

**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«BLITZ IDENTITY PROVIDER»**

Версия 5.11.3

РУКОВОДСТВО АДМИНИСТРАТОРА

1147746651733.62.01.000.001.И1

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	7
1. ПОДГОТОВКА К УСТАНОВКЕ	8
1.1. МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К РАЗВЕРТЫВАНИЮ	8
1.2. РЕКОМЕНДУЕМЫЕ ТРЕБОВАНИЯ К РАЗВЕРТЫВАНИЮ В КЛАСТЕРЕ	10
2. УСТАНОВКА	13
2.1. ОБЩАЯ ИНСТРУКЦИЯ ПО УСТАНОВКЕ	13
2.1.1. Установка JDK	13
2.1.2. Установка memcached	15
2.1.3. Установка и настройка СУБД	15
2.1.4. Установка и настройка сервера очередей RabbitMQ	18
2.1.5. Установка приложений Blitz Identity Provider	19
2.1.6. Настройка опций запуска приложений Blitz Identity Provider	23
2.1.7. Настройка синхронизации файлов конфигурации	25
2.1.8. Настройка веб-сервера	27
2.1.9. Установка и настройка LDAP-каталога	28
2.1.10. Вход в консоль управления	29
2.1.11. Установка лицензионного ключа	30
2.1.12. Управление учетными записями администраторов	31
2.1.13. Перезапуск приложений Blitz Identity Provider	32
2.2. ЭКСПРЕСС-ИНСТРУКЦИИ ПО УСТАНОВКЕ	32
2.2.1. Astra Linux Special Edition 1.7 вариант «Орел»	33
2.2.2. Альт 8 СП Сервер	35
2.2.3. Альт Сервер 10	38
2.2.4. ОСнова 2.5.1	40
2.2.5. Red OS 7.3	43
2.2.6. Rocky Linux 8	45
2.2.7. Rocky Linux 9	48
3. НАСТРОЙКА АТТРИБУТОВ УЧЕТНЫХ ЗАПИСЕЙ	52
3.1. КОНФИГУРИРОВАНИЕ ДОСТУПНЫХ АТТРИБУТОВ	52
3.1.1. Настройка хранимых атрибутов	52
3.1.2. Настройка вычисляемых атрибутов	54
3.1.3. Настройка правил преобразования входных значений	55
3.1.4. Настройка правил преобразования выходных значений	56
3.1.5. Настройка назначения атрибутов	56
3.2. ПОДКЛЮЧЕНИЕ ХРАНИЛИЩ АТТРИБУТОВ	58
3.2.1. Типы хранилищ	58
3.2.2. Подключение хранилища по протоколу LDAP	59
3.2.3. Подключение к хранилищу по REST	63
3.2.4. Настройка внутреннего хранилища	70
4. НАСТРОЙКИ АУТЕНТИФИКАЦИИ	71
4.1. НАСТРОЙКА ПАРОЛЬНОЙ ПОЛИТИКИ	72
4.2. НАСТРОЙКА ДОСТУПНЫХ МЕТОДОВ АУТЕНТИФИКАЦИИ	73
4.3. НАСТРОЙКА ВХОДА ПО ЛОГИНУ И ПАРОЛЮ	75
4.4. НАСТРОЙКА ВХОДА С ПОМОЩЬЮ СРЕДСТВА ЭЛЕКТРОННОЙ ПОДПИСИ	80
4.4.1. Настройка метода аутентификации в консоли управления	80
4.4.2. Использование и обновление плагина	82
4.5. НАСТРОЙКА ВХОДА ЧЕРЕЗ ВНЕШНИЕ СЕРВИСЫ ИДЕНТИФИКАЦИИ	82

4.6.	НАСТРОЙКА ВХОДА С ПОМОЩЬЮ ПРОКСИ-АУТЕНТИФИКАЦИИ	83
4.7.	НАСТРОЙКА ВХОДА С ПОМОЩЬЮ СЕАНСА ОПЕРАЦИОННОЙ СИСТЕМЫ	84
4.7.1.	Настройки контроллера домена (Kerberos-сервера)	85
4.7.2.	Настройки в консоли управления Blitz Identity Provider	87
4.7.3.	Настройки браузеров пользователей	89
4.7.4.	Настройки запуска приложений Blitz Identity Provider	91
4.7.5.	Настройки веб-сервера	91
4.7.6.	Отладка проблем с входом по сеансу операционной системы	91
4.8.	НАСТРОЙКА ВХОДА С ПОМОЩЬЮ КОДОВ ПОДТВЕРЖДЕНИЯ	92
4.9.	НАСТРОЙКА ВХОДА С ИЗВЕСТНОГО УСТРОЙСТВА	94
4.10.	Вход по РАЗОВОЙ ССЫЛКЕ	94
4.11.	Вход по QR-КОДУ	95
4.12.	Вход с помощью ключей БЕЗОПАСНОСТИ (WebAuthn, Passkey, FIDO2)	96
4.13.	ПОДТВЕРЖДЕНИЕ ВХОДА РАЗОВЫМ ПАРОЛЕМ НА ОСНОВЕ СОСТОЯНИЯ (HOTP)	98
4.14.	ПОДТВЕРЖДЕНИЕ ВХОДА РАЗОВЫМ ПАРОЛЕМ ОСНОВЕ ВРЕМЕНИ (TOTP)	100
4.15.	ПРИВЯЗКА УСТРОЙСТВ К УЧЕТНЫМ ЗАПИСЯМ ПОЛЬЗОВАТЕЛЕЙ	101
4.15.1.	Привязка аппаратных брелоков	101
4.15.2.	Привязка мобильного приложения	103
4.16.	Коды подтверждения, отправляемые в SMS и PUSH-УВЕДОМЛЕНИЯХ	104
4.17.	Коды подтверждения, отправляемые по ЭЛЕКТРОННОЙ ПОЧТЕ	105
4.18.	ПОДТВЕРЖДЕНИЕ ВХОДА С ПОМОЩЬЮ DUO MOBILE	106
4.19.	ПОВТОРНОЕ ПОДТВЕРЖДЕНИЕ ПРИ ВХОДЕ С ИЗВЕСТНОГО УСТРОЙСТВА	110
4.20.	ПОДТВЕРЖДЕНИЕ ВХОДА С ПОМОЩЬЮ КЛЮЧЕЙ БЕЗОПАСНОСТИ (WebAuthn, Passkey, FIDO2, U2F) ...	110
4.21.	НАСТРОЙКА ВНЕШНЕГО МЕТОДА АУТЕНТИФИКАЦИИ	111
5.	РЕГИСТРАЦИЯ ПРИЛОЖЕНИЙ	114
5.1.	СОЗДАНИЕ УЧЕТНОЙ ЗАПИСИ НОВОГО ПРИЛОЖЕНИЯ	114
5.2.	НАСТРОЙКА SAML И WS-FEDERATION	118
5.2.1.	Подключение по SAML 1.0/1.1/2.0	118
5.2.2.	Подключение по WS-Federation	120
5.2.3.	Настройка SAML-атрибутов	122
5.3.	НАСТРОЙКА OAuth 2.0 И OPENID CONNECT 1.0	123
5.3.1.	Настройка приложения	123
5.3.2.	Общие настройки OAuth 2.0	128
5.3.3.	Добавление атрибутов в маркер идентификации	131
5.3.4.	Настройка динамической регистрации клиентов OAuth 2.0	134
5.4.	НАСТРОЙКА SIMPLE	136
5.5.	НАСТРОЙКА КЛИЕНТА REST-СЕРВИСОВ BLITZ IDENTITY PROVIDER	139
6.	НАСТРОЙКА ПРОЦЕДУР ВХОДА В ПРИЛОЖЕНИЯ	141
6.1.	СОЗДАНИЕ ПРОЦЕДУР ВХОДА	141
6.2.	ПРИМЕРЫ ПРОЦЕДУР ВХОДА	143
6.2.1.	Принудительная двухфакторная аутентификация в приложение	144
6.2.2.	Ограничение перечня доступных методов первого фактора	144
6.2.3.	Разрешить вход в приложение только при определенном значении атрибута у пользователя ...	145
6.2.4.	Запрет входа в приложение после истечения срока действия учетной записи	146
6.2.5.	Разрешение входа в приложение только из определенных сетей	147
6.2.6.	Запрет работы в нескольких одновременных сессиях	148
6.2.7.	Сохранение в утверждениях (claims) перечня групп пользователя	148
6.2.8.	Отображение пользователю объявления при входе	149
6.2.9.	Запрос ввода пользователем атрибута или актуализации телефона и email	150
6.2.10.	Регистрация ключа безопасности (WebAuthn, Passkey, FIDO2) при входе	152
6.2.11.	Отображение пользователю списка выбора значений при входе	154

7.	НАСТРОЙКА СЕРВИСОВ САМООБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ.....	156
7.1.	ОБЩИЕ НАСТРОЙКИ.....	156
7.2.	РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ.....	158
7.2.1.	Форма регистрации.....	158
7.2.2.	Настройки сервиса регистрации.....	160
7.2.3.	Процедура регистрации.....	161
7.2.4.	Изменение текста условий использования.....	161
7.3.	Личный КАБИНЕТ.....	161
7.3.1.	Отображение атрибутов пользователя.....	162
7.3.2.	Дополнительные параметры.....	163
7.4.	ВОССТАНОВЛЕНИЕ ДОСТУПА.....	165
8.	ВХОД ЧЕРЕЗ ВНЕШНИЕ ПОСТАВЩИКИ ИДЕНТИФИКАЦИИ.....	167
8.1.	ВХОД ЧЕРЕЗ APPLE ID.....	167
8.2.	ВХОД ЧЕРЕЗ GOOGLE.....	173
8.3.	ВХОД ЧЕРЕЗ ЯНДЕКС.....	178
8.4.	ВХОД ЧЕРЕЗ FACEBOOK.....	182
8.5.	ВХОД ЧЕРЕЗ ВКОНТАКТЕ.....	186
8.6.	ВХОД ЧЕРЕЗ ОДНОКЛАССНИКИ.....	190
8.7.	ВХОД ЧЕРЕЗ MAIL ID.....	194
8.8.	ВХОД ЧЕРЕЗ ЕДИНУЮ СИСТЕМУ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ (ЕСИА).....	198
8.9.	ВХОД ЧЕРЕЗ ЦИФРОВОЙ ПРОФИЛЬ ЕСИА.....	204
8.10.	ВХОД ЧЕРЕЗ СИСТЕМУ ИДЕНТИФИКАЦИИ СБЕРБАНКА (СБЕР ID).....	210
8.11.	ВХОД ЧЕРЕЗ СИСТЕМУ ИДЕНТИФИКАЦИИ TINKOFF ID.....	214
8.12.	ВХОД ЧЕРЕЗ СИСТЕМУ ИДЕНТИФИКАЦИИ Mos ID (СУДИР).....	218
8.13.	ВХОД ЧЕРЕЗ ДРУГУЮ УСТАНОВКУ BLITZ IDENTITY PROVIDER.....	222
9.	УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЕЙ.....	226
9.1.	ПОИСК УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ.....	226
9.2.	ДОБАВЛЕНИЕ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ.....	227
9.3.	ПРОСМОТР И ИЗМЕНЕНИЕ АТТРИБУТОВ ПОЛЬЗОВАТЕЛЯ.....	228
9.3.1.	Редактирование атрибутов пользователя.....	229
9.3.2.	Смена пароля пользователя.....	229
9.3.3.	Просмотр и отвязка привязанных учетных записей внешних поставщиков идентификации.....	229
9.3.4.	Привязка устройств для проведения двухфакторной аутентификации по разовому паролю.....	230
9.3.5.	Привязка мобильного приложения Duo Mobile.....	231
9.3.6.	Просмотр групп, в которые включен пользователь, управление членством пользователя в группах.....	232
9.3.7.	Просмотр прав, назначение и отзыв прав.....	233
9.3.8.	Просмотр и удаление запомненных устройств и браузеров.....	235
9.3.9.	Управление ключами безопасности.....	235
9.3.10.	Просмотр и удаление выданных приложениям разрешений.....	236
10.	УПРАВЛЕНИЕ ГРУППАМИ ПОЛЬЗОВАТЕЛЕЙ.....	238
11.	УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА.....	240
12.	ПРОСМОТР СОБЫТИЙ БЕЗОПАСНОСТИ.....	241
13.	НАСТРОЙКА УВЕДОМЛЕНИЙ И ОТПРАВКИ СООБЩЕНИЙ.....	242
13.1.	Настройка подключения к SMS-шлюзу.....	243
13.2.	Настройка подключения к сервису отправки PUSH-уведомлений.....	245
13.3.	Настройка подключения к SMTP-шлюзу.....	247

14. НАСТРОЙКА ВНЕШНЕГО ВИДА СТРАНИЦЫ ВХОДА	248
14.1. РЕДАКТИРОВАНИЕ ШАБЛОНА ПО УМОЛЧАНИЮ	248
14.2. СОЗДАНИЕ И ИЗМЕНЕНИЕ НОВЫХ ШАБЛОНОВ С ПОМОЩЬЮ КОНСТРУКТОРА	251
14.3. СОЗДАНИЕ И ИЗМЕНЕНИЕ НОВЫХ ШАБЛОНОВ В РУЧНОМ РЕЖИМЕ	252
15. НАСТРОЙКИ ШЛЮЗА БЕЗОПАСНОСТИ.....	256
15.1. НАСТРОЙКА BLITZ-KEEPER	257
15.2. СОЗДАНИЕ ПРАВИЛ ДОСТУПА К СЕРВИСАМ	259
15.3. НАСТРОЙКА ПРАВИЛ ОБМЕНА МАРКЕРОВ ДОСТУПА	262
16. НАСТРОЙКИ КОНФИГУРАЦИОННЫХ ФАЙЛОВ	263
16.1. ФАЙЛ НАСТРОЕК BLITZ.CONF	263
16.1.1. Ограничение количества одновременных проверок пароля пользователя.....	264
16.1.2. Отключение функции смены пароля при входе	265
16.1.3. Настройка внешнего валидатора атрибута	265
16.1.4. Настройка транслятора атрибута.....	266
16.1.5. Настройка времени отображения экрана логаута.....	267
16.1.6. Настройка вызова внешнего сервиса проверки электронной подписи	267
16.1.7. Настройка вызова плагина электронной подписи	267
16.1.8. Настройка CAPTCHA	268
16.1.9. Настройка отправки событий в сервер очередей.....	272
16.1.10. Настройка использования сервера очередей в качестве брокера сообщений.....	274
16.1.11. Запрос проверочного атрибута при восстановлении пароля.....	275
16.1.12. Настройка хранения объектов в Couchbase Server	276
16.1.13. Настройка времени хранения объектов в базе данных.....	276
16.1.14. Настройка домена Blitz Identity Provider	277
16.1.15. Расширенные настройки подключения к хранилищам	278
16.1.16. Блокирование неактивных пользователей.....	280
16.1.17. Запрет повторного использования идентификатора удаленного пользователя.....	281
16.1.18. Настройка групп пользователей	281
16.1.19. Настройка контейнера ключей для работы с ЕСИА и Цифровым профилем.....	282
16.1.20. Вход через ЕСИА в режиме выбора сотрудника организации.....	287
16.1.21. Настройка аутентификации по ключам безопасности (WebAuthn, Passkey, FIDO2, U2F).....	291
16.1.22. Блокирование перебора кодов подтверждения.....	293
16.1.23. Включение режима запоминания множества учетных записей.....	294
16.1.24. Настройки сервиса OIDC Discovery.....	295
16.1.25. Изменение адресов вызовов внешних поставщиков идентификации.....	295
16.1.26. Настройка внешнего SAML поставщика входа.....	295
16.1.27. Настройка внешнего поставщика входа СУДИС	298
16.1.28. Включение режима регистрации незавершенных попыток входа.....	300
16.1.29. Настройка передачи событий безопасности в файл или Kafka.....	301
16.1.30. Изменение системных имен полей ввода логина и пароля	309
16.1.31. Настройка использования базы геоданных	309
16.1.32. Настройки вспомогательных приложений (pipes).....	310
16.1.33. Одновременное использование нескольких СУБД	311
16.2. НАСТРОЙКИ ТЕКСТОВ ИНТЕРФЕЙСА.....	312
16.2.1. Мультиязычность.....	312
16.2.2. Модификация текстовых сообщений веб-интерфейса	314
16.2.3. Модификация шаблонов писем и SMS-сообщений.....	314
16.2.4. Настройка логотипов кнопок входа через внешние поставщики идентификации	319
16.2.5. Модификация имен устройств и браузеров.....	319

16.2.6.	Модификация сообщений для разных приложений.....	320
16.2.7.	Настройка сообщений вспомогательных приложений (pipes)	321
16.3.	ФАЙЛЫ НАСТРОЕК КОНСОЛИ УПРАВЛЕНИЯ.....	323
16.3.1.	Настройка входа в консоль управления через SSO.....	323
16.3.2.	Ограничение сессий.....	325
16.3.3.	Настройка ролей и прав доступа в консоль управления	326
17.	РЕШЕНИЕ ПРОБЛЕМ	327
ПРИЛОЖЕНИЕ 1. ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ BLITZ IDENTITY PROVIDER		329
ПРИЛОЖЕНИЕ 2. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ МЕР ЗАЩИТЫ ИНФОРМАЦИИ СОГЛАСНО ТРЕБОВАНИЯМ ФСТЭК.....		334
ПРИЛОЖЕНИЕ 3. МЕТОДИКА ПРОВЕРКИ ОСНОВНЫХ ПАРАМЕТРОВ И ХАРАКТЕРИСТИК ПО.....		336

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, банков, Единой системы идентификации и аутентификации (ЕСИА, Госуслуги), Mos ID (СУДИР), 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 используется 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.

При работе с сертифицированной версией приемка Blitz Identity Provider осуществляется в соответствии правилами, указанными в документе 1147746651733.62.01.000.001.TU «Программное обеспечение «Blitz Identity Provider». Технические условия». Комплектность должна соответствовать комплектности, приведенной в документе 1147746651733.62.01.000.001.TU «Программное обеспечение «Blitz Identity Provider». Технические условия».

Безопасная установка и настройка Blitz Identity Provider должна осуществляться в соответствии с настоящим Руководством администратора.

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, PostgreSQL², Postgres Pro, Jatoba.
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.
5. Сервер очередей – используется RabbitMQ. Также можно настроить передачу событий безопасности в Kafka.

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.

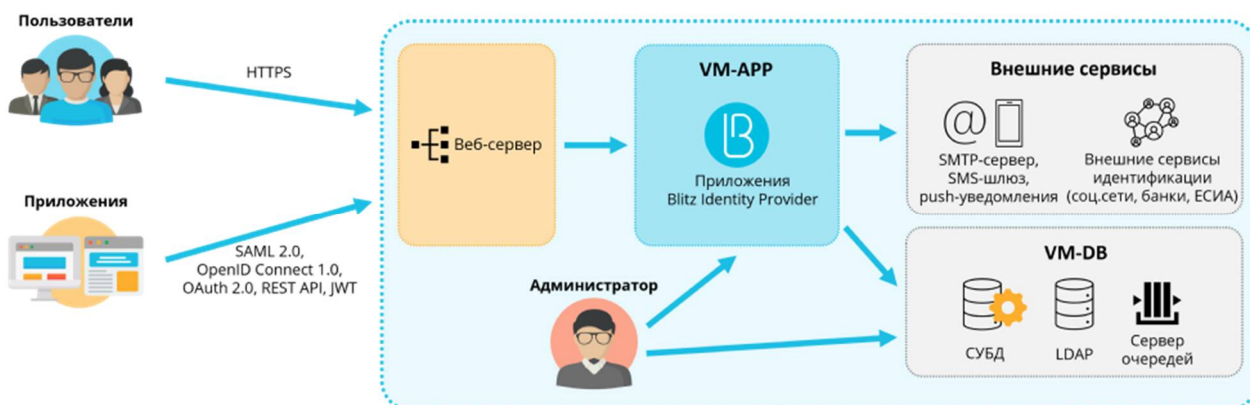


Рисунок 1 – Развертывание в минимальной конфигурации

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

² Взаимодействие Blitz Identity Provider с PostgreSQL осуществляется по JDBC. Вместо PostgreSQL можно использовать любую реляционную СУБД с поддержкой JDBC, но это должно быть отдельно согласовано с ООО «РЕАК СОФТ» в рамках соответствующих проектов внедрения.

Таблица 1

Минимальные требования к серверам для развертывания

Описание	Поддерживаемые ОС	Технические характеристики	Программное обеспечение
ВМ для приложений (VM-APP)	CentOS 7/8 Rocky Linux 8/9 RHEL 7/8	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)	Astra Linux SE 1.6/1.7 РЕД ОС 7.3 Альт Сервер 10 Альт 8 СП Сервер ОСнова 2.5.1	8 ядер ЦПУ, 16 ГБ ОЗУ, 100 ГБ НЖМД (HDD)	Couchbase Server Community Edition (6.0 или новее) или PostgreSQL (9.6 или новее), 389 Directory Server или FreeIPA, RabbitMQ (опционально)

Требуемые версии системного ПО:

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

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://appleid.apple.com>
<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 и цифровой профиль <https://esia-portal1.test.gosuslugi.ru>
<https://esia.gosuslugi.ru>
 Банки <https://online.sberbank.ru>
<https://business.tinkoff.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);
- к сервису Kafka (при его использовании для приема событий безопасности).

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 разворачиванию в кластере

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

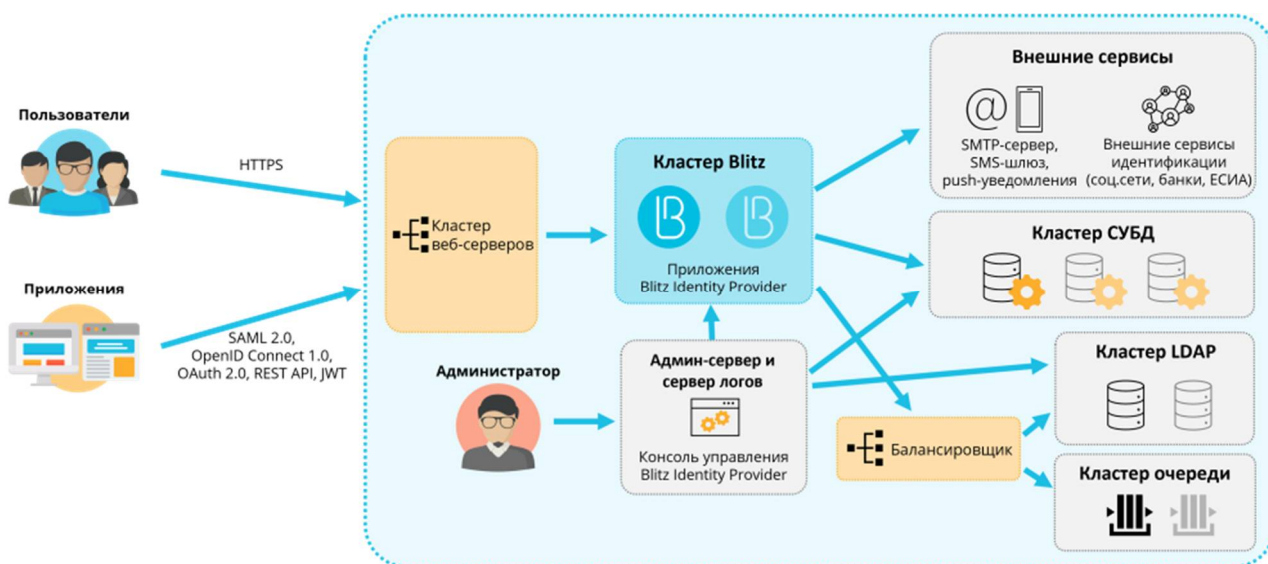


Рисунок 2 – Развертывание в кластерной конфигурации

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

Таблица 2

Рекомендуемые требования к серверам для разворачивания в кластере

Описание	Кол-во	Поддерживаемые ОС	Технические характеристики	Программное обеспечение	Комментарий
ВМ веб-серверов (VM-WEB)	1-2	CentOS 7/8 Rocky Linux 8/9 RHEL 7/8 Astra Linux SE 1.6/1.7 РЕД ОС 7.3	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
ВМ приложений Blitz Identity Provider (VM-APP)	2	Альт Сервер 10 Альт 8 СП Сервер ОСнова 2.5.1	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 разворачивать каждое приложение Blitz Identity Provider в своем кластере на отдельных серверах
ВМ 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	Поддерживаемые 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) ³	Couchbase Server Community Edition (6.0 или новее) или PostgreSQL (9.6 или новее)	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	Использование сервера очередей опционально
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, Axiom JDK 8 Certified 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:
 - 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://appleid.apple.com>
<https://accounts.google.com>

³ См.: <https://docs.couchbase.com/server/current/install/install-linux.html>

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

	https://graph.facebook.com
	https://oauth.yandex.ru
	https://oauth.vk.com
	https://account.mail.ru
	https://api.ok.ru
ЕСИА и цифровой	https://esia-portal1.test.gosuslugi.ru
профиль	https://esia.gosuslugi.ru
Банки	https://online.sberbank.ru
	https://business.tinkoff.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);
- к сервису Kafka (при его использовании для приема событий безопасности).
- 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);
 - к сервису Kafka (при его использовании для приема событий безопасности).
- 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 (опционально).
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).

В зависимости от используемой операционной системы есть своя специфика по установке необходимого окружения. Далее приводятся:

1. общая инструкция по установке на операционных системах CentOS 7, RHEL 7 и Astra Linux Special Edition 1.6 вариант «Смоленск»;
2. специализированные экспресс-инструкции по установке для следующих операционных систем с использованием СУБД PostgreSQL:
 - Astra Linux Special Edition 1.7 вариант «Орел»;
 - Альт 8 СП Сервер;
 - Альт Сервер 10;
 - ОСнова 2.5.1;
 - Red OS 7.3;
 - Rocky Linux 8;
 - Rocky Linux 9.

2.1. Общая инструкция по установке

2.1.1. 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;
- Axiom JDK 8 Certified;

- Oracle JDK 8.

При использовании сертифицированной версии Blitz Identity Provider рекомендуется использовать один из следующих JDK:

- OpenJDK 8;
- Axiom JDK 8 Certified.

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 1.6:

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

```
dpkg -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 Axiom JDK 8 Certified в Astra Linux Special Edition 1.7:

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

```
dpkg -i bellsoft-jdk-certified8u322+7-linux-amd64-astra.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 `tar`⁵;
- скопировать загруженный дистрибутив на сервера (например, в директорию `/tmp`);
- 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
```

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

Если версия Oracle JDK 1.8.0_144 и ниже:

- загрузить дистрибутив Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files ⁶;
- 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/
```

2.1.2. 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 1.6:

- выполнить команду:

```
apt-get install memcached
```

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

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

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.

2.1.3. 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.

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

- 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 отечественных операционных систем.

2.1.3.1. Установка и настройка Couchbase Server

Инструкция по установке Couchbase Server приводится для CentOS 7 и RHEL 7. В случае развертывания под отечественные операционные системы в качестве СУБД рекомендуется использовать PostgreSQL.

