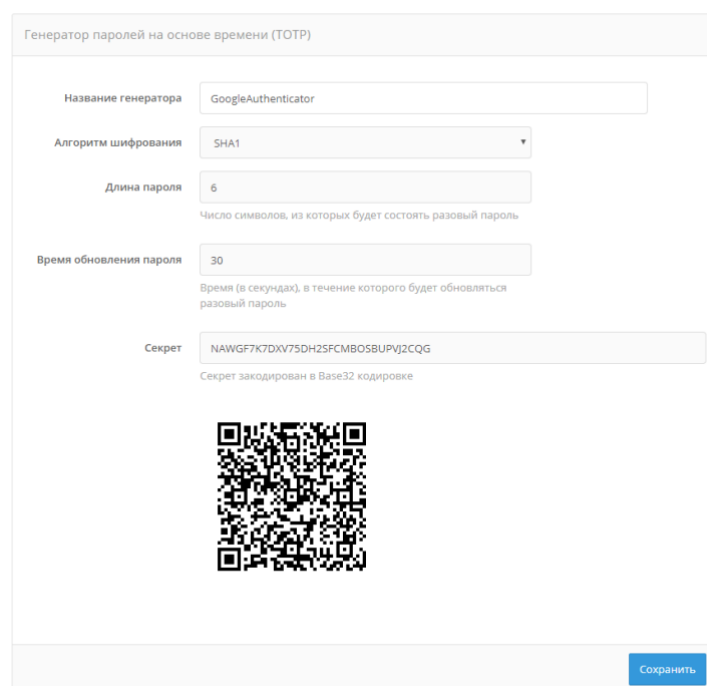


Рисунок 101 – Привязка TOTP-приложения по QR-коду администратором

9.3.5. Привязка мобильного приложения Duo Mobile

Для проведения аутентификации средствами Duo Mobile необходимо провести привязку мобильного приложения к учетной записи пользователя. Рекомендуемый сценарий – пользователь самостоятельно привязывает свое мобильное приложение в веб-приложении «Личный кабинет».

Альтернативный способ привязки – через консоль управления. Для этого необходимо в разделе «Пользователи» найти необходимую учетную запись и блок настроек «Приложение Duo Mobile (QR-код)». В этом блоке следует нажать на кнопку «Привязать Duo Mobile», далее отсканировать отображенный QR-код мобильным приложением Duo Mobile.

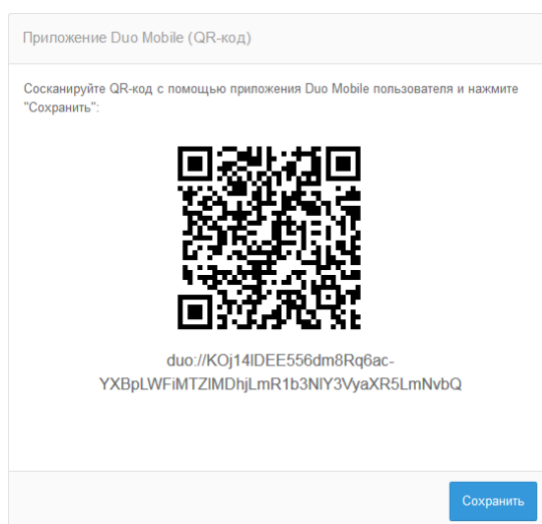


Рисунок 102 – Привязка мобильного приложения Duo Mobile

9.3.6. Просмотр групп, в которые включен пользователь

Если пользователь включен в группы, то эта информация будет отображена в блоке «Членство в группах» (Рисунок 103). По каждой группе будут отображены следующие данные:

- идентификатор группы;
- значения атрибутов группы.

Членство в группах	
Идентификатор	Данные группы
admins	name: Администраторы

Рисунок 103 – Просмотр групп пользователя

9.3.7. Просмотр прав

Если в отношении пользователя есть права со стороны приложений или других учетных записей, то это будет отображено в блоке «Права в отношении пользователя» (Рисунок 104). Если пользователь имеет права в отношении объектов, например, других учетных записей, то это будет отображено в блоке «Права пользователя в отношении объектов» (Рисунок 105).

Каждое право характеризуется следующими параметрами:

- идентификатор объекта;
- имя;
- право.

Права в отношении пользователя		
Идентификатор	Имя	Право
test-system	АИС (Тест)	Назначать права (registrator)
prod-system	АИС (Прод)	Назначать права (registrator)

Рисунок 104 – Просмотр прав в отношении пользователя

Права пользователя в отношении объектов		
Идентификатор	Имя	Право
018180a6	Петров Илья Андреевич	Менять пароль (parent)
ec43af55	Сергеев Иван Петрович	Менять пароль (parent)

Рисунок 105 – Просмотр прав пользователя в отношении объектов

9.3.8. Просмотр и удаление выданных приложениям разрешений

Администратор имеет возможность просмотреть перечень выданных пользователем разрешений приложениям на доступ к его данным (Рисунок 106). Каждое разрешение описывается:

- идентификатор приложения;
- перечень разрешений (scope);
- дата выдачи разрешений.


Разрешения приложений	
oauth2_test_app scopes: openid, profile date: 09.09.2019	

Рисунок 106 – Просмотр выданных разрешений

10. Просмотр групп пользователей

Если в Blitz Identity Provider настроена возможность работы с группами пользователей (см. п. 15.1.14), то в консоли управления появится раздел «Группы». В данном разделе можно осуществлять поиск групп по одному из сконфигурированных атрибутов.

По каждой найденной группе отображаются ее атрибуты (см. Рисунок 107). Кроме того, в блоке «Члены группы» отображаются все пользователи, включенные в данную группу. По каждому пользователю отображается:

- идентификатор;
- имя пользователя – согласно шаблону, определенному в разделе «Источники данных» («Имя пользователя в консоли»).

The screenshot displays the 'Группы' (Groups) management interface. At the top, there is a search section with three input fields: 'Профиль' (Profile) containing 'grps', 'Атрибут' (Attribute) containing 'id', and 'Значение' (Value) containing 'powerusers'. A blue 'Найти' (Find) button is to the right. Below the search section, the 'Группы пользователей' (User Groups) section shows a list with 'powerusers' selected. To the right of the selected group, there are sections for 'Данные группы' (Group Data) and 'Члены группы' (Group Members). The 'Данные группы' section shows a 'name' attribute with the value 'Расширенные права'. The 'Члены группы' section contains a table with two columns: 'Идентификатор' (Identifier) and 'Имя пользователя' (User Name). The table lists one member with the identifier 'e99495e8-ef2b-4a48-b15b-5840849bdf41' and the name 'Иванова Ксения Сергеевна'.

Идентификатор	Имя пользователя
e99495e8-ef2b-4a48-b15b-5840849bdf41	Иванова Ксения Сергеевна

Рисунок 107 – Просмотр групп пользователей

11. Просмотр событий безопасности

Для ведения аудита безопасности и для просмотра зарегистрированных в журнале Blitz Identity Provider событий безопасности используется раздел «События» консоли управления. Здесь имеется возможность осуществлять фильтрацию событий безопасности по различным критериям:

- по пользователю (указание идентификатора пользователя обязательно);
- по диапазону дат;
- по конкретному приложению;
- по группам событий;
- по IP-адресам;
- по протоколам взаимодействия.

После настройки фильтров и их применения предусмотрен просмотр детальной информации о найденных событиях.

Просмотр событий

Значение

0d3f5621-9725-4a48-b0f0-210d9b890dd0

Идентификатор объекта

Полный IP-адрес или маска

Название приложения

Период

28.05.2021 00:00 28.05.2021 23:59

за сегодня за неделю за месяц

Группа событий

Вход Выход Авторизация доступа

Изменение аутентификационных данных

Изменения учетной записи Операции с группами

Протокол

OAuth 2.0 SAML Другие

Применить **Очистить**

ID процесса	Время	Событие	Субъект	Объект	Приложение	IP-адрес
e0341сба...	28.05.2021 14:02:28	Выполнен выход	0d3f5621-9725-4a48-b0f0-210d9b890dd0	0d3f5621-9725-4a48-b0f0-210d9b890dd0	Личный кабинет	89.255.71.120
d14cc309...	28.05.2021 14:02:26	Выполнен вход	0d3f5621-9725-4a48-b0f0-210d9b890dd0	0d3f5621-9725-4a48-b0f0-210d9b890dd0	Личный кабинет	89.255.71.120

Рисунок 108 – Просмотр событий безопасности

12. Настройка уведомлений и отправки сообщений

Для задания настроек уведомлений и подключения к системам отправки сообщений используется раздел «Сообщения» консоли управления Blitz Identity Provider (Рисунок 109). В этом разделе можно настроить уведомления и подключение к:

- сервису отправки SMS-сообщений;
- сервису отправки push-уведомлений;
- SMTP-серверу.

Для настройки уведомлений необходимо на основной странице раздела:

- выбрать канал для восстановления (электронная почта, мобильный телефон) и указать атрибут со значением этого контакта. Атрибут задается с помощью регулярного выражения, например, `{mobile}` означает, что информация будет отправлена на телефон `mobile`;
- выбрать события, по которым требуется отправлять уведомления. Возможно уведомление при следующих событиях:
 - вход с неизвестного устройства;
 - смена пароля;
 - смена пароля в зависимой учетной записи;
 - восстановление доступа;
 - восстановление доступа в зависимой учетной записи;
 - привязка учетной записи социальной сети;
 - настройка метода двухфакторной аутентификации;
 - изменение режима подтверждения входа;
 - получение права менять пароль в зависимой учетной записи;
 - предоставление права менять пароль;
 - отзыв права менять пароль в зависимой учетной записи;
 - отзыв предоставленного права менять пароль;
 - регистрация учетной записи.

Уведомления

Настройте уведомления и пользователи будут оповещаться о различных событиях безопасности

Способы уведомления

Способ уведомления	Атрибут с контактом	
Электронная почта	\$(email-)	X

[+ Добавить способ уведомления](#)

Уведомлять пользователя о событиях

- Вход с неизвестного устройства
- Смена пароля
- Смена пароля в зависимой учетной записи
- Восстановление доступа
- Восстановление доступа в зависимой учетной записи
- Привязка учетной записи социальной сети
- Настройка метода двухфакторной аутентификации
- Изменение режима подтверждения входа
- Получение права менять пароль в зависимой учетной записи
- Предоставление права менять пароль
- Отзыв права менять пароль в зависимой учетной записи
- Отзыв предоставленного права менять пароль
- Регистрация учетной записи

[Сохранить](#)

Рисунок 109 – Настройка уведомлений и подключения к системам отправки сообщений

12.1. Настройка подключения к SMS-шлюзу

Blitz Identity Provider необходима возможность отправлять SMS-сообщения, если используются следующие функции:

- аутентификация на основе отправки по SMS кода подтверждения (первый и второй фактор);
- информирование о важных событиях безопасности по SMS;
- изменение номера мобильного телефона через «Профиль пользователя»;
- восстановление забытого пароля с использованием мобильного телефона как канала подтверждения владения учетной записью;
- подтверждение номера мобильного телефона при регистрации пользователя.

Настройки задаются в консоли управления Blitz Identity Provider в разделе «Сообщения». Экран настроек приведен на рисунке 110.

Настройка сервиса отправки SMS

Протокол доставки: HTTP-GET
Протокол доставки сообщений

При формировании URL и заголовков HTTP-запроса используйте строки подстановки:

- `${login}` - логин для доступа к сервису
- `${password}` - пароль для доступа к сервису
- `${message}` - сообщение (обязательный параметр)
- `${mobile}` - номер мобильного телефона (обязательный параметр)

URL: `https://smc.ru/sys/send.php?psw=${password}&login=${login}&phones=${mobile}&mes=${message}&charset=utf-8`

Логин: reaxoft
Логин для доступа к сервису отправки сообщений

Пароль: Изменить значение

Использовать Basic HTTP аутентификацию

Заголовки

Шаблон ответа успешной отправки: *OK*
Регулярное выражение, определяющее успешную отправку сообщения. Например, *OK +

Шаблон ответа при ошибке: *ERROR +
Регулярное выражение, определяющее наличие ошибки при отправке сообщения. Например, *ERROR +

Отмена Сохранить

Рисунок 110 – Настройка подключения к SMS-шлюзу

Необходимо задать следующие настройки:

- вид протокола доставки (GET или POST);
- URL SMS-шлюза – задается в виде паттерна для формирования запроса к SMS-шлюзу для инициирования отправки им SMS. Пример настройки для SMS-шлюза:

```
https://smc.ru/sys/send.php?psw=${password}&login=${login}&phones=${mobile}&mes=${message}&charset=utf-8
```

- логин и пароль для доступа к SMS-шлюзу. Логин и пароль могут быть переданы в качестве параметров GET-запроса или в виде HTTP-заголовка запроса (схема авторизации HTTP Basic Authorization);
- HTTP-заголовке запроса на SMS-шлюз;
- шаблон проверки ответа от шлюза, означающего успешную отправку. Задается в виде регулярного выражения;
- шаблон проверки ответа от шлюза, означающего ошибку отправки сообщения. Задается в виде регулярного выражения.

12.2. Настройка подключения к сервису отправки push-уведомлений

Настройки push-уведомлений задаются в веб-приложении администрирования в разделе «Сообщения».

Необходимо задать следующие настройки:

- вид протокола доставки (GET или POST);
- URL сервиса отправки push-уведомлений, например:

```
http://api.system.ru/json/v1.0/communication/mobile/push
```

- данные – сообщение, передаваемое в теле (body) запроса, например:

```
{"token":"${password}","title":"${title}","body":"${message}","msisdn":"${subscriberId}"}
```

- логин и пароль для доступа к сервису. Логин и пароль могут быть переданы в качестве параметров GET-запроса или в виде HTTP-заголовка запроса (схема авторизации HTTP Basic Authorization);
- HTTP-заголовки запроса;
- шаблон проверки ответа от сервиса, означающего успешную отправку. Задается в виде регулярного выражения, например:

```
.\+"errorCode\:0.+
```

- шаблон проверки ответа от сервиса, означающего ошибку отправки сообщения.

Задается в виде регулярного выражения, например:

```
.\+"errorCode\":[1-9].+
```

Пример настройки интеграции с сервисом отправки push-уведомлений отображен ниже).

Настройка сервиса отправки Push-уведомлений

Протокол доставки: HTTP-POST
Протокол доставки сообщений

При формировании URL, тела и заголовков HTTP-запроса используйте строки подстановки:

- `${login}` - логин для доступа к сервису
- `${password}` - пароль для доступа к сервису
- `${message}` - текст сообщения (обязательный параметр)
- `${title}` - заголовок сообщения (обязательный параметр)
- `${subscriberId}` - идентификатор пользователя push (обязательный параметр)

URL: `http://api.system.ru/json/v1.0/communication/mobile/push`

Данные: `{"token":"${password}","title":"${title}","body":"${message}","msisdn":"${subscriberId}"}`
Данные передаваемые в теле HTTP-запроса

Логин: `test`
Логин для доступа к сервису отправки сообщений

Пароль: [Изменить значение](#)

Использовать Basic HTTP аутентификацию

Заголовки:
Заголовки HTTP-запроса. Каждый заголовок описывается в отдельной строке. Название и значение заголовка должны быть разделены символом `:`.

Шаблон ответа успешной отправки: `.\\"errorCode\":0.+`
Регулярное выражение, определяющее успешную отправку сообщения. Например, `^OK.+`

Шаблон ответа при ошибке: `.\\"errorCode\":[1-9].+`
Регулярное выражение, определяющее наличие ошибки при отправке сообщения. Например, `^ERROR.+`

[Отмена](#) [Сохранить](#)

Рисунок 111 – Настройка интеграции с сервисом отправки push-уведомлений

12.3. Настройка подключения к SMTP-шлюзу

В Blitz Identity Provider необходимо настроить возможность отправлять по email сообщения, если используются следующие функции:

- информирование о важных событиях безопасности по email.
- изменение адреса электронной подписи через «Профиль пользователя».
- восстановление забытого пароля с использованием email как канала подтверждения владения учетной записью.
- подтверждение адреса электронной почты при регистрации учетной записи пользователя.