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

<https://docs.couchbase.com/server/current/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 находятся в директории `couchbase` в архиве `resources.zip` в составе дистрибутива Blitz Identity Provider;

⁷ См.: <https://docs.couchbase.com/server/current/manage/manage-nodes/initialize-node.html>

- 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 создастся 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-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.

2.1.3.2. Установка и настройка PostgreSQL

Версия PostgreSQL должна быть 9.6 или новее.

В случае CentOS и RHEL необходимо установить PostgreSQL согласно инструкции:

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

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

В случае Astra Linux Special Edition 1.6 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:

```
su - postgres

createdb blitzdb

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;

psql -d blitzdb -U blitz -f 000-SCRIPT000.sql
...
psql -d blitzdb -U blitz -f NNN-SCRIPTNNN.sql
```

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

вместо `000-SCRIPT000.sql` ... `NNN-SCRIPTNNN.sql` нужно вставить имена скриптов из директории `postgres/ddl` из архива `resources.zip`. Например, для релиза 5.11 это скрипты:

```
psql -d blitzdb -U blitz -f 000-service-tasks.sql
psql -d blitzdb -U blitz -f 001-init-database.sql
psql -d blitzdb -U blitz -f 002-new_pp_columns.sql
psql -d blitzdb -U blitz -f 003-usd_id_table.sql
psql -d blitzdb -U blitz -f 004-usr_auth_table.sql
psql -d blitzdb -U blitz -f 005-usr_agt_table.sql
psql -d blitzdb -U blitz -f 006-usr_htp_hmc_alg.sql
psql -d blitzdb -U blitz -f 007-usr_atr_cfm.sql
psql -d blitzdb -U blitz -f 008-wak.sql
psql -d blitzdb -U blitz -f 009-fix_pp_column.sql
psql -d blitzdb -U blitz -f 010-add_usr_prp.sql
psql -d blitzdb -U blitz -f 011-pp_audit.sql
psql -d blitzdb -U blitz -f 012-geo_to_audit.sql
psql -d blitzdb -U blitz -f 013-tasks.sql
psql -d blitzdb -U blitz -f 014-sec_ch_ua.sql
```

- настроить резервное копирование БД, используя инструкцию⁹.

2.1.4. Установка и настройка сервера очередей RabbitMQ

Установка сервера очередей RabbitMQ опциональна и требуется если сервер очередей будет использоваться для передачи событий в смежные системы (см. п. 16.1.9) или в качестве брокера сообщений (см. п. 16.1.10).

В случае CentOS и RHEL необходимо установить RabbitMQ согласно инструкции: <https://www.rabbitmq.com/install-rpm.html>.

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

В случае Astra Linux Special Edition 1.6 для установки RabbitMQ необходимо:

- выполнить команду:

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

- после завершения установки запустить сервис:

```
systemctl start rabbitmq-server
```

2.1.5. 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. 2.1.1) и memcached (см. п. 2.1.2).

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 и Axiom JDK

Certified, `/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
You can change user credentials at file - /usr/share/identityblitz/blitz-config/credentials
```

Если при запуске установщика были допущены ошибки ввода, так что установка была проведена с неправильными параметрами, то можно воспользоваться следующей командой для удаления файлов, которые создал установщик, чтобы иметь возможность вновь провести установку начисто:

```
rm -rf /usr/share/identityblitz /etc/default/blitz-* /etc/blitz-* /var/log/identityblitz/
/lib/systemd/system/blitz-*
```

- 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.stores` настройку `default-type` изменить в значение `cb`. 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"`). Номера портов в `nodes` задавать не нужно. 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. Также в настройках¹⁰ `ioConf` и `timeoutConf` скорректировать при необходимости параметры пула коннектов:

```
"internal-store-cb" : {
```

¹⁰ См.: <https://docs.couchbase.com/java-sdk/current/ref/client-settings.html>


```

"nodes" : [ CB_NODES ],
"user" : "CB_USERNAME",
"password" : "CB_PASSWORD",
"metrics": false,
"ioConf": {
    "numKvConnections": 1,
    "maxHttpConnections": 12,
    "idleHttpConnectionTimeout": 5
},
"timeoutConf": {
    "connectTimeout": 10,
    "kvTimeout": 3,
    "kvDurableTimeout": 10,
    "queryTimeout": 75
}
}

```

- в случае использования в качестве СУБД PostgreSQL проверить в блоке настроек `blitz.prod.local.idp.stores`, что настройка `default-type` имеет значение `jdbc`. 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&tcpKeepAlive=true",
    "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.net`, добавив в настройку `trustedServers` адреса подсетей серверов приложений Blitz Identity Provider:

```

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

```

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

```

"memcached" : {
    "operationTimeout" : 1000,
    "timeoutExceptionThreshold" : 1,
    "maxReconnectDelay" : 10,
    "servers" : [
        "[MEMCACHED]"
    ]
}

```

`[MEMCACHED]` – указать хост и порт службы memcached (например, `ld-s-blitz1-`

`dev.ao.company:11211")`.

Также при необходимости можно скорректировать настройки управления подключением к memcached:

- `operationTimeout` – время ожидания выполнения запроса к memcached в мс;
 - `timeoutExceptionThreshold` – количество попыток выполнения запроса, после которых узел считается не доступным;
 - `maxReconnectDelay` – интервал между попытками установить соединение с узлом в секундах.
- 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 и Axiom JDK Certified, `/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
```

2.1.6. Настройка опций запуска приложений Blitz Identity Provider

Для приложений Blitz Identity Provider доступны следующие Java-опции, определяющие включение особых режимов функционирования приложений и переопределить стандартные режимы работы:

- `blitz.login.cookie.sameSite` – задает флаг, с которым должны создаваться сессионные cookies в Blitz Identity Provider. По умолчанию cookies создаются с флагом `sameSite=Lax`. Можно переопределить на значение `None`.
- `blitz.login.outside.flow.callback.ttl.sec` – задает время ожидания ответа от вызванного из Blitz Identity Provider внешнего метода аутентификации. По умолчанию значение `300` секунд.
- `blitz.login.mus.cookie.unused.ttl.sec` – задает срок жизни cookie, отвечающей за запоминание списка залогиненных в текущем браузере пользователей. По умолчанию значение соответствует 365 дней (значение задается в секундах);
- `blitz.login.bua.cookie.ttl.sec` – задает время действия cookie, используемой для запоминания браузера пользователя. По умолчанию значение соответствует 365 дней (значение задается в секундах);
- `blitz.login.setLastAuth.disabled` – позволяет отключить запись в базу данных времени последней аутентификации пользователя. По умолчанию время последней аутентификации пользователя пишется в базу данных. Отключение записи времени последней аутентификации позволяет повысить производительность базы данных, но не позволяет задействовать функцию блокирования учетных записей по неактивности (см. п. 16.1.16);
- `blitzDispatchedQueues` – задает имя очереди, из которой приложение Blitz Identity Provider обрабатывает задачи на отправку писем, регистрацию пользователей и восстановление паролей. По умолчанию используется очередь с именем `default`;
- `blitz.stores.united.u-cache.ttlInSec` – срок действия кэша данных учетной записи, предоставляемых через REST API. По умолчанию `1` секунда;
- `blitz.csrf.cookie.ttlInSec` – задает время действия cookie, препятствующей CSRF. По умолчанию соответствует 6 часам (значение задается в секундах). Это максимальное время с момента открытия пользователем страницы и до выполнения заполненной страницы пользователем на сервер;
- `blitz.jdbc.cols.types.strings` – задает тип колонки, используемой для сохранения строковых атрибутов в реляционной СУБД (PostgreSQL). По умолчанию используется тип `text`;

- `blitz.jdbc.pool.stat-period` – задает периодичность, с которой статистика использования JDBC записывается в лог. По умолчанию 300 секунд;
- `saml.numThreads` – задает количество потоков, которые в Blitz Identity Provider обрабатывают запросы на вход через SAML. По умолчанию 32 потока;
- `blitz.oauth.exchange.rules.fs.cache.capacity` – задает размер кэша, используемый Blitz Identity Provider для проверки правил доступа к микросервисам. По умолчанию размер кэша в 10000 проверок;
- `blitz.oauth.dyn.reg.clientSecretLength` – задает размер `client_secret`, генерируемого при динамической регистрации пары `client_id` и `client_secret`. По умолчанию генерируется `client_secret` размером в 15 символов.
- `blitz.oauth.dyn.reg.clientAttachingTtlInSec` – задает время, в течение которого сгенерированная при динамической регистрации пара `client_id` и `client_secret` должна быть ассоциирована с пользователем (если в течение этого времени пара не будет ассоциирована с пользователем, то она будет аннулирована). По умолчанию соответствует 1 часу (значение задается в секундах).
- `extensionsDir` – адрес директории с модулями расширений для Blitz Identity Provider (см. п. 16.1.3).
- `couchbase.durability.mode` – задает режим сохранения данных в Couchbase Server. В случае использования Couchbase Server версии 6.0.1 и более старых должен обязательно использоваться режим `clientVerified`. В случае использования Couchbase Server версий 6.5, 7.0 или новее режим `clientVerified` использовать нельзя. Параметр в Couchbase Server версий 6.5, 7.0 становится опционален (при отсутствии параметра используется режим `majority`) и позволяет выбрать требуемый режим гарантированности сохранения данных в кластере с репликацией из следующих вариантов¹¹:
 - `disabled` – ожидание записи только в память на основном узле кластера;
 - `majority` – ожидание записи в память на основном узле и большинстве реплик;
 - `majorityAndPersistActive` – ожидание записи на диск на основном узле и записи в память большинства реплик;
 - `persistToMajority` – ожидание записи на диск на основном узле и в большинстве реплик.
- `akka.http.parsing.max-uri-length` – задает максимальную длину URI в строке браузера. В некоторых случаях может потребоваться увеличить размер строки, тогда

¹¹ См.: <https://docs.couchbase.com/server/current/learn/data/durability.html>

рекомендуется в этом параметре задать значение **16k**.

- **akka.coordinated-shutdown.phases.service-stop.timeout** – задает время ожидания после получения команды на остановку сервиса, в течение которого сервис может завершить взятые в работу задачи. В случае использования встроенного в Blitz Identity Provider брокера сообщений рекомендуется выставить для приложения параметр в значение **30s**.

Перед установкой опций рекомендуется проконсультироваться с технической поддержкой Blitz Identity Provider.

Не гарантируется, что используемые опции будут сохранены в будущих версиях Blitz Identity Provider.

Для задания опций со значениями, отличающимися от значений по умолчанию, необходимо отредактировать файл **/etc/default/blitz-idp**. Задать в нем необходимые **JAVA_OPTS**. Ниже приведен пример файла, в котором среди Java-опций также заданы опции **blitz.csrf.cookie.ttlInSec** и **blitz.login.cookie.sameSite**. После изменения **JAVA_OPTS** необходимо перезапустить приложения Blitz Identity Provider, на которых сделаны изменения.

```
export JAVA_HOME=/usr/java/default
export PIDFILE=/usr/share/identityblitz/blitz-idp/RUNNING_PID
export JAVA_OPTS="-server -Xms512m -Xmx1G -XX:MaxMetaspaceSize=512m -Xmn256m -
Dcom.couchbase.connectTimeout=30000 -Dakka.http.parsing.max-uri-length=16k"
export JAVA_OPTS="$JAVA_OPTS -Dblitz.csrf.cookie.ttlInSec=36000 -Dblitz.login.cookie.sameSite=None -
Dplay.filters.headers.frameOptions=null"
```

2.1.7. Настройка синхронизации файлов конфигурации

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

1. На сервере с консолью управления Blitz Console:

- установить **rsync** и **incron**:

```
sudo yum install rsync incron
```

или (для Astra Linux Special Edition 1.6)

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

```
/usr/share/identityblitz/blitz-config/assets/services
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh assets $# %
/usr/share/identityblitz/blitz-config/assets/themes
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh assets $# %
/usr/share/identityblitz/blitz-config/saml IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh saml $# %
/usr/share/identityblitz/blitz-config/saml/conf
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh saml $# %
/usr/share/identityblitz/blitz-config/saml/credentials
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh saml $# %
/usr/share/identityblitz/blitz-config/saml/metadata
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh saml $# %
/usr/share/identityblitz/blitz-config/custom_messages
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh custom_messages $# %
/usr/share/identityblitz/blitz-config/custom_messages/dics
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh custom_messages $# %
/usr/share/identityblitz/blitz-config/devices IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh devices $# %
/usr/share/identityblitz/blitz-config/simple IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh simple $# %
/usr/share/identityblitz/blitz-config/certs IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh certs $# %
/usr/share/identityblitz/blitz-config/flows/login
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh flows $# %
/usr/share/identityblitz/blitz-config/flows/reg
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh flows $# %
/usr/share/identityblitz/blitz-config/flows/extIdps
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh flows $# %
/usr/share/identityblitz/blitz-config/token_exchange
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh token_exchange $# %
/usr/share/identityblitz/blitz-config/token_exchange/rules
IN_MODIFY,IN_ATTRIB,IN_CREATE,IN_DELETE,IN_CLOSE_WRITE
/usr/share/identityblitz/scripts/config_sync.sh token_exchange $# %
```

- 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 узлов кластера Blitz (кроме узла консоли управления Blitz Console).

Вписывать значения нужно через пробел. Например:

```
node_list="app1.local app2.local"
```

- 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 1.6)

```
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.

2.1.8. 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`.

2.1.9. 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.

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 1.6:

- 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
```

2.1.10. 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. 2.1.5).

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:

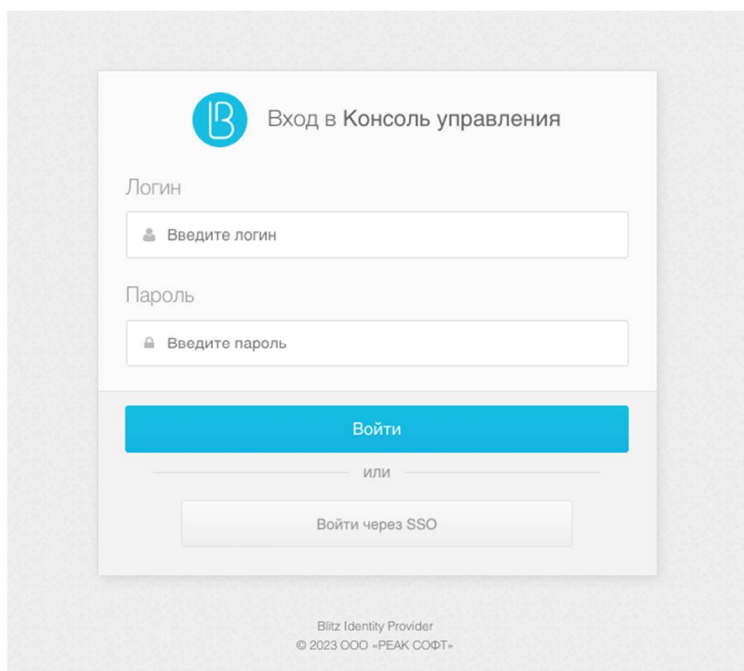


Рисунок 3 – Стандартный вид экрана входа в консоль управления

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.

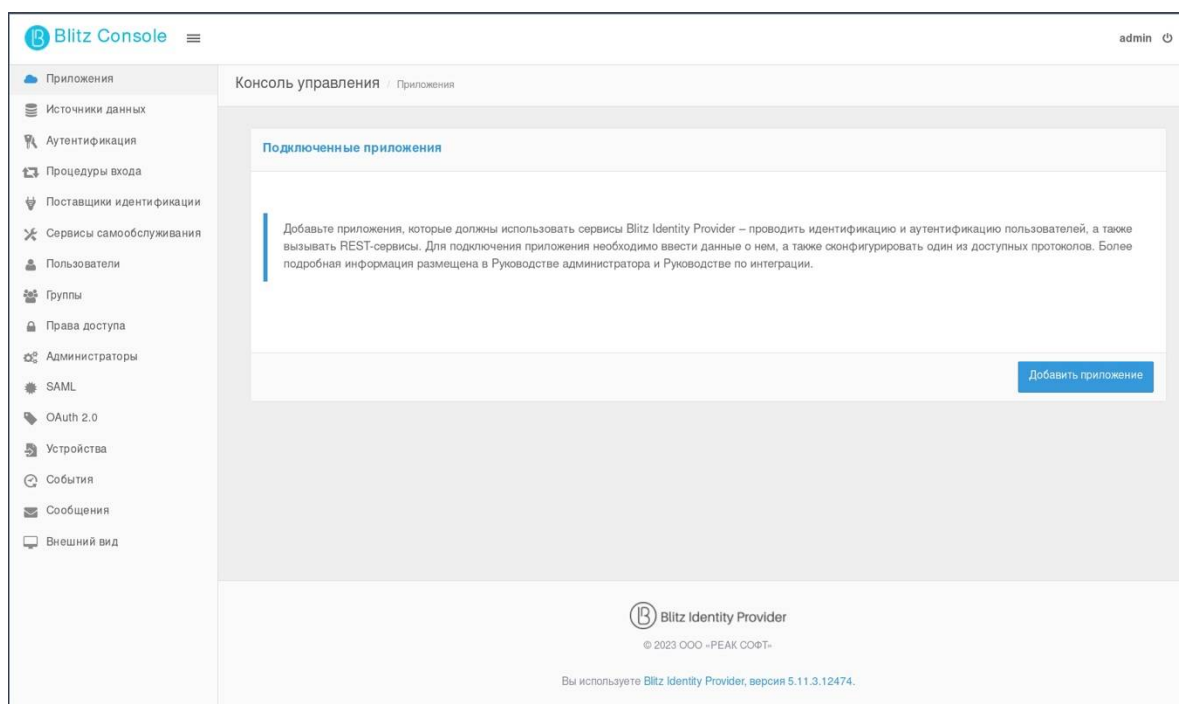


Рисунок 4 – Вид главного экрана консоли управления

2.1.11. 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.

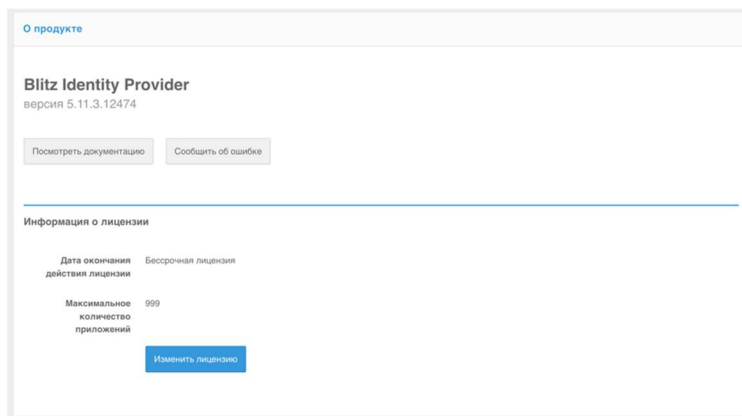


Рисунок 5 – Просмотр информации о лицензии

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

Также задать лицензионный ключ можно 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"
}
```

2.1.12. 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).

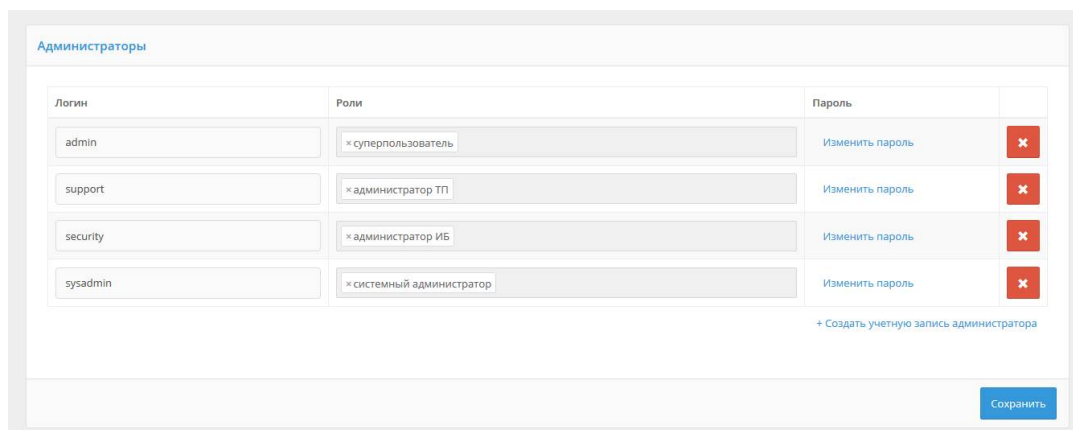


Рисунок 6 – Управление администраторами

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. 16.3.3).

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 (<code>app_admin</code>)	«Приложения»
Администратор интерфейса (<code>ui_admin</code>)	«Сервисы самообслуживания», «Внешний вид»
администратор ТП (<code>support</code>)	«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. 16.3.1).

2.1.13. 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
```

2.2. Экспресс-инструкции по установке

В экспресс-инструкциях по установке рассматривается минимальная конфигурация без обеспечения отказоустойчивости с размещением всех компонент на 1 виртуальной машине.

Инструкции приводятся для случая наличия подключения виртуальной машины к сети интернет. В качестве доменного имени для установки в инструкциях используется имя

`testinstallation.local` (его нужно скорректировать). В применяемых для настройки скриптах в качестве пароля используется строка `CHANGE_ME` (его нужно скорректировать).

Все действия выполняются с привилегиями пользователя `root`.

Перед выполнением работ необходимо обновить операционную систему до актуальных патчей.

Перед установкой на сервер в каталог `~/tmp/blitz` должны быть загружены и распакованы файлы дистрибутива Blitz Identity Provider (проверить правильность версии в `BLITZ_REL`):

```
export BLITZ_REL=5.11.0
mkdir -p ~/tmp/blitz
wget -q
'https://nc.reaxoft.ru/nextcloud/index.php/s/Dwdjbxe86ER8X3y/download?path=%2F'$BLITZ_REL'&files=blitz-'$BLITZ_REL'.bin -O ~/tmp/blitz/blitz-$BLITZ_REL.bin
wget -q
'https://nc.reaxoft.ru/nextcloud/index.php/s/Dwdjbxe86ER8X3y/download?path=%2F'$BLITZ_REL'&files=resources.zip' -O ~/tmp/blitz/resources.zip
unzip ~/tmp/blitz/resources.zip -d ~/tmp/blitz
find ~/tmp/blitz -name *.sh -o -name *.bin|xargs chmod +x
```

2.2.1. Astra Linux Special Edition 1.7 вариант «Орел»

2.2.1.1. Установка JDK

Установить дистрибутив Liberica JDK:

```
apt install ./bellsoft-jdk8u292+10-linux-amd64.deb
```

2.2.1.2. Установка memcached

Установить дистрибутив:

```
apt install memcached
```

Запустить службу:

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

2.2.1.3. Установка PostgreSQL

Установить дистрибутив:

```
apt install postgresql-11
```

Добавить разрешение в `/etc/postgresql/11/main/pg_hba.conf` на подключение к СУБД пользователю `blitz`:

```
host    blitzdb    blitz    127.0.0.1/32    scram-sha-256
```

Указать алгоритм шифрования паролей в `/etc/postgresql/11/main/postgresql.conf`:

```
password_encryption = scram-sha-256
```

Перезапустить службу:

```
systemctl restart postgresql@11-main
```

Подключиться к СУБД и провести первичную настройку

```
su - postgres
psql
create database blitzdb;
create user blitz with encrypted password 'CHANGE_ME';
grant ALL PRIVILEGES ON DATABASE blitzdb to blitz;
grant ALL on ALL tables in schema public to blitz;
```

Вернуться в shell пользователя `root` и выполнить скрипты создания и обновления структуры БД `blitzdb`:

```
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/000-service-tasks.sql
```

```
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/001-init-database.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/002-new_pp_columns.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/003-usd_id_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/004-usr_auth_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/005-usr_agt_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/006-usr_htp_hmc_alg.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/007-usr_atr_cfm.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/008-wak.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/009-fix_pp_column.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/010-add_usr_prp.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/011-pp_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/012-geo_to_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/013-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/014-sec_ch_ua.sql
```

2.2.1.4. Установка RabbitMQ

Установка сервера очередей RabbitMQ опциональна и требуется если сервер очередей будет использоваться для передачи событий в смежные системы (см. п. 16.1.9) или в качестве брокера сообщений (см. п. 16.1.10).

Установить дистрибутив:

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

Запустить службу:

```
systemctl enable rabbitmq-server && systemctl start rabbitmq-server
```

Подготовить очередь для взаимодействия:

```
rabbitmqctl add_user blitz CHANGE_ME
rabbitmqctl set_permissions blitz ".*" ".*" ".*"
rabbitmq-plugins enable rabbitmq_management
curl -vvk 127.0.0.1:15672/cli/rabbitmqadmin >rabbitmqadmin
chmod +x rabbitmqadmin
./rabbitmqadmin declare exchange name=blitz-tasks-exh type=direct
./rabbitmqadmin declare queue name=blitz-tasks durable=true
./rabbitmqadmin declare binding source="blitz-tasks-exh"
destination_type="queue" destination="blitz-tasks"
routing_key="blitz-tasks"
```

2.2.1.5. Установка 389 Directory Server

Установить дистрибутив:

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

Включить автоматический запуск службы:

```
systemctl enable dirsrv.target
```

Инициализировать LDAP-каталог:

```
dscreate interactive
```

Выполнить первичную настройку каталога:

```
/tmp/blitz/ldap/ldap_init.sh
```

2.2.1.6. Установка nginx

Установить дистрибутив:

```
apt-get install nginx-light
```

Скопировать файлы для использования:

```
cp /tmp/blitz/nginx/blitz-idp.conf /etc/nginx/sites-enabled/
cp -R /tmp/blitz/static_errors /usr/share/nginx/html
```

2.2.1.7. Установка Blitz Identity Provider

Установить дистрибутив (подставить в имя файла правильную версию):

```
/tmp/blitz/blitz-5.X.X.bin
```

В случае использования ключей, созданных на этапе установки, перезапустить nginx:

```
systemctl restart nginx
```

Внести изменения в конфигурационный файл `/etc/blitz-config/blitz.conf` – указать в блоке `blitz.prod.local.idp.internal-store-jdbc`:

- `conn_url` – адрес сервера, имя БД, имя пользователя;
- `db_name` – имя БД;
- `enc_params.pswd` – пароль для подключения к СУБД (пароль указывается в открытом виде и будет автоматически зашифрован при запуске Blitz Identity Provider).

```
"internal-store-jdbc" : {
  "conn_url" :
"jdbc:postgresql://127.0.0.1:5432/blitzdb?user=blitz&password=${pswd}&loggerLevel=DEBUG",
  "db_name" : "blitzdb",
  "enc_params" : {
    "pswd" : "CHANGE_ME"
  },
  "keyAlias" : "jdbc",
  "pool" : {
    "max_idle_conn" : 5,
    "max_total_conn" : 20,
    "max_wait_conn_ms" : 30000,
    "min_idle_conn" : 1
  }
}
```

Добавить сопоставление адреса loopback-интерфейса и доменного имени, указанного при установке в `/etc/hosts`:

```
127.0.0.1          localhost.localdomain    localhost    testinstallation.local
```

Запустить службы:

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

После успешного завершения установки и настройки Blitz Identity Provider возможно подключиться к консоли управления по доменному имени, указанному на этапе установки дистрибутива, например, `https://testinstallation.local/blitz/console`.

2.2.2. Альт 8 СП Сервер

2.2.2.1. Установка JDK

Установить дистрибутив JDK:

```
apt-get install java-1.8.0-openjdk-devel
```

2.2.2.2. Установка memcached

Установить дистрибутив:

```
apt-get install memcached
```

Запустить службу:

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

2.2.2.3. Установка PostgreSQL

Установить дистрибутив:

```
apt-get install postgresql-server
```

Инициализировать СУБД командой:

```
/etc/init.d/postgresql initdb
```

Добавить разрешение в `/etc/postgresql/11/main/pg_hba.conf` на подключение к СУБД пользователю **blitz**:

```
host    blitzdb    blitz    127.0.0.1/32    scram-sha-256
```

Указать алгоритм шифрования паролей в `/etc/postgresql/11/main/postgresql.conf`:

```
password_encryption = scram-sha-256
```

Запустить службу:

```
systemctl enable postgresql && systemctl start postgresql
```

Подключиться к СУБД и провести первичную настройку

```
psql -U postgres
```

```
create database blitzdb;
create user blitz with encrypted password 'CHANGE_ME';
grant ALL PRIVILEGES ON DATABASE blitzdb to blitz;
grant ALL on ALL tables in schema public to blitz;
```

Вернуться в shell и выполнить скрипты создания и обновления структуры БД blitzdb:

```
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/000-service-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/001-init-database.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/002-new_pp_columns.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/003-usd_id_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/004-usr_auth_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/005-usr_agt_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/006-usr_htp_hmc_alg.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/007-usr_atr_cfm.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/008-wak.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/009-fix_pp_column.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/010-add_usr_prp.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/011-pp_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/012-geo_to_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/013-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/014-sec_ch_ua.sql
```

2.2.2.4. Установка RabbitMQ

Установка сервера очередей RabbitMQ опциональна и требуется если сервер очередей будет использоваться для передачи событий в смежные системы (см. п. 16.1.9) или в качестве брокера сообщений (см. п. 16.1.10).

Установить дистрибутив:

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

Запустить службу:

```
systemctl enable rabbitmq && systemctl start rabbitmq
```

Подготовить очередь для взаимодействия:

```
rabbitmqctl add_user blitz CHANGE_ME
rabbitmqctl set_permissions blitz ".*" ".*" ".*"
rabbitmq-plugins enable rabbitmq_management
curl -vvk 127.0.0.1:15672/cli/rabbitmqadmin >rabbitmqadmin
chmod +x rabbitmqadmin
./rabbitmqadmin declare exchange name=blitz-tasks-exh type=direct
./rabbitmqadmin declare queue name=blitz-tasks durable=true
./rabbitmqadmin declare binding source="blitz-tasks-exh"
destination_type="queue" destination="blitz-tasks"
routing_key="blitz-tasks"
```

2.2.2.5. Установка 389 Directory Server

Установить дистрибутив:

```
apt-get install 389-ds-base openldap-clients
```

Включить автоматический запуск службы:

```
systemctl enable dirsrv.target
```


Инициализировать LDAP-каталог:

```
dscreate interactive
```

Выполнить первичную настройку каталога:

```
/tmp/blitz/ldap/ldap_init.sh
```

2.2.2.6. Установка *nginx*

Установить дистрибутив:

```
apt-get install nginx
```

Скопировать файлы для использования:

```
mkdir -p /var/www/html
cp /tmp/blitz/nginx/blitz-idp.conf /etc/nginx/sites-enabled.d/
cp -R /tmp/blitz/static_errors /var/www/html
```

Добавить директиву в `/etc/nginx/sites-enabled.d/blitz-idp.conf`:

```
location /static_errors {
    root /var/www/html;
}
```

Включить автоматический запуск службы:

```
systemctl enable nginx
```

2.2.2.7. Установка *Blitz Identity Provider*

Установить дистрибутив (подставить в имя файла правильную версию):

```
/tmp/blitz/blitz-5.X.X.bin
```

В случае использования ключей, созданных на этапе установки, запустить *nginx*:

```
systemctl start nginx
```

Внести изменения в конфигурационный файл `/etc/blitz-config/blitz.conf` – указать в блоке `blitz.prod.local.idp.internal-store-jdbc`:

- `conn_url` – адрес сервера, имя БД, имя пользователя;
- `db_name` – имя БД;
- `enc_params.pswd` – пароль для подключения к СУБД (пароль указывается в открытом виде и будет автоматически зашифрован при запуске *Blitz Identity Provider*).

```
"internal-store-jdbc" : {
  "conn_url" :
  "jdbc:postgresql://127.0.0.1:5432/blitzdb?user=blitz&password=${pswd}&loggerLevel=DEBUG",
  "db_name" : "blitzdb",
  "enc_params" : {
    "pswd" : "CHANGE_ME"
  },
  "keyAlias" : "jdbc",
  "pool" : {
    "max_idle_conn" : 5,
    "max_total_conn" : 20,
    "max_wait_conn_ms" : 30000,
    "min_idle_conn" : 1
  }
}
```

Добавить сопоставление адреса *loopback*-интерфейса и доменного имени, указанного при установке в `/etc/hosts`:

```
127.0.0.1      localhost.localdomain  localhost      testinstallation.local
```

Запустить службы:

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

После успешного завершения установки и настройки Blitz Identity Provider возможно подключиться к консоли управления по доменному имени, указанному на этапе установки дистрибутива, например, <https://testinstallation.local/blitz/console>.

2.2.3. Альт Сервер 10

2.2.3.1. Установка JDK

Установить дистрибутив JDK:

```
apt-get install java-1.8.0-openjdk-devel
```

2.2.3.2. Установка memcached

Установить дистрибутив:

```
apt-get install memcached
```

Запустить службу:

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

2.2.3.3. Установка PostgreSQL

Установить дистрибутив:

```
apt-get install postgresql14-server
```

Инициализировать СУБД командой:

```
/etc/init.d/postgresql initdb
```

Запустить службу:

```
systemctl enable postgresql && systemctl start postgresql
```

Подключиться к СУБД и провести первичную настройку

```
psql -U postgres

create database blitzdb;
create user blitz with encrypted password 'CHANGE_ME';
grant ALL PRIVILEGES ON DATABASE blitzdb to blitz;
grant ALL on ALL tables in schema public to blitz;
```

Вернуться в shell и выполнить скрипты создания и обновления структуры БД blitzdb:

```
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/000-service-tasks.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/001-init-database.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/002-new_pp_columns.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/003-usd_id_table.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/004-usr_auth_table.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/005-usr_agt_table.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/006-usr_http_hmc_alg.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/007-usr_atr_cfm.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/008-wak.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/009-fix_pp_column.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/010-add_usr_prp.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/011-pp_audit.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/012-geo_to_audit.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/013-tasks.sql
psql -d blitzdb -U blitz -f ~/tmp/blitz/postgres/ddl/014-sec_ch_ua.sql
```

2.2.3.4. Установка RabbitMQ

Установка сервера очередей RabbitMQ опциональна и требуется если сервер очередей будет использоваться для передачи событий в смежные системы (см. п. 16.1.9) или в качестве брокера сообщений (см. п. 16.1.10).

Установить дистрибутив:

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

Запустить службу:

```
systemctl enable rabbitmq && systemctl start rabbitmq
```

Подготовить очередь для взаимодействия:

```
rabbitmqctl add_user blitz CHANGE_ME
rabbitmqctl set_permissions blitz ".*" ".*" ".*"
rabbitmq-plugins enable rabbitmq_management
curl -vvk 127.0.0.1:15672/cli/rabbitmqadmin >rabbitmqadmin
chmod +x rabbitmqadmin
./rabbitmqadmin declare exchange name=blitz-tasks-exh type=direct
./rabbitmqadmin declare queue name=blitz-tasks durable=true
./rabbitmqadmin declare binding source="blitz-tasks-exh"
destination_type="queue" destination="blitz-tasks"
routing_key="blitz-tasks"
```

2.2.3.5. Установка 389 Directory Server

Установить дистрибутив:

```
apt-get install 389-ds-base
apt-get install openldap-clients
```

Включить автоматический запуск службы:

```
systemctl enable dirsrv.target
```

Инициализировать LDAP-каталог:

```
dscreate interactive
```

Выполнить первичную настройку каталога:

```
/tmp/blitz/ldap/ldap_init.sh
```

2.2.3.6. Установка nginx

Установить дистрибутив:

```
apt-get install nginx
```

Создать каталог для размещения страниц с ошибками:

```
mkdir -p /var/www/html
```

Скопировать файлы для использования:

```
cp /tmp/blitz/nginx/blitz-idp.conf /etc/nginx/sites-enabled.d/
cp -R /tmp/blitz/static_errors /var/www/html
```

Добавить директиву в `/etc/nginx/sites-enabled.d/blitz-idp.conf`:

```
location /static_errors {
    root /var/www/html;
}
```

Включить автоматический запуск службы:

```
systemctl enable nginx && systemctl start nginx
```

2.2.3.7. Установка Blitz Identity Provider

Установить дистрибутив (подставить в имя файла правильную версию):

```
/tmp/blitz/blitz-5.X.X.bin
```

В случае использования ключей, созданных на этапе установки, запустить nginx:

```
systemctl start nginx
```

Внести изменения в конфигурационный файл `/etc/blitz-config/blitz.conf` – указать в блоке `blitz.prod.local.idp.internal-store-jdbc`:

- `conn_url` – адрес сервера, имя БД, имя пользователя;
- `db_name` – имя БД;
- `enc_params.pswd` – пароль для подключения к СУБД (пароль указывается в открытом виде и будет автоматически зашифрован при запуске Blitz Identity Provider).

```
"internal-store-jdbc" : {
  "conn_url" :
"jdbc:postgresql://127.0.0.1:5432/blitzdb?user=blitz&password=${pswd}&loggerLevel=DEBUG",
  "db_name" : "blitzdb",
  "enc_params" : {
    "pswd" : "CHANGE_ME"
  },
  "keyAlias" : "jdbc",
  "pool" : {
    "max_idle_conn" : 5,
    "max_total_conn" : 20,
    "max_wait_conn_ms" : 30000,
    "min_idle_conn" : 1
  }
}
```

Добавить сопоставление адреса loopback-интерфейса и доменного имени, указанного при установке в `/etc/hosts`:

```
127.0.0.1      localhost.localdomain  localhost      testinstallation.local
```

Запустить службы:

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

После успешного завершения установки и настройки Blitz Identity Provider возможно подключиться к консоли управления по доменному имени, указанному на этапе установки дистрибутива, например, `https://testinstallation.local/blitz/console`.

2.2.4. ОСнова 2.5.1

2.2.4.1. Установка JDK

Установить дистрибутив Liberica JDK:

```
apt install ./bellsoft-jdk8u292+10-linux-amd64.deb
```

2.2.4.2. Установка memcached

Установить дистрибутив:

```
apt install memcached
```

Запустить службу:

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

2.2.4.3. Установка PostgreSQL

Установить дистрибутив:

```
apt install postgresql-11 postgresql-client-11
```

Инициализировать СУБД командой:

```
/etc/init.d/postgresql initdb
```

Добавить разрешение в `/etc/postgresql/11/main/pg_hba.conf` на подключение к БД пользователю `blitz`:

```
host      blitzdb  blitz      127.0.0.1/32      scram-sha-256
```

Указать алгоритм шифрования паролей в `/etc/postgresql/11/main/postgresql.conf`:

```
password_encryption = scram-sha-256
```

Перезапустить службу:

```
systemctl restart postgresql
```

Подключиться к СУБД и провести первичную настройку

```
su - postgres
psql
```

```
create database blitzdb;
create user blitz with encrypted password 'CHANGE_ME';
grant ALL PRIVILEGES ON DATABASE blitzdb to blitz;
grant ALL on ALL tables in schema public to blitz;
```

Вернуться в shell пользователя root и выполнить скрипты создания и обновления структуры БД blitzdb:

```
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/000-service-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/001-init-database.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/002-new_pp_columns.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/003-usd_id_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/004-usr_auth_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/005-usr_agt_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/006-usr_htp_hmc_alg.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/007-usr_atr_cfm.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/008-wak.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/009-fix_pp_column.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/010-add_usr_prp.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/011-pp_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/012-geo_to_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/013-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/014-sec_ch_ua.sql
```

2.2.4.4. Установка RabbitMQ

Установка сервера очередей RabbitMQ опциональна и требуется если сервер очередей будет использоваться для передачи событий в смежные системы (см. п. 16.1.9) или в качестве брокера сообщений (см. п. 16.1.10).

Установить дистрибутив:

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

Запустить службу:

```
systemctl enable rabbitmq && systemctl start rabbitmq
```

Подготовить очередь для взаимодействия:

```
rabbitmqctl add_user blitz CHANGE_ME
rabbitmqctl set_permissions blitz ".*" ".*" ".*"
rabbitmq-plugins enable rabbitmq_management
curl -vvk 127.0.0.1:15672/cli/rabbitmqadmin >rabbitmqadmin
chmod +x rabbitmqadmin
./rabbitmqadmin declare exchange name=blitz-tasks-exh type=direct
./rabbitmqadmin declare queue name=blitz-tasks durable=true
./rabbitmqadmin declare binding source="blitz-tasks-exh"
destination_type="queue" destination="blitz-tasks"
routing_key="blitz-tasks"
```

2.2.4.5. Установка 389 Directory Server

Установить дистрибутив:

```
apt-get install 389-ds-base openldap-clients
```

Включить автоматический запуск службы:

```
systemctl enable dirsrv.target
```

Инициализировать LDAP-каталог:

```
dscreate interactive
```

Выполнить первичную настройку каталога:

```
/tmp/blitz/ldap/ldap_init.sh
```

2.2.4.6. Установка nginx

Установить дистрибутив:

```
apt-get install nginx
```

Скопировать файлы для использования:

```
mkdir -p /var/www/html
cp /tmp/blitz/nginx/blitz-idp.conf /etc/nginx/sites-enabled.d/
cp -R /tmp/blitz/static_errors /var/www/html
```

Добавить директиву в `/etc/nginx/sites-enabled.d/blitz-idp.conf`:

```
location /static_errors {
    root /var/www/html;
}
```

Включить автоматический запуск службы:

```
systemctl enable nginx
```

2.2.4.7. Установка Blitz Identity Provider

Установить дистрибутив (подставить в имя файла правильную версию):

```
/tmp/blitz/blitz-5.X.X.bin
```

В случае использования ключей, созданных на этапе установки, запустить nginx:

```
systemctl start nginx
```

Внести изменения в конфигурационный файл `/etc/blitz-config/blitz.conf` – указать в блоке `blitz.prod.local.idp.internal-store-jdbc`:

- `conn_url` – адрес сервера, имя БД, имя пользователя;
- `db_name` – имя БД;
- `enc_params.pswd` – пароль для подключения к СУБД (пароль указывается в открытом виде и будет автоматически зашифрован при запуске Blitz Identity Provider).

```
"internal-store-jdbc" : {
    "conn_url" :
"jdbc:postgresql://127.0.0.1:5432/blitzdb?user=blitz&password=${pswd}&loggerLevel=DEBUG",
    "db_name" : "blitzdb",
    "enc_params" : {
        "pswd" : "CHANGE_ME"
    },
    "keyAlias" : "jdbc",
    "pool" : {
        "max_idle_conn" : 5,
        "max_total_conn" : 20,
        "max_wait_conn_ms" : 30000,
        "min_idle_conn" : 1
    }
}
```

Добавить сопоставление адреса loopback-интерфейса и доменного имени, указанного при установке в `/etc/hosts`:

```
127.0.0.1      localhost.localdomain  localhost      testinstallation.local
```

Запустить службы:

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

После успешного завершения установки и настройки Blitz Identity Provider возможно подключиться к консоли управления по доменному имени, указанному на этапе установки дистрибутива, например, `https://testinstallation.local/blitz/console`.

2.2.5. Red OS 7.3

2.2.5.1. Установка JDK

Установить дистрибутив:

```
dnf install java-1.8.0-openjdk-devel
```

2.2.5.2. Установка memcached

Установить дистрибутив:

```
dnf install memcached
```

Запустить службу:

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

2.2.5.3. Установка PostgreSQL

Установить дистрибутив:

```
dnf install postgresql14-server
```

Инициализировать СУБД командой:

```
/usr/bin/postgresql-14-setup initdb
```

Добавить разрешение в `/var/lib/pgsql/14/data/pg_hba.conf` на подключение к БД пользователю `blitz`:

```
host    blitzdb    blitz    127.0.0.1/32    scram-sha-256
```

Указать алгоритм шифрования паролей в `/var/lib/pgsql/14/data/postgresql.conf`:

```
password_encryption = scram-sha-256
```

Запустить службу:

```
systemctl enable postgresql-14 && systemctl start postgresql-14
```

Подключиться к СУБД и провести первичную настройку

```
su - postgres
psql

create database blitzdb;
create user blitz with encrypted password 'CHANGE_ME';
grant ALL PRIVILEGES ON DATABASE blitzdb to blitz;
grant ALL on ALL tables in schema public to blitz;
```

Вернуться в shell пользователя `root` и выполнить скрипты создания и обновления структуры БД `blitzdb`:

```
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/000-service-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/001-init-database.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/002-new_pp_columns.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/003-usd_id_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/004-usr_auth_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/005-usr_agt_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/006-usr_htp_hmc_alg.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/007-usr_atr_cfm.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/008-wak.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/009-fix_pp_column.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/010-add_usr_prp.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/011-pp_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/012-geo_to_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/013-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/014-sec_ch_u.sql
```

2.2.5.4. Установка RabbitMQ

Установка сервера очередей RabbitMQ опциональна и требуется если сервер очередей будет использоваться для передачи событий в смежные системы (см. п. 16.1.9) или в качестве брокера сообщений (см. п. 16.1.10).

Установить дистрибутив:

```
dnf install rabbitmq-server
```

Запустить службу:

```
systemctl enable rabbitmq-server && systemctl start rabbitmq-server
```

Подготовить очередь для взаимодействия:

```
rabbitmqctl add_user blitz CHANGE_ME
rabbitmqctl set_permissions blitz ".*" ".*" ".*"
rabbitmq-plugins enable rabbitmq_management
curl -vvk 127.0.0.1:15672/cli/rabbitmqadmin >rabbitmqadmin
chmod +x rabbitmqadmin
./rabbitmqadmin declare exchange name=blitz-tasks-exh type=direct
./rabbitmqadmin declare queue name=blitz-tasks durable=true
./rabbitmqadmin declare binding source="blitz-tasks-exh"
destination_type="queue" destination="blitz-tasks"
routing_key="blitz-tasks"
```

2.2.5.5. Установка 389 Directory Server

Установить дистрибутив:

```
dnf install 389-ds-base
```

Включить автоматический запуск службы:

```
systemctl enable dirsrv.target
```

Инициализировать LDAP-каталог:

```
dscreate interactive
```

Выполнить первичную настройку каталога:

```
/tmp/blitz/ldap/ldap_init.sh
```

2.2.5.6. Установка nginx

Установить дистрибутив:

```
dnf install nginx
```

Скопировать файлы для использования:

```
cp /tmp/blitz/nginx/blitz-idp.conf /etc/nginx/sites-enabled.d/
cp -R /tmp/blitz/static_errors /usr/share/nginx/html
```

Включить автоматический запуск службы:

```
systemctl enable nginx
```

2.2.5.7. Установка Blitz Identity Provider

Установить дистрибутив (подставить в имя файла правильную версию):

```
/tmp/blitz/blitz-5.X.X.bin
```

В случае использования ключей, созданных на этапе установки, запустить nginx:

```
systemctl start nginx
```

Внести изменения в конфигурационный файл `/etc/blitz-config/blitz.conf` – указать в блоке `blitz.prod.local.idp.internal-store-jdbc`:

- `conn_url` – адрес сервера, имя БД, имя пользователя;
- `db_name` – имя БД;
- `enc_params.pswd` – пароль для подключения к СУБД (пароль указывается в открытом виде и будет автоматически зашифрован при запуске Blitz Identity Provider).

```
"internal-store-jdbc" : {
  "conn_url" :
"jdbc:postgresql://127.0.0.1:5432/blitzdb?user=blitz&password=${pswd}&loggerLevel=DEBUG",
  "db_name" : "blitzdb",
  "enc_params" : {
    "pswd" : "CHANGE_ME"
```



```
},
"keyAlias" : "jdbc",
"pool" : {
    "max_idle_conn" : 5,
    "max_total_conn" : 20,
    "max_wait_conn_ms" : 30000,
    "min_idle_conn" : 1
}
}
```

Добавить сопоставление адреса loopback-интерфейса и доменного имени, указанного при установке в `/etc/hosts`:

```
127.0.0.1      localhost.localdomain    localhost      testinstallation.local
```

Запустить службы:

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

После успешного завершения установки и настройки Blitz Identity Provider возможно подключиться к консоли управления по доменному имени, указанному на этапе установки дистрибутива, например, <https://testinstallation.local/blitz/console>.

2.2.6. Rocky Linux 8

2.2.6.1. Установка JDK

Установить дистрибутив:

```
dnf install java-1.8.0-openjdk-devel
```

2.2.6.2. Установка memcached

Установить дистрибутив:

```
dnf install memcached
```

Запустить службу:

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

2.2.6.3. Установка PostgreSQL

Установить дистрибутив:

```
dnf install postgresql
```

Инициализировать СУБД командой:

```
postgresql-setup initdb
```

Добавить разрешение в `/var/lib/pgsql/data/pg_hba.conf` на подключение к БД пользователю `blitz`:

```
host      blitzdb    blitz    127.0.0.1/32    scram-sha-256
```

Указать алгоритм шифрования паролей в `/var/lib/pgsql/data/postgresql.conf`:

```
password_encryption = scram-sha-256
```

Запустить службу:

```
systemctl enable postgresql && systemctl start postgresql
```

Подключиться к СУБД и провести первичную настройку

```
su - postgres
psql

create database blitzdb;
create user blitz with encrypted password 'CHANGE_ME';
grant ALL PRIVILEGES ON DATABASE blitzdb to blitz;
grant ALL on ALL tables in schema public to blitz;
```

Вернуться в shell пользователя root и выполнить скрипты создания и обновления структуры БД blitzdb:

```
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/000-service-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/001-init-database.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/002-new_pp_columns.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/003-usd_id_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/004-usr_auth_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/005-usr_agt_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/006-usr_htp_hmc_alg.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/007-usr_atr_cfm.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/008-wak.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/009-fix_pp_column.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/010-add_usr_prp.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/011-pp_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/012-geo_to_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/013-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/014-sec_ch_ua.sql
```

2.2.6.4. Установка RabbitMQ

Установка сервера очередей RabbitMQ опциональна и требуется если сервер очередей будет использоваться для передачи событий в смежные системы (см. п. 16.1.9) или в качестве брокера сообщений (см. п. 16.1.10).

Подготовить конфигурационный файл с репозиториями для RabbitMQ в `/etc/yum.repos.d/rabbitmq.repo`:

```
##
## Zero dependency Erlang
##

[rabbitmq_erlang]
name=rabbitmq_erlang
baseurl=https://packagecloud.io/rabbitmq/erlang/el/8/$basearch
repo_gpgcheck=1
gpgcheck=1
enabled=1
# PackageCloud's repository key and RabbitMQ package signing key
gpgkey=https://packagecloud.io/rabbitmq/erlang/gpgkey

https://github.com/rabbitmq/signingkeys/releases/download/2.0/rabbitmq-release-signing-key.asc
sslverify=1
sslcacert=/etc/pki/tls/certs/ca-bundle.crt
metadata_expire=300

##
## RabbitMQ server
##

[rabbitmq_server]
name=rabbitmq_server
baseurl=https://packagecloud.io/rabbitmq/rabbitmqserver/el/8/$basearch
repo_gpgcheck=1
gpgcheck=0
enabled=1
# PackageCloud's repository key and RabbitMQ package signing key
gpgkey=https://packagecloud.io/rabbitmq/rabbitmq-server/gpgkey

https://github.com/rabbitmq/signingkeys/releases/download/2.0/rabbitmq-release-signing-key.asc
sslverify=1
sslcacert=/etc/pki/tls/certs/ca-bundle.crt
metadata_expire=300
```

Установить дистрибутив:

```
dnf install rabbitmq-server
```

Запустить службу:

```
systemctl enable rabbitmq-server && systemctl start rabbitmq-server
```

Подготовить очередь для взаимодействия:

```
rabbitmqctl add_user blitz CHANGE_ME
```

```
rabbitmqctl set_permissions blitz ".*" ".*" ".*"
rabbitmq-plugins enable rabbitmq_management
curl -vvk 127.0.0.1:15672/cli/rabbitmqadmin >rabbitmqadmin
chmod +x rabbitmqadmin
./rabbitmqadmin declare exchange name=blitz-tasks-exh type=direct
./rabbitmqadmin declare queue name=blitz-tasks durable=true
./rabbitmqadmin declare binding source="blitz-tasks-exh"
destination_type="queue" destination="blitz-tasks"
routing_key="blitz-tasks"
```

2.2.6.5. Установка 389 Directory Server

Установить дистрибутив:

```
dnf module enable 389-directory-server:stable
dnf install 389-ds-base
```

Включить автоматический запуск службы:

```
systemctl enable dirsrv.target
```

Инициализировать LDAP-каталог:

```
dscreate interactive
```

Выполнить первичную настройку каталога:

```
/tmp/blitz/ldap/ldap_init.sh
```

2.2.6.6. Установка nginx

Установить дистрибутив:

```
dnf install nginx
```

Скопировать файлы для использования:

```
cp /tmp/blitz/nginx/blitz-idp.conf /etc/nginx/conf.d/
cp -R /tmp/blitz/static_errors /usr/share/nginx/html
```

Включить автоматический запуск службы:

```
systemctl enable nginx
```

2.2.6.7. Установка Blitz Identity Provider

Установить дистрибутив (подставить в имя файла правильную версию):

```
/tmp/blitz/blitz-5.X.X.bin
```

В случае использования ключей, созданных на этапе установки, запустить nginx:

```
systemctl start nginx
```

Внести изменения в конфигурационный файл `/etc/blitz-config/blitz.conf` – указать в блоке `blitz.prod.local.idp.internal-store-jdbc`:

- `conn_url` – адрес сервера, имя БД, имя пользователя;
- `db_name` – имя БД;
- `enc_params.pswd` – пароль для подключения к СУБД (пароль указывается в открытом виде и будет автоматически зашифрован при запуске Blitz Identity Provider).

```
"internal-store-jdbc" : {
  "conn_url" :
"jdbc:postgresql://127.0.0.1:5432/blitzdb?user=blitz&password=${pswd}&loggerLevel=DEBUG",
  "db_name" : "blitzdb",
  "enc_params" : {
    "pswd" : "CHANGE_ME"
  },
  "keyAlias" : "jdbc",
  "pool" : {
    "max_idle_conn" : 5,
    "max_total_conn" : 20,
    "max_wait_conn_ms" : 30000,
    "min_idle_conn" : 1
  }
}
```

Добавить сопоставление адреса loopback-интерфейса и доменного имени, указанного при установке в `/etc/hosts`:

```
127.0.0.1      localhost.localdomain    localhost      testinstallation.local
```

Запустить службы:

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

После успешного завершения установки и настройки Blitz Identity Provider возможно подключиться к консоли управления по доменному имени, указанному на этапе установки дистрибутива, например, <https://testinstallation.local/blitz/console>.