Настройки задаются в консоли управления Blitz Identity Provider в разделе «Сообщения». Экран настроек приведен на рисунке 112.

Настройка SMTP-сервера

Хост: mail01.reaxoft.loc

Порт: 25

Использовать TLS

Отправитель: notif@reaxoft.ru
email-адрес отправителя

Логин: Совпадает с адресом отправителя
Логин учетной записи для соединения с SMTP-сервером

Пароль: [Изменить значение](#)

Отмена Сохранить

Рисунок 112 – Настройка подключения к SMTP-шлюзу

Необходимо задать следующие настройки:

- имя хоста SMTP-шлюза;
- порт хоста SMTP-шлюза;
- необходимо или нет использовать TLS для защищенного подключения к шлюзу;
- email отправителя сообщений;
- логин учетной записи на SMTP-шлюзе, от имени которой Blitz Identity Provider будет производить отправку email (если логин совпадает с email отправителя, то следует отметить соответствующий чекбокс);
- пароль от учетной записи на SMTP-шлюзе, от имени которой Blitz Identity Provider будет производить отправку email.

13. Настройка внешнего вида страницы входа

Администратор консоли управления должен самостоятельно проверять корректность помещаемых на страницу входа JS-скриптов и содержимое страниц входа на предмет возможных уязвимостей.

В разделе «Внешний вид» консоли управления администратор может настроить параметры отображения единой страницы входа. Если применяются приложения Blitz Identity Provider по регистрации пользователей и восстановлению пароля, то их внешний вид также будет соответствовать заданным настройкам внешнего вида единой страницы входа.

При входе в раздел «Внешний вид» отображается перечень настроенных шаблонов страницы входа. Каждый шаблон описывается:

- идентификатором;
- названием;
- перечнем приложений;
- описанием.

По умолчанию создан шаблон с идентификатором `default` – он используется для всех приложений, подключенных к Blitz Identity Provider, а также для страниц единого логота.

Редактирование шаблона по умолчанию осуществляется с помощью специального конструктора (см. п. 13.1).

Также имеется возможность:

- создавать и изменять новые шаблоны с помощью конструктора и назначать их разным приложениям (п. 13.2);
- создавать и изменять новые шаблоны в ручном режиме (п. 13.3).

13.1. Редактирование шаблона по умолчанию

При открытии страницы редактирования шаблона по умолчанию отображается информация о самом шаблоне (идентификатор шаблона, название шаблона, описание и перечень приложений), а также интерфейс конструктора страницы входа.

Свойства шаблона




Идентификатор шаблона	<input type="text" value="default"/>
Название шаблона	<input type="text" value="Стандартный шаблон"/>
Описание	<input type="text" value="Используется по умолчанию"/>
Приложения	<input type="text" value="http://jira.rexoft.ru/secure/Dashboard.jspa, oauth2_demo_app02, openschool, re"/>

[Сохранить](#)

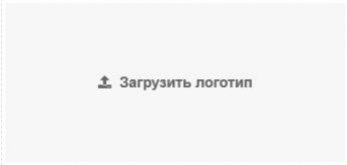
Внешний вид страницы входа

Тема:

Расположение основного блока: Слева По центру Справа



Логотип

 Загрузить логотип

Рекомендуемая высота логотипа 32px

Фоновый рисунок

Рекомендуемый размер файла не более 1MB

Или выбрать из предложенных рисунков

Рисунок 1 Рисунок 2






Рисунок 3



Настройка футера

Добавьте фрагмент HTML-кода для отображения в футере страницы входа.

- Скопируйте сюда фрагмент HTML-кода

[Сохранить](#)

Рисунок 113 – Настройка внешнего вида страницы входа

В стандартной поставке конструктор Blitz Identity Provider предоставляет следующие возможности:

- три цветовых темы оформления элементов интерфейса;
- возможность определить местоположения блока ввода сведений (идентификации и аутентификации, регистрации, восстановления пароля);
- возможность загрузки логотипа компании для отображения в заголовке страницы;
- выбор фонового рисунка (можно выбрать из 3 стандартных рисунков в каждой теме оформления, либо загрузить свой собственный фоновый рисунок);
- настройка содержания футера страницы входа.

На рисунках 114, 115, 116 приведены примеры страниц входа в результате стандартной настройки.

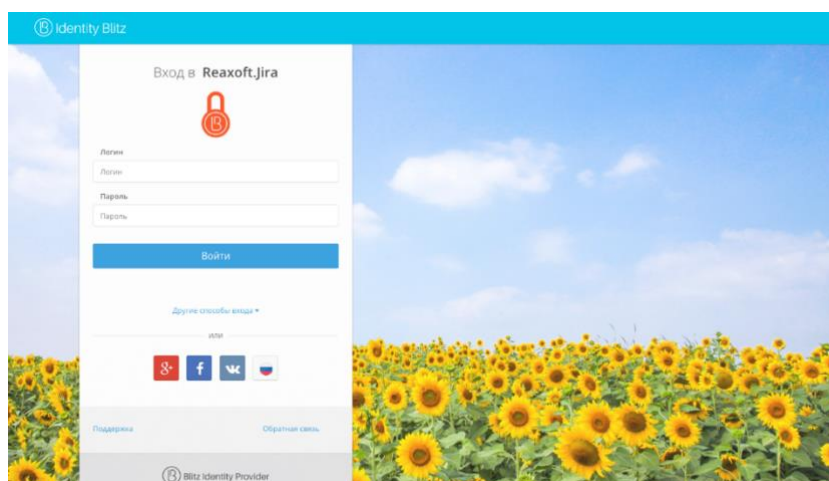


Рисунок 114 – Пример страницы входа с social login и дополнительным футером

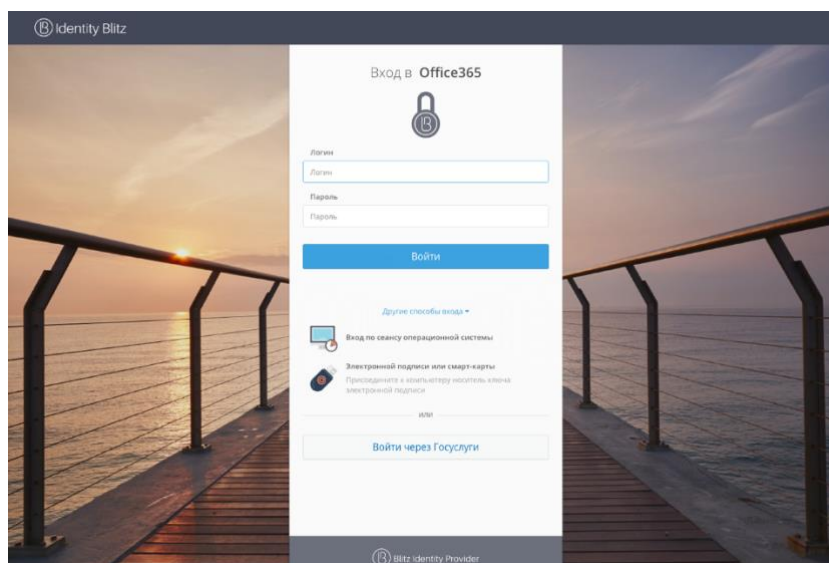


Рисунок 115 – Пример страницы входа в темном интерфейсе и с режимами входа по электронной подписи, сеансу операционной системы или через ЕСИА

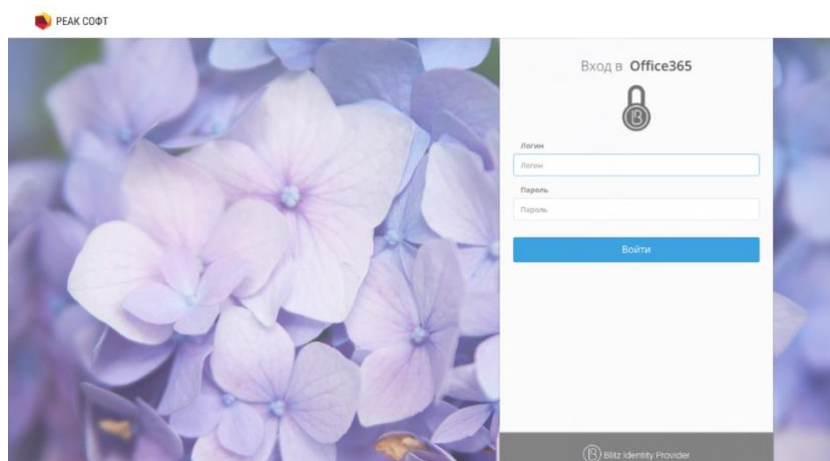


Рисунок 116 – Пример страницы входа в светлом интерфейсе, с логотипом в заголовке страницы и без специальных режимов входа

13.2. Создание и изменение новых шаблонов с помощью конструктора

Blitz Identity Provider позволяет настроить разный вид страниц входа для случая входа пользователя в различные подключенные приложения. Для этого необходимо создавать новые шаблоны входа – проще всего это сделать на базе существующего default-шаблона, нажав на кнопку «Копировать». После этого будет создан новый шаблон, который можно редактировать с помощью конструктора.

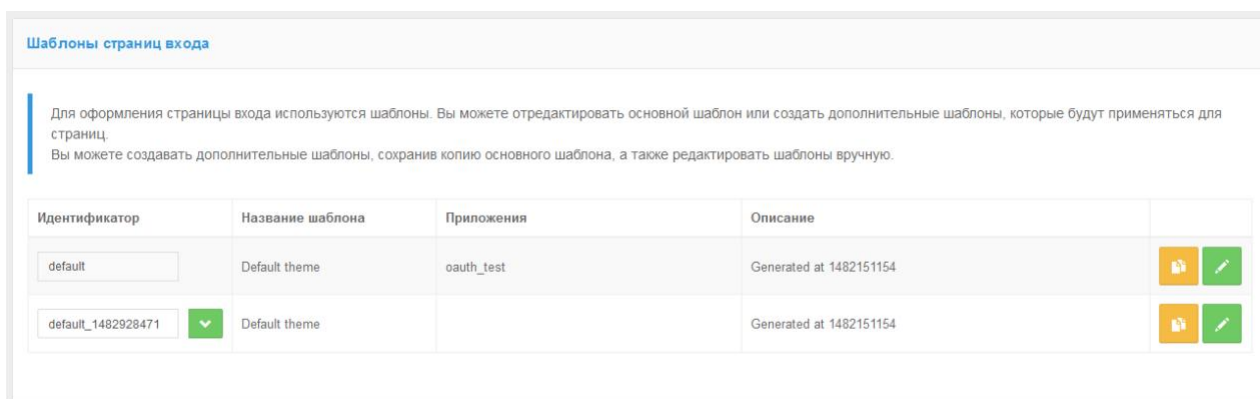


Рисунок 117 – Создание нового шаблона на базе существующего основного шаблона

Чтобы новый шаблон использовался при входе в некоторое приложение, необходимо в разделе «Приложения» перейти к редактированию нужного приложения и выбрать требуемый шаблон страниц.

Параметры приложения

Идентификатор (entityID или client_id)
Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).

Название
Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider

Домен
Ссылка на стартовую страницу приложения, например, http://testdomain.ru/. При TLS-аутентификации приложения проверяется, что в сертификате приложения указан именно этот домен

Ключ шифрования идентификаторов
Если ключ задан, то идентификатор пользователя для приложения будет зашифрован с использованием данного ключа. Значение ключа можно выбрать из списка. Также можно назначить новый ключ, для этого введите его в строке поиска и нажмите Enter

Шаблон страниц
Шаблон страниц определяет внешний вид страниц входа. Если шаблон не указан, то используется шаблон по умолчанию.

Префиксы ссылок возврата при выходе
Список URL используется для проверки ссылок возврата (post_logout_redirect_uri). Если в запросе на выход указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в выходе будет отказано

Рисунок 118 – Назначение шаблона страницы входа приложению


13.3. Создание и изменение новых шаблонов в ручном режиме

Можно настроить вид страницы входа под индивидуальные требования организации, т.е. нет необходимости ограничиваться только возможностями конструктора.

Каждый шаблон страницы входа представляет собой zip-архив. Все шаблоны размещены в директории:

```
\assets\themes
```

Самый простой способ перейти к ручному редактированию шаблона – выполнить следующие шаги:

- создать копию существующего шаблона (например, default-шаблона), нажав в консоли кнопку  ;
- перейти в соответствующую директорию с шаблонами;

- распаковать архив с только что созданным шаблоном;
- отредактировать файл `meta.conf`, содержащийся в архиве, удалив параметр `builder` (см. рисунок 119);
- обратно заархивировать файлы шаблона, убедившись, что файл `meta.conf` находится в корневой директории.

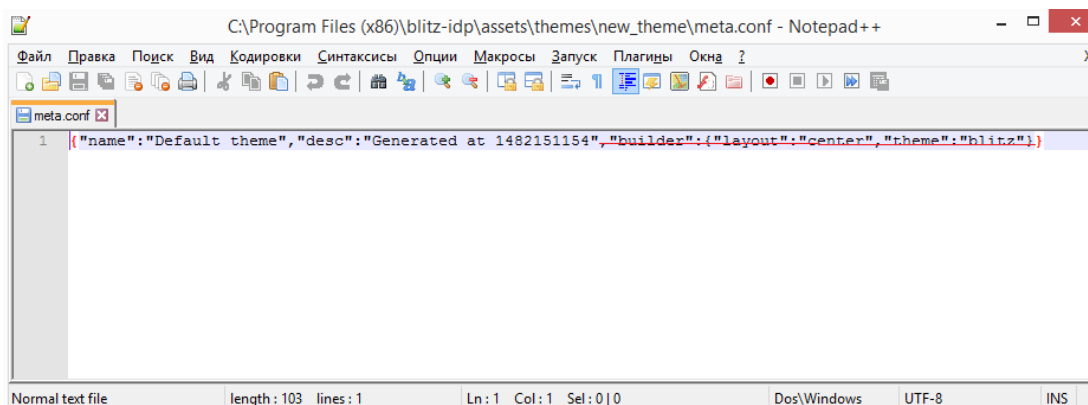


Рисунок 119 – Удаление параметра `builder` из файла `meta.conf`

После выполнения этих шагов появится возможность редактирования темы в ручном режиме. Помимо стандартных полей, описывающих саму тему, доступен блок «Шаблон страниц». Он позволяет создать или изменить шаблон – текстовый файл, который компилируется с помощью шаблонизатора Twirl⁴¹.

Шаблон должен иметь сигнатуру:

```
@(headers: Html, form: Html, scripts: Html, pathAssets: String)(implicit request: RelyingPartyRequest[_], messages: Messages)
```

В качестве параметров при создании шаблона следует использовать:

- `headers` – HTML-код заголовка страницы, который надо расположить в теге `head`;
- `form` – HTML-код основной формы, который необходимо расположить в теге `body`;
- `scripts` – HTML-код с JavaScript, который необходимо расположить в теге `body`;
- `pathAssets` – контекстный путь к ресурсам шаблона.

Функция `@form` добавляет на страницу код основной формы аутентификации (пример основной формы приведен на рисунке 120). Форма аутентификация (перечень и состав полей, расположение кнопок) не настраивается за исключением изменений, реализуемых средствами CSS. Иными словами, через CSS можно изменить цвет отдельных элементов или скрыть их – для этого следует найти соответствующий класс в CSS-файле темы и изменить его свойства.

⁴¹ См.: <https://www.playframework.com/documentation/2.5.x/ScalaTemplates>

Рисунок 120 – Блок с основной формой аутентификации

Листинг простейшего шаблона приведен ниже:

```
@(headers: Html, form: Html, scripts: Html, path: String)(implicit request: RelyingPartyRequest[ ],
messages: Messages)

<!DOCTYPE html>
<html>

<head>
  @headers
</head>

<body>
  <div id="main">
    <section id="content_wrapper">
      @form
    </section>
    <div>
      <div>
        @Html(messages("author.copyright"))
      </div>
    </div>
  </div>
  @scripts
</body>

</html>
```

При использовании такого шаблона страница входа будет иметь вид, приведенный на рисунке 121.