2.2.7. Rocky Linux 9

2.2.7.1. Установка JDK

Установить дистрибутив:

```
dnf install java-1.8.0-openjdk-devel
```

2.2.7.2. Установка memcached

Установить дистрибутив:

```
dnf install memcached
```

Запустить службу:

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

2.2.7.3. Установка PostgreSQL

Установить дистрибутив:

```
dnf install postgresql-server
```

Инициализировать СУБД командой:

```
postgresql-setup -initdb -unit postgresql
```

Добавить разрешение в `/var/lib/pgsql/data/pg_hba.conf` на подключение к БД пользователю `blitz`:

```
host      blitzdb  blitz      127.0.0.1/32      scram-sha-256
```

Указать алгоритм шифрования паролей в `/var/lib/pgsql/data/postgresql.conf`:

```
password_encryption = scram-sha-256
```

Запустить службу:

```
systemctl enable postgresql && systemctl start postgresql
```

Вернуться в shell пользователя `root` и выполнить скрипты создания и обновления структуры БД `blitzdb`:

```
su - postgres
psql
```

```
create database blitzdb;
create user blitz with encrypted password 'CHANGE_ME';
grant ALL PRIVILEGES ON DATABASE blitzdb to blitz;
grant ALL on ALL tables in schema public to blitz;
```

Выполнить скрипты создания и обновления структуры БД `blitzdb`:

```
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/000-service-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/001-init-database.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/002-new_pp_columns.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/003-usd_id_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/004-usr_auth_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/005-usr_agt_table.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/006-usr_htp_hmc_alg.sql
```

```
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/007-usr_atr_cfm.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/008-wak.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/009-fix_pp_column.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/010-add_usr_prp.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/011-pp_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/012-geo_to_audit.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/013-tasks.sql
psql -U blitz -h 127.0.0.1 blitzdb -f ~/tmp/blitz/postgres/ddl/014-sec_ch_ua.sql
```

2.2.7.4. Установка RabbitMQ

Установка сервера очередей RabbitMQ опциональна и требуется если сервер очередей будет использоваться для передачи событий в смежные системы (см. п. 16.1.9) или в качестве брокера сообщений (см. п. 16.1.10).

Подготовить конфигурационный файл с репозиториями для RabbitMQ в `/etc/yum.repos.d/rabbitmq.repo`:

```
##
## Zero dependency Erlang
##

[rabbitmq_erlang]
name=rabbitmq_erlang
baseurl=https://packagecloud.io/rabbitmq/erlang/el/9/$basearch
repo_gpgcheck=1
gpgcheck=1
enabled=1
# PackageCloud's repository key and RabbitMQ package signing key
gpgkey=https://packagecloud.io/rabbitmq/erlang/gpgkey

https://github.com/rabbitmq/signingkeys/releases/download/2.0/rabbitmq-release-signing-key.asc
sslverify=1
sslcacert=/etc/pki/tls/certs/ca-bundle.crt
metadata_expire=300

##
## RabbitMQ server
##

[rabbitmq_server]
name=rabbitmq_server
baseurl=https://packagecloud.io/rabbitmq/rabbitmqserver/el/9/$basearch
repo_gpgcheck=1
gpgcheck=0
enabled=1
# PackageCloud's repository key and RabbitMQ package signing key
gpgkey=https://packagecloud.io/rabbitmq/rabbitmq-server/gpgkey

https://github.com/rabbitmq/signingkeys/releases/download/2.0/rabbitmq-release-signing-key.asc
sslverify=1
sslcacert=/etc/pki/tls/certs/ca-bundle.crt
metadata_expire=300
```

Установить дистрибутив:

```
dnf install rabbitmq-server
```

Запустить службу:

```
systemctl enable rabbitmq-server && systemctl start rabbitmq-server
```

Подготовить очередь для взаимодействия:

```
rabbitmqctl add_user blitz CHANGE_ME
rabbitmqctl set_permissions blitz ".*" ".*" ".*"
rabbitmq-plugins enable rabbitmq_management
curl -vvk 127.0.0.1:15672/cli/rabbitmqadmin >rabbitmqadmin
chmod +x rabbitmqadmin
./rabbitmqadmin declare exchange name=blitz-tasks-exh type=direct
./rabbitmqadmin declare queue name=blitz-tasks durable=true
./rabbitmqadmin declare binding source="blitz-tasks-exh"
destination_type="queue" destination="blitz-tasks"
routing_key="blitz-tasks"
```

2.2.7.5. Установка 389 Directory Server

Установить дистрибутив:

```
dnf install 389-ds-base
```

Включить автоматический запуск службы:

```
systemctl enable dirsrv.target
```

Инициализировать LDAP-каталог:

```
dscreate interactive
```

Выполнить первичную настройку каталога:

```
/tmp/blitz/ldap/ldap_init.sh
```

2.2.7.6. Установка nginx

Установить дистрибутив:

```
dnf install nginx
```

Скопировать файлы для использования:

```
cp /tmp/blitz/nginx/blitz-idp.conf /etc/nginx/conf.d/
cp -R /tmp/blitz/static_errors /usr/share/nginx/html
```

Включить автоматический запуск службы:

```
systemctl enable nginx
```

2.2.7.7. Установка Blitz Identity Provider

Установить дистрибутив (подставить в имя файла правильную версию):

```
/tmp/blitz/blitz-5.X.X.bin
```

В случае использования ключей, созданных на этапе установки, запустить nginx:

```
systemctl start nginx
```

Внести изменения в конфигурационный файл `/etc/blitz-config/blitz.conf` – указать в блоке `blitz.prod.local.idp.internal-store-jdbc`:

- `conn_url` – адрес сервера, имя БД, имя пользователя;
- `db_name` – имя БД;
- `enc_params.pswd` – пароль для подключения к СУБД (пароль указывается в открытом виде и будет автоматически зашифрован при запуске Blitz Identity Provider).

```
"internal-store-jdbc" : {
  "conn_url" :
"jdbc:postgresql://127.0.0.1:5432/blitzdb?user=blitz&password=${pswd}&loggerLevel=DEBUG",
  "db_name" : "blitzdb",
  "enc_params" : {
    "pswd" : "CHANGE_ME"
  },
  "keyAlias" : "jdbc",
  "pool" : {
    "max_idle_conn" : 5,
    "max_total_conn" : 20,
    "max_wait_conn_ms" : 30000,
    "min_idle_conn" : 1
  }
}
```

Добавить сопоставление адреса loopback-интерфейса и доменного имени, указанного при установке в `/etc/hosts`:

```
127.0.0.1      localhost.localdomain  localhost      testinstallation.local
```

Запустить службы:

```
systemctl enable blitz-idp && systemctl start blitz-idp
systemctl enable blitz-console && systemctl start blitz-console
systemctl enable blitz-registration && systemctl start blitz-registration
```

```
systemctl enable blitz-recovery && systemctl start blitz-recovery
```

После успешного завершения установки и настройки Blitz Identity Provider возможно подключиться к консоли управления по доменному имени, указанному на этапе установки дистрибутива, например, <https://testinstallation.local/blitz/console>.

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 (колонок «Поиск»)¹²;
 - является ли атрибут обязательным (колонок «Обяз.»);
 - должно ли значение атрибута быть уникальным в системе (колонок «Уник.»).

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

В разделе «Пользователи» в карточке пользователя (см. п. 9.3) атрибуты будут показываться в том порядке, в котором они созданы. Через консоль управления изменить порядок атрибутов нельзя. При необходимости изменить порядок атрибутов необходимо вручную их переупорядочить в конфигурационном файле `blitz.conf` в секции настроек `blitz.prod.local.idp.id-attrs`.

Чтобы в разделе «Пользователи» вместо системных имен атрибутов показывались их текстовые названия с учетом языка интерфейса пользователя, необходимо для созданных атрибутов определить в `messages` (см. п. 16.2.2) строки с описанием названий атрибутов для используемых языков. Строки должны иметь вид `custom.user.attr.name.<имя атрибута>`.

Пример строчек:

```
custom.user.attr.name.sub=Идентификатор
custom.user.attr.name.family_name=Фамилия
custom.user.attr.name.given_name=Имя
custom.user.attr.name.middle_name=Отчество
custom.user.attr.name.email=E-mail
custom.user.attr.name.phone_number=Телефон
```

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.

¹² Если это атрибут из подключенного хранилища, то в целях производительности рекомендуется создать по нему поисковый индекс.

Если в качестве СУБД используется PostgreSQL, то необходимо создать колонку в таблице **USR_ATTR**, а также в таблице **USR** (только в случае, если используется внутреннее хранилище, см. п. 3.2.1). 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**.

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.	
sub	String	☒	☒	☒	☒
family_name	String	☒	☐	☐	☒
given_name	String	☒	☐	☐	☒
middle_name	String	☒	☐	☐	☒
email	String	☒	☐	☒	☒
phone_number	String	☒	☐	☒	☒

+ Добавить атрибут

Рисунок 7 – Пример настройки хранимых атрибутов

Предусмотрена возможность назначить для атрибута LDAP-каталога транслятор, осуществляющий преобразование атрибута из хранимого в LDAP формате в требуемый формат в Blitz Identity Provider. Например, это может быть полезно при необходимости обрабатывать в Blitz Identity Provider атрибут **objectGUID** из LDAP-каталога Active Directory, чтобы этот атрибут представлялся не в байтовом виде, а в форме строки GUID. Настройка выполняется через конфигурационный файл, см. п. 16.1.4.

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 `family_name` и `given_name` необходимо определить хранимые атрибуты `family_name` и `given_name`, а далее задать вычисляемый атрибут `full_name` с правилом вычисления – `${family_name} ${given_name}`;
- чтобы создать атрибут «домен электронной почты» из хранимого атрибута `email` необходимо определить хранимый атрибут `email`, а далее задать вычисляемый атрибут `domain` и определить его правило вычисления `${email##*@}`¹³.

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:

¹³ Справку по поддерживаемым параметрам строк подстановки можно посмотреть здесь: <http://tldp.org/LDP/abs/html/parameter-substitution.html>

- для проверки, что атрибут **email** содержит знак **@**, необходимо указать выражение декомпозиции **^(.+)@(.+)\$** и выражение компоновки **\${0-}**;
- для проверки формата мобильного телефона (**phone_number**) 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	
email	^(.+)@(.+)\$	\${0-}	✖
phone_number	^(\+7)([78]?)?\([([0-9]{3})\)\? ?([0-9]{3})[-]?([0-9]{2})[-]?([0-9]{2})\$	+7(\${3-})\${4-}\${5-}\${6-}	✖

[+ 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.

Правила преобразования выходных значений

Эти правила позволяют совершить дополнительные преобразования с вычисляемыми атрибутами.

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 `${family_name} ${given_name} ${middle_name-}` позволяет отображать 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	sub
Признак блокировки	locked
Имя пользователя в консоли	\${family_name} \${given_name-} \${middle_name-}, \${email-}
Электронная почта	× email
Мобильный телефон	× phone_number

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 такового 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».

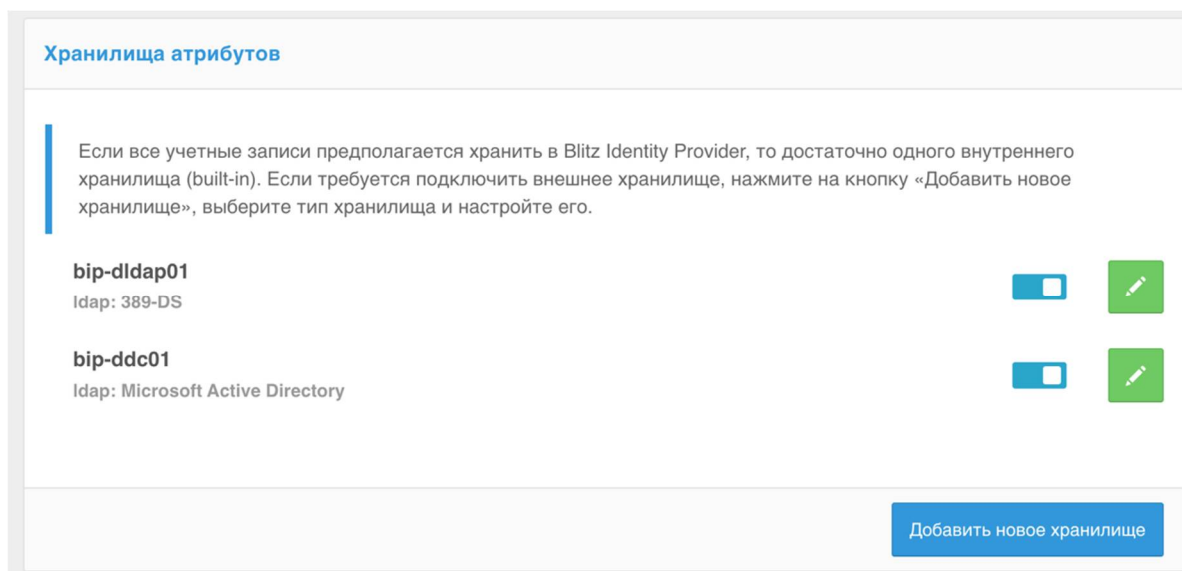


Рисунок 12 – Хранилища атрибутов

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 или построению метакаталога.

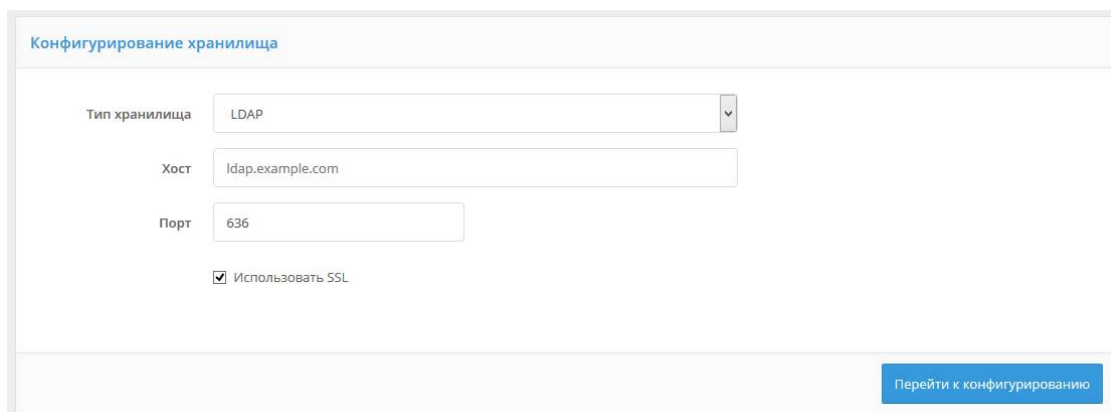


Рисунок 13 – Экран добавления хранилища учетных записей

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-балансировки¹⁴ 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 данных¹⁵), а также базовый DN – раздел каталога с учетными записями пользователей;
- указать настройки поиска – глубину поиска и максимальное число возвращаемых учетных записей (это влияет на число пользователей, отображаемых в разделе «Пользователи» консоли управления).

¹⁴ 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».

¹⁵ Допустимо указать пользователя только с правами на чтение, если хранилище используется только для чтения.

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

Начальное количество соединений

Таймаут ответа, мс

Максимальное количество соединений

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 `family_name`, то выберите атрибут `family_name` и укажите `sn` в качестве его названия в LDAP. Пример такой настройки приведен на рисунке ниже;
- использовать специальные правила записи атрибутов в данный LDAP-каталога. 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	
sub	uid					✖
family_name	sn					✖
given_name	givenName					✖
middle_name	middleName					✖
email	mail					✖
phone_number	mobile					✖

+ 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 Provider 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 хранилища¹⁶.

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
Например: objectclass.

Название	Формат	Значение
objectClass	Array of strings	top,blitz-schema

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

¹⁶ Например, objectclass, определяющий тип создаваемой учетной записи в LDAP. Для Microsoft Active Directory objectclass должен иметь формат Array of string и значение - top,person.

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

Параметры REST-сервисов

Идентификатор:

Описание:

Только для чтения:

Максимальное количество записей, возвращаемых при поиске:

Перечень доступных атрибутов:

Атрибуты пользователя, которые доступны в запросах к REST-сервисам

Адреса REST-сервисов

URL сервиса поиска пользователей:

HTTP метод запроса: **GET**. Параметр запроса:

- * **rq1** — 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:

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 **rq1** указывается поисковый запрос. Запрос имеет формат Resource Query Language (RQL)¹⁷ и должен поддерживать следующие операции:

- **limit** — количество возвращаемых записей;
- **and** — одновременное выполнение поисковых условий;
- **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 (*)).

¹⁷ См.: <https://github.com/kriszyp/rql>

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

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

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

```
rql=and(or(eq(sub,test@mail.com),eq(email,test@mail.com)),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(sub,BIP*),limit(10)) HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
[
  {
    "id": "ID123",
    "attrs": {
      "sub": "BIP123",
      "given_name": "Ivan",
      "family_name": "Ivanov",
      "email": "ivanov@test.org",
      "phone_number": "+79991234567"
    }
  },
  {
    "id": "ID456",
    "attrs": {
      "sub": "BIP456",
      "given_name": "Elena",
      "family_name": "Ivanova",
      "email": "ivanova@test.org",
      "phone_number": "+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": {
    "sub": "BIP123",
    "given_name": "Ivan",
    "family_name": "Ivanov",
    "email": "ivanov@test.org",
    "phone_number": "+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": {
    "sub": "ivanov@test.org",
    "email": "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": {
    "sub": "ivanov@test.org",
    "email": "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": {
    "email": "ivanov@domain.org"
  },
  "deleted": ["family_name"],
  "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": [
    "sub": "BIP123",
    "given_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 four input fields: "Идентификатор" (Identifier) with the value "built-in", "Описание" (Description) with the value "Built-in store", "Только для чтения" (Read-only) with a dropdown menu showing "Нет" (No), and "Максимальное количество записей, возвращаемых при поиске" (Maximum number of records returned during search) with the value "100". At the bottom right, 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. Настройки аутентификации

Настройки аутентификации задаются в разделе «Аутентификация» консоли управления (см. Рисунок 19).

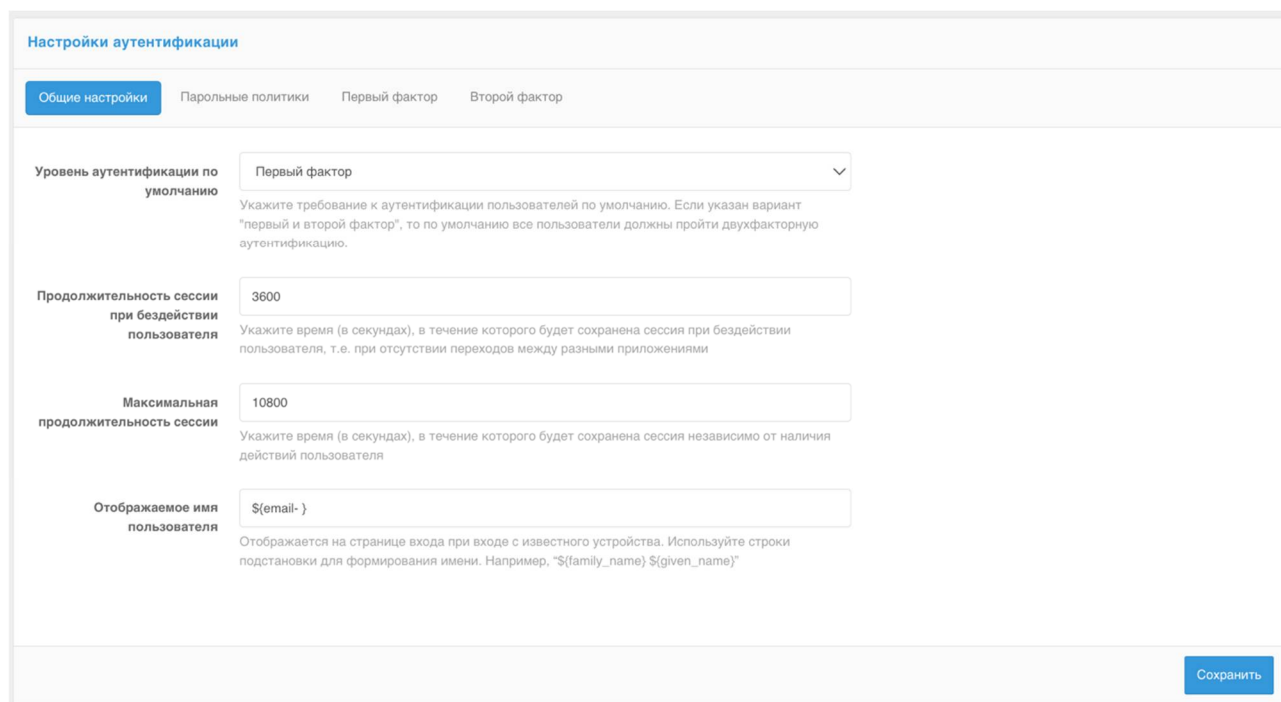


Рисунок 19 – Настройки аутентификации – вкладка «Общие настройки»

Настройки аутентификации разделены по вкладкам:

- Общие настройки – задаются общие настройки, см. описание далее в этой главе;
- Парольные политики – задаются настройки парольной политики (см. п. 4.1);
- Первый фактор – можно перейти к настройкам методов аутентификации, применяемых при первичной идентификации и аутентификации (см. 4.2);
- Второй фактор – можно перейти к настройкам методов аутентификации, применяемых для подтверждения входа (см. 4.2);
- Третий фактор – опциональная вкладка, отображается, только если сконфигурировано наличие метода аутентификации, применяемого дополнительно после прохождения проверок первого и второго фактора.

На вкладке «Общие настройки» можно задать:

- 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: `${email-$phone_number}`. Такое регулярное выражение позволяет отображать один из контактов, сохраненных в атрибутах `email` или `phone_number` (если имеются оба, то отображается `email`).

4.1. Настройка парольной политики

Парольные политики настраиваются на вкладке «Парольные политики» раздела «Аутентификация» консоли управления (см. Рисунок 20).

Настройки аутентификации
Общие настройки
Парольные политики
Первый фактор
Второй фактор

Сложность пароля

Минимальная длина пароля
8
Укажите минимальное количество символов в пароле

Словарь паролей
Обзор...
Выберите файл со словарем паролей, где каждый пароль размещен на новой строке. Формат файла должен быть txt.

Группы символов
3
Задайте минимальное количество групп символов, необходимых в пароле

Название группы	Допустимые символы	Минимум символов
Цифры	[0-9]	1
Нижний регистр	[a-z]	1
Верхний регистр	[A-Z]	1
Специальные символы	[!@#\$%^&*()_+~?~...~"{}(){}<=>~_]]	1

Политика повторного использования

Запрет использования старых паролей, шт.
5

Минимальное время жизни пароля, сек.
86400

Максимальное время жизни пароля, сек.
2592000

Минимальное число отличающихся символов, шт.

Сохранить

Рисунок 20 – Настройка парольных политик

Предусмотрены следующие настройки:

- Минимальная длина пароля – число символов в пароле (рекомендуется не менее 8);
- Словарь паролей – указывается текстовый файл, содержащий список запрещенных паролей. Каждый пароль должен быть на отдельной строке. В случае использования больших файлов рекомендуется загружать их непосредственно на сервер, и задавать путь к файлу в настройке `dicPath` в блоке настроек `blitz.prod.local.idp.password-policy` в файле `blitz.conf`.
- Группа символов – задает минимально необходимое количество групп символов в пароле. По каждой группе символов можно задать настройки в таблице групп символов:
 - Допустимые символы – с помощью регулярного выражения задается множество символов группы. Например, можно расширить допустимые символы цифр, изменив регулярное выражение на следующее – `[0-99-.]`, можно расширить допустимые наборы символов букв – `[a-za-я]` и `[A-ZА-Я]`, добавить или убрать допустимые спецсимволы – `[!@#$$%^&*()+\-.?.,;:'"{}[\]><=~/\ ]`.
 - Минимум символов – сколько минимум символов из группы должно использоваться в пароле, что считалось, что группа задействована в пароле.
- Запрет использования старых паролей – настройка указывает, какое количество старых паролей должно запоминаться, чтобы при задании нового пароля не допускать ввод пароля из истории использованных паролей.
- Минимальное время жизни пароля – 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 задать пустое значение настройки.
- Максимальное время жизни пароля – максимальное время жизни пароля, в секундах; как только это время истечет, пользователю потребуются задать новый пароль. Если такую проверку не следует выполнять, то нужно задать пустое значение настройки;
- Минимальное число отличающихся символов – сколько измененных символов должно быть в новом пароле по сравнению с предыдущим (для случаев, когда пользователь меняет текущий пароль на новый). Если такую проверку не следует выполнять, то нужно задать пустое значение настройки.

4.2. Настройка доступных методов аутентификации

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.

Доступные для настройки методы первого фактора и второго фактора приведены на вкладках «первый фактор» (Рисунок 21) и «второй фактор» (Рисунок 22). Набор методов может отличаться в зависимости от типа используемой лицензии. 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 последующих разделах. Для включения или отключения метода аутентификации необходимо установить переключатель в требуемое положение.

The screenshot shows the 'Настройки аутентификации' (Authentication Settings) page, specifically the 'Первый фактор' (First Factor) tab. The page has a top navigation bar with tabs: 'Общие настройки', 'Парольные политики', 'Первый фактор' (selected), and 'Второй фактор'. A link 'Добавить внешний метод аутентификации' is in the top right. The main content area is a grid of 10 authentication methods, each with a toggle switch, a description, and a button to configure it.

Метод аутентификации	Статус	Описание	Действие
Вход по сеансу операционной системы	Выключен	При входе будет использоваться текущий сеанс операционной системы	Перейти к конфигурации метода
Логин и пароль	Включен	При входе в систему пользователю необходимо ввести логин и пароль	Перейти к настройкам
Средство электронной подписи	Выключен	При входе в систему пользователю необходимо использовать средство электронной подписи или смарт-карту	Перейти к конфигурации метода
Прокси-аутентификация	Выключен	Для аутентификации используются HTTP-заголовки прокси-сервера. В частности, в таком заголовке может быть указан сертификат, полученный в результате установленного двустороннего SSL/TLS соединения	Сконфигурируйте метод для использования
Вход через внешние сервисы идентификации	Выключен	Для входа пользователь будет перенаправлен на внешний сервис идентификации. Пользователю потребуется дать согласие на передачу данных своей учетной записи в Blitz Identity Provider.	Перейти к настройкам
Вход по разовой ссылке	Включен	Вход в систему осуществляется по специальной ссылке. Ссылка действует однократно в течение ограниченного периода времени.	Перейти к настройкам
Вход с известного устройства	Включен	После успешного входа устройство запоминается. В течение определенного периода вход в систему осуществляется автоматически	Перейти к настройкам
Подтверждение с помощью кода	Включен	После успешного первичного входа пользователю нужно ввести код из сообщения, переданного на номер мобильного телефона	Перейти к настройкам
Подтверждение с помощью ключа безопасности	Выключен	Аутентификация осуществляется с помощью ключей безопасности WebAuthn или U2F	Перейти к конфигурации метода
Вход по QR-коду	Выключен	Для входа в систему пользователь должен считать QR-код в мобильном приложении	Сконфигурируйте метод для использования

Рисунок 21 – Настройка аутентификации – вкладка «Первый фактор»

Настройки аутентификации

Общие настройки | Парольные политики | Первый фактор | **Второй фактор**

[Добавить внешний метод аутентификации](#)

Разовый пароль на основе секрета (HOTP) ☐

После успешного первичного входа пользователю нужно ввести код, сгенерированный специальным устройством - генератором одноразовых паролей

[Перейти к настройкам](#)

Разовый пароль на основе времени (TOTP) ☐

После успешного первичного входа пользователю нужно ввести код, сгенерированный мобильным приложением или устройством

[Перейти к конфигурации метода](#)

Duo push-аутентификация ☐

Подтверждение входа с помощью мобильного приложения Duo Mobile - необходимо ответить на push-уведомление

[Перейти к конфигурации метода](#)

Вход с известного устройства ☐

Позволяет не требовать усиленную аутентификацию (второй фактор) при входе с известного устройства.

Подтверждение с помощью кода ☒

После успешного первичного входа пользователю нужно ввести код из сообщения, переданного на номер мобильного телефона

[Перейти к настройкам](#)

Подтверждение с помощью электронной почты ☐

После успешного первичного входа пользователю нужно ввести код из сообщения, переданного на адрес электронной почты

[Перейти к конфигурации метода](#)

Подтверждение с помощью ключа безопасности ☐

Аутентификация осуществляется с помощью ключей безопасности WebAuthn или U2F

[Перейти к конфигурации метода](#)

Рисунок 22 – Настройка аутентификации – вкладка «Второй фактор»

4.3. 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: `${login}` – это строка, введенная пользователем в поле «логин». В результате, например, правило `email=${login}` означает, что строка, введенная пользователем, будет сравниваться с атрибутом `email` в хранилище данных (пример настройки см. Рисунок 23);

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](#)

sub = \$(login) ✖ + добавить условие

OR

email = \$(login) ✖ + добавить условие

OR

phone_number = \$(login) ✖ + добавить условие

+ добавить альтернативное правило

Рисунок 23 – Настройка входа по логину и паролю

В настройках входа по логину и пароля можно включить проверку на соответствие пароля парольной политике (см. п. 4.1). 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 (см. Рисунок 24):

- 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 24 – 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 25).

Защита от подбора пароля

При включенной защите происходит замедление процесса аутентификации. В этом случае после ввода пароля пользователь будет ожидать результата в течение периода, определенного настройкой «Время задержки». Предусмотрены следующие автоматические режимы защиты:

- на уровне системы в целом. Включается, если процент неуспешных аутентификаций достигнет определенного порога (настройка «Порог включения системной защиты»);
- на уровне пользователя. Включается, если пользователь вводит подряд определенное количество неверных паролей (настройка «Порог включения пользовательской защиты»).

Защита: Автоматический режим на уровне пользователей

Время задержки, в секундах: 3

Порог включения пользовательской защиты: 5

Порог включения системной защиты: 40

Порог выключения системной защиты: 30

Отмена Сохранить

Рисунок 25 – Настройка защиты от подбора пароля

Для усложнения автоматического подбора пароля можно включить в Blitz Identity Provider настройки «Доказательство выполнения работы». Тогда при каждом входе по логину и паролю браузер пользователя должен будет выполнить вычислительно сложную задачу. Если не предоставить решение, предоставить неправильное решение или предоставить решение не вовремя, то Blitz Identity Provider вернет ошибку. В итоге нельзя будет понять, правильные ли логин и пароль.

Доказательство выполнения работы

При каждой проверке пароля на стороне браузера будет выполняться достаточно длительная работа. Результат выполнения работы будет проверяться сервером одновременно с проверкой пароля.

☒ Запрашивать доказательство выполнения работы

Показатель сложности работы: 15

Коэффициент от 1 до 160 бит. Каждый бит увеличивает сложность в 2 раза.

Максимальный срок решения:

Максимальное время в секундах, за которое браузер должен прислать результат работы. Если значение не задано, то решение задачи ожидается за 1800 секунд.

Тестовый расчет

Отмена Сохранить

Рисунок 26 – Настройка доказательства выполнения работы браузером

В блоке настроек «Доказательство выполнения работы» можно настроить следующее:

- включить настройку «Запрашивать доказательство выполнения работы»;
- при необходимости задать настройку «Запрашивать только при наличии HTTP заголовка» — это полезно, если нужно оставить возможность автотестам выполнять вход по паролю без необходимости прохождения проверки. В этом случае на веб-сервере нужно для пользовательских запросов настроить установку заголовка из этой

- настройки, а для запросов, приходящих от автотестов, заголовков не устанавливать.
- установить «Показатель сложности работы» – задается значение коэффициента от 1 до 160 бит. Каждый бит увеличивает сложность в 2 раза. Рекомендуется значение 15 бит.
 - «Максимальный срок решения» – время в секундах, за которое браузер должен прислать результат работы. Если значение не задано, то решение задачи ожидается за 1800 секунд. Время отсчитывается с момента генерации задачи сервером в момент отображения страницы входа.

После установки настройки перед сохранением рекомендуется нажать кнопку «Тестовый расчет», чтобы получить примерное представление о времени выполнения работы на текущем устройстве.

В блоке «Правила выбора хранилища атрибутов» (см. Рисунок 27) можно настроить правила, при выполнении которых поиск пользователя будет осуществляться только в указанном хранилище. По умолчанию поиск пользователей для аутентификации происходит во всех активных хранилищах атрибутов. 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`.

Правила выбора хранилища атрибутов

По умолчанию поиск пользователей для аутентификации происходит во всех активных хранилищах. В данном блоке можно настроить правила, при выполнении которых поиск пользователя будет осуществляться в определенном хранилище.

Можно задать несколько альтернативных правил выбора хранилища. Это позволит аутентифицировать одних пользователей по одному хранилищу, других - по другому.

Для создания правила используйте [строки подстановки](#).

[Посмотреть строки подстановки](#)

Хранилище атрибутов	Правило соответствия
main	☐ not \${_rpld_} ^{.*}\$ ✖
test_db	☐ not \${_rpld_} test_app ✖

+ Добавить альтернативное условие

+ Добавить правило

Отмена Сохранить

Рисунок 27 – Настройка правил выбора хранилища атрибутов

4.4. Настройка входа с помощью средства электронной подписи

4.4.1. 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. 16.1.6);
- 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 28).
- 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 `email=${SUBJECT.E}` означает, что в атрибут `email` 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

Отмена

Сохранить

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](#)

email

=

\${SUBJECT.E}

+ добавить условие

+ добавит альтернативное правило

Отмена

Сохранить

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	Мастер	
email	= \${SUBJECT.E}		
sub	= \${SUBJECT.E}		

+ Добавить атрибут

Отмена

Сохранить

Сертификаты

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

Укажите путь к сертификату для загрузки

Обзор...

Загрузить

Серийный номер	Кому выдан	Кем выдан	Период действия	
*****	*****	*****	с 01.01.00 по 01.01.99	

Рисунок 28 – Настройка входа по электронной подписи

4.4.2. 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`.

Также можно при необходимости скорректировать настройки использования плагина электронной подписи (см. п. 16.1.7).

4.5. Настройка входа через внешние сервисы идентификации

Возможен вход с использованием следующих внешних сервисов идентификации:

- поставщика идентификации Apple ID;
- 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);
- поставщика идентификации ЕСИА (gosuslugi.ru);
- поставщика идентификации ЕСИА в режиме «Цифровой профиль» (gosuslugi.ru);
- поставщика идентификации Сбер ID;
- поставщика идентификации Tinkoff ID;
- поставщика идентификации Mos ID (СУДИР);
- поставщика идентификации, работающего по OpenID Connect;
- поставщика идентификации, работающего по SAML.

Подключения к внешним сервисам идентификации должны быть предварительно сконфигурированы в консоли управления в разделе «Поставщики идентификации» (см. п. 8 документа).

В разделе настроек «Вход через внешние сервисы идентификации» необходимо выбрать, какие из настроенных поставщиков идентификации должны использоваться при входе (см. Рисунок 29).

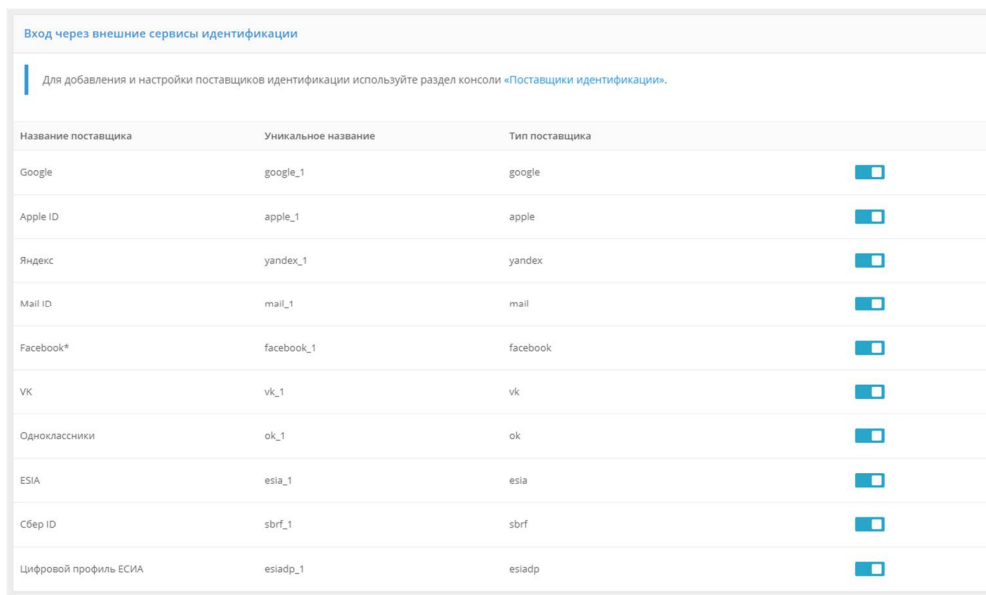


Рисунок 29 – Включение необходимых внешних сервисов идентификации

4.6. 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 30.

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
X-SSL-Client-Serial x
X-SSL-Client-S-DN x
X-SSL-Client-Email x

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.](#)

email

=

X-SSL-Client-Email

✖

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

[Отмена](#) [Сохранить](#)

Рисунок 30 – Настройка входа с помощью прокси-аутентификации

4.7. 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.

4.7.1. 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» (см. Рисунок 31).

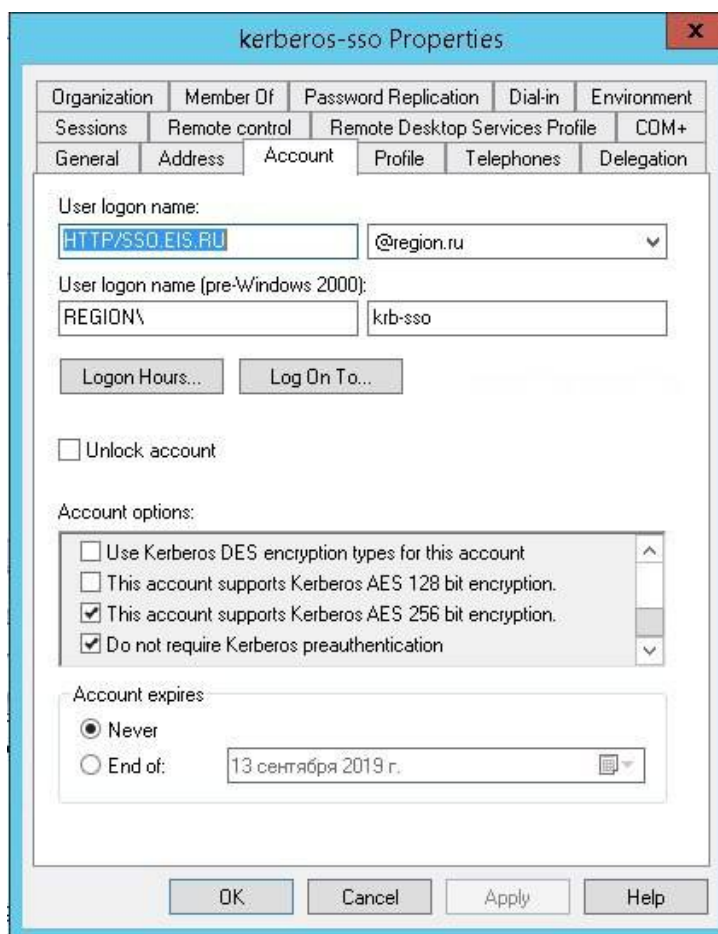


Рисунок 31 – Свойства Kerberos

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:

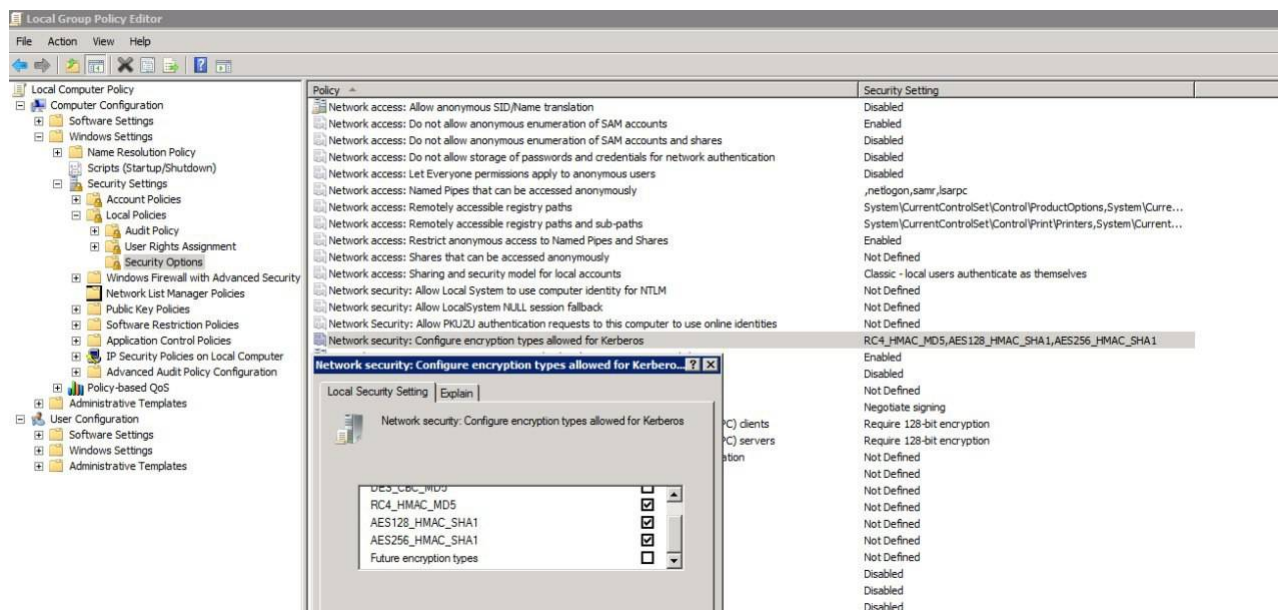


Рисунок 32 – Настройка политик шифрования

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.

4.7.2. 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 33).

При необходимости можно:

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

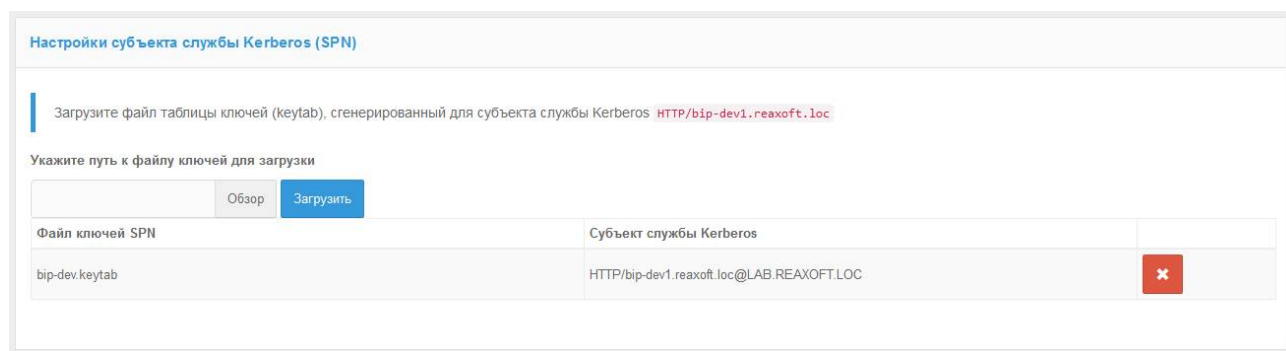


Рисунок 33 – Keytab-файл успешно загружен

Далее необходимо определить параметры соответствия Kerberos-токена (TGS) и учетной записи в Blitz Identity Provider (см. Рисунок 34).

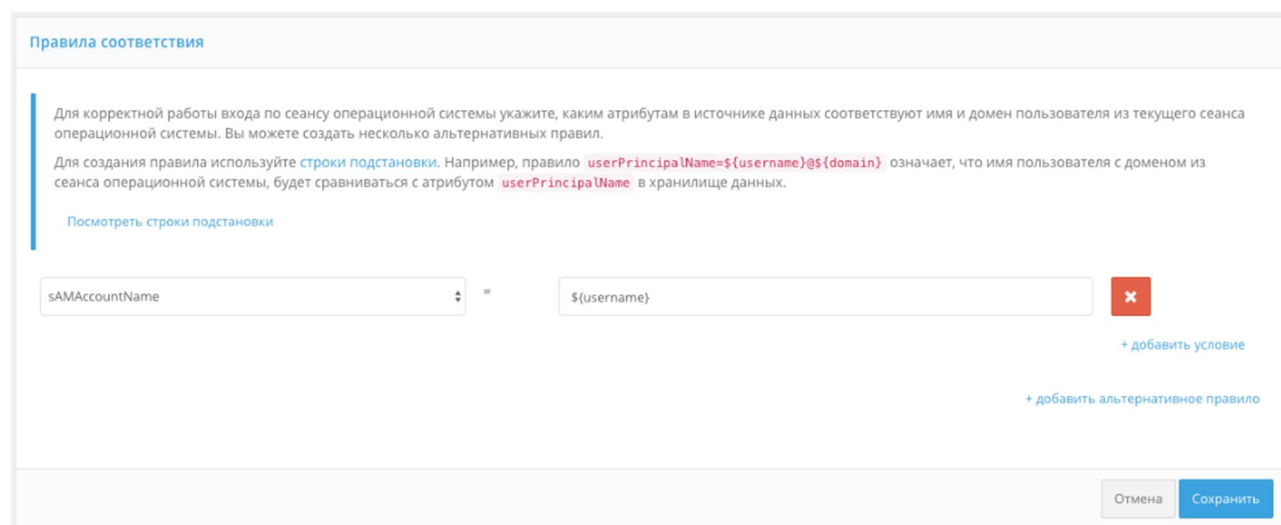


Рисунок 34 – Настройка соответствия Kerberos-идентификатора пользователя и его учетной записи в хранилище

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 (см. Рисунок 35).

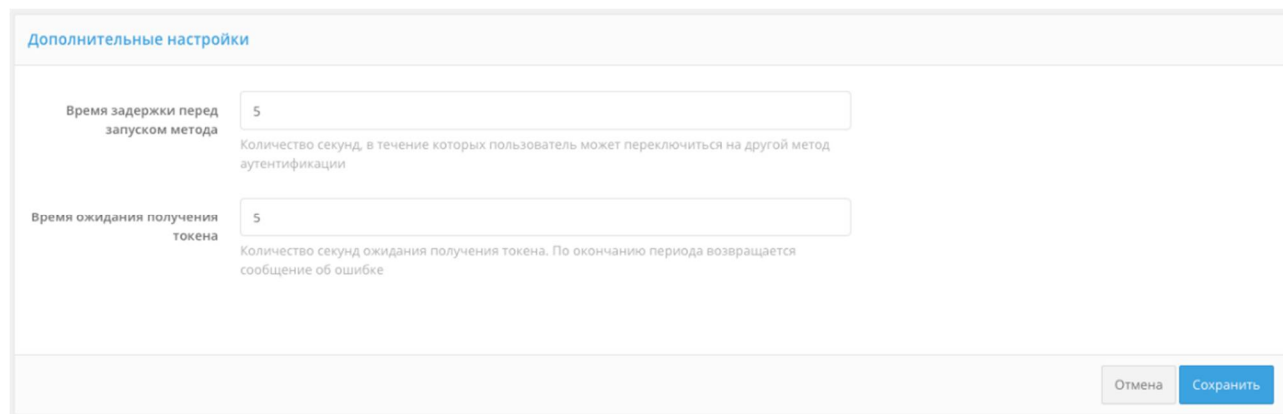


Рисунок 35 – Дополнительные настройки

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. 4.3).

4.7.3. Настройки браузеров пользователей

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

Для браузеров под операционной системой Windows нужно задать следующие настройки:

- открыть «Пуск → Панель управления», изменить вариант просмотра с «Категория» на «Мелкие значки», в открывшихся настройках выбрать «Свойства браузера»;
- в новом окне выбрать «Безопасность → Местная интрасеть» и нажать кнопку «Сайты». В открывшемся окне нажать кнопку «Дополнительно» и внести сайт с Blitz Identity Provider в список сайтов «Местная интрасеть», нажав «Добавить» (см. Рисунок 36);
- в окне «Свойства: Интернет → 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. Рисунок 37).

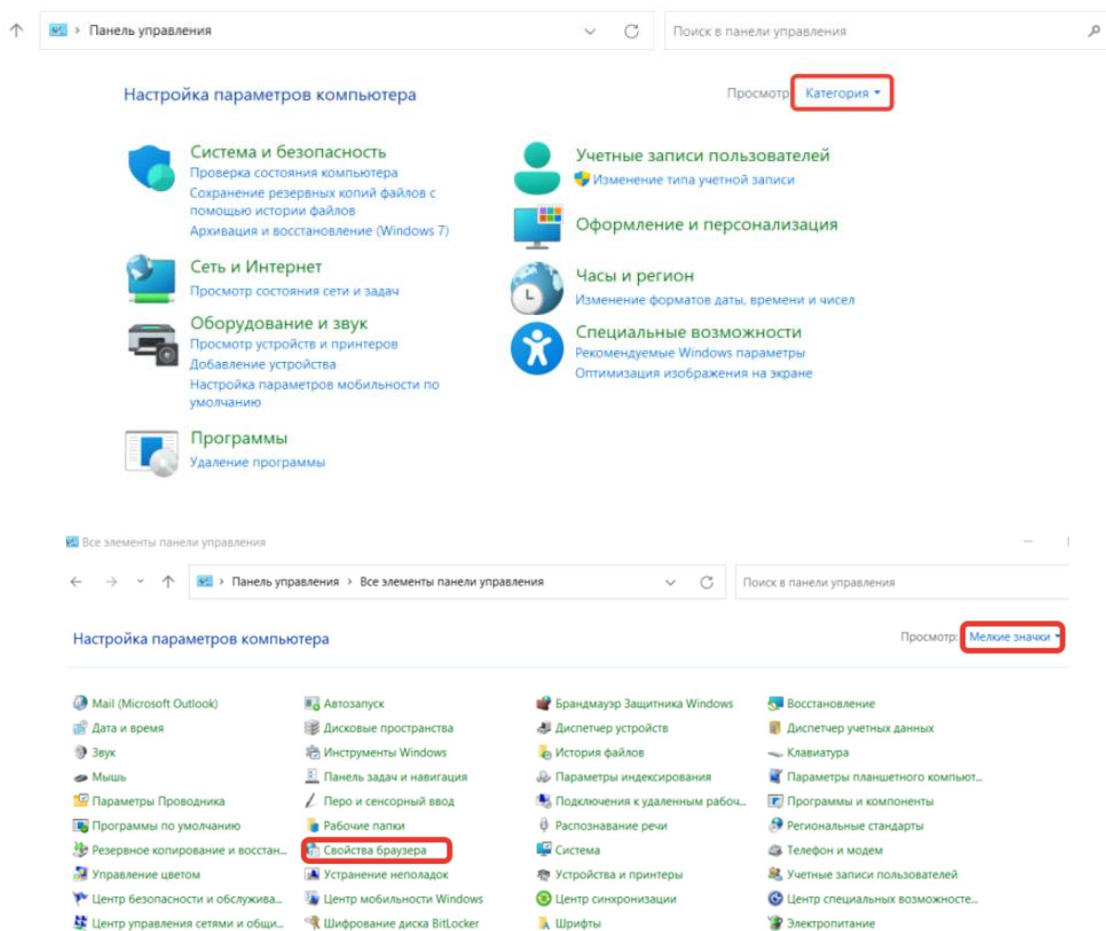


Рисунок 36 – Настройки Internet Explorer для Kerberos – включение Blitz Identity Provider в ресурсы Локальной вычислительной сети

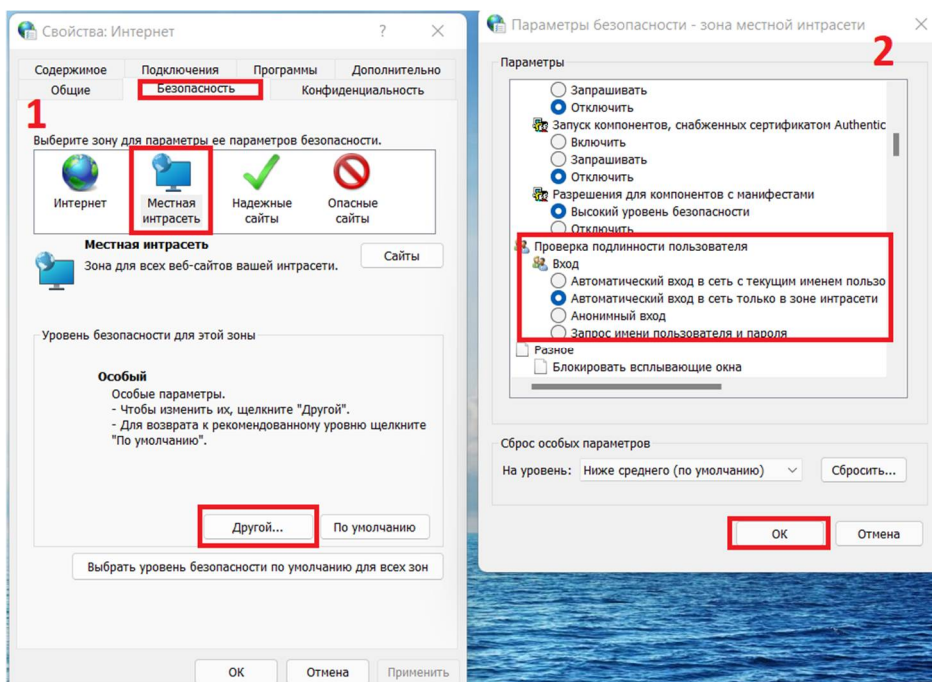


Рисунок 37 – Настройки Internet Explorer для Kerberos – включение встроенной идентификации

Можно не задавать для операционной системы Windows описанные выше настройки и в качестве альтернативы для возможности входа по сеансу операционной системы в браузере Google Chrome тогда можно запускать браузер со следующими параметрами запуска:

```
Chrome.exe -auth-server-whitelist="idp.domain.ru" -auth-negotiate-delegatewhitelist="idp.domain.ru" -auth-schemes="digest,ntlm,negotiate"
```

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

Также можно задать следующие настройки в реестр Windows, чтобы запускать браузер Google Chrome без параметров запуска.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google]

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome]
"AuthNegotiateDelegateWhitelist"="idp.domain.ru"
"AuthSchemes"="basic,digest,ntlm,negotiate"
"AuthServerWhitelist"="idp.domain.ru"
```

Для Mozilla Firefox нужно задать следующие настройки (для любых операционных систем):

- 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 «ОК»;
- 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 «ОК»;

- открыть параметр «network.auth-sspi», установить его значение в `true`;
- перезапустить браузер.