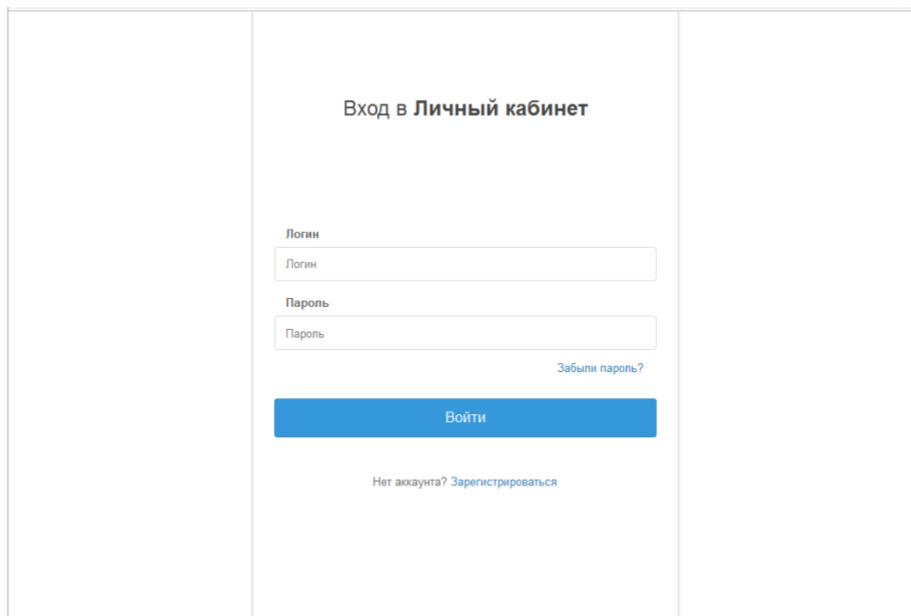


Рисунок 121 – Внешний вид простейшей страницы входа

При формировании шаблона страницы входа имеется возможность использовать ресурсы – например, таблицы стилей или рисунки.

Для их загрузки следует использовать блок «Ресурсы» внешнего вида страницы, который позволяет загрузить необходимые файлы в zip-архиве. Чтобы соответствующие файлы были доступны, их следует размещать в директории архива с названием `assets`. Необходимые ресурсы также можно вручную включить в состав исходного zip-архива с шаблоном страницы.

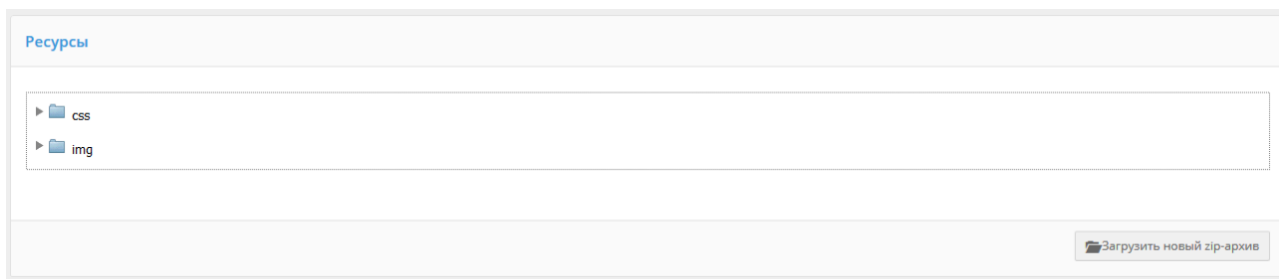


Рисунок 122 – Внешний вид: доступные ресурсы

14. Настройки шлюза безопасности

С помощью Blitz Identity Provider можно осуществлять контроль доступа при вызове приложениями защищаемых сервисов.

Обеспечение авторизации при вызове приложениями сервисов основано на спецификациях OAuth 2.0. Перед использованием сервисов приложение должно получить у Blitz Identity Provider маркер доступа (access_token). Для получения маркера доступа приложению доступны различные способы взаимодействия (см. «Руководство по интеграции»). При этом маркер доступа может быть получен:

- в контексте входа пользователя – маркер будет включать информацию о пользователе и наборе согласий (разрешений), предоставленных пользователем приложению;
- на приложение вне контекста входа пользователя – маркер будет включать набор согласий (разрешений) из числа разрешенных приложению.

Далее с использованием полученного маркера доступа приложение может вызывать сервисы. При этом будут следующие сложности:

- внутри каждого сервиса необходимо будет реализовывать собственную логику авторизации – проверять предоставленный маркер доступа, извлекать из него информацию о пользователе и предоставленных согласиях(разрешениях) и анализировать, достаточно ли их для выполнения сервиса или нет. Осуществлять протоколирование принятого решения по доступу.
- приложение будет использовать единый маркер доступа для вызова различных сервисов. Маркер доступа в таком случае может содержать больше информации о пользователе и больший набор согласий (разрешений), чем нужно конкретному вызванному сервису. Это будет нарушать принцип наименьших привилегий – сервис получит больше прав доступа, чем ему необходимо для выполнения своей задачи.

Чтобы решить вышеописанные сложности в Blitz Identity Provider предусмотрено специальное приложение – шлюз безопасности (blitz-keeper). Это приложение представляет собой специализированный прокси-сервер, используемый при вызове защищаемых сервисов – приложение вызывает сервисы не напрямую, а через шлюз безопасности. При этом шлюз безопасности берет на себя выполнение следующих задач:

- Проверяет включенный в вызов сервиса заголовок авторизации, извлекает из заголовка маркер доступа и, во взаимодействии с сервисом авторизации (blitz-idp) выполняет проверку, действителен ли маркер доступа, а также, достаточно ли у пользователя и приложения прав для вызова защищаемого сервиса.
- Во взаимодействии с сервисом авторизации (blitz-idp) заменяет маркер доступа таким

образом, чтобы передаваемый от шлюза безопасности к защищаемому сервису маркер безопасности содержал только тот набор сведений о пользователе и разрешений, который необходим для работы защищаемого сервиса. При этом из маркера безопасности могут быть как изъяты излишние разрешения и сведения о пользователе, так и наоборот, добавлены в маркер доступа дополнительные разрешения и сведения, если такое установлено политикой безопасности.

- Протоколирует в журнале событий безопасности Blitz Identity Provider события успешной и неуспешной проверки прав доступа.

Взаимодействие шлюза безопасности с сервисом авторизации осуществляется на основе спецификации OAuth 2.0 Token Exchange⁴². Иллюстрация взаимодействия приведена на схеме (см. рисунок 123).



Рисунок 123 – Схема взаимодействия при вызове приложением защищаемого сервиса

Настройка использования шлюза безопасности для защиты сервисов заключается в выполнении следующих шагов и описана в последующих подразделах:

- Настройка blitz-keeper.
- Создание правил доступа к сервисам.
- Регистрация правил обмена маркеров доступа в blitz.conf.

14.1. Настройка blitz-keeper

Настройка blitz-keeper осуществляется путем редактирования конфигурационного файла `blitz-keeper.conf`, расположенного в каталоге `/etc/blitz-keeper`.

⁴² Спецификация, описывающая способы обмена маркеров в целях делегирования вызовов между сервисами и для задач имперсонификации пользователей. См.: <https://tools.ietf.org/html/rfc8693>.

Пример конфигурационного файла:

```

{
  "authenticators": {
    "prod-auth": {
      "type": "token-exchange",
      "te": "https://blitz-host/blitz/oauth/te",
    },
  },
  "services": {
    "api-1": {
      "display-name": "secured services",
      "host": "service-host.com",
      "locations": {
        "/api/service1/**": {
          "methods": ["GET", "POST"],
          "authenticator": "prod-auth",
          "required-scopes": ["scope1", "scope2"]
        },
        "/path/api/user/*/getdata/**": {
          "methods": ["GET", "PUT"],
          "authenticator": "prod-auth",
          "required-scopes": ["scope3"]
        }
      }
    }
  }
}

```

В блоке `authenticators` нужно зарегистрировать все используемые сервисы авторизации `blitz-idp`. Обычно достаточно использовать один единственный сервис авторизации для защиты сервисов, и тогда нужно заполнить только один блок как в примере (в примере зарегистрирован один сервис авторизации с именем `prod-auth`). Если в системе используется несколько отдельных установок Blitz Identity Provider (например, ПРОД- и ТЕСТ-среда или внутренний контур для сотрудников и внешний контур для клиентов), то можно использовать общий шлюз безопасности, который будет взаимодействовать с несколькими разными сервисами авторизации – тогда нужно в блоке `authenticators` задать настройки нескольких сервисов авторизации. Для каждого сервиса авторизации задается имя (в примере использован `prod-auth`, но можно задать любое имя). В блоке настроек сервиса авторизации задается тип взаимодействия (`type`) в значении `token-exchange` (пока это единственный поддерживаемый тип взаимодействия) и адрес (`te`) вызова обработчика Token Endpoint сервиса авторизации. Если `blitz-keeper` развернут на отдельных серверах, то рекомендуется задать адрес обработчика с `https` и доменным именем. Если приложение `blitz-keeper` развернуто на том же сервере что сервис авторизации `blitz-idp`, то рекомендуется задать в `te` локальное имя, например, `http://localhost:9000/blitz/oauth/te`.

В блоке `services` нужно зарегистрировать защищаемые сервисы. Для всех защищаемых сервисов можно создать общий блок настроек или несколько отдельных блоков. Каждый блок имеет имя (в примере, `api-1`). Внутри блока задаются настройки:

- `display-name` – текстовое описание сервиса (любой комментарий или описание);
- `host` – адрес сервера защищаемого сервиса;
- `locations` – допустимые пути и операции вызова сервиса.

В блоке `locations` указываются настройки всех путей сервиса и разрешенных методов. В качестве имени каждого вложенного блока указывается адрес сервиса. Допустимо в адресе использовать звезду (*), чтобы указать на пропуск отдельного компонента в адресе пути сервиса и допустимо использовать двойную звезду (**), чтобы указать, что вся оставшаяся часть пути сервиса может быть любая. Внутри вложенного блока с адресом сервиса можно опционально перечислить разрешенные методы сервиса (настройка `methods`), указать имя используемого сервиса авторизации (настройка `authenticator`) и перечень разрешений (настройка `required-scopes`) для целевого маркера доступа, которые будут включены в маркер доступа, передаваемый в защищаемый сервис.

После изменения настроек в `blitz-keeper.conf` необходимо перезапустить шлюз безопасности.

14.2. Создание правил доступа к сервисам

Правила доступа к сервисам создаются в директории `/usr/share/identityblitz/blitz-config/token-exchange/rules/`. Каждое правило создается как отдельный текстовый файл без расширения.

Пример файла с правилом доступа:

```
{
  "name": "rule-name",
  "type": "specialize",
  "desc": "",
  "subjectTokenCond": {
    "clientRights": [],
    "userRights": [],
    "scopes": ["openid"],
    "userClaims": {},
    "userGroups": []
  },
  "issue": {
    "ttlInSec": 3600,
    "allowedScopes": ["openid","profile"],
    "allowedClaims": ["sub","global_role","org_id","rights"],
    "addingScopes": [],
    "addingClaims": []
  }
}
```

Нужно заполнить следующие атрибуты правила доступа:

- `name` – имя правила, которое должно совпадать с именем файла с правилом доступа;
- `type` – тип правила. Пока поддерживается один тип правил – `specialize`;
- `desc` – описание правила. Можно ввести любую текстовую информацию;
- `subjectTokenCond` – условия выполнения правила. Если все указанные в правиле условия будут выполняться, то правило считается выполненным. Если хотя бы одно из условий в правиле не будет выполнено, то все правило считается невыполненным.

Условия выполнения правил могут быть следующие:

- `clientRights` – проверка наличия у приложения указанных прав доступа

(см. п. 15.1.10);

Пример правила:

```
"clientRights": [
  {
    "rights": ["right1"],
    "target": {
      "type": "its",
      "name": "app1"
    }
  }
]
```

В указанном примере проверяется наличие у вызывающего приложения права доступа `right1` в отношении другого приложения (`app1`). Параметр `its` в настройке `target` указывает тип объекта, в отношении которого проверяется наличие права доступа. Возможные значения: `its` – право на приложение; `grps` – право на группу доступа; отсутствие `type` – право на учетную запись пользователя.

- `userRights` – проверка наличия у пользователя указанных прав доступа (см. п. 15.1.10).

Пример 1 правила:

```
"userRights": [
  {
    "rights": ["right2"],
    "target": {
      "type": "grps",
      "name": "org1",
      "ext": "orgs"
    }
  }
]
```

В указанном примере проверяется наличие у пользователя права доступа `right2` в отношении группы пользователей (`org1`). В случае типа объекта группы доступа указывается дополнительный параметр `ext`, определяющий профиль группы доступа (см. п. 15.1.14).

Пример 2 правила:

```
"userRights": [
  {
    "rights": ["security_administrator"],
    "target": {
      "type": "grps",
      "name": "${org_id}",
      "ext": "orgs"
    }
  }
]
```

В указанном правиле проверяется наличие у пользователя права доступа `security_administrator` в отношении группы пользователей из профиля `orgs`, имеющей идентификатор, совпадающий со значением атрибута `org_id` из состава исходного маркера доступа. В отличие от примера 1 в данном примере иллюстрируется возможность в качестве имени объекта права доступа указывать не конкретное значение объекта, а ссылаться на объект на основе

значений из присланного маркера доступа (`$org_id`).

Пример 3 правила:

```
"userRights": [
  {
    "rights": ["right3"],
    "target": {
      "type": "its",
      "name": "app1"
    }
  }
]
```

В данном примере проверяется наличие у пользователя права доступа `right3` в отношении приложения `app1`.

- `scopes` – проверка присутствия в маркере доступа требуемых разрешений (см. п. 5.3.2);

Пример правила:

```
"scopes": ["scope1"]
```

В данном примере проверяется наличие в исходном маркере доступа разрешения с именем `scope1`.

- `userClaims` – проверка, что у учетной записи пользователя атрибуты имеют указанные значения.

Пример правила:

```
"userClaims": {"role": "FIN"}
```

В данном примере проверяется наличие у пользователя в учетной записи атрибута `role` с заполненным значением `FIN`. Допустимо использовать только атрибуты с типом `String`.

- `userGroups` – проверка, что учетная запись пользователя входит в указанные группы доступа.

Пример правила:

```
"userGroups": [
  {
    "name": "admin",
    "profile": "roles"
  }
]
```

В данном примере проверяется, что пользователь входит в группу доступа `admin` с профилем `roles`.

- `issue` – правила выпуска нового маркера доступа, применяемые в случае, если правило было успешно выполнено. Правила выпуска нового маркера доступа состоят из:
 - `ttlInSec` – время жизни (в секундах) выпускаемого маркера доступа;
 - `allowedScopes` – разрешения, которые можно оставить в выпускаемом маркере доступа;
 - `allowedClaims` – атрибуты пользователя, которые можно оставить в выпускаемом маркере доступа;

- `addingScopes` – добавляемые в маркер доступа разрешения;
- `addingClaims` – добавляемые в маркер доступа атрибуты пользователя.

14.3. Настройка правил обмена маркеров доступа

Чтобы определить, для каких защищаемых сервисов какие должны применяться правила доступа, необходимо в конфигурационном файле `blitz.conf` добавить блок настроек `blitz.prod.local.idp.token-exchange` следующего вида:

```
"token-exchange" : {
  "resources" : [
    {
      "rules" : [
        "rule1", "rule2"
      ],
      "audience" : "secured-api",
      "uri" : http://secured service host/api/service1,
      "methods" : ["GET","POST"]
    },
    {
      "rules" : [
        "rule3"
      ],
      "uri" : http://secured_service_host/api/service2
    },
    ...
  ]
}
```

В блоке `resources` нужно для каждого сервиса заполнить настройки:

- `rules` – перечислить имена правил доступа к сервису. Каждому правилу соответствует свой файл настроек (см. п. 14.2). Доступ к сервису разрешается, если хотя бы одно из правил из этого списка будет выполненным. Если все перечисленные правила не будут выполнены, то тогда доступ к сервису будет запрещен;
- `uri` – адрес защищаемого сервиса. В задании адреса сервиса допустимо использовать звезду (*) для пропуска одного компонента пути адреса и двойную звезду (**) для пропуска оставшейся части пути адреса сервиса;
- `audience` – необязательный параметр, может задавать логическое имя вызываемого сервиса. Данное значение будет включено в выпущенный новый маркер доступа в атрибут `aud`;
- `methods` – необязательный параметр, указывает перечень HTTP-методов вызываемого сервиса.