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 Apple Safari в macOS отдельная настройка не требуется.

4.7.4. 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
```

4.7.5. 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;
```

4.7.6. Отладка проблем с входом по сеансу операционной системы

Если при выполненных настройках у пользователей все же не работает вход по сеансу операционной системы, то рекомендуется на компьютере пользователя в командной строке выполнить следующую команду:

```
klist
```

Если команда успешно вернет TGS мандаты для SPN, настроенного для Blitz Identity Provider, значит нужно проверять корректность настроек на стороне браузера пользователя и в Blitz Identity Provider. Если TGS мандаты для Blitz Identity Provider отсутствуют, то можно их запросить, используя следующую команду (необходимо указать правильные SPN и имя домена компании):

```
klist get HTTP/idp.company.ru@DOMAIN.LOC
```

Если команда не вернет полученных TGS мандатов, значит нужно проверять корректность настроек на Kerberos-сервере.

4.8. 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. 4.16).

Для использования кодов подтверждения необходимо:

- настроить и включить метод аутентификации «Подтверждение с помощью кода» (см. Рисунок 38). Необходимо настроить:
 - способ идентификации учетной записи – задать регулярное выражение. Например, правило `phone_number=${login}` означает, что введенный пользователем логин в форме входа будет сопоставлен с атрибутом `phone_number`;
 - длину кода подтверждения;
 - время действия кода подтверждения;
 - количество попыток ввода кода подтверждения;
 - сконфигурировать способы отправки кода:
 - отправлять push-уведомление – нужно указать атрибут с номером мобильного телефона или иным необходимым сервису идентификатором пользователя, например, `${phone_number}`;
 - отправлять SMS – указать атрибут с номером мобильного телефона пользователя, например, `${phone_number}`;
- настроить подключение Blitz Identity Provider к SMS-шлюзу и сервису отправки push-уведомления (см. п. 13.1).

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](#)

phone_number

=

\${login}

✖

[+ добавить условие](#)

[+ добавить альтернативное правило](#)

Параметры кодов подтверждения

Длина

6

Количество символов в коде подтверждения

Время действия

300

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

Количество попыток

10

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	\${phone_number-} ✖	
SMS	\${phone_number-} ✖	

[+ 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 38 – Настройки входа с помощью кода подтверждения

4.9. 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 (см. Рисунок 39).

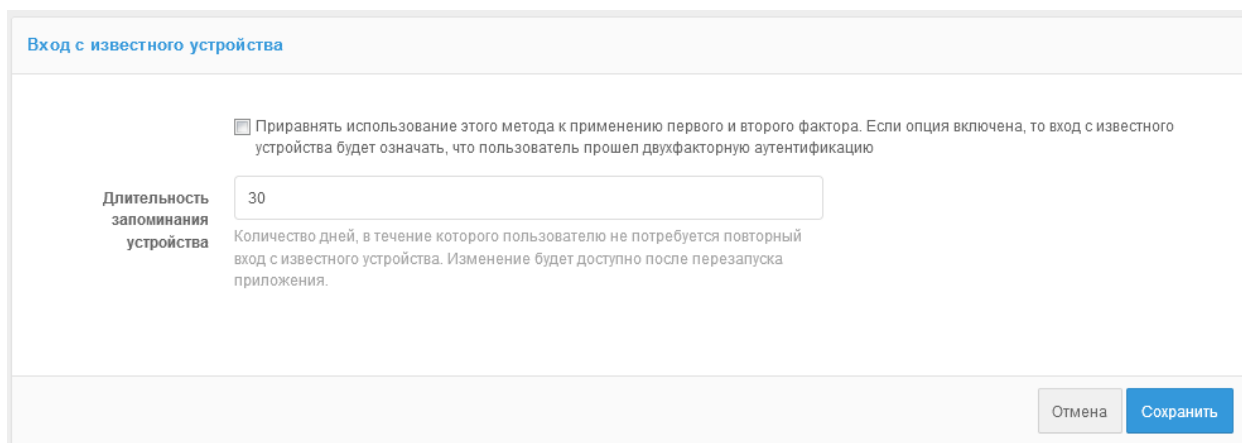


Рисунок 39 – Настройка входа с известного устройства

4.10. Вход по разовой ссылке

Вход по разовой ссылке используется для обеспечения автоматического входа после самостоятельной регистрации пользователем учетной записи, восстановлении забытого пароля или при использовании специального режима входа при открытии веб-браузера из мобильного приложения, в которое предварительно вошел пользователь¹⁸.

Настройка метода включает в себя указание времени действия ссылки (см. Рисунок 40), используемой для автоматического входа. Чтобы сработал автоматический вход, с момента выработки ссылки (после успешного окончания регистрации или восстановления пароля или получения параметра css мобильным приложением) до момента инициирования входа пользователя прошло не больше указанного в настройке времени, и что ссылка ранее не была использована.

¹⁸ Подробно этот сценарий описан в «Руководстве по интеграции» в главе «Открытие веб-ресурсов из мобильного приложения в режиме сквозной аутентификации»

Рисунок 40 – Настройка времени действия ссылки

4.11. Вход по QR-коду

В Blitz Identity Provider предусмотрена возможность настроить вход в веб-приложение по QR-коду в качестве первого фактора аутентификации. Процесс входа устроен следующим образом:

- Пользователь в браузере инициирует вход в веб-приложение. В Blitz Identity Provider отображается страница входа. На странице входа пользователь выбирает «Войти по QR-коду».
- Blitz Identity Provider отображает на странице входа пользователю QR-код и инструкцию. QR-код имеет ограниченный срок действия (пользователю показывается таймер со сроком действия QR-кода).
- Пользователь запускает мобильное приложение компании, в которое встроена¹⁹ поддержка режима входа по QR-коду, и считывает с помощью этого приложения QR-код.
- Мобильное приложение показывает пользователю детальную информацию о входе, полученную от Blitz Identity Provider (имя приложения, в которое осуществляется вход, IP-адрес, браузер и имя операционной системы устройства, на котором осуществляется вход).
- Пользователь в мобильном приложении принимает решение, разрешить или запретить вход.
- В зависимости от решения пользователя на компьютере происходит успешный вход пользователя в приложение или запрос входа отклоняется.

Настройка метода включает в себя указание следующих параметров (см. Рисунок 41):

- Время действия QR-кода – в течение этого срока пользователь должен считать QR-код и принять решение по входу;

¹⁹ Описание интеграции мобильного приложения с Blitz Identity Provider описано в «Руководство по интеграции» в главе «Добавление в мобильное приложение функции входа по QR-коду».

- Ссылка, которая будет закодирована в QR-коде – указывает, какое приложение или веб-страницу нужно запустить в случае считывания QR-кода стандартным приложением «Камера». В качестве параметра в ссылку будет передан закодированный QR-код (ссылка будет иметь вид `QR_URL?code=b0671081-cb73-4839-8bc1-8cf020457228`);
- Ссылка на логотип (опционально) – данный логотип будет отображаться в центре QR-кода.

Рисунок 41 – Настройка входа по QR-коду

4.12. Вход с помощью ключей безопасности (WebAuthn, Passkey, FIDO2)

Можно использовать ключи безопасности (WebAuthn, Passkey, FIDO2²⁰) для входа в Blitz Identity Provider. Для взаимодействия с ключами безопасности используется спецификация WebAuthn²¹. Поддерживаются следующие типы ключей:

- Внешние ключи – представляют собой аппаратные устройства в виде USB-ключей или брелоков, подключаемые к ПК, планшету и телефону с помощью USB-порта, Bluetooth или NFC. Для использования ключей не требуется установка на устройство драйверов, плагинов – взаимодействие с ключами осуществляется через встроенные возможности браузеров.
- Встроенные ключи – встроенные в устройстве и операционной системе механизмы аутентификации, поддерживающие WebAuthn:
 - Windows Hello – можно входить с помощью ПИН-кода Windows, проверки отпечатка пальца или распознавания лица;
 - Touch ID или пароль на MacBook;
 - Touch ID или Face ID на мобильном телефоне iOS или проверки отпечатка пальца

²⁰ См.: <https://fidoalliance.org/fido2/>

²¹ См.: <https://www.w3.org/TR/webauthn-2/>

или распознавания лица в Android.

Для использования ключей безопасности необходимо задать настройки в конфигурационном файле, описанные в п. 16.1.21, а также сконфигурировать метод аутентификации в консоли управления (см. Рисунок 42). В консоли управления необходимо задать следующие настройки:

- Разрешенные режимы аттестации – использование только режимов **FULL** и **FULL_NO_ROOT** повысит безопасность, но не позволит использовать для входа некоторые ключи, а также ПИН-код Windows, так как при регистрации таких ключей аттестационный объект приходит без подписи производителя чипсета или ключа или с использованием самоподписанного ключа. Использование режима **SELF** позволяет атакующему реализовать атаку «человек по середине» на подмену ключа в момент регистрации, в случае если устройство пользователя контролируется атакующим.
- Показывать метод только пользователям, которые привязали к учетной записи ключ безопасности – если Blitz Identity Provider уже идентифицировал пользователя, то он уже знает, настроены ли для учетной записи пользователя ключи безопасности. Если ключи безопасности не настроены, то можно настроить, чтобы пользователю метод входа с помощью ключа безопасности не показывался.
- Приравнять использование этого метода к применению первого и второго фактора – если опция включена, то вход по ключу безопасности будет означать, что пользователь прошел двухфакторную аутентификацию.
- Правила соответствия – при входе по ключу безопасности пользователя просят ввести логин. Настройка правил соответствия позволяет указать правила поиска соответствия учетной записи введенному логину. Для найденной учетной записи будет запрошена проверка входа по ключу безопасности. Для создания правила используется строка подстановки: **\${login}** – это строка, введенная пользователем в поле «логин». В результате, например, правило **email=\${login}** означает, что строка, введенная пользователем, будет сравниваться с атрибутом **email** в хранилище данных
- Правила выбора хранилища атрибутов – 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. 4.3).

Аутентификация по ключам безопасности

Разрешенные режимы аттестации: ☒ FULL ☒ FULL_NO_ROOT ☒ SELF

Режим аттестации проверяется при регистрации ключа безопасности пользователем. FULL - при проверке проверяется наличие root сертификата в доверенном хранилище. FULL_NO_ROOT - наличие root сертификата не обязательно. SELF - позволяет принимать самоподписанное аттестационное утверждение. По умолчанию разрешен только режим FULL.

☐ Показывать метод только пользователям, которые привязали к учетной записи ключ безопасности. По умолчанию метод показывается всем пользователям.

☐ Привязать использование этого метода к применению первого и второго фактора. Если опция включена, то вход по ключу безопасности будет означать, что пользователь прошел двухфакторную аутентификацию

Правила соответствия

Для корректной работы входа по ключам безопасности укажите, каким образом должен формироваться логин и какому атрибуту в источнике данных он соответствует. Вы можете создать несколько альтернативных правил определения логина.

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](#)

sub = \${login} ☒ + [добавить условие](#)

OR

email = \${login} ☒ + [добавить условие](#)

+ [добавить альтернативное правило](#)

Правила выбора хранилища атрибутов

По умолчанию поиск пользователей для аутентификации происходит во всех активных хранилищах. В данном блоке можно настроить правила, при выполнении которых поиск пользователя будет осуществляться в определенном хранилище.

Можно задать несколько альтернативных правил выбора хранилища. Это позволит аутентифицировать одних пользователей по одному хранилищу, других - по другому.

Для создания правила используйте **строки подстановки**.

[Посмотреть строки подстановки](#)

[Создать правило](#)

Рисунок 42 – Настройка входа с помощью ключей безопасности

4.13. Подтверждение входа разовым паролем на основе состояния (HOTP)

Для проверки второго фактора аутентификации с использованием метода аутентификации «Разовый пароль на основе секрета (HOTP)» можно использовать любой аппаратный брелок, совместимый со стандартом RFC 4226 «HOTP: An HMAC-Based One-Time Password Algorithm»²².

²² См.: <https://tools.ietf.org/html/rfc4226>

Для использования НОТР необходимо:

- настроить и включить метод аутентификации (см. Рисунок 43);
- 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;
- 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. 7.3).

Общие настройки

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

Допустимое отклонение: 10
Количество последующих кодов, которые могут быть введены для успешного входа

Отклонение для синхронизации: 100
Величина диапазона, в пределах которого будет произведен поиск кодов при выполнении синхронизации

Отмена Сохранить

Рисунок 43 – 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.

4.14. Подтверждение входа разовым паролем основе времени (TOTP)

Для проверки второго фактора аутентификации с использованием метода аутентификации «Разовый пароль на основе времени (TOTP)» можно использовать любые устройства и программы, совместимые со стандартом RFC 6238 «TOTP: Time-Based One-Time Password Algorithm»²³. В качестве таковых могут быть:

- аппаратные брелоки (генераторы разовых паролей) на основе времени;
- мобильные приложения²⁴.

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 (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».

²³ См.: <https://tools.ietf.org/html/rfc6238>

²⁴ 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

Android

Windows Mobile

Рисунок 44 – Общие настройки TOTP-аутентификации

4.15. 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.

4.15.1. 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» (см. Рисунок 45) 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 45 – 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 присутствуют в системе).

Пример загружаемого файла формата **Aladdin/SafeNet XML** для HOTP устройств с алгоритмом SHA-1 с минимальным набором параметров:

```
<?xml version="1.0" encoding="utf-8"?>
<Tokens>
  <Token serial="SN123">
    <Applications>
      <Application>
        <Seed>7bba106e428231c4d4e78361375d161c2d59b40b</Seed>
        <MovingFactor>0</MovingFactor>
      </Application>
    </Applications>
  </Token>
</Tokens>
```

Пояснения по значениям параметров в файле:

- **serial** – серийный номер устройства.
- **Seed** – ключ устройства в шестнадцатеричном (hex) формате²⁵.
- **MovingFactor** – начальное значение генератора (обычно 0).

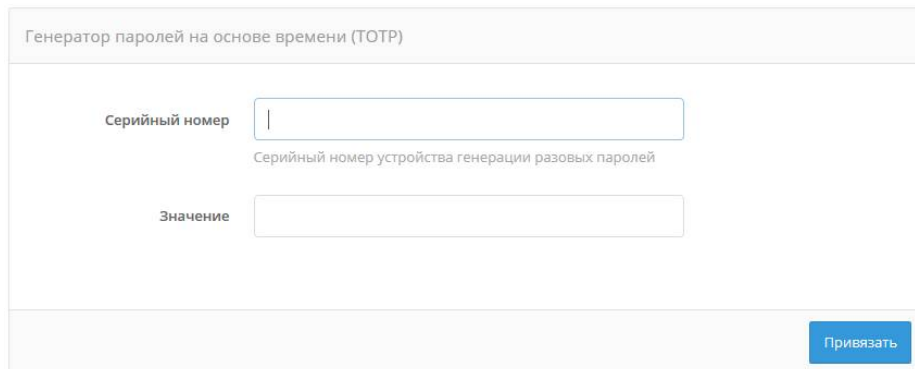
В разделе «Устройства» также можно выполнить поиск устройства по серийному номеру, посмотреть, было ли привязано и к какой учетной записи найденное устройство.

После загрузки файла следует:

- перейти к учетной записи пользователя (меню «Пользователи», см. п. 9.3.4 документа);

²⁵ Если для эмуляции HOTP-устройства используется программный генератор одноразовых кодов, то обычно в программном генераторе в качестве секрета вводится строка в формате Base32. В этом случае значение из Seed нужно из hex перекодировать в Base32, и полученное значение использовать в программном генераторе.

- 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.



The screenshot shows a web form titled "Генератор паролей на основе времени (TOTP)". It contains two input fields: "Серийный номер" (Serial number) with a placeholder "Серийный номер устройства генерации разовых паролей" (Serial number of the one-time password generation device), and "Значение" (Value). A blue button labeled "Привязать" (Bind) is located at the bottom right of the form.

Рисунок 46 – Привязка аппаратного TOTP-генератора

4.15.2. Привязка мобильного приложения

Для привязки мобильного приложения следует:

- перейти к учетной записи пользователя, которому необходимо привязать мобильное приложение (меню «Пользователи», см. п. 9.3.4 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 строку-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: NAWGF7K7DXV75DH25FCMBQ5BUPVJ2CQG
Секрет закодирован в Base32 кодировке

QR code

Сохранить

Рисунок 47 – Привязка мобильного приложения, генерирующего TOTP-коды

4.16. 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, `${phone_number}`;
 - отправлять SMS – указать атрибут с номером мобильного телефона пользователя, например, `${phone_number}`;
- настроить подключение Blitz Identity Provider к SMS-шлюзу и сервису отправки push-уведомления (см. п. 13.1).

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. 4.7.6). 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	\$(phone_number-)	✖
SMS	\$(phone_number-)	✖

+ 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 48 – Настройки кодов подтверждения для двухфакторной аутентификации

4.17. Коды подтверждения, отправляемые по электронной почте

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

Для этого необходим:

- 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. 13.3).

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.

Подтверждение с помощью электронной почты

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

Параметры отправки

Атрибут с контактом
Выражение, по которому будет формироваться адрес электронной почты для отправки кода подтверждения

Отмена Сохранить

Рисунок 49 – Настройки кодов подтверждения, отправляемых по электронной почте

4.18. Подтверждение входа с помощью Duo Mobile

Можно использовать мобильное приложение Duo Mobile²⁶ (компания Cisco) для подтверждения входа (второго фактора аутентификации).

Для этого необходимо выполнить настройки на стороне сервиса Duo Security:

- зарегистрировать учетную запись на сайте Duo²⁷;
- войти в панель администратора²⁸ 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.

²⁶ См.: <https://duo.com/product/multi-factor-authentication-mfa/duo-mobile-app>

²⁷ См.: <https://signup.duo.com/>

²⁸ См.: <https://admin.duosecurity.com/>

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

- сконфигурировать метод аутентификации «Duo push-аутентификация» (см. Рисунок 50). 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».

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)	api-123ec1a1.duosecurity.com
Интеграционный ключ (integration key)	Изменить значение
Секретный ключ (secret key)	Изменить значение

Параметры взаимодействия

Шаблон имени пользователя	\${email}	Строка подстановки, определяющая имя пользователя в запросе на вход. Например, "\${mail}"
Время действия кода активации	86400	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	=	\${given_name}	✕

[+ 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.duomobile
Windows Mobile	https://www.microsoft.com/ru-ru/store/p/duo-mobile/9nblggh08m1g

Отмена

Сохранить

Рисунок 50 – 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.

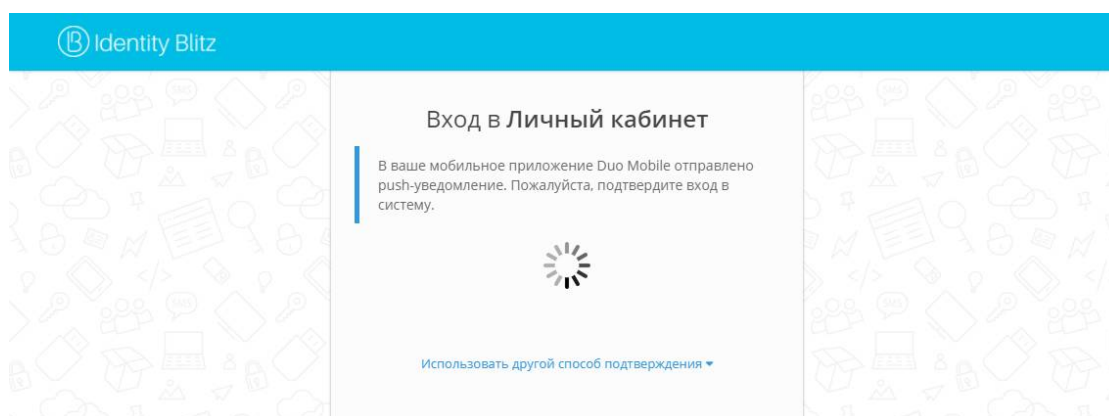


Рисунок 51 – Инициирование push-аутентификации



Рисунок 52 – Запрос push-аутентификации на смартфоне (приложение Duo Mobile)

4.19. Повторное подтверждение при входе с известного устройства

Blitz Identity Provider запоминает устройства, на которых пользователь в процессе входа подтверждал вход с помощью одного из поддерживаемых Blitz Identity Provider методов подтверждения входа.

Можно настроить в процедуре входа, чтобы после успешного подтверждения входа пользователю показывался экран с вопросом, доверяет ли пользователь браузеру, чтобы при повторных входах с этого устройства и браузера у него не запрашивалось подтверждение входа (см. Рисунок 53).

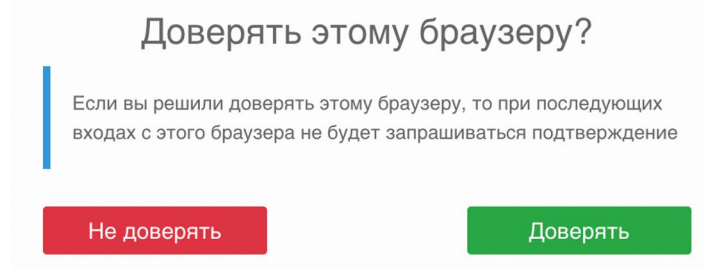


Рисунок 53 – Запрос, доверяет ли пользователь браузеру

В случае повторного входа с доверенного браузера у пользователя не будет запрашиваться подтверждение входа, если в меню «Аутентификация» в блоке «Второй фактор» включен метод аутентификации «Вход с известного устройства».

4.20. Подтверждение входа с помощью ключей безопасности (WebAuthn, Passkey, FIDO2, U2F)

Можно использовать ключи безопасности (WebAuthn, Passkey, FIDO2²⁹, U2F) для входа в Blitz Identity Provider. Поддерживаются следующие типы ключей:

- Внешние ключи – представляют собой аппаратные устройства в виде USB-ключей или брелоков, подключаемые к ПК, планшету и телефону с помощью USB-порта, Bluetooth или NFC. Для использования ключей не требуется установка на устройство драйверов, плагинов – взаимодействие с ключами осуществляется через встроенные возможности браузеров.
- Встроенные ключи – встроенные в устройстве и операционной системе механизмы аутентификации, поддерживающие WebAuthn:
 - Windows Hello – можно входить с помощью ПИН-кода Windows, проверки отпечатка пальца или распознавания лица;
 - Touch ID или пароль на MacBook;

²⁹ См.: <https://fidoalliance.org/fido2/>

- Touch ID или Face ID на мобильном телефоне iOS или проверки отпечатка пальца или распознавания лица в Android.

Для использования ключей безопасности необходимо задать настройки в конфигурационном файле, описанные в п. 16.1.21, а также сконфигурировать метод аутентификации в консоли управления (см. Рисунок 54).

В консоли управления необходимо задать настройку «Разрешенные режимы аттестации».

- Разрешенные режимы аттестации – использование только режимов **FULL** и **FULL_NO_ROOT** повысит безопасность, но не позволит использовать для входа некоторые ключи, а также ПИН-код Windows, так как при регистрации таких ключей аттестационный объект приходит без подписи производителя чипсета или ключа или с использованием самоподписанного ключа. Использование режима **SELF** позволяет атакующему реализовать атаку «человек по середине» на подмену ключа в момент регистрации, в случае если устройство пользователя контролируется атакующим.
- Показывать метод только пользователям, которые привязали к учетной записи ключ безопасности – если ключи безопасности не настроены, то можно настроить, чтобы пользователю метод подтверждения входа с помощью ключа безопасности не показывался.

Рисунок 54 – Настройка использования ключей безопасности для подтверждения входа

4.21. 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;
 - передаваемые утверждения – перечень утверждений, которые должны быть переданы внешнему методу (если параметр не задан, то внешнему методу будут переданы все доступные в сеансе входа утверждения);
 - дополнительные параметры – задаются в формате JSON. Указанные параметры будут переданы внешнему методу. Это может быть полезно, чтобы иметь возможность конфигурировать настройки внешнего метода аутентификации через консоль управления Blitz Identity Provider.
 - после сохранения включить метод – чекбокс, указывающий на то, что необходимо сразу включить метод аутентификации после сохранения настроек.
2. На стороне внешнего метода необходимо предусмотреть обработку запросов на аутентификацию и определение применимости согласно документу «Руководству по интеграции».

Добавление внешнего метода аутентификации

Идентификатор		Уникальное название (идентификатор) внешнего метода аутентификации. Будет использоваться в том числе и в аудите
URL сервиса		Адрес основного сервиса внешнего метода аутентификации. Принимает на вход текущую информацию о процессе аутентификации и возвращает HTTP-ответ, который отображается пользователю
Названия утверждений		Названия утверждений, которые сервис может установить пользователю
Передаваемые cookie		Названия cookies, которые будут пробрасываться при вызове сервиса метода
Передаваемые заголовки		Названия заголовков, которые будут пробрасываться при вызове сервиса 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
Передаваемые утверждения		Перечислите утверждения, которые необходимо отправить внешнему методу аутентификации. Если перечень не задан, то отправляются все имеющиеся утверждения
Дополнительные параметры		Укажите дополнительные параметры в формате json, которые должны быть переданы в запросе к внешнему методу аутентификации
☐ После сохранения включить метод		

ОтменаСоздать

Рисунок 55 – 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 (см. Рисунок 56).