15. Настройки конфигурационных файлов

Конфигурационные файлы всех приложений Blitz Identity Provider кроме приложения `blitz-keeper` расположены в каталоге `/usr/share/identityblitz/blitz-config`.

Используются следующие конфигурационные файлы:

- `assets/*` – настройки пользовательского интерфейса (см. п. 4.2.2, п. 7, п. 13);
- `custom_messages/*` – строки пользовательского интерфейса (см. п. 15.2);
- `devices/*` – вспомогательные каталоги для обработки загрузки HOTP и TOTP устройств (см. п. 4.10.1);
- `flows/*` – процедуры входа (см. п. 6.1);
- `saml/*` – настройки SAML (см. п. 5.2);
- `simple/*` – настройки подключения приложений по протоколу Simple (см. п. 5.1);
- `token_exchange/rules/*` – настройки правил обмена маркеров доступа (см. п. 14);
- `blitz.conf` – основной файл конфигурации (см. п. 15.1);
- `boot.conf` – настройки путей к конфигурационным файлам;
- `console.conf` – настройки консоли управления (см. п. 15.3);
- `credentials` – учетные записи администраторов консоли управления (см. п. 15.3.3);
- `play.conf` – настройки серверов приложений (см. п. 2.5 и п. 15.1.9);
- `logback.xml` – настройки журналирования событий и ошибок.

Большинство настроек задается с использованием консоли управления. Для ряда настроек необходимо самостоятельное редактирование конфигурационных файлов. Такие настройки описаны далее в подразделах.

Конфигурационный файл приложения `blitz-keeper` расположен в `/etc/blitz-keeper`.

Используются следующие конфигурационные файлы:

- `blitz-keeper.conf` – настройки шлюза безопасности (см. п. 14);
- `blitz-keeper-log4j.xml` – настройки журналирования событий и ошибок.

15.1. Файл настроек `blitz.conf`

Основной конфигурационный файл `blitz.conf` состоит из следующих блоков настроек, имеющих следующее назначение:

- `blitz.prod.local.idp.apps` – настройки подключенных приложений;
- `blitz.prod.local.idp.federation` – настройки внешних поставщиков идентификации;
- `blitz.prod.local.idp.flexible-flows` – настройки процедур входа;
- `blitz.prod.local.idp.id-attrs` – настройки атрибутов;
- `blitz.prod.local.idp.id-stores` – настройки хранения атрибутов в LDAP-каталоге;

- `blitz.prod.local.idp.internal-store` – настройки подключения к СУБД;
- `blitz.prod.local.idp.keystore` – настройки доступа к хранилищу ключей;
- `blitz.prod.local.idp.license` – лицензионный ключ Blitz Identity Provider;
- `blitz.prod.local.idp.logger` – настройки логгеров;
- `blitz.prod.local.idp.login` – настройки методов аутентификации;
- `blitz.prod.local.idp.logout` – настройки процесса логгута;
- `blitz.prod.local.idp.messages` – настройки файлов сообщений;
- `blitz.prod.local.idp.messaging` – настройки вызова сервисов информирования;
- `blitz.prod.local.idp.captcha` – настройки взаимодействия с сервисом CAPTCHA;
- `blitz.prod.local.idp.events` – настройки отправки событий в очередь;
- `blitz.prod.local.idp.net` – настройки сети;
- `blitz.prod.local.idp.notifier` – настройки уведомлений о событиях;
- `blitz.prod.local.idp.oauth` – настройки разрешений (scope);
- `blitz.prod.local.idp.password-policy` – настройки парольной политики;
- `blitz.prod.local.idp.play` – настройки сервера приложений Blitz Identity Provider;
- `blitz.prod.local.idp.provisioning` – настройки сервисов регистрации пользователей и восстановления забытого пароля;
- `blitz.prod.local.idp.realms` – настройки шифрования идентификаторов приложений («домены приватности»);
- `blitz.prod.local.idp.saml` – настройки SAML;
- `blitz.prod.local.idp.tasks` – настройки механизма обработки задач;
- `blitz.prod.local.idp.user-profile` – настройки личного кабинета;
- `home` – путь к каталогу установки Blitz Identity Provider на сервере приложений.

Далее приведено описание настроек, недоступных из консоли управления, и проводимых посредством редактирования конфигурационного файла `blitz.conf`.

15.1.1. Настройка парольных политик

Блок настроек `blitz.prod.local.idp.password-policy` содержит запись с настройками парольной политики Blitz Identity Provider.

Пример настройки приведен ниже:

```
"password-policy" : {
  "groups": [
    {
      "desc": "password.policy.desc.digits",
      "group": "[0-9]",
      "minCount": 1
    },
    {
      "desc": "password.policy.desc.lowercase",
      "group": "[a-z]",
      "minCount": 1
    }
  ]
}
```

```

    },
    {
      "desc": "password.policy.desc.capital",
      "group": "[A-Z]",
      "minCount": 1
    },
    {
      "desc": "password.policy.desc.special",
      "group": "[!@#$%^&* ()+\\-?.,;:'`\"{}\\|\\><=~/\\\\\\_]",
      "minCount": 1
    }
  ],
  "minGroups": 3,
  "minLength": 6,
  "dicPath": "/usr/share/identityblitz/blitz-config/password dic.txt",
  "passwordHistoryLen": 5,
  "minPasswordAgeSec": 3600,
  "maxPasswordAgeSec": 2592000,
  "minNewChars": 1
}

```

Предусмотрены следующие настройки:

- **groups** – задает описание (**desc**) группы символов, набор символов (**group**), минимально достаточное количество символов группы в пароле (**minCount**).
- **minGroups** – задает минимально необходимое количество групп символов в пароле.
- **minLength** – задает минимальную длину пароля.
- **dicPath** – задает путь к файлу со словарем паролей; это должен быть текстовый файл, где каждый пароль размещен на новой строке;
- **passwordHistoryLen** – количество старых паролей, которое требуется хранить и не допускать задания нового пароля при наличии его в перечне использованных паролей;
- **minPasswordAgeSec** – минимальное время жизни пароля, в секундах; пока это время не истекло, пользователю не будет разрешено поставить новый пароль. Если такую проверку не следует выполнять, то нужно удалить данный параметр;
- **maxPasswordAgeSec** – максимальное время жизни пароля, в секундах; как только это время истечет, пользователю потребуется задать новый пароль. Если такую проверку не следует выполнять, то нужно удалить данный параметр;
- **minNewChars** – минимальное количество новых символов при задании нового пароля (для случаев, когда пользователь меняет текущий пароль на новый).

15.1.2. Ограничение количества одновременных проверок пароля пользователя

Можно установить ограничение на количество одновременных парольных аутентификаций с одинаковым логином пользователя за период времени. По умолчанию установлен режим, что Blitz Identity Provider разрешает пройти не более 3 аутентификаций на один и тот же логин в течение 600 мс. Чтобы скорректировать стандартные настройки, необходимо в конфигурационном файле `blitz.conf` добавить в раздел `blitz.prod.local.idp.login.methods.password` следующий блок:

```
"throughput": {
```

```
"limit": 3,
"window": 600
}
```

15.1.3. Настройка времени отображения экрана логута

По умолчанию при вызове приложением логута в Blitz Identity Provider пользователю в течение 5 секунд отображается экран, поясняющий, что происходит логут. После этого экран автоматически закрывается, а пользователь перенаправляется на страницу, указанную при вызове логута в качестве параметра возврата.

Скорректировать время отображения страницы логута можно через конфигурационный файл. Для этого в разделе `blitz.prod.local.idp.logout` нужно скорректировать параметр `timeout-sec`:

```
"logout" : {
  "timeout-sec" : 2
}
```

15.1.4. Настройка вызова внешнего сервиса проверки электронной подписи

Для интеграции с внешним сервисом проверки электронной подписи должна быть разработана специальная библиотека проверки подписи. Система будет производить проверку электронной подписи через эту систему после прописывания данной библиотеки в конфигурационном файле, в разделе `blitz.prod.local.idp.login.methods.x509`, следующим образом:

```
"x509-verifier" : {
  "javaClass" : "<Java-класс реализации коннектора>",
  "pathToJar" : "/usr/.../check-signature-1.0.0.jar",
  "signatureValidationServiceUrl" : "<адрес сервиса >"
}
```

15.1.5. Настройка CAPTCHA

Для отображения сервиса CAPTCHA при входе по логину и паролю необходимо внести изменения в конфигурационный файл, а также загрузить необходимые файлы (CSS и JS).

Изменения конфигурационного файла должны быть произведены

- в блоке настроек `blitz.prod.local.idp.captcha`. Пример записи настройки приведен ниже:

```
"captcha" : {
  "exampleCaptcha": {
    "operations": [
      {
        "call": {
          "headers": [
            "accept:application/json",
            "Authorization:Bearer ${cfg.bearerToken}"
          ],
          "method": "post",
          "url":
            "https://captcha.example.com/captcha/1.0.0/check?uniqueFormHash=${ste.uniqueFormHash}&code=${ocp.code}&options[system]=${cfg.system}&options[token]=${cfg.token}"
        },
        "check": {
          "errRegExp": {},
          "okRegExp": {
            "error": "0"
          }
        }
      }
    ]
  }
}
```

```

    },
    "name": "check",
    "newState": {
      "uniqueFormHash": "${rsp.result.uniqueFormHash-}"
    }
  },
  {
    "call": {
      "headers": [
        "accept:application/json",
        "Authorization:Bearer ${cfg.bearerToken}"
      ],
      "method": "get",
      "url":
"https://captcha.example.com/captcha/1.0.0/create?type=${cfg.type}&options[system]=${cfg.system}&options[token]=${cfg.token}"
    },
    "name": "create",
    "newState": {
      "uniqueFormHash": "${rsp.result.uniqueFormHash-}"
    }
  },
  {
    "call": {
      "headers": [
        "accept:application/json",
        "Authorization:Bearer ${cfg.bearerToken}"
      ],
      "method": "post",
      "url":
"https://captcha.example.com/captcha/1.0.0/refresh?uniqueFormHash=${ste.uniqueFormHash}&type=${cfg.type}&options[system]=${cfg.system}&options[token]=${cfg.token}"
    },
    "name": "refresh"
  }
],
"plainParams": {
  "type": "arithmetic"
},
"secureParams": {
  "bearerToken": "<access_token>",
  "system": "<system_id>",
  "token": "<system_token>"
}
}
}

```

В этом блоке содержатся параметры вызова трех методов сервиса CAPTCHA (**create**, **check**, **refresh**), а также секретные параметры – маркер доступа (**bearerToken**), идентификатор системы (**system**), а также токен системы (**token**).

- в блоке настроек входа по логину и паролю `blitz.prod.local.idp.password`. Внутри этого блока следует добавить блок `captcha` и настроить согласно примеру:

```

"captcha" : {
  "enabled": true,
  "initJs": "require(['https://demo.reaxoft.ru/themes/default/assets/js/passwordCaptcha.js',
'captcha-conf'], function(captcha, conf){ captcha(conf,
'https://demo.reaxoft.ru/themes/default/assets/css/passwordCaptcha.css');});",
  "mode": {
    "type": "always_on"
  },
  "name": "exampleCaptcha"
}

```

В этом блоке следует настроить следующие параметры:

- **enabled** – признак того, включена CAPTCHA или нет (`true/false`);
- **initJs** – содержит ссылки на JS-скрипт и CSS-стили, загружаемые на странице входа и необходимые для отображения/вызова CAPTCHA на странице входа;
- **mode** – режим отображения CAPTCHA, предусмотрены следующие режимы:

- `always_on` – CAPTCHA отображается всегда
- `on_header` – CAPTCHA отображается, если в запросе есть заголовок, указанный в параметре `name`, и значением, указанным в параметре `value`.

В случае использования в качестве CAPTCHA сервиса Google reCAPTCHA v3⁴³ необходимо:

- задать следующие настройки в `blitz.prod.local.idp.captcha`:

```
"captcha" : {
  "reCAPTCHAv3" : {
    "operations" : [
      {
        "call" : {
          "headers" : [],
          "method" : "post",
          "url" :
"https://www.google.com/recaptcha/api/siteverify?secret=${cfg.secret}&response=${ocp.response}"
        },
        "check" : {
          "errRegExp" : {},
          "okRegExp" : {
            "score" : "1\\.0|0\\. (5|6|7|8|9)",
            "success" : "true"
          }
        },
        "name" : "verify"
      }
    ],
    "plainParams" : {
      "sitekey" : "SITE_KEY"
    },
    "secureParams" : {
      "secret" : "SITE_SECRET"
    }
  }
}
```

Вместо `SITE_KEY` и `SITE_SECRET` нужно заполнить значения, полученные при регистрации Google reCAPTCHA v3 на сайте <https://g.co/recaptcha/v3>. Также нужно скорректировать значение в параметре `score` – установить требуемый порог успешного прохождения проверки (в примере выставлен порог не ниже 0,5).

- задать следующие настройки в `blitz.prod.local.idp.password.captcha`:

```
"captcha" : {
  "mode" : {
    "name" : "X-Captcha-Check",
    "type" : "on_header",
    "value" : "true"
  },
  "enabled" : true,
  "initJs" : "require(['blitz/assets/blitz-common/javascripts/recaptcha_v3.js', 'captcha-conf'],
function(captcha, conf){ captcha(conf);});",
  "mode" : {
    "type" : "always_on"
  },
  "name" : "reCAPTCHAv3"
}
```

15.1.6. Настройка отправки событий в сервер очередей

В сервер очередей могут быть отправлены следующие события:

- регистрация пользователя (`USER_REGISTERED`);

⁴³ См.: <https://developers.google.com/recaptcha/docs/v3>

- смена пароля (`USER_PASSWORD_SET`);
- смена признака аннулирования сессий (`USER_CRID_CHANGED`);
- изменения атрибутов пользователя (`USER_ATTRIBUTE_CHANGED`);
- очистка атрибутов пользователя (`USER_ATTRIBUTE_REMOVED`);
- удаление пользователя (`USER_REMOVED`);
- привязка внешней учетной записи (`FEDERATION_POINT_BOUND`);
- отвязка внешней учетной записи (`FEDERATION_POINT_UNBOUND`);
- отзыв выданного приложению разрешения (scopes) (`SCOPES_REVOKED`);
- создание группы (`GROUP_CREATED`);
- изменение атрибутов группы (`GROUP_UPDATED`);
- удаление группы (`GROUP_REMOVED`);
- включение пользователя в группу (`GROUP_MEMBER_ADDED`);
- исключение пользователя из группы (`GROUP_MEMBER_REMOVED`).

Для отправки событий в очередь следует создать блок `blitz.prod.local.idp.events` следующего содержания (на примере регистрации пользователя и смены пароля):

```
"events" : {
  "drivers" : {
    "rabbit_driver" : {
      "properties" : {},
      "server" : {
        "host" : "<RMQ HOST>",
        "port" : 5672
      },
      "type" : "RMQ",
      "user" : {
        "password" : "<RMQ PASS>",
        "username" : "<RMQ_USERNAME>"
      }
    }
  },
  "routes" : {
    "USER_PASSWORD_SET" : [
      "password_sync"
    ],
    "USER_REGISTERED" : [
      "registration"
    ]
  },
  "targets" : [
    {
      "discardList" : "PSWD SYNC DISCARD",
      "driver" : {
        "ext" : {
          "exchange_name" : "users",
          "routing_key" : "pwd_sync"
        },
        "id" : "rabbit_driver"
      },
      "encCertificate" : "rmqkey",
      "name" : "password_sync",
      "redelivery" : 3
    },
    {
      "discardList" : "REG DISCARD",
      "driver" : {
        "ext" : {
          "exchange name" : "users",
          "routing key" : "registration"
        }
      }
    }
  ]
}
```

```
        "id" : "rabbit_driver"
      },
      "encCertificate" : "rmqkey",
      "name" : "registration",
      "redelivery" : 3
    }
  ]
}
```

В данных настройках следует задать:

- `RMQ_HOST` – домен сервера очередей RabbitMQ;
- `RMQ_USERNAME` – имя пользователя для работы с сервером очередей;
- `RMQ_PASS` – пароль для работы с сервером очередей.

Кроме того, для шифрования паролей, отправляемых в очередь, в параметре `encCertificate` следует указать псевдоним ключа электронной подписи (в стандартном хранилище ключей `BlitzIdPKeystore.jks`), которым следует шифровать пароли в сообщениях.

15.1.7. Запрос проверочного атрибута при восстановлении пароля

Можно настроить веб-приложение «Восстановление доступа», чтобы при восстановлении пароля пользователь вводил значение дополнительного атрибута для подтверждения владения учетной записью. Добавление такой проверки усложняет атаку на сброс пароля через множественный перебор в форме восстановления забытого пароля. На главной странице у пользователя будут запрошены атрибуты для сверки (например, фамилия) и восстановление будет выполнено только в том случае, если найденная учетная запись будет иметь идентичное значение атрибута.

Для настройки атрибутов сверки следует отредактировать параметр `security-question` в блоке `blitz.prod.local.idp.provisioning.recovery`. Пример настройки, позволяющей запрашивать фамилию на форме восстановления доступа:

```
"security-question" : {
  "attrs" : [
    "LastName"
  ]
}
```

15.1.8. Настройка хранения объектов в Couchbase Server

Можно переназначить внутренние хранилища (buckets) Blitz Identity Provider в СУБД Couchbase Server, используемые для хранения данных. Предусмотрена возможность для следующих наборов данных указать необходимость использования иных хранилищ (buckets), чем стандартно используемые.

Для настройки иных хранилищ (buckets) нужно в блоке `blitz.prod.local.idp.internal-store-cb` добавить настройки:

- `buckets` – перечисление используемых хранилищ (buckets), в случае если отличаются от стандартных;
- `bucketsMapping` – переопределение стандартных размещений наборов данных на

размещение в других хранилищах.

Пример настройки в конфигурационном файле представлен ниже. В результате набор данных `acl` размещается в хранилище `users`, а `clt` и `iat` – в `apps`. По умолчанию все три набора данных записывались в хранилище `oauth`.

```
"internal-store-cb" : {
  ...
  "buckets" : {
    ["users", "oauth", "audit", "builtin_idstore", "ctxs"]
  },
  "bucketsMapping" : {
    "acl" : "users",
    "clt" : "apps",
    "iat" : "apps"
  },
  ...
}
```

Можно настроить для данных аудита ограничение по сроку хранения записей (по умолчанию записи хранятся бессрочно). Для этого в блоке `blitz.prod.local.idp.internal-store-cb` нужно добавить настройку `ttlMapping` с указанием `doc_type` записи (`aud`) и времени хранения в секундах.

Пример настройки (время хранения аудита ограничено до 90 суток):

```
"internal-store-cb": {
  ...
  "ttlMapping": {
    "aud": 7776000
  },
  ...
}
```

15.1.9. Настройка домена Blitz Identity Provider

Изменение домена Blitz Identity Provider осуществляется путем редактирования в блоке настроек `blitz.prod.local.idp.net` конфигурационного файла настройки `domain`.

Пример настройки:

```
"net" : {
  "domain" : "demo.identityblitz.com"
}
```

При необходимости можно изменить путь до приложений (по умолчанию приложения доступны с использованием пути `/blitz`). Отредактировать путь можно в конфигурационном файле `play.conf`. Нужно изменить параметр `context` в блоке `play.http`:

```
"http" : {
  "context": "/blitz",
  ...
}
```

15.1.10. Настройка справочника прав доступа

Чтобы использовать REST API в Blitz Identity Provider по назначению и отзыву прав доступа субъектов (пользователи и приложения) на объекты (пользователи, группы пользователей, приложения) необходимо зарегистрировать справочник прав доступа. Для этого в конфигурационный файл добавить блок настроек `blitz.prod.local.idp.rights` следующего вида, указывая в `name` и `desc` имя и описания права доступа:


```
"rights" : {
  "meta" : [
    {
      "desc" : "Текстовое описание права доступа",
      "name" : "right1"
    },
    {
      "desc" : "",
      "name" : "right2"
    },
    ...
  ]
}
```

15.1.11. Расширенные настройки подключения к хранилищам

В консоли управления можно создать настройки подключения к хранилищам атрибутов, работающим по LDAP-протоколу. При этом через консоль управления можно задать настройки пула коннектов к LDAP. Blitz Identity Provider будет использовать общие настройки пула коннектов для установки подключений каждым приложением, использующим подключение к хранилищам. Это может привести к созданию большого числа коннектов к LDAP. Через конфигурационный файл `blitz.conf` можно настроить параметры начального и максимального числа коннектов в разрезе различных приложений Blitz Identity Provider (например, для консоли управления задать меньшие значения коннектов в пуле, чем для сервиса аутентификации). Для этого в блоке `blitz.prod.local.id-stores` в настройках соответствующего хранилища наряду с настройками `initialConnections` и `maxConnections` можно создать настройки вида `initialConnections#BLITZ_APP` и `maxConnections#BLITZ_APP`, где в качестве `BLITZ_APP` указывается имя соответствующего приложения (`blitz-console`, `blitz-idp`, `blitz-registration`, `blitz-recovery`). Пример настройки, когда для консоли управления задается меньший размер пула коннектов, чем для остальных приложений:

```
"id-stores" : {
  "list" : [
    {
      "type" : "LDAP",
      ...
      "initialConnections" : 10,
      "initialConnections#blitz-console" : 1,
      "maxConnections" : 20,
      "maxConnections#blitz-console" : 1
    }
  ]
}
```

При выполнении запросов в LDAP хранилище атрибутов Blitz Identity Provider берет имеющееся соединение с LDAP-каталогом из пула соединений. После выполнения запроса Blitz Identity Provider не закрывает соединение, а возвращает его обратно в пул соединений для возможности повторного использования. Такой порядок взаимодействия с LDAP обеспечивает высокую производительность, но требует длительное время поддерживать соединения с LDAP-каталогом открытыми. Настройки межсетевых экранов или самих LDAP-каталогов могут препятствовать длительному сохранению открытых соединений приложений Blitz Identity Provider с LDAP-каталогом. TCP-соединения Blitz Identity Provider с LDAP-каталогом могут быть закрыты без согласованного разрыва соединения, так что а

LDAP-каталоге соединение будет закрыто, а Blitz Identity Provider об этом уведомлен не будет. При попытке использования такого соединения из пула может возникнуть длительный таймаут, прежде чем Blitz Identity Provider расценит соединение как закрытое и исключит его из пула соединений. Чтобы такая ситуация не влияла на пользователей, в Blitz Identity Provider предусмотрен алгоритм периодической проверки действительности открытых LDAP-соединений. С периодом `healthCheckInterval` (в миллисекундах) выполняется проверка состояния соединения, а время таймаута при отсутствии ответа LDAP-каталога на запрос задается параметром `connectionTimeout` (в миллисекундах). Сам описанный режим оптимального взаимодействия с пулом соединений по умолчанию включен (настройка `useSyncMode` в значении `false`). В случае нестабильной работы соединений с LDAP-каталогом рекомендуется попробовать включить синхронный режим взаимодействия с каталогом (установить `useSyncMode` в значении `true`). Примеры рекомендуемых настроек приведены ниже:

```
"id-stores" : {
  "list" : [
    {
      "type" : "LDAP",
      ...
      "connectionTimeout" : 3000,
      "healthCheckInterval" : 300000,
      "useSyncMode" : false
    }
  ]
}
```

В случае подключения к Blitz Identity Provider одновременно нескольких хранилищ атрибутов может возникнуть такая ситуация, что при идентификации и аутентификации пользователя по логину и паролю в нескольких хранилищах может обнаружиться несколько учетных записей, возможно принадлежащих разным людям, с совпадающими логинами. Необходимо избегать такой ситуации при внедрении Blitz Identity Provider, и по умолчанию при выявлении такой ситуации Blitz Identity Provider при выявленных дублях будет выдавать пользователю ошибку входа, указывающую на наличие некорректной ситуации с учетной записью пользователя. Тем не менее, в ряде случаев может возникнуть ситуация, когда при внедрении намеренно допускают, что по одному логину может быть найдено несколько учетных записей разных пользователей в разных хранилищах. В этом случае можно указать в блоке настроек `blitz.prod.local.idp.login` режим `firstSucceeded` в настройке `authStrategy`. В этом случае все найденные учетные записи будут проверены, и к какой из них первой подойдет пароль пользователя, с этой учетной записью и будет выполнен вход.

Пример настройки:

```
"login" : {
  "authStrategy" : {
    "mode" : "firstSucceeded"
  },
  ...
}
```

15.1.12. Блокирование неактивных пользователей

Blitz Identity Provider отслеживает время последней активности пользователя. Предусмотрена возможность выполнять блокирование учетных записей пользователей, которые долгое время неактивны. Для активации этой возможности необходимо запустить в cron выполнение скрипта `lockinactive.sh`. Скрипт находится в директории `/usr/share/identityblitz/blitz-console/bin` на сервере с приложением `blitz-console`. Рекомендуется выполнять скрипт раз в день во время минимальной активности в системе. Перед запуском скрипта необходимо отредактировать его в текстовом редакторе – установить:

- `inactive_period` – требуемый период неактивности (в днях), после которого должна быть произведена блокировка учетной записи;
- `range_size` – диапазон охвата учетных записей (в днях), под блокировку попадут учетные записи, последняя активность по которым была в период с `(текущая дата – inactive_period – range_size)` до `(текущая дата – inactive_period)`.

15.1.13. Запрет повторного использования идентификатора удаленного пользователя

Blitz Identity Provider отслеживает использованные ранее идентификаторы пользователей, чтобы их нельзя было использовать повторно после удаления учетной записи пользователя в течение установленного периода времени. Для этого в блок `blitz.prod.local.idp.provisioning` нужно добавить раздел `remove` следующего содержания, указав нужное число дней (`days`), в течение которых идентификатор пользователя нельзя будет использовать при повторной регистрации:

```
"provisioning" : {
  ...
  "remove": {
    "mode": "keepRemovedId",
    "days": 365
  }
}
```

15.1.14. Настройка групп пользователей

Чтобы включить возможность просмотра групп пользователей, необходимо добавить блок настроек `blitz.prod.local.idp.groups` следующего вида:

```
"groups": {
  "profiles": [
    {
      "type": "mirror",
      "id": "orgs",
      "groupStore": "389ds",
      "attrsMap": {
        "name": "displayname",
      },
      "filter": "objectClass=group"
    }
  ],
  "stores": {
    "list": [
      {
        "type": "ldap_based",
```

```
"id": "389ds",
"desc": "Группы",
"ldapStore": "389ds",
"baseDN": "ou=external,ou=groups,dc=test",
"searchScope": "SUB",
"idAttrName": "cn",
"membersAttrName": "uniqueMember",
"memberOfAttrName": "memberOf",
"newGroupAttrs": [
  {
    "attr": "objectclass",
    "format": "strings",
    "value": "top,groupOfUniqueNames,group"
  },
  {
    "attr": "dn",
    "format": "string",
    "value": "cn=${id},ou=external,ou=groups,dc=test"
  }
]
}
]
```

Особенности указания настроек:

- в `profiles.groupStore`, `stores.list.id`, `stores.ldapStore` должен быть идентификатор LDAP-каталога, используемый для хранения пользователей;
- в `profiles.attrsMap` и в `stores.list.idAttrName` должны быть указаны атрибуты группы (класс `groups`), например `name`. Имена атрибутов при желании можно назвать и по-другому, поддерживаются только LDAP-атрибуты типа `string`;
- в `stores.list.baseDN` нужно проверить (и исправить если необходимо) путь для хранения организаций в LDAP. Если путь будет исправлен, то скорректировать также настройку `"value": "cn=${id},ou=external,ou=groups,dc=test"` соответствующим образом.

15.1.15. Вход через ЕСИА в режиме выбора сотрудника организации

Когда для входа в Blitz Identity Provider сконфигурирован внешний поставщик идентификации ЕСИА, то к обычному режиму входа пользователя (см. п. 8.7) можно сконфигурировать следующие дополнительные возможности:

- Отображение пользователю экрана выбора режима входа и организации, если вошедший через ЕСИА пользователь имеет в ЕСИА роли сотрудника индивидуального предпринимателя, юридического лица или органа государственной власти (см. рисунок 124).

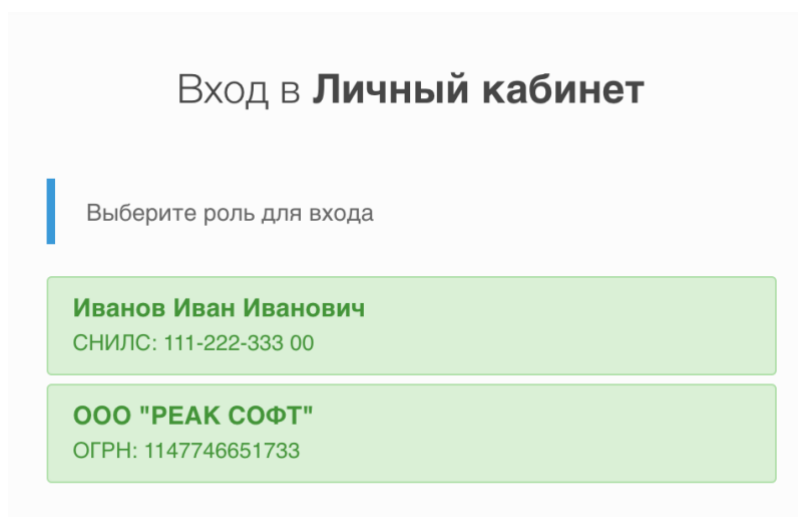


Рисунок 124 – Пример страницы выбора режима входа через ЕСИА

- Получение из ЕСИА сведений о выбранной при входе организации, автоматическое создание на основе этих сведений в LDAP-хранилище группы пользователей с атрибутами, соответствующими организации (если соответствующая организации группа не найдена в момент входа), добавление пользователя в созданную (или найденную) группу пользователей.
- Обновление атрибутов группы пользователя значениями атрибутов организации из ЕСИА в момент входа, если атрибуты в ЕСИА изменились.
- Возможность добавления в маркер доступа и маркер обновления сведений о выбранной в момент входа пользователя роли в ЕСИА (физическое лицо, индивидуальный предприниматель, должностное лицо юридического лица, должностное лицо органа государственной власти).