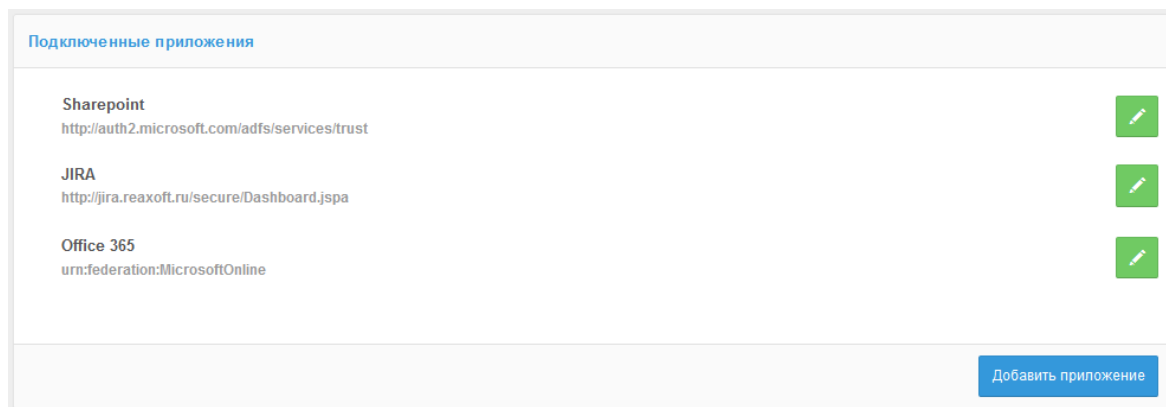


Рисунок 56 – Главный экран настройки приложений

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 и тильду), его название и домен, т.е. URL, по которому доступно данное приложение (см. Рисунок 57).

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_uri, но при этом выполняется сверка, что redirect_uri 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

Отмена Сохранить

Рисунок 57 – Базовые настройки приложения

Шаг 2. Задание стартовой страницы приложения и выбор шаблона страницы входа (см. Рисунок 58). В поле «Стартовая страница приложения» рекомендуется задать ссылку на вход в приложение, инициирующую запрос идентификации и аутентификации.

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. 14.

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.

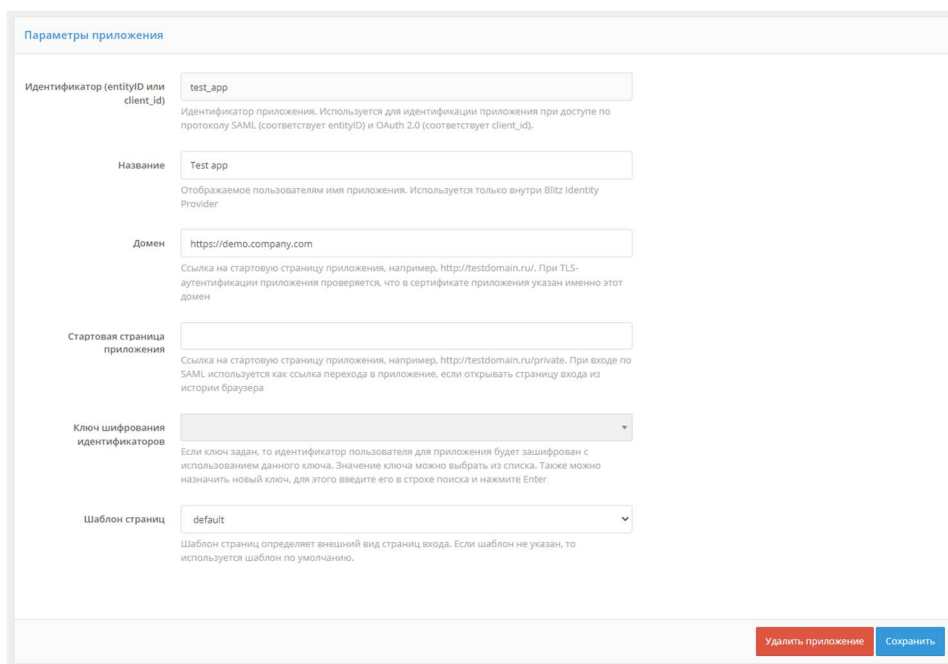


Рисунок 58 – Выбор шаблона страницы входа и настройка логгута

Шаг 3. Настройка правил доступа в приложения (см. Рисунок 59). Можно настроить правила, на основе которых Blitz Identity Provider будет принимать решение, впускать или нет пользователя в приложение.

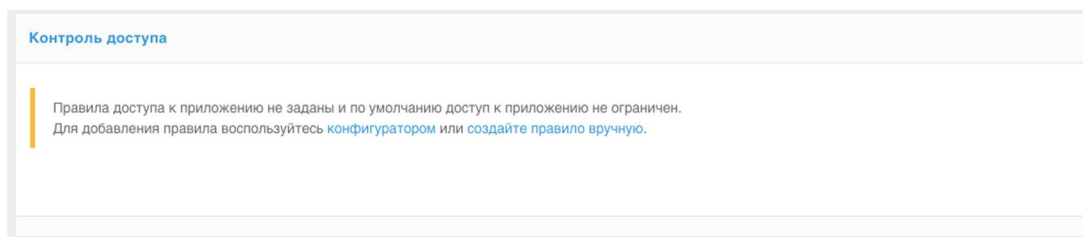


Рисунок 59 – Настройка правил контроля доступа

Правила контроля доступа можно добавить с помощью конфигулятора (см. Рисунок 60) или вручную с помощью RQL-выражения (см. Рисунок 61). В правилах можно проверять, что пользователь включен в нужную группу пользователей (настройка «Группы» в конфигураторе или правило `contains(grps,GRP1,GRP2,...)`), имеет требуемое право доступа (настройка «Полномочие» в конфигураторе или правило `contains(rights.its.SYSTEM,RIGHT_1,RIGHT2,...)`) или имеет указанное значение атрибута (настройка «Утверждение» в конфигураторе или выражение с атрибутом).

Контроль доступа

☒ В случае блокирования доступа к приложению перенаправить пользователя на страницу отказа в доступе. Если не отмечено, то пользователь будет перенаправлен в приложение с ошибкой согласно протоколу подключения

Настроенные правила доступа к приложению

В данном блоке задаются разрешающие правила доступа к приложению с использованием Resource Query Language (RQL). Для успешного доступа достаточно, чтобы хотя бы одно правило было выполнено.

Правила можно задавать вручную или использовать конфигуратор для создания простых правил.

Также у правила присутствуют название и описание. Если указано название, то оно запишется в аудит, иначе в аудит запишется текстовое представление RQL. Описание не используется в обработке и может содержать любые заметки, ассоциированные с правилом.

[Доступные данные и выражения в правилах](#)

Группы

Пользователь должен входить в указанную группу

Полномочие

к приложению

Пользователь должен иметь указанное полномочие на заданный объект. В качестве объекта могут выступать приложения, группы и пользователи

Утверждение

=

Пользователь должен иметь указанное значение утверждения

Название правила

Если у правила указано название, то оно будет записываться в аудит

Добавить правило

Сохранить

Рисунок 60 – Добавление правила доступа с помощью конфигулятора

Контроль доступа

☒ В случае блокирования доступа к приложению перенаправить пользователя на страницу отказа в доступе. Если не отмечено, то пользователь будет перенаправлен в приложение с ошибкой согласно протоколу подключения

Настроенные правила доступа к приложению

В данном блоке задаются разрешающие правила доступа к приложению с использованием Resource Query Language (RQL). Для успешного доступа достаточно, чтобы хотя бы одно правило было выполнено.

Правила можно задавать вручную или использовать конфигуратор для создания простых правил.

Также у правила присутствуют название и описание. Если указано название, то оно запишется в аудит, иначе в аудит запишется текстовое представление RQL. Описание не используется в обработке и может содержать любые заметки, ассоциированные с правилом.

[Доступные данные и выражения в правилах](#)

Текущие утверждения в сессии пользователя

Любое утверждение может быть проверено на соответствие значению

Пример: `age>=18`

Вхождение пользователя в группы

Проверяет, что пользователь входит в какую-то из указанных групп

Пример: `contains(grps,GRP1,GRP2 ...)`

Наличие у пользователя полномочий

Проверяет, что у пользователя присутствуют хотя бы одного указанное полномочие к объекту

Объекты могут быть приложением (its), группой (grps) и пользователем (пусто)

Пример проверки полномочий к приложению tech_portal : `contains(rights.its.tech_portal,CHANGE_CONFIG,VIEW_CONFIG ...)`

Правило	Название	Описание	Активировано	
			☒	☒

Конфигуратор

+ Добавить правило вручную

Сохранить

Рисунок 61 – Добавление правила доступа вручную

117

Шаг 4. Настройки протоколов подключения (см. Рисунок 62). Необходимо настроить один или несколько протоколов подключения приложения к Blitz Identity Provider.

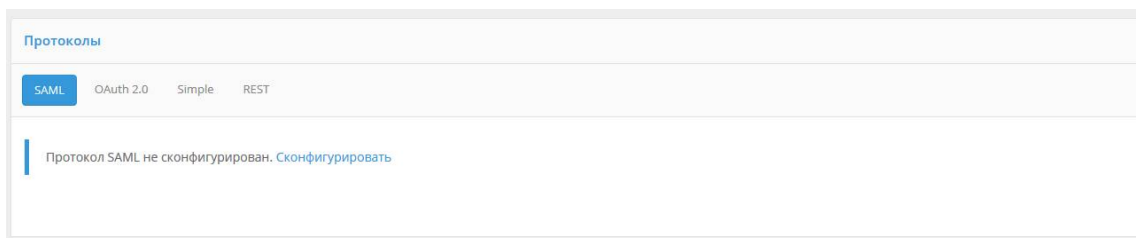


Рисунок 62 – Настройка протоколов подключения

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 проху-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 (см. Рисунок 63):

- 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).

5.2.2. Подключение по WS-Federation

- 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 периода³⁰, 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:mdext"
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	☐	✗
upn	☒	✗

+ Добавить

Сохранить

Рисунок 64 – Настройки протокола WS-Federation для приложения

³⁰ См.: <http://www.ifap.ru/library/gost/86012001.pdf>

5.2.3. Настройка SAML-атрибутов

Для регистрации SAML-атрибутов пользователя в Blitz Identity Provider используется раздел «SAML» консоли управления (см. Рисунок 65).

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).

Атрибуты

Определите, какие атрибуты пользователя из хранилища могут передаваться в SAML-приложения (поставщики услуг) в виде SAML-атрибутов

Поиск...

Атрибуты:

- UserID
- UserMail
- eduPersonPrincipalName
- urn:blitz:email
- urn:blitz:upn
- urn:blitz:givenName
- urn:blitz:sn
- urn:blitz:role

[+ Добавить новый SAML-атрибут](#)

Свойства SAML-атрибута

Название: UserID

Источник: uid

[Сохранить](#)

Кодировщик

Тип: SAML2String

Название: urn:blitz:userid

Короткое название: userid

Формат имени: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

[Удалить](#)

Кодировщик

Тип: SAML2StringNameID

Название: urn:blitz:userid

Формат имени: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

[Удалить](#)

[+ Добавить кодировщик](#)

[Удалить SAML-атрибут](#)

Рисунок 65 – 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) в блоке «Настройки взаимодействия с приложением» необходимо задать следующие настройки взаимодействия с приложением (см. Рисунок 66):

- 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 режим 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.

- указать время жизни маркера обновления (в секундах). Если параметр не задан, то берется из общих настроек из раздела «OAuth 2.0»;
- указать добавляемые в маркер идентификации (id_token) утверждения. Если приложение взаимодействует с Blitz Identity Provider по протоколу OIDC (OpenID Connect 1.0), то в качестве одного из разрешений (scope) необходимо также 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 маркер идентификации будет включен идентификатор пользователя `sub`, а также дополнительные атрибуты, перечисленные в этой настройке. Возможно добавление как атрибутов, сконфигурированных в разделе «Источники данных», так и дополнительных сессионных атрибутов (подробнее см. п. 5.3.3);
- выбрать формат маркера доступа – можно выбрать opaque или JWT. 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 переадресован пользователь после прохождения авторизации (redirect_uri)

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.

Разрешения по умолчанию

Разрешения (scope), которые будут по умолчанию выданы приложению после авторизации. 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

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

Допустимые response type

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 online-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.

Добавляемые в маркер идентификации (id_token) утверждения

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

Формат маркера доступа

Задает формат маркера доступа для данного приложения. Если формат не указан, то формат берется из общей настройки OAuth 2.0

Рисунок 66 – Настройки взаимодействия с приложением по OAuth 2.0 и OIDC

При использовании в приложении функции логута³¹ в блоке «Выход из приложения» необходимо задать следующие настройки (см. Рисунок 67):

- указать префиксы ссылок возврата при выходе. Необходимо перечислить префиксы допустимых URL страниц перенаправления пользователя после инициирования

³¹ См.: https://openid.net/specs/openid-connect-rpinitiated-1_0.html#RPLLogout

- приложением логаута. Допустимо задать один или несколько префиксов ссылок возврата;
- предопределенная ссылка возврата при выходе – ссылка, на которую будет перенаправлен пользователь после логаута из приложения, если в параметрах вызова логаута от приложения не был передан адрес возврата `post_logout_redirect_uri`;
 - отметить при необходимости опцию «Не показывать пользователю экран с подтверждением выхода из системы» – если эту настройку не отметить, то пользователю будет показан экран с запросом подтверждения выхода из приложения;
 - ссылка для очистки сессии пользователя в браузере (Front channel) – указанный адрес обработчика приложения будет вызван из фрейма браузера в случае инициирования логаута пользователя;
 - отметить при необходимости опцию «Добавлять идентификатор сессии и эмитента в ссылку очистки сессии в браузере (Front channel)» – в этом случае в браузерный обработчик логаута приложения будет передан идентификатор сессии (sid);
 - ссылка для очистки сессии пользователя в приложении (Back channel) – указанный адрес обработчика приложения будет вызван с сервера Blitz Identity Provider в случае инициирования логаута пользователя;
 - отметить при необходимости опцию «Добавлять идентификатор сессии и эмитента в ссылку очистки сессии в приложении (Back channel)» – в этом случае на адрес обработчика приложения, вызванный с сервера Blitz Identity Provider в случае инициирования логаута пользователя, будет передан `logout_token`, содержащий идентификатор сессии пользователя (sid).

Выход из приложения

Префиксы ссылок возврата при выходе

Для добавления нового URL введите его и нажмите Enter

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

Предопределенная ссылка возврата при выходе

URL, на который по умолчанию будет переадресован пользователь после успешного выхода из системы

☐ Не показывать пользователю экран с подтверждением выхода из системы

Ссылка для очистки сессии пользователя в браузере (Front channel)

URL, на который будет направлен браузер для очистки сессионной информации

☐ Добавлять идентификатор сессии и эмитента в ссылку очистки сессии в браузере (Front channel)

Ссылка для очистки сессии пользователя в приложении (Back channel)

URL, на который будет выполнен запрос для очистки сессионной информации

☐ Добавлять идентификатор сессии и эмитента в ссылку очистки сессии в приложении (Back channel)

Рисунок 67 – Настройки выхода из приложения

При использовании приложением авторизации по спецификации Device Authorization Grant³² (например, для подключения IoT-устройств, смарт ТВ, чат ботов, приложений голосовых помощников) в блоке «Настройки взаимодействия с приложением» 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`. Также в блоке «Device Authorization Grant» необходимо задать следующие настройки (см. Рисунок 68):

- формат пользовательского кода, для этого следует использовать регулярные выражения;
- время жизни пользовательского кода;
- ссылка на страницу ввода пользовательского кода;
- отметить при необходимости опцию «Добавлять в URL пользовательский код». В этом случае Blitz Identity Provider при авторизации будет 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`).

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

☐ Добавлять в URL пользовательский код

Сохранить

Рисунок 68 – Настройки Device Authorization Grant

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 (см. Рисунок 69).

³² См.: <https://tools.ietf.org/html/rfc8628>

Свойства

URL с метаданными Blitz Identity Provider: `/blitz/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: `/blitz/oauth/ae`
 На данный URL (authorization endpoint) должен быть направлен запрос на проведение авторизации пользователя

URL для получения и обновления маркера: `/blitz/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:

Время жизни маркера обновления, сек:

☐ 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

Рисунок 69 – 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 Provider³³. 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;
- изменить «Время жизни маркера обновления», используемое по умолчанию при выпуске маркеров для всех приложений;
- 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

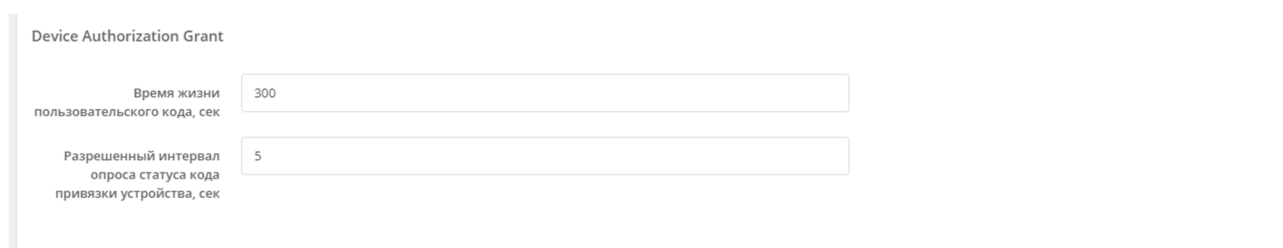
³³ См.: <https://tools.ietf.org/html/draft-ietf-oauth-discovery-10>

«Common Name (CN)» сертификата системы должен быть указан домен системы подключаемого приложения.

В разделе можно Device Authorization Grant можно определить общие настройки для взаимодействия с приложениями по этой спецификации:

- 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).



Device Authorization Grant

Время жизни пользовательского кода, сек	300
Разрешенный интервал опроса статуса кода привязки устройства, сек	5

Рисунок 70 – Настройки Device Authorization Grant

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);
- атрибуты пользователя, которые будут предоставлены по данному разрешению (атрибуты должны быть определены в меню «Источники данных»);
- 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).

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	
openid	Информация, позволяющая провести идентификацию и аутентификацию		☐	✖
profile	Основные данные профиля пользователя	☐ sub ☐ family_name ☐ middle_name ☐ given_name	☐	✖
email	Электронная почта	☐ email	☐	✖
phone_number	Номер телефона	☐ phone_number	☐	✖

+ Добавить scope

Сохранить

Рисунок 71 – Настройки scopes

Для корректной работы аутентификации по OpenID Connect 1.0 нужно убедиться, что разрешение с названием `openid` определено в этом разделе консоли. Также можно прописать атрибуты, передаваемые по этому разрешению³⁴.

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 66).

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" : [
{
```

³⁴ В этом случае указанные данные могут быть получены по маркеру доступа (access token), выданному на разрешение `openid`.

```

    "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).

Таблица 4

Пример данных, получаемых из сертификата ключа электронной подписи

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

Пример добавляемой в конфигурационный файл структуры:

```

"claims" : [
  {
    "name" : "org_OGRN",
    "value" : "SUBJECT.ОGRN"
  },
  {
    "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).

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» (см. Рисунок 72).

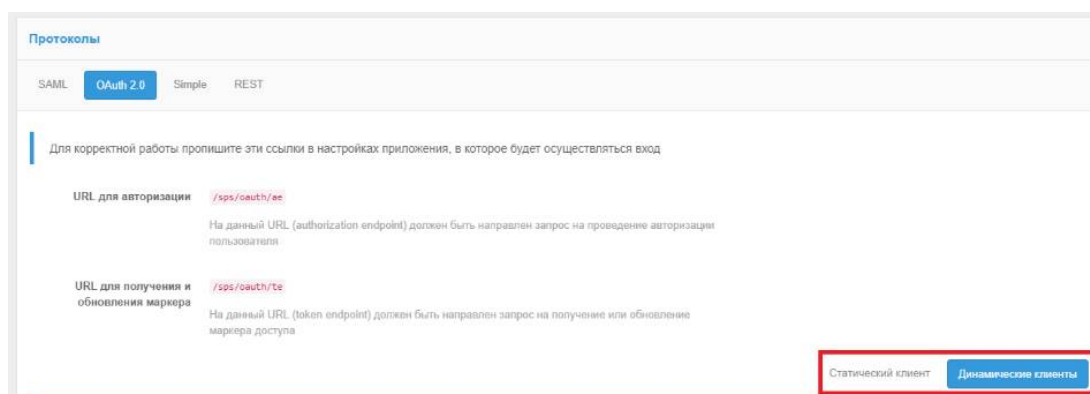


Рисунок 72 – Включение динамической регистрации клиентов

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 (см. Рисунок 73).

Настройки динамической регистрации клиентов

Разрешить динамическую регистрацию клиентов

Идентификатор приложения (software_id)

Допустимые к прямой передаче утверждения

oauth2_test_app

Используется для регистрации динамических клиентов

× Тип устройства (device_type)

Эти утверждения допускается 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

Префиксы ссылок возврата

Допустимые разрешения

Метод аутентификации при обращении к сервису выдачи маркеров

Допустимые значения grant type

Допустимые значения response type

2

Версия приложения в метаданных должна соответствовать версии в первичном маркере

http://localhost ×
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

× openid × profile
Разрешения (scope), которые будут доступны приложению.

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

× authorization_code × client_credentials
Список grant type, которые будут доступны инстансу приложения

× code × token
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	
LP5fobUKu5uPhnZBew2qheePdwW/5pA_Y2xsJdv5ybNG4QBKF8xqW3epqpbZROE8-sSrHuXisPMWNB5a_gQ8jmg	04.06.2019 16:11:34	1	×

Версия ПО

Выпустить

Рисунок 73 – Настройки динамической регистрации клиентов

5.4. Настройка Simple

Данный способ подключения приложения к Blitz Identity Provider можно применять при следующих условиях:

- Приложение нельзя подключить к Blitz Identity Provider с использованием стандартных протоколов SAML или OIDC.
- Приложение представляет собой веб-приложение, развернутое в собственной

инфраструктуре (On-Premise). Доступ пользователей к приложениям можно организовать через реверсивный прокси-сервер.

Чтобы подключить приложение к Blitz Identity Provider по протоколу Simple, необходимо:

1. В настройках приложения в консоль управления выбрать протокол Simple и задать его настройки:
 - SSL – настройка, указывающая, производится ли за прокси вызов подключаемого по Simple приложения по HTTP или по HTTPS. Рекомендуется в качестве прокси-сервера, защищающего приложение, использовать существующий веб-сервер приложения, и в таком случае соединение прокси-сервера с приложением будет осуществляться без TLS/SSL шифрования.
 - Селектор формы – задается CSS-селектор, позволяющий определить положение формы входа на странице подключаемого приложения.
 - Селектор поля с логином – задается CSS-селектор, позволяющий определить положение поля ввода логина на странице входа подключаемого приложения.
 - URL выхода по умолчанию (опциональная настройка) – указывает, какой адрес должен вызвать Blitz Identity Provider при необходимости инициировать логат в подключенном по Simple приложении в случае единого логата в Blitz Identity Provider.
 - URL для перехода после успешного выхода – указывает, какой адрес должен вызвать Blitz Identity Provider для перенаправления пользователя после успешного логата, инициированного подключенным по Simple приложением.
 - JavaScript (опциональная настройка) – встраиваемый в страницу входа подключаемого по Simple приложения JS-код, позволяющий обработать полученный от приложения ответ с результатами входа (проверить, что вход произведен успешно) и показать об этом ошибку в Blitz Identity Provider.

Пример значения:

```
var fm = document.querySelector('form[name=login]');

if (fm) {
    document.body.style.display = "none";
    var err = document.getElementById('lost-password');
    var errKey = err && err.innerHTML.indexOf('Неправильный пароль.') !== -1 ?
'incorrect_password' : 'unknown_error';
    var kvp = document.location.search.substr(1).split('&');
    kvp.push([encodeURIComponent('error'), encodeURIComponent(errKey)].join('='));
    window.location.search = kvp.join('&');
}

var aLogout = document.querySelector('#logout');
var href = aLogout ? aLogout.getAttribute("href") : null;
if (href) {
    var lp = encodeURIComponent(href);
    var slp = document.createElement('script');
```

```
slp.setAttribute('src', 'https://idp.company.com/blitz/simple/slp?app=app_id&lp=' + lp);
document.head.appendChild(slp);
}
```

Пример настроек протокола Simple для приложения представлен на рисунке ниже (см. Рисунок 74).

SSL ☐

Селектор формы
CSS селектор используется для определения расположения формы входа на странице

Селектор поля с логином
CSS селектор используется для определения поля ввода логина

URL выхода по умолчанию
URL, на который необходимо перенаправить пользователя для выхода из приложения по умолчанию

URL для перехода после успешного выхода
URL, на который пользователь будет перенаправлен в случае инициирования процедуры выхода из приложения после успешного выхода

JavaScript [Изменить](#)

[Сохранить](#)

Рисунок 74 –Настройки взаимодействия с приложением по Simple

2. Задать настройки проксирования запросов к приложению на веб-сервере.

Пример конфига для веб-сервера nginx:

```
map "" $idp_host {
    default <hostname сервера Blitz>:9000;
}

map "$http_Blitz_Idp" $idp_post_login {
    default "0";
    "prepare-login" "1";
}

map "$arg_passive" $activLogout {
    default "1";
    "true" "0";
}

upstream oc-web {
    server <hostname сервера приложения>:<порт приложения>;
}

server {
    listen 80;
    server_name <доменное имя приложения>;
    # enforce https
    return 301 https://$server_name$request_uri;
}

server {
    listen 443 ssl;
    server_name <доменное имя приложения>;

    resolver 172.27.0.20 172.25.0.50 valid=300s;
    #resolver 8.8.8.8 valid=300s;

    #ssl_certificate /etc/nginx/cert/<путь к сертификату в случае подключения по SSL>.pem;
```

```

#ssl_certificate_key      /etc/nginx/cert/<путь к контейнеру в случае подключения по SSL>.pem;

#ssl_certificate /etc/letsencrypt/live/app.company.com/fullchain.pem; # managed by Certbot
#ssl_certificate_key /etc/letsencrypt/live/app.company.com/privkey.pem; # managed by Certbot

access_log                /var/log/nginx/oc-acs.log full;
error_log                 /var/log/nginx/oc-err.log error;

### force timeouts if one of backend is died ##
proxy_next_upstream error timeout invalid_header http_500 http_502 http_503 http_504;

### Set headers #####
proxy_set_header          Accept-Encoding    "";
proxy_set_header          Host              $host;
proxy_set_header          X-Real-IP         $remote_addr;
proxy_set_header          X-Forwarded-For   $proxy_add_x_forwarded_for;
proxy_set_header          X-Forwarded-Proto $scheme;
add_header                Front-End-Https  on;
proxy_redirect            off;

proxy_set_header          Cookie "$http_cookie;domain2auth=$host";
proxy_hide_header         Content-Security-Policy;

add_header Content-Security-Policy "default-src 'self' https://$idp_host; script-src 'self'
https://$idp_host 'unsafe-eval'; img-src 'self' data: https://$idp_host; style-src 'self' 'unsafe-
inline'; font-src 'self' data:; frame-src 'self'; connect-src 'self'";

location ~ <path страницы входа в приложение>$ {
    #if ($http_referer ~* "/blitz/simple") {
    #    set $idp_post_login "1";
    #}
    if ($http_referer ~* "<доменное имя Blitz>") {
        set $idp_post_login "1";
    }
    if ($idp_post_login = "1" ) {
        proxy_pass http://oc-web$request_uri;
    }
    if ($idp_post_login = "0" ) {
        proxy_pass http://$idp_host/blitz/simple/prepare$request_uri;
        break;
    }
}
location ~ /logout$ {
    if ($activLogout = "1") {
        return 302 https://<доменное имя Blitz>/blitz/simple/active_logout?app=$host;
    }
    proxy_pass http://oc-web$request_uri;
}
location / {
    proxy_pass http://oc-web;
}
}

```

5.5. 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 (см. Рисунок 75):

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

Протоколы

SAML OAuth 2.0 Simple **REST**

Для аутентификации приложения при доступе к программному интерфейсу Blitz Identity Provider с помощью Basic-аутентификации задайте пароль. В качестве логина используйте идентификатор приложения

Пароль

Для использования TLS-аутентификации укажите допустимые значения CN из сертификата приложения. Вы можете указать несколько значений

Допустимые CN

Укажите Common Name (CN) и нажмите Enter

Сохранить

Рисунок 75 – 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 (см. Рисунок 76).

Настроенные процедуры входа			
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 76 – 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:
Идентификатор процесса должен быть корректным java-идентификатором. java-класс, описывающий процесс входа, будет иметь такое же название.

Описание:
При необходимости укажите комментарий, описывающий особенности и назначение процесса.

Приложения:
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.

Рисунок 77 – Экран создания новой процедуры входа

2. Написание исходного кода процедуры (см. Рисунок 78). 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 78 – 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`);
- запрет входа в приложение после истечения срока действия учетной записи (`AccountExpiresCheck`);
- разрешение входа в приложение только из определенных сетей (`AllowedIPs`);
- запрет работы в нескольких одновременных сессиях (`RestrictSessions`);
- сохранение в утверждениях (claims) перечня групп пользователя (`AddGroupsToToken`);
- отображение пользователю объявления при входе (`InfoPipe`);

- запрос ввода пользователем атрибута или актуализации телефона и email (`PipeAttrActAdd`);
- регистрация ключа безопасности (`WebAuthn`, `Passkey`, `FIDO2`) при входе (`PipeWebAuthn`).

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

Процедура `Require2ndFactor` 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 сработает.