Для настройки режимов входа необходимо предварительно настроить в Blitz Identity Provider использование групп доступа (см. п. 15.1.14) и вход через ЕСИА (см. п. 8.7). После этого необходимо в конфигурационном файле в секции `blitz.prod.local.idp.federation` в блоке `esia` создать дополнительный блок настроек `org` следующего вида:

```
"federation" : {
  "points" : {
    "esia" : [
      {
        ...
        "org" : {
          "embeds" : [
            "documents.elements-1",
            "addresses.elements-1",
            "contacts.elements-1"
          ],
          "group" : {
            "id" : "${org.oid}",
            "mapping" : [
              {
                "attr" : "org_ogrn",
                "master" : true,
                "value" : "${org.ogrn}"
              }
            ]
          }
        }
      }
    ]
  }
}
```

```
    "attr" : "org_inn",
    "master" : true,
    "value" : "${org.inn}"
  },
  {
    "attr" : "org_fullname",
    "master" : true,
    "value" : "${org.fullName-}"
  },
  {
    "attr" : "org_shortname",
    "master" : true,
    "value" : "${org.shortName-}"
  },
  {
    "attr" : "org_type",
    "master" : true,
    "value" : "${org.type-}"
  },
  {
    "attr" : "org_oktmo",
    "master" : true,
    "value" : "${org.oktmo-}"
  },
  {
    "attr" : "org_leg",
    "master" : true,
    "value" : "${org.leg-}"
  },
  {
    "attr" : "org_kpp",
    "master" : true,
    "value" : "${org.kpp-}"
  },
  {
    "attr" : "org_phone",
    "master" : true,
    "value" : "${org.phone-}"
  },
  {
    "attr" : "org_email",
    "master" : true,
    "value" : "${org.email-}"
  },
  {
    "attr" : "org_fax",
    "master" : true,
    "value" : "${org.fax-}"
  },
  {
    "attr" : "org_agencytype",
    "master" : true,
    "value" : "${org.agencyType-}"
  },
  {
    "attr" : "org_agencyterrangerange",
    "master" : true,
    "value" : "${org.agencyTerRange-}"
  },
  {
    "attr" : "org_address_post",
    "master" : true,
    "value" : "${org.postAddress-}"
  },
  {
    "attr" : "org_address_leg",
    "master" : true,
    "value" : "${org.legalAddress-}"
  }
],
"matchingRules" : [
  [
    {
      "attr" : "id",
      "value" : "${org.oid}"
    }
  ]
],
"profile" : "orgs"
```

```

    },
    "scopes" : [
      "http://esia.gosuslugi.ru/org addr",
      "http://esia.gosuslugi.ru/org leg",
      "http://esia.gosuslugi.ru/org oktmo",
      "http://esia.gosuslugi.ru/org inn",
      "http://esia.gosuslugi.ru/org type",
      "http://esia.gosuslugi.ru/org kpp",
      "http://esia.gosuslugi.ru/org ctts",
      "http://esia.gosuslugi.ru/org agencyterrange",
      "http://esia.gosuslugi.ru/org ogrn",
      "http://esia.gosuslugi.ru/org shortname",
      "http://esia.gosuslugi.ru/org fullname",
      "http://esia.gosuslugi.ru/org agencytype"
    ]
  },
  ...
]
}
}

```

В добавленном блоке нужно скорректировать:

- набор получаемых из ЕСИА сведений об организации и их маппинг на атрибуты группы пользователей (блок `group.mapping`), признаком `master` отметить те атрибуты, которые должны перезаписываться в группе пользователей при каждом обновлении из ЕСИА, полученном в момент входа;
- набор запрашиваемых в ЕСИА разрешений (настройка `scopes`).

Если необходимо передавать в маркер идентификации и маркер доступа сведения о текущей выбранной организации и о роли пользователя в ЕСИА, то необходимо настроить соответствие необходимых атрибутов ЕСИА сессионным утверждениям в Blitz Identity Provider. Это выполняется с помощью настройки `claims` в блоке настроек ЕСИА:

```

"federation" : {
  "points" : {
    "esia" : [
      {
        ...
        "claims" : [
          {
            "name" : "org_id",
            "value" : "org.oid"
          },
          {
            "name" : "global_role",
            "value" : "globalRole"
          },
          {
            "name" : "org_shortname",
            "value" : "org.shortName"
          },
          {
            "name" : "org_fullname",
            "value" : "org.fullName"
          },
          {
            "name" : "org_type",
            "value" : "org.type"
          },
          {
            "name" : "org_ogrn",
            "value" : "org.ogrn"
          },
          {
            "name" : "org_inn",
            "value" : "org.inn"
          },
          {
            "name" : "org_oktmo",

```

```
    "value" : "org.oktmo"  
  }  
},  
...  
]  
}  
}
```

15.2. Настройки текстов интерфейса

15.2.1. Мультиязычность

Веб-интерфейс Blitz Identity Provider поддерживает мультиязычность. По умолчанию предусмотрено два языка – русский и английский.

По умолчанию пользователю отображается интерфейс на том языке, который соответствует его системному языку в ОС и предпочтительному языку в браузере. В этом случае переключение языка осуществляется посредством изменения основного языка ввода (языка отображения веб-страниц) в используемом браузере. Например, для изменения языка в браузере Chrome нужно выполнить шаги:

- перейти к настройкам браузера (`chrome://settings/`);
- выбрать пункт «Показать дополнительные настройки»;
- нажать на кнопку «Изменить языковые настройки»;
- переместить нужный язык на первое место в списке (рис. 125).

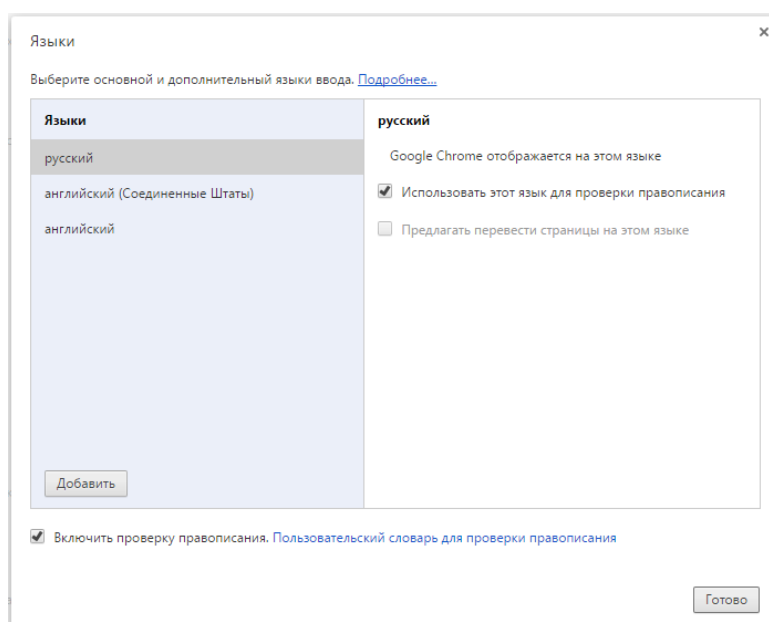


Рисунок 125 – Настройка языка для браузера Chrome

Для изменения языка в браузере Firefox нужно выполнить шаги:

- перейти к настройкам браузера (`about:preferences`);
- выбрать раздел «Содержимое» настроек;
- в подразделе «Языки» нажать на кнопку «Выбрать»;
- переместить нужный язык на первое место в списке:

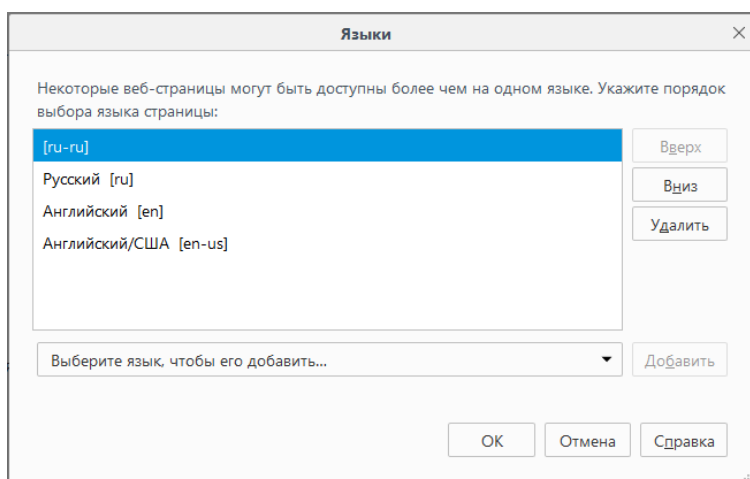


Рисунок 126 – Настройка языка для браузера Firefox

Дополнительно возможно провести настройку языка через конфигурационный файл `blitz.conf`. Для этого следует отредактировать раздел для настройки языка `blitz.prod.local.idp.lang` со следующими параметрами:

- `languages` – список доступных языков. Первый язык в списке считается языком по умолчанию;
- `portal-lang-cookie` – имя (name) и домен установки (domain) cookie с текущим языком портала (опциональный). Если порталная cookie задана, то смена языка в Blitz Identity Provider сохраняется в указанной cookie;
- `ignore-browser` – включен или нет режим игнорирования языка браузера.

Пример фрагмента конфигурационного файла:

```
"lang" : {
  "ignore-browser" : true,
  "languages" : [
    "ru",
    "en"
  ],
  "portal-lang-cookie" : {
    "domain" : "domain.com",
    "name" : "blitzlng"
  }
}
```

Таким образом, например, если применение английского языка интерфейса не требуется, то его можно удалить из параметра `languages`.

15.2.2. Модификация текстовых сообщений веб-интерфейса

Blitz Identity Provider позволяет менять текстовые строки, используемые в интерфейсе системы. Для этого необходимо отредактировать файл `messages`, размещенный в директории `/custom_messages/`, добавив строку вида «параметр=значение», где параметр – идентификатор текстовой строки, а значение – необходимый текст.

Все текстовые строки, используемые Blitz Identity Provider по умолчанию, сохранены в архиве `messages.zip`, входящий в состав ПО.

Например, следующая строка отвечает за текст на форме регистрации, где размещена ссылка на условия использования:

```
reg.page.reg.action.agreement=Нажимая на   кнопку &laquo;Зарегистрироваться&raquo;  
вы   соглашаетесь с   <a href="{0}" target="_blank">условиями использования</a>
```

Для корректного отображения файл должен быть сохранен в кодировке UTF-8.

При необходимости изменить английский язык следует добавить в указанную директорию файл `messages.en` и изменить в нем необходимые файлы.

При необходимости использовать в текстах символ @ его следует ввести дважды.

15.2.3. Модификация шаблонов писем и SMS-сообщений

Шаблоны писем представляют собой текстовые строки, сохраняемые аналогично обычным строкам в веб-интерфейсе. Их изменение производится аналогичным образом (см п. 15.2.2 документа).

Используется унифицированный формат кодов сообщений, который имеет вид:

```
message.{$[группа_сообщений]}.{$[тип_сообщения]}.{$[вариация]}.{$[канал]}.{$[часть]}
```

Используются группы сообщения:

- `notif` – для информационных сообщений;
- `auth` – для взаимодействия с пользователем при аутентификации;
- `reg` – для взаимодействия с пользователем при регистрации;
- `recovery` – для взаимодействия с пользователем при восстановлении доступа;
- `profile` – для взаимодействия с пользователем в Личном кабинете;
- `api` – для взаимодействия с пользователем при использовании API;

Вариации позволяют помимо базового шаблона сообщения задать его варианты (например, отдельный шаблон в разрезе приложений). Наличие вариации проверяется по основному шаблону с текстом сообщения (часть `body`). Если вариация основного шаблона описана в системе, то все остальные шаблоны (`email.subject`, `email.from`, `push.title`) будут применяться с этой же вариацией. Если вариаций несколько, то они будут проверяться в некотором заданном порядке (обычно от большей детализации к меньшей). При отсутствии вариаций будет использован базовый шаблон. В большинстве случаев вариации отсутствуют

Возможны следующие каналы:

- «`sms`» - отправка сообщений по SMS. Части для этого канала отсутствуют;
- «`email`» - отправка сообщений по электронной почты. Части для этого канала:
 - «`subject`» - тема;
 - «`body`» - основное содержание;
 - «`from`» - отправитель (необязательно);

- «push» - отправка push-уведомлений. Части для этого канала:
 - «title» - тема;
 - «body» - основное содержание.

Пример ключей для сообщений типа `login_unknown_device`:

- `message.notif.login_unknown_device.email.subject` – тема сообщения по email;
- `message.notif.login_unknown_device.email.body` – текст сообщения по email;
- `message.notif.login_unknown_device.email.from` – отправитель email сообщения;
- `message.notif.login_unknown_device.sms` – текст сообщения по SMS.

В таблицах ниже представлены описания типов сообщений из различных групп.

Таблица 6

Типы сообщений из группы «информирование» (notif)

Тип сообщения	Описание	Параметры
<code>login_unknown_device</code>	Информирование пользователя о входе с неизвестного устройства	<ul style="list-style-type: none"> – <code>device</code> – код устройства – <code>device.msg</code> – название устройства, вычисленное через строку <code>msg(audit.device.\$[device])</code> – <code>browser</code> – браузер пользователя – атрибуты из сессии пользователя
<code>link_social_network</code>	Информирование пользователя о присоединении к социальной сети	<ul style="list-style-type: none"> – <code>fp.humanReadableName</code> – название внешнего поставщика идентификации – атрибуты пользователя
<code>change_pwd</code>	Информирование пользователя о смене пароля	<ul style="list-style-type: none"> – атрибуты пользователя
<code>changed_pwd_to_object</code>	Информирование о смене пароля в зависимой учетной записи	<ul style="list-style-type: none"> – атрибуты зависимой учетной записи с префиксом <code>obj.</code>
<code>access_recovery</code>	Информирование пользователя о восстановлении пароля	<ul style="list-style-type: none"> – атрибуты пользователя
<code>access_recovery_by_object</code>	Информирование о восстановлении пароля в зависимой учетной записи	<ul style="list-style-type: none"> – атрибуты зависимой учетной записи с префиксом <code>obj.</code>
<code>set_2factor_auth</code>	Информирование пользователя о назначении второго фактора аутентификации	<ul style="list-style-type: none"> – <code>method</code> – код метода аутентификации – <code>method.msg</code> – имя метода аутентификации, полученное через строку

Тип сообщения	Описание	Параметры
		<ul style="list-style-type: none"> - <code>msg(message.method.name.\$[method])</code> - атрибуты пользователя
<code>granted_access_to</code>	Информирование субъекта о предоставлении доступа к объекту	<ul style="list-style-type: none"> - <code>blitz_right</code> – код права доступа - атрибуты субъекта - атрибуты объекта с префиксом <code>obj.</code>
<code>granted_access_on</code>	Информирование объекта о предоставлении доступа к нему	<ul style="list-style-type: none"> - <code>blitz_right</code> – код права доступа - атрибуты объекта - атрибуты субъекта с префиксом <code>obj.</code>
<code>revoked_access_to</code>	Информирование субъекта об отзыве доступа к объекту	<ul style="list-style-type: none"> - <code>blitz_right</code> – код права доступа - атрибуты субъекта - атрибуты объекта с префиксом <code>obj.</code>
<code>revoked_access_on</code>	Информирование объекта об отзыве доступа к нему	<ul style="list-style-type: none"> - <code>blitz_right</code> – код права доступа - атрибуты объекта - атрибуты субъекта с префиксом <code>obj.</code>
<code>on_registration</code>	Информирование пользователя о регистрации его учетной записи	<ul style="list-style-type: none"> - <code>_entryPoint</code> – канал регистрации - <code>_appId</code> – приложение - <code>_requesterId</code> - атрибуты пользователя

Таблица 7

Типы сообщений из группы «регистрация» (reg)

Тип сообщения	Описание	Параметры
<code>vrf_code</code>	Отправка кода подтверждения контакта при регистрации	<ul style="list-style-type: none"> - <code>code</code> – код подтверждения - <code>link</code> – ссылка для подтверждения (только для email) - <code>req.ip</code> – IP-адрес - <code>req.userAgent</code> – userAgent пользователя - <code>cfg.domain</code> - атрибуты пользователя из контекста регистрации с префиксом <code>attrs.</code>
<code>set_pwd_link</code>	Отправка ссылки на смену пароля при регистрации (только для канала email)	<ul style="list-style-type: none"> - <code>link</code> – ссылка на страницу смены пароля - <code>req.ip</code> – IP-адрес - <code>req.userAgent</code> – userAgent пользователя - <code>cfg.domain</code>

Тип сообщения	Описание	Параметры
		– атрибуты пользователя из контекста регистрации с префиксом <code>attrs</code> .
<code>generated_pwd</code>	Отправка назначенного при регистрации пароля (только для канала SMS)	– <code>pwd</code> – сгенерированный пароль – <code>req.ip</code> – IP-адрес – <code>req.userAgent</code> – userAgent пользователя – <code>cfg.domain</code> – атрибуты пользователя из контекста регистрации с префиксом <code>attrs</code> .

Таблица 8

Типы сообщений из группы «восстановление доступа» (recovery)

Тип сообщения	Описание	Параметры
<code>vrf_code</code>	Отправка кода подтверждения контакта при восстановлении доступа	– <code>code</code> – код подтверждения – <code>link</code> – ссылка для подтверждения (только для email)

Таблица 9

Типы сообщений из группы «аутентификация» (auth)

Тип сообщения	Описание	Параметры
<code>vrf_code</code>	Отправка кода подтверждения мобильного номера (каналы: SMS/push)	– <code>code</code> – код подтверждения

Таблица 10

Типы сообщений из группы «личный кабинет» (profile)

Тип сообщения	Описание	Параметры
<code>vrf_code</code>	Отправка кода подтверждения контакта при изменении его в Личном кабинете	– <code>attr.msg</code> – наименование атрибута в форме профиля – <code>attr</code> – код атрибута – <code>link</code> – ссылка для подтверждения (только для email) – <code>code</code> – код подтверждения

Таблица 11

Типы сообщений из группы «программный интерфейс» (api)

Тип сообщения	Вариации	Описание	Параметры
vrf_code	<ul style="list-style-type: none"> – <code>\$attr.\$rpld</code> – отдельно для данного приложения и атрибута – <code>\$attr</code> – отдельно для данного атрибута 	Отправка кода подтверждения контакта через API	<ul style="list-style-type: none"> – <code>code</code> – код подтверждения – <code>link</code> – ссылка (только для email) – <code>attr.value</code> – новый контакт (email или мобильный номер) – <code>attr</code> – код атрибута контакта

15.2.4. Модификация сообщений для разных приложений

Возможно изменение всех текстовых сообщений и шаблонов таким образом, чтобы использовались специфические тексты и шаблоны для разных приложений. Таким образом можно, например, брендировать письма, отправляемые при регистрации на разных сайтах, подключенных к одной установке Blitz Identity Provider, или давать ссылку на скачивание различных правил использования ресурса.

Для привязки набора шаблонов к конкретному приложению следует выполнить шаги:

1. Создать экземпляр файла с текстами, который будет использоваться исключительно для данного приложения. Для этого в директории `custom_messages/` создать текстовый файл `messages.ru-123456` (`messages.en-123456`) для данного приложения, где `123456` – последовательность из 5-8 символов (допускаются как цифры, так и буквы латинского алфавита).
2. Отредактировать файл `messages.ru-123456` (`messages.en-123456`), добавив в него специфические строки для данного приложения (подробнее см. п. 15.2.2). Все остальные строки будут взяты из базы строк по умолчанию.
3. Отредактировать файл `blitz.conf` следующим образом:
 - в разделе `blitz.prod.local.idp.apps` файла найти идентификатор приложения, который должен использовать созданный файл шаблона;
 - добавить параметр вида `"lang-variant" : "123456"`, где `123456` – использованная для маркировки шаблона последовательность символов. Пример:

```
"demo-application" : {
  "domain" : "http://testdomain.ru",
  "lang-variant" : "123456",
  "name" : "test",
  "oauth" : {
    "autoConsent" : false,
    "clientSecret" : "1234567890",
    "defaultScopes" : [],
    "enabled" : true,
    "redirectUriPrefixes" : [
      "http://localhost"
```

```
    ],  
    },  
    "theme" : "default"  
  }  
}
```

После этого при входе в данное приложение будет использоваться специально созданный файл сообщений.

15.3. Файлы настроек консоли управления

Консоль управления настраивается с помощью файлов `console.conf` и `credentials`. Далее в подразделах описаны возможные настройки.

15.3.1. Настройка входа в консоль управления через SSO

В консоль управления Blitz Identity Provider можно настроить вход через поставщика идентификации OIDC. В качестве такого поставщика может выступить как текущая установка Blitz Identity Provider, так и отдельная его установка или даже стороннее ПО, если оно совместимо с OIDC.

Поддерживаются следующие режимы входа в консоль управления:

- стандартный режим по логину/паролю учетных записей, заведенных в разделе «Администраторы» (см. п. 2.11);
- режим входа через SSO;
- гибридный режим входа, когда администратор может войти как по логину/паролю в стандартном режиме, так и через SSO.

При использовании режима SSO учетные записи администраторов все равно должны быть заведены в разделе «Администраторы», и им должны быть назначены роли. Просто при SSO задание пароля учетной записи администратора становится необязательным, если указанный пользователь будет использовать для входа только SSO.

Для настройки режима входа в консоль управления с помощью SSO необходимо:

- В настройках внешнего поставщика идентификации (SSO) зарегистрировать приложение. В разрешенные префиксы возврата (`redirect_uri`) нужно, чтобы был прописан домен установки Blitz Identity Provider. По итогам регистрации получить `client_id` и `client_secret` приложения для консоли управления;
- в конфигурационном файле `console.conf` создать блок настроек `login` следующего содержания:

```
{  
  "login" : {  
    "fp" : {  
      "authUri" : "https://idp-host.com/blitz/oauth/ae",  
      "clientId" : "blitz-console",  
      "clientSecret" : "client_secret_value",  
      "logoutUrl" :  
"https://idp-host.com/blitz/login/logout?post_logout_redirect_uri=https://idp-host.com/blitz/console",  
      "scopes" : [  

```

```
"openid"  
  ],  
  "subjectClaim" : "sub",  
  "tokenUri" : "https://idp-host.com/blitz/oauth/te"  
  },  
  "mode" : "sso"  
  }  
}
```

Необходимо уточнить параметры:

- В параметрах `authUri` и `tokenUri` нужно указать адреса Authorization Endpoint и Token Endpoint обработчиков внешнего поставщика идентификации.
- В параметрах `clientId` и `clientSecret` указать значения `client_id` и `client_secret`, присвоенный зарегистрированному во внешнем поставщике идентификации приложению, соответствующему консоли управления.
- В параметре `logoutUrl` прописать ссылку, на которую должен перенаправляться пользователь при выходе из консоли управления, чтобы был произведен единый выход через внешний поставщик идентификации.
- В параметре `scopes` прописать список разрешений, который должны быть запрошены (минимально необходимо только разрешение `openid`).
- В `subjectClaim` указать имя атрибута из маркера идентификации (`id_token`), используемого в качестве идентификатора учетной записи. Именно с таким идентификатором должна быть создана учетная запись в разделе «Администраторы» консоли управления, чтобы администратор мог войти в консоль управления.
- В параметре `mode` нужно указать требуемый режим страницы входа: `sso` – вход только через внешний поставщик идентификации (Рисунок 127); `credentials` – вход только по логину и паролю из настроек консоли управления (Рисунок 3); если параметр не задан, то доступны оба варианта на выбор пользователя (Рисунок 128).

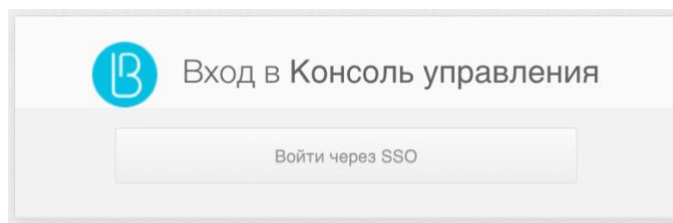


Рисунок 127 – Окно входа в консоль при включенном режиме SSO

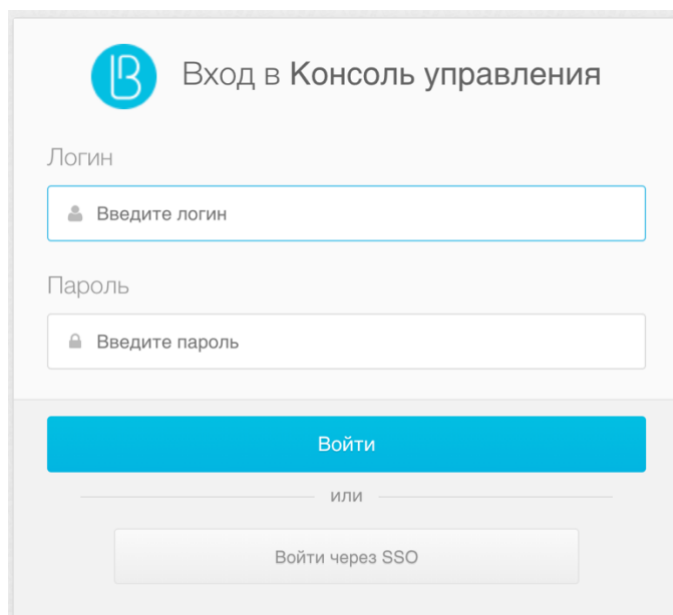


Рисунок 128 – Окно входа в консоль при всех включенных режимах входа

Чтобы не показывался промежуточный экран входа, в котором пользователь нажимает кнопку «Войти через SSO», можно вызывать консоль управления с помощью ссылки следующего вида: `https://hostname:port/blitz/console?mode=SSO`.

15.3.2. Ограничение сессий

По политике безопасности может требоваться, чтобы пользователь или администратор одновременно не мог быть залогинен с нескольких устройств. Для удовлетворения такой политики безопасности при доступе администратора в консоль управления необходимо в конфигурационном файле `console.conf` добавить блок `session`:

```
"session" : {  
  "mode" : "exclusive",  
  "check-interval" : 10  
}
```

При наличии такой настройки в случае, если будет зафиксирован вход администратора с учетной записью, которой уже выполнен вход, то в прежнем входе при любом действии в консоли управления будет отображена страница входа. Настройка `check-interval` (задается в секундах) указывает в секундах период, как быстро в прежней сессии произойдет выход при появлении новой сессии.

Если по политике безопасности требуется также запретить наличие нескольких сессий для обычных пользователей, то такой режим можно включить избирательно для определенных пользователей при входе в определенные приложения. Это выполняется с помощью настройки процедуры входа (см. п. б). Также может требоваться ограничить вход временных учетных записей после истечения срока их действия. Пример процедуры входа, реализующей обе политики, приведен ниже:

```
@Override public StrategyBeginState begin(final Context ctx) {  
  if ("login".equals(ctx.prompt())) {
```

```

List<String> methods = new ArrayList<String>(Arrays.asList(ctx.availableMethods()));
methods.remove("cls");
return StrategyState.MORE(methods.toArray(new String[0]), true);
} else {
if(ctx.claims("subjectId") != null)
return StrategyState.ENOUGH();
else
return StrategyState.MORE(new String[]{});
}
}

@Override public StrategyState next(final Context ctx) {
/*закомментировать следующий if, если временные учетные записи не используются*/
if (ctx.claims("valid until") != null && isExpired(ctx.claims("valid until")))
return StrategyState.DENY("account expired", true);
String reqFactor = ctx.userProps("requiredFactor");
if(reqFactor == null || Integer.valueOf(reqFactor) == ctx.justCompletedFactor())
/* раскомментировать этот блок и закомментировать следующий, если нужна мультисессионность
return StrategyState.ENOUGH();*/
return StrategyState.ENOUGH_BUILDER().withClaims(ctx.claimsBuilder().addClaim("__touch_crid",
true).build()).build();
else
return StrategyState.MORE(new String[]{});
}

public static boolean isExpired(String strData) {
try {
Date now = new Date();
Date date = new SimpleDateFormat("yyyy-M-d").parse(strData);
return now.after(date);
} catch (ParseException e) {
throw new RuntimeException(e);
}
}
}

```

Дополнительно в веб-приложении «Личный кабинет» нужно включить настройку, согласно которой будет происходить досрочный выход из веб-приложения в случае, если учетная запись пользователя заблокирована или была нарушена политика, запрещающая множественный вход пользователя. В конфигурационный файл `blitz.conf` в блок настроек `blitz.prod.local.idp.user-profile` нужно добавить настройку `check-session-interval`, задающую период проверки веб-приложением активности сессии:

```

"user-profile" : {
  "check-session-interval" : 10,
  ...
}

```

15.3.3. Настройка ролей и прав доступа в консоль управления.

Стандартные роли администраторов описаны в п. 2.11. В конфигурационном файле `credentials` можно создать дополнительные роли администраторов или исправить права доступа в существующих ролях. Для этого в блоке `roles` нужно скорректировать состав прав доступа (`privileges`), соответствующих роли (`name`). Пример настройки:

```

"roles" : [
{
  "name" : "new-role",
  "privileges" : ["w_app", "w_system", "w_ui", "w_user", "w_admin", "r_audit"]
}
]

```

В случае создания новых ролей для них также нужно определить текстовые строки с названием ролей (см. п. 15.2). Пример текстовой строки для новой роли `new_role`:

```
page.admins.role.new-role=имя новой роли
```

Список доступных прав доступа для заполнения настройки **privileges** приведен в таблице 12:

Таблица 12

Права доступа консоли управления Blitz Identity Provider

Право доступа	Доступные разделы консоли управления
w_app	«Приложения»
w_system	«Источники данных», «Аутентификация», «Процедуры входа», «Поставщики идентификации», «SAML», «OAuth 2.0», «Устройства», «Сообщения»
w_ui	«Сервисы самообслуживания», «Внешний вид»
w_admin	«Администраторы», «События»
w_user	«Пользователи», «Группы»
r_user	«Пользователи» (только просмотр), «Группы» (только просмотр)
r_audit	«События» (только просмотр)

16. Решение проблем

Логи работы Blitz Identity Provider записываются в директорию `/var/log/identityblitz` на каждом сервере. Журнал событий каждого приложения называется в соответствии с приложением:

- `blitz-console.log` – журнал событий консоли управления;
- `blitz-idp.log` – журнал событий сервиса аутентификации.
- `blitz-registration.log` – журнал событий сервиса регистрации;
- `blitz-recovery.log` – журнал событий сервиса восстановления доступа;
- `blitz-keeper.log` – журнал событий шлюза безопасности.

При возникновении ошибок, связанных с работой Blitz Identity Provider (записываются в лог как `[ERROR]`), рекомендуется обратиться в техническую поддержку Blitz Identity Provider по адресу `support@reaxoft.ru`.

При необходимости повысить уровень логирования необходимо в конфигурационном файле `/usr/share/identityblitz/blitz-config/blitz.conf` в блоке `logger` изменить уровни логирования.

По умолчанию все уровни логирования выставлены в `INFO`:

```
"levels" : {
  "ROOT" : "INFO",
  "application" : "INFO",
  "com.couchbase.client" : "INFO",
  "com.identityblitz" : "INFO",
  "com.identityblitz.idp" : "INFO",
  "com.identityblitz.idp.events" : "INFO",
  "com.identityblitz.idp.flow.dynamic" : "INFO",
  "com.identityblitz.idp.flow.dynamic.extend" : "INFO",
  "com.identityblitz.idp.rabbitmq" : "INFO",
  "com.identityblitz.idp.task.processing" : "INFO",
  "com.identityblitz.login-framework" : "INFO",
  "com.identityblitz.login-framework.ldap-timings" : "INFO",
  "com.identityblitz.login.store" : "INFO",
  "com.identityblitz.play.memcached" : "INFO",
  "com.identityblitz.play.memcached.RefreshableMemcachedConnection" : "INFO",
  "com.unboundid.ldap.sdk" : "INFO",
  "org.asynchttpclient.netty" : "INFO",
  "org.opensaml" : "INFO",
  "org.opensaml.util.resource" : "INFO",
  "play" : "INFO",
  "plugin.memcached" : "INFO"
}
```

Для повышения уровня логирования необходимо параметрам `ROOT` и всем `com.identityblitz.*` присвоить значение `TRACE`.

В случае если случайно было произведено изменение конфигурации Blitz Identity Provider в консоли управления, то в скрытой директории `/usr/share/identityblitz/blitz-config/.snapshot` сохранились предыдущие версии конфигурационных файлов `blitz.conf` и `console.conf`. Можно использовать эти файлы для отката к предыдущей конфигурации или для определения отличий с текущими конфигурационными файлами.

Чтобы узнать, в какое время и кем был изменен конфигурационный файл, в начало

конфигурационных файлов blitz.conf и console.conf помещаются комментарии с указанием времени редактирования и автора изменений. Пример записи аудита изменения конфигурационного файла приведен ниже:

```
#####  
# modified: 2021-05-09 20:55:55 MSK  
# author: admin  
# ip: 0:0:0:0:0:0:1  
# user agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0  
#####
```

Приложение 1. Функциональная спецификация Blitz Identity Provider

Группа функций	Функция	Доступность функции в редакции		
		Standard	Enterprise	Ultimate
Технологии единого входа				
OpenID Connect и OAuth 2.0	RFC 6749 "The OAuth 2.0 Authorization Framework"	да	да	да
	OpenID Connect Core 1.0	да	да	да
	Передача атрибутов пользователя в составе id_token/access_token в JSON Web Token (JWT)	да	да	да
	Конфигурируемый REST-сервис UserInfo, настройка возвращаемых атрибутов в зависимости от scope	да	да	да
	RFC 7636 "Proof Key for Code Exchange by OAuth Public Clients"	да	да	да
	RFC 7662 "OAuth 2.0 Token Introspection"	да	да	да
	RFC 7591 "OAuth 2.0 Dynamic Client Registration Protocol"	нет	да	да
	RFC 7592 "OAuth 2.0 Dynamic Client Registration Management Protocol"	нет	да	да
	RFC 8252 "OAuth 2.0 for Native Apps"	нет	да	да
	RFC 8414 "OAuth 2.0 Authorization Server Metadata"	да	да	да
RFC 8693 "OAuth 2.0 Token Exchange" с проверкой правил доступа	нет	нет	да	
SAML	SAML Web Browser SSO Profile	да	да	да
	SAML Single Logout Profile	да	да	да
WS-Federation	WS-Federation (для подключения Microsoft-приложений)	да	да	да
Proxy SSO	Подключения веб-приложений, получающих состояние сессии из HTTP-заголовков и cookies	нет	нет	да
	Поддержка возможности заполнения за пользователя логина/пароля от учетной записи в размещенное за проху веб-приложение, не поддерживающее стандартным образом подключения к SSO	нет	нет	да
	Обеспечение контроля доступа к REST-сервисам через Blitz Keeper (API Security Gateway)	нет	нет	да
Другое	Единый вход работает между приложениями, которые подключены к IDP с использованием любых поддерживаемых технологий (например, SSO между OpenID Connect и SAML-приложениями)	да	да	да
	Поддержка SSO-входа с использованием Kerberos SSO	да	да	да
	Поддержка единого SSO с приложениями IBM, использующими для единого входа Ltpa2Token	нет	нет	да
Идентификация и аутентификация пользователей				
Вход по логину и паролю	Проверка логина/пароля при аутентификации	да	да	да
	Возможность в качестве логина одновременно использовать несколько сущностей (телефон, email, логин) и вводить логин в разных форматах (например, вводить телефон как +7..., 8..., с разным вариантом ввода скобок, дефисов, пробелов)	да	да	да
	Запоминание логина, если пользователь ранее уже входил с этого устройства	да	да	да
	Обработка события «пароль требует смены» при входе. Возможности сменить пароль в момент входа	да	да	да
	Проверка соответствия пароля действующей парольной политике при входе. Рекомендация сменить пароль	да	да	да
	Встроенная защита от подбора пароля (перебор паролей на одну учетную запись) и подбора логина (попытка подбора пароля на набор учетных записей):	нет	да	да
	– проверка CAPTCHA;	нет	да	да
	– временное блокирование входа по паролю учетной записи при выявленных попытках перебора	нет	да	да
	– замедление входа пользователя	нет	да	да
Предупреждение пользователя о попытке входа с паролем, который был недавно изменен	да	да	да	

Сервер аутентификации Blitz Identity Provider. Руководство администратора

Вход на основе сеанса ОС	Идентификация пользователя на основе результата входа в домен (Kerberos)	да	да	да
	Возможность подключения системы входа одновременно к нескольким доменам и обеспечения сквозного входа пользователей из разных доменов	нет	да	да
	Возможность настройки, чтобы режим входа на основе сеанса ОС применялся только при входе из внутренних сетей и с ПК, но не применялся при входе с мобильных приложений и из вне рабочей сети	нет	да	да
Вход через аккаунт социальной сети / стороннего поставщика идентификации	Социальные сети и внешние поставщики идентификации, через которые поддерживается возможность входа пользователей без необходимости доработок и написания коннекторов	Facebook, Google, Mail ID, VK, Одноклассники, Яндекс		
	Вход через ЕСИА в режиме физического лица	нет	да	да
	Вход через ЕСИА в режиме представителя организации (с выбором организации при входе)	нет	нет	да
	Вход через Сбер ID	нет	нет	да
	Вход через Mos ID (СУДИР)	нет	да	да
	Сопоставление/регистрация учетной записи в процессе первичного входа через социальную сеть	да	да	да
	Возможность привязки к одной учетной записи пользователя одновременно нескольких учетных записей социальных сетей	да	да	да
Вход на основе запомненного устройства	Автоматическая идентификация пользователя, если он уже входил с этого устройства и согласился запомнить свой вход	да	да	да
	Возможность пользователю отследить, на каких устройствах запомнен вход, и выйти с этих устройств	да	да	да
	Автоматический выход с запомненных устройств при смене/восстановлении пароля пользователем	да	да	да
Вход с помощью смарт-карты / USB-ключа	Вход с помощью средств квалифицированной электронной подписи	нет	да	да
	Поддерживаемые средства электронной подписи: КриптоПро CSP 3.9 и выше, VipNet CSP 4.2, Signal-COM CSP 3.0, Рутокен, JaCarta, ISBC ESMART, SafeNet eToken	нет	да	да
	Поддерживаемые пользовательские ОС: Windows 7/8.1/10, macOS 10.13/10.14/10.15/11.3, Linux Debian 9, Mint 19, Ubuntu 18	нет	да	да
	Поддерживаемые браузеры: Internet Explorer 11, Chrome, Firefox, Yandex, Спутник	нет	да	да
	Возможность сопоставления/регистрации учетных записей в процессе первичного входа на основе данных из сертификата квалифицированной электронной подписи	нет	да	да
	Возможность проверки действительности подписи/сертификата встроенными возможностями ПО	нет	да	да
	Возможность проверки действительности подписи/сертификата через вызов внешнего сервиса проверки	нет	да	да
Двухфакторная аутентификация	Подтверждение входа разовым паролем из SMS (SMS-шлюз предоставляет Заказчик)	да	да	да
	Подтверждение входа разовым паролем из email	да	да	да
	Подтверждение входа разовым паролем TOTP-приложения (RFC 6238 "TOTP: Time-Based One-Time Password Algorithm")	да	да	да
	Подтверждение входа разовым паролем из аппаратного брелока. Поддержка брелоков HOTP (RFC 4226 "HOTP: An HMAC-Based One-Time Password Algorithm"). Брелоки предоставляет Заказчик.	нет	да	да
	Подтверждения входа разовым паролем в push-уведомлении в мобильном приложении Заказчика (сервис для отправки push и мобильное приложение предоставляет Заказчик)	нет	нет	да
Другое	Возможность Заказчику самостоятельно добавить собственный метод аутентификации	нет	да	да
	Возможность Заказчику настроить вызов вспомогательного внешнего приложения, вызываемого в процессе входа, и выполняющего взаимодействие с пользователем в процессе входа	нет	да	да
	Возможность Заказчику самостоятельно настроить внешний вид страницы входа отдельно для каждого приложения, в которое осуществляется вход	да	да	да
	Предоставление API, позволяющее мобильным приложениям зарегистрировать событие входа и получить маркеры безопасности при входах с использованием ПИН-кода, Touch ID, Face ID	нет	да	да
	Блокирование учетных записей в случае длительной неактивности	нет	да	да
	Запрет на повторное использование идентификатора удаленной учетной записи в течение установленного времени	нет	да	да

Сервер аутентификации Blitz Identity Provider. Руководство администратора

Логаут				
	Завершение пользовательской сессии при инициировании логаута пользователем	да	да	да
	Завершение пользовательской сессии при смене пароля пользователя в другой сессии или при сбросе/восстановлении пароля пользователю	да	да	да
	Ограничение допустимых ссылок для возврата в приложение после успешного логаута	да	да	да
Возможности пользователя по управлению своей учетной записью				
Регистрация	Настраиваемое веб-приложение самостоятельной регистрации пользователей. Можно настроить набор атрибутов, заполняемых пользователем при регистрации, требования к подтверждению email/телефона, настроить внешний вид страницы регистрации, вызов сервисов проверки Заказчика	да	да	да
	Можно задать различные настройки веб-приложения самостоятельной регистрации пользователя для различных сценариев вызова регистрации	нет	да	да
	Возможность вызова внешнего приложения регистрации с передачей ему контекста входа и сведений, полученных из внешнего поставщика (ЕСИА или соц.сети) в процессе входа	нет	да	да
	По результатам успешной регистрации пользователь автоматически входит в приложение, при попытке входа в которое изначально была инициирована регистрация	да	да	да
Настройки безопасности учетной записи	Веб-приложение, позволяющее пользователю управлять настройками безопасности его учетной записи:	да	да	да
	– возможность самостоятельно сменить пароль	да	да	да
	– возможность редактирования некоторых атрибутов. В т.ч. возможность редактирования телефона с подтверждением через код по SMS и возможность редактирования email с подтверждением через код/ссылку по email	да	да	да
	– возможность настроить двухфакторную аутентификацию для своей учетной записи	да	да	да
	– возможность посмотреть/отредактировать список запомненных устройств, привязанных учетных записей внешних поставщиков входа	да	да	да
	– возможность посмотреть события безопасности со своей учетной записью	да	да	да
	предоставление API для возможности встраивания всех вышеперечисленных функций управления настройками безопасности учетной записи в стороннее веб-приложение	нет	да	да
Восстановление забытого пароля	Веб-приложения, позволяющего восстановить забытый пароль, с подтверждением email или телефона	да	да	да
	По результатам успешного восстановления пароля пользователь автоматически входит в приложение, при попытке входа в которое изначально была инициирована процедура восстановления	да	да	да
Парольные политики	Проверка пароля на соответствие парольной политике: минимальная длина, требования к алфавиту, запрет словарных паролей, запрет повтора паролей, проверка срока действия паролей	да	да	да
Мониторинг и аудит				
Оповещения пользователей о событиях безопасности	Оповещение пользователей о событиях безопасности с их учетными записями: вход с необычного устройства, изменение пароля (сам сменил, администратор сбросил, смена в результате восстановления пароля), привязка учетной записи социальной сети, включение/выключение двухфакторной аутентификации	да	да	да
	Возможность настроить набор событий оповещения и тексты оповещений для SMS и для email	да	да	да
Регистрация событий безопасности	Регистрация успешных и неуспешных событий безопасности с учетной записью: события входа, регистрации, изменения настроек безопасности, восстановления пароля. Должны регистрироваться как действия, инициированные пользователем, так и действия, инициированные администратором	да	да	да
	Интерфейс администратора для поиска/просмотра событий безопасности	да	да	да
Мониторинг	Возможность в момент входа пользователя вызывать системы сбора метрик и статистики, антифрод системы	нет	да	да
	Возможность осуществлять мониторинг компонент из внешней системы мониторинга (Zabbix и аналоги)	нет	да	да
Очереди	Возможность передавать в очередь RabbitMQ события, связанные с учетными записями пользователей и групп доступа	нет	да	да

Администрирование				
	Веб-приложение администрирования:	да	да	да
	– задание настроек подключенных приложений (параметры приложений, разрешенные режимы взаимодействия)	да	да	да
	– настройка атрибутов пользователей и сопоставление атрибутов хранилищ учетных записей	да	да	да
	– настройка подключения к хранилищам учетных записей на основе LDAP	да	да	да
	– настройка подключения к произвольным хранилищам (через предоставленный Заказчиком сервис)	нет	да	да
	– поддержка работы одновременно с несколькими хранилищами учетных записей	нет	да	да
	– настройка методов идентификации/аутентификации и внешних поставщиков входа	да	да	да
	– настройка подключения к SMTP-службе и к SMS-шлюзу	да	да	да
	– поддержка ролевого доступа для входа в веб-приложение администратора. Возможность для разных пользователей задать разный набор доступных действий	нет	да	да
	– управление настройками веб-приложений регистрации, управления настройками безопасности, восстановления пароля	да	да	да
	– администрирование учетных записей пользователей (поиск, просмотр, управление атрибутами, настройками двухфакторной аутентификации, привязками запомненных устройств и социальных сетей, сброс пароля, блокирование/разблокирование учетной записи)	да	да	да
	– администрирование групп пользователей, управления членством пользователей в группах	нет	да	да
	– настройка внешнего вида страниц входа в приложения	да	да	да
	– просмотр и фильтрация зарегистрированных событий безопасности	да	да	да
	– возможность входа в веб-приложение администрирования через SSO	нет	да	да
	Интерфейс администратора на русском и английском языках	да	да	да
	Возможность добавления переводов на дополнительные языки	да	да	да

Приложение 2. Рекомендации по обеспечению мер защиты информации согласно требованиям ФСТЭК

Условное обозначение и номер меры	Мера защиты информации в информационных системах	Рекомендации по настройке
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Настроить методы аутентификации пользователей, см. п. 4. Для администраторов консоли управления настроить вход через Blitz (см. п. 15.3.1). Настроить через процедуры входа для администраторов и пользователей требования к прохождению двухфакторной аутентификации (см. п. 6) Задать для подключаемых приложений client_id и client_secret (см. п. 5)
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Задать атрибут, который будет использоваться в качестве идентификатора учетной записи (см. п. 3.1.5). Настроить запрет на повторное использование идентификатора после удаления учетной записи (см. 15.1.13) и блокирование неактивных учетных записей (см. 15.1.12)
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Установить парольную политику (см. п. 15.1.1). Управлять учетными записями пользователей (см. п. 9).
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Специальная настройка не требуется
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Настроить вход через внешние поставщики идентификации (см. п. 8.7, п. 8.9, п. 8.10)
Управление доступом субъектов доступа к объектам доступа		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	При необходимости разделения учетных записей на внешние и внутренние завести атрибут с типом учетной записи (см. п. 3) и настроить политику доступа пользователей в приложения (см. п. 6). Для временных учетных записей настроить правила блокирования входа по истечению срока действия записей (см. п. 15.3.2). Для использования функций работы с группами пользователей настроить группы пользователей (см. п. 15.1.14). Управлять учетными записями через консоль управления (см. п. 9)
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Настроить права доступа (см. п. 15.1.10), разрешения (см. п. 5.3.2), установить разрешения приложений (см. п. 5.3.1), настроить шлюз безопасности (см. п. 14), настроить атрибуты пользователей (см. п. 3) и группы пользователей (см. п. 15.1.14), процедуры входа в приложения (см. п. 6).

Сервер аутентификации Blitz Identity Provider. Руководство администратора

УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Использовать сервисы изменения атрибутов, включения и исключения пользователей в группы, назначения и отзыва прав доступа (см. «Руководство по интеграции»)
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Назначать роли администраторов (см. п. 2.11), управлять атрибутами пользователей (см. п. 9), назначать права доступа с использованием сервисов (см. «Руководство по интеграции»)
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Настроить политику ограничения числа попыток входа с последующим блокированием учетной записи (см. п. 4.1)
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации	Настроить для приложений экран согласия пользователя (см. п. 5.3.1, п. 5.3.2, п. 15.2)
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему	Настроить доступ к аудиту по себе для пользователей (см. п. 7.2.2)
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	Настроить политику ограничения числа параллельных сеансов (см. п. 15.3.2)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Настроить период неактивности (см. п. 4)
Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Специальная настройка не требуется
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Специальная настройка не требуется
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11)
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	Просматривать журналы событий на предмет возникновения ошибок (см. п. 16)
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11)
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	При установке ПО сконфигурировать использование сервиса точного времени (NTP)
РСБ.7	Защита информации о событиях безопасности	Настроить резервное копирование СУБД (см. п. 2.3)
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11)