```
public class Require2ndFactor implements Strategy {  
  
    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");  
  
    @Override public StrategyBeginState begin(final Context ctx) {  
        if(ctx.claims("subjectId") != null){  
            if (ctx.sessionTrack().split(",").length < 2)  
                return StrategyState.MORE(new String[]{});  
            else  
                return StrategyState.ENOUGH();  
        }  
        else {  
            return StrategyState.MORE(new String[]{});  
        }  
    }  
  
    @Override public StrategyState next(final Context ctx) {  
        if(ctx.justCompletedFactor() == 1)  
            return StrategyState.MORE(new String[]{});  
        else  
            return StrategyState.ENOUGH();  
    }  
}
```

6.2.2. Ограничение перечня доступных методов первого фактора

Процедура `FFmethods` 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;
- **qrCode** – вход по QR-коду;
- **webAuthn** – вход с помощью ключей безопасности (WebAuthn, Passkey, FIDO2).

```
public class FFmethods implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");

    @Override public StrategyBeginState 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) {
        Integer reqFactor = (ctx.user() == null) ? null : ctx.user().requiredFactor();
        if(reqFactor == null || reqFactor == 0)
            return StrategyState.ENOUGH();
        else {
            if(reqFactor == ctx.justCompletedFactor())
                return StrategyState.ENOUGH();
            else
                return StrategyState.MORE(new String[]{});
        }
    }
}
```

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

Процедура **AccessByAttribute** 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.

```
public class AccessByAttribute implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");

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

    @Override public StrategyState next(final Context ctx) {
```

```

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;
Integer reqFactor = 0;
if (ctx.user() != null) {
    reqFactor = ctx.user().requiredFactor();
}
if (reqFactor == 0)
    return StrategyState.ENOUGH();
else {
    if (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 StrategyBeginState begin(final Context ctx) {
    if (ctx.claims("subjectId") != null) {
        if ("ivanov@company.ru".equals(ctx.claims("email")))
            return StrategyState.ENOUGH();
        else
            return StrategyState.DENY;
    }
    else
        return StrategyState.MORE(new String[]{});
}

@Override public StrategyState next(final Context ctx) {
    if (!"ivanov@company.ru".equals(ctx.claims("email")))
        return StrategyState.DENY;
    Integer reqFactor = (ctx.user() == null) ? null : ctx.user().requiredFactor();
    if (reqFactor == null)
        return StrategyState.ENOUGH();
    else {
        if (reqFactor == ctx.justCompletedFactor())
            return StrategyState.ENOUGH();
        else
            return StrategyState.MORE(new String[]{});
    }
}
}

```

6.2.4. Запрет входа в приложение после истечения срока действия учетной записи

Процедура `AccountExpiresCheck` использует атрибут `accountExpires` для принятия решения о доступе пользователя к приложению. Для работы этой процедуры необходимо создать атрибут `accountExpires` с типом строка (String). В этот атрибут необходимо сохранить дату (в формате `гггг-мм-дд ЧЧ:мм`, например, `2021-09-23 13:58`), после наступления которой доступ в приложение будет заблокирован для данного пользователя. Если значение атрибута не указано, то пользователь будет допущен в приложение.

```

public class AccountExpiresCheck implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");

    @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) {
    if (ctx.claims("accountExpires") != null && isExpired(ctx.claims("accountExpires")))
        return StrategyState.DENY("account_expired", true);
    Integer reqFactor = (ctx.user() == null) ? null : ctx.user().requiredFactor();
    if(reqFactor == null || reqFactor == ctx.justCompletedFactor())
        return StrategyState.ENOUGH();
    else
        return StrategyState.MORE(new String[]{});
}

public static boolean isExpired(String strData) {
    try {
        Date now = new Date();
        Date date = new SimpleDateFormat("yyyy-M-d HH:mm").parse(strData);
        return now.after(date);
    } catch (ParseException e) {
        throw new RuntimeException(e);
    }
}
}

```

6.2.5. Разрешение входа в приложение только из определенных сетей

Процедура `AllowedIPs` использует константу `ALLOW_IP` для принятия решения о доступе пользователя к приложению. В данной константе необходимо прописать перечень сетей, из которых возможен доступ в приложение, допустимо указать несколько сетей. При входе в приложение будет проверен IP адрес пользователя на предмет его соответствия одному из значений, включенных в константу. Если он соответствует, то пользователь будет допущен в приложение, если не соответствует – в доступе будет отказано.

```

public class AllowedIPs implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");
    private final static String[] ALLOW_IP = {"179.218", "180.219"};

    @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) {
        if (!_allowed_ip(ctx.ip())) {
            return StrategyState.DENY("ip_not_allowed", true);
        }
        Integer reqFactor = (ctx.user() == null) ? null : ctx.user().requiredFactor();
        if(reqFactor == null || reqFactor == ctx.justCompletedFactor()) {
            return StrategyState.ENOUGH_BUILDER()
                .build();
        } else
            return StrategyState.MORE(new String[]{});
    }

    private Boolean _allowed_ip(final String IP) {

```

```

        int IpListIdx = 0;
        boolean ipAllowed = false;
        while (IpListIdx > -1) {
            String ip_part = ALLOW_IP[IpListIdx];
            if (IP.startsWith(ip_part)) {
                ipAllowed = true;
                IpListIdx = -1;
            } else if (ALLOW_IP.length == (IpListIdx + 1)) {
                IpListIdx = -1;
            } else {
                IpListIdx ++;
            }
        }
        return ipAllowed;
    }
}

```

6.2.6. Запрет работы в нескольких одновременных сессиях

Процедура `RestrictSessions` запрещает работу в нескольких сессиях.

```

public class RestrictSessions implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");

    @Override public StrategyBeginState begin(final Context ctx) {
        List<String> methods = new ArrayList<String>(Arrays.asList(ctx.availableMethods()));
        if ("login".equals(ctx.prompt())) {
            methods.remove("cls");
            return StrategyState.MORE(methods.toArray(new String[0]), true);
        } else {
            if (ctx.claims("subjectId") != null)
                return StrategyState.ENOUGH();
            else {
                methods.remove("cls");
                return StrategyState.MORE(methods.toArray(new String[0]));
            }
        }
    }

    @Override public StrategyState next(final Context ctx) {
        Integer reqFactor = (ctx.user() == null) ? null : ctx.user().requiredFactor();
        if (reqFactor == null || reqFactor == ctx.justCompletedFactor()) {
            return StrategyState.ENOUGH_BUILDER().singleSession(true).build();
        } else {
            return StrategyState.MORE(new String[]{});
        }
    }
}

```

6.2.7. Сохранение в утверждениях (claims) перечня групп пользователя

Процедура `AddGroupsToToken` сохраняет в утверждение `grps` перечень групп пользователя. Чтобы эта процедура работала, должны быть выполнены условия:

- сконфигурирован атрибут `memberOf`, в котором отображаются группы пользователя;
- в конфигурационный файл добавлено сессионное утверждение `grps` (см. п. 5.3.3).

При входе в приложение будет проверено наличие групп у пользователя в атрибуте `memberOf`, и если они там присутствуют, то они будут добавлены в утверждение `grps`.

```

public class AddGroupsToToken implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");

    @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) {
    Integer reqFactor = (ctx.user() == null) ? null : ctx.user().requiredFactor();
    if(reqFactor == null || reqFactor == ctx.justCompletedFactor()) {
        List<String> grps = new ArrayList<String>();
        int groupListIdx = 0;
        while (groupListIdx > -1) {
            String group = ctx.claims("memberOf." + groupListIdx + "");
            logger.debug("### group [" + groupListIdx + "] = " + group);
            if (group == null) {
                groupListIdx = -1;
            } else {
                grps.add(ctx.claims("memberOf." + groupListIdx + ""));
                groupListIdx++;
            }
        }

        LClaimsBuilder claimsBuilder = ctx.claimsBuilder();
        if (grps.size() > 0) {
            claimsBuilder.addClaim("grps", grps);
        }
        LClaims claims = claimsBuilder.build();
        return StrategyState.ENOUGH_BUILDER()
            .withClaims(claims)
            .build();
    } else
        return StrategyState.MORE(new String[]{});
}
}

```

6.2.8. Отображение пользователю объявления при входе

Процедура **InfoPipe** позволяет с периодичностью в 30 дней показывать пользователю при входе объявления. Перед использованием в процедуру нужно внести следующие изменения:

- в функции **requiredNews()** скорректировать критерии отображения объявления – например, в примере настроено, что показывать раз в 30 дней в случае если в прошлый раз пользователь при показе объявления нажал кнопку отказа;
- в функции **showNews()** вместо **<BLITZ-HOST>** указать URI, по которому из браузера пользователя доступен Blitz Identity Provider, а вместо **<CLIENT_ID>** указать идентификатор приложения (с правами на `scope openid`), от имени которого будет выполняться вспомогательное приложение;
- настроить в конфигурационном файле тип уведомления – см. п. 16.1.32;
- настроить в сообщениях текст уведомления и названия кнопок – см. п. 16.2.7.

```

public class InfoPipe implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");

    @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(Context ctx) {
    if (ctx.user() == null || ctx.user().requiredFactor() == null ||
        ctx.user().requiredFactor().equals(ctx.justCompletedFactor()))
        if (requiredNews("user_agreement", ctx)) return showNews("user_agreement", ctx);
        else return StrategyState.ENOUGH();
    else
        return StrategyState.MORE(new String[] {});
}

private boolean requiredNews(final String pipeId, final Context ctx) {
    Long readOn = ctx.user().userProps().numProp("pipes.info." + pipeId + ".disagreedOn");
    return (readOn == null || Instant.now().getEpochSecond() - readOn > 30*86400);
}

private StrategyState showNews(final String pipeId, final Context ctx) {
    String uri = "https://<BLITZ-HOST>/blitz/pipes/info/start?&pipeId=" + pipeId;
    Set<String> claims = new HashSet<String>(){
        add("instanceId");
    };
    Set<String> scopes = new HashSet<String>(){
        add("openid");
    };
    return StrategyState.ENOUGH_BUILDER()
        .withPipe(uri, "<CLIENT_ID>", scopes, claims)
        .build();
}
```

6.2.9. Запрос ввода пользователем атрибута или актуализации телефона и email

Процедура `PipeAttrActAdd` позволяет запросить у пользователя ввод значения атрибута. Для мобильного телефона и для email реализована периодическая актуализация контакта. Для обычного атрибута (в примере используется `family_name`) разовое заполнение атрибута. В случае если пользователь не захотел заполнять атрибут, то следующий запрос ввода атрибута реализован спустя определенное время.

Перед использованием в процедуру нужно внести следующие изменения:

- в константе `DOMAIN` указать URI, по которому из браузера пользователя доступен Blitz Identity Provider;
- в константах `MOBILE_ATTR`, `EMAIL_ATTR`, `COMMON_ATTR` указать имена заполняемых атрибутов;
- в константе `SKIP_TIME_IN_SEC` указать время, не чаще которого пользователю будут предлагать заполнить атрибут;
- в константе `ACT_TIME_IN_SEC` указать время, не чаще которого пользователю будут предлагать актуализировать телефон или email;
- в константе `ASK_AT_1ST_LOGIN` изменить значение, если запрос заполнения контакта нужно выполнять при первом же входе (обычно первый вход происходит сразу после регистрации учетной записи, потому сделана настройка, чтобы пользователю при первом входе не предлагали сразу заполнить данные);
- в теле процедуры вместо `_blitz_profile` указать идентификатор другого приложения, если изменение атрибутов должно делаться от приложения, отличного от Личного

кабинета;

- настроить в сообщениях тексты для атрибута из COMMON_ATTR (для email и телефона также можно скорректировать тексты по умолчанию) – см. п. 16.2.7.

```
public class PipeAttrActAdd implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");
    private final static String DOMAIN = "example.com";
    private final static String MOBILE_ATTR = "phone_number";
    private final static String EMAIL_ATTR = "email";
    private final static String COMMON_ATTR = "family_name";
    private final static Integer SKIP_TIME_IN_SEC = 30*86400;
    private final static Integer ACT_TIME_IN_SEC = 30*86400;
    private final static Boolean ASK_AT_1ST_LOGIN = false;

    @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) {
        Instant instant = Instant.now();
        Boolean new_device = false;
        if (ctx.ua().getNewlyCreated() && ctx.justCompletedFactor() == 1 && !ASK_AT_1ST_LOGIN){
            logger.debug("User with sub={} is signing in, pid={}, on a new device",
                ctx.claims("subjectId"), ctx.id());
            new_device = true;
        }
        Integer reqFactor = ctx.user().requiredFactor();
        if(reqFactor == null || reqFactor == ctx.justCompletedFactor()) {
            Enough.Builder en_builder = StrategyState.ENOUGH_BUILDER();
            if (MOBILE_ATTR !=null && !new_device && requireActualizeAttr(MOBILE_ATTR, ctx)) {
                String uri = "https://" + DOMAIN + "/blitz/pipes/act/attr?attr="
                    + MOBILE_ATTR + "&canSkip=true&appId=_blitz_profile&verified=true";
                Set<String> clms = new HashSet<String>(){
                    add("instanceId");
                    add(MOBILE_ATTR);
                };
                Set<String> scps = new HashSet<String>(){
                    add("openid");
                };
                logger.debug("User has no {} or a non-actualized {}, so opening pipe",
                    MOBILE_ATTR, MOBILE_ATTR);
                en_builder = en_builder.withPipe(uri, "_blitz_profile", scps, clms);
            } else if (EMAIL_ATTR !=null && !new_device && requireActualizeAttr(EMAIL_ATTR, ctx)) {
                String uri = "https://" + DOMAIN + "/blitz/pipes/act/attr?attr="
                    + EMAIL_ATTR + "&canSkip=true&appId=_blitz_profile&verified=true";
                Set<String> clms = new HashSet<String>(){
                    add("instanceId");
                    add(EMAIL_ATTR);
                };
                Set<String> scps = new HashSet<String>(){
                    add("openid");
                };
                logger.debug("User has no {} or a non-actualized {}, so opening pipe",
                    EMAIL_ATTR, EMAIL_ATTR);
                en_builder = en_builder.withPipe(uri, "_blitz_profile", scps, clms);
            } else if (COMMON_ATTR !=null && !new_device &&
                requireActualizeAttr(COMMON_ATTR, ctx)) {
                String uri = "https://" + DOMAIN + "/blitz/pipes/act/attr?attr="
                    + COMMON_ATTR + "&canSkip=true&appId=_blitz_profile";
                Set<String> clms = new HashSet<String>(){
                    add("instanceId");
                    add(COMMON_ATTR);
                };
                Set<String> scps = new HashSet<String>(){
                    add("openid");
                };
            }
        }
    }
}
```

```

        logger.debug("User has no {}, so opening pipe", COMMON_ATTR);
        en_builder = en_builder.withPipe(uri, "_blitz_profile", scps, clms);
    }
    return en_builder.build();
} else {
    return StrategyState.MORE(new String[]{});
}
}

private Boolean requireActualizeAttr(final String attrName, final Context ctx) {
    if (attrName.equals(MOBILE_ATTR) && (ctx.passedTrack().startsWith("1:sms") ||
        ctx.passedTrack().endsWith("sms"))) {
        logger.debug("User subjectId = {}, pid = {} used SMS, so no actualization needed",
            ctx.claims("subjectId"), ctx.id());
        return false;
    }
    if (attrName.equals(EMAIL_ATTR) && ctx.passedTrack().endsWith("email")) {
        logger.debug(
            "User subjectId = {}, pid = {} used EMAIL while auth, so no actualization needed",
            ctx.claims("subjectId"), ctx.id());
        return false;
    }
    Long skipTime = null;
    Long actTime = null;
    long now = Instant.now().getEpochSecond();
    if (ctx.user().userProps().numProp("pipes.act."+attrName+".skippedOn") != null) {
        skipTime = ctx.user().userProps().numProp("pipes.act."+attrName+".skippedOn");
    }
    if (skipTime != null && (now - skipTime) < SKIP_TIME_IN_SEC) {
        logger.debug(
            "User subjectId = {}, pid = {} has skipped update '{}' only {} seconds ago, no
actualization needed", ctx.claims("subjectId"), ctx.id(), attrName, (now - skipTime));
        return false;
    }
    if (ctx.claims(attrName) == null) return true;
    else {
        if (ctx.user().attrsCfmTimes() != null) {
            actTime = ctx.user().attrsCfmTimes().get(attrName);
        }
        if (actTime == null) return true;
        else {
            logger.debug(
                "User subjectId = {}, pid = {} has updated '{}' {} seconds ago, actualization
needed = {}", ctx.claims("subjectId"), ctx.id(), attrName, (now - actTime), ((now - actTime) >
ACT_TIME_IN_SEC));
            return ((now - actTime) > ACT_TIME_IN_SEC);
        }
    }
}
}
}

```

6.2.10. Регистрация ключа безопасности (WebAuthn, Passkey, FIDO2) при входе

Процедура `PipeWebAuthn` позволяет запросить у пользователя регистрацию ключа безопасности (WebAuthn, Passkey, FIDO2) при входе.

Перед использованием в процедуру нужно внести следующие изменения:

- в константе `DOMAIN` указать URI, по которому из браузера пользователя доступен Blitz Identity Provider;
- в константе `SKIP_TIME_IN_SEC` указать время, не чаще которого пользователю будут предлагать заполнить атрибут;
- в константе `ASK_AT_1ST_LOGIN` изменить значение, если запрос выпуска ключа безопасности нужно выполнять при первом же входе (обычно первый вход происходит сразу после регистрации учетной записи, потому сделана настройка, чтобы

- пользователю при первом входе не предлагали сразу заполнить данные);
- в теле процедуры вместо `_blitz_profile` указать идентификатор другого приложения, если изменение атрибутов должно делаться от приложения, отличного от Личного кабинета.

```
public class PipeWebAuthn implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");
    private final static String DOMAIN = "example.com";
    private final static Integer SKIP_TIME_IN_SEC = 30*86400;
    private final static Boolean ASK_AT_1ST_LOGIN = true;

    @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(Context ctx) {
        Boolean new_device = false;
        if (ctx.ua().getNewlyCreated() && ctx.justCompletedFactor() == 1 && !ASK_AT_1ST_LOGIN){
            logger.debug("User with sub={} is signing in, pid={}, on a new device",
                ctx.claims("subjectId"), ctx.id());
            new_device = true;
        }
        if (ctx.user() == null || ctx.user().requiredFactor() == null ||
            ctx.user().requiredFactor().equals(ctx.justCompletedFactor()))
            if (!new_device && requiredWebAuthn(ctx))
                return webAuthn(ctx);
            else
                return StrategyState.ENOUGH();
        else
            return StrategyState.MORE(new String[] {});
    }

    private boolean requiredWebAuthn(final Context ctx) {
        LBrowser br = ctx.ua().asBrowser();
        String deviceType = br.getDeviceType();
        String os = br.getOsName();
        List<WakMeta> keyList = null;
        logger.trace("User subjectId = {}, pid = {} is logging using device '{}' and OS '{}',
checking configured webAuthn keys", ctx.claims("subjectId"), ctx.id(), deviceType, os);
        ListResult<WakMeta> keys = ctx.dataSources().webAuthn().keysOfCurrentSubject();
        if (keys != null) {
            keyList = keys.filter(k -> deviceType.equals(k.addedOnUA().deviceType()))
                .filter(k -> os.equals(k.addedOnUA().osName())).list();
        }
        if (keys != null && keyList.size() > 0) {
            logger.debug("User subjectId = {}, pid = {} has '{}' webAuthn keys for device '{}' and
OS '{}'", ctx.claims("subjectId"), ctx.id(), keyList.size(), deviceType, os);
            return false;
        } else {
            logger.debug("User subjectId = {}, pid = {} has no configured webAuthn keys for device
'{}' and OS '{}'", ctx.claims("subjectId"), ctx.id(), deviceType, os);
        }
        Long disagreedOn = ctx.user().userProps().numProp("pipes.addKey." + deviceType + "." + os +
".disagreedOn");
        if (disagreedOn == null) {
            return true;
        } else if (Instant.now().getEpochSecond() - disagreedOn > SKIP_TIME_IN_SEC) {
            logger.debug("User subjectId = {}, pid = {} has skipped Webauthn '{}' seconds ago, so
open webAuthn pipe", ctx.claims("subjectId"), ctx.id(), (Instant.now().getEpochSecond() -
disagreedOn));
            return true;
        } else {

```

```

        logger.debug("User subjectId = {}, pid = {} has skipped Webauthn '{}' seconds ago, no
need to open webAuthn pipe", ctx.claims("subjectId"), ctx.id(), (Instant.now().getEpochSecond() -
disagreedOn));
        return false;
    }
}

private StrategyState webAuthn(final Context ctx) {
    String uri =
"https://"+DOMAIN+"/blitz/pipes/conf/webAuthn/start?&canSkip=true&appId=_blitz_profile";
    Set<String> claims = new HashSet<String>(){
        add("instanceId");
    };
    Set<String> scopes = new HashSet<String>(){
        add("openid");
    };
    Map<String, Object> urParams = new HashMap<String, Object>();
    return StrategyState.ENOUGH_BUILDER()
        .withPipe(uri, "_blitz_profile", scopes, claims).build();
}
}

```

6.2.11. Отображение пользователю списка выбора значений при входе

Процедура `ChoicePipe` позволяет показывать пользователю при входе страницы выбора списка значений. Перед использованием в процедуру нужно внести следующие изменения:

- в константе `DOMAIN` вместо `<BLITZ-HOST>` указать URI, по которому из браузера пользователя доступен Blitz Identity Provider, а в константе `CLIENT_ID` вместо `<CLIENT_ID>` указать идентификатор приложения (с правами на scope `openid`), от имени которого будет выполняться вспомогательное приложение;
- настроить в конфигурационном файле тип уведомления – см. п. 16.1.32;
- настроить в сообщениях текст уведомления и названия кнопок – см. п. 16.2.7.

```

public class ChoicePipe implements Strategy {

    private final Logger logger = LoggerFactory.getLogger("com.identityblitz.idp.flow.dynamic");

    private final static String DOMAIN = "<BLITZ-HOST>";
    private final static String CLIENT_ID = "<CLIENT_ID>";

    @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(Context ctx) {
        List<List<String>> choice = new ArrayList<List<String>>(){};
        choice.add(Arrays.asList("Value 1"));
        choice.add(Arrays.asList("Value 2"));
        try {
            if (ctx.user() == null || ctx.user().requiredFactor() == null
                || ctx.user().requiredFactor().equals(ctx.justCompletedFactor())) {
                String res = new ObjectMapper().writeValueAsString(choice);
                String choiceJson = Base64.getUrlEncoder().encodeToString(res.getBytes("UTF-8"));
                return choice(ctx, choiceJson);
            }
        } else
            return StrategyState.MORE(new String[]{});
    }
}

```

```
        } catch (Exception e) {
            e.printStackTrace();
            return null;
        }
    }

    private StrategyState choice(final Context ctx, final String choiceJson) {
        String uri = "https://" + DOMAIN + "/blitz/pipes/choice/start?appId=" + CLIENT_ID +
"&pipeId=select_value&choices=" + choiceJson;
        Set<String> claims = new HashSet<String>() {{
            add("instanceId");
        }};
        Set<String> scopes = new HashSet<String>() {{
            add("openid");
        }};
        return StrategyState.ENOUGH_BUILDER()
            .withPipe(uri, CLIENT_ID, scopes, claims)
            .build();
    }
}
```

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 ☒

Самостоятельная регистрация пользователей.

[Перейти к настройкам](#)

Восстановление доступа ☒

Самостоятельное восстановление доступа посредством отправки ссылки на адрес электронной почты или кода подтверждения в SMS-сообщении.

[Перейти к настройкам](#)

Личный кабинет ☒

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

Число символов в коде подтверждения

Время действия

Количество секунд, после которого код перестает действовать

Количество попыток

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

Параметры кода подтверждения, отправляемого по электронной почте

Длина

Число символов в коде подтверждения

Время действия

Количество секунд, после которого код перестает действовать

Сохранить

Рисунок 79 – Сервисы самообслуживания и их общие настройки

В подразделах осуществляется настройка каждого сервиса самообслуживания в отдельности.

157

7.2. 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).

7.2.1. 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"), "input-type" -> "mail"))` – 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. Для элемента задается `input-type` равный `mail`;
- `@attrInput("family_name", "Фамилия", Map("placeholder" -> "Фамилия", "error-messages" -> "Ошибка"))` – отображает на странице поле для ввода фамилии пользователя в переменную `family_name`. 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("family_name", "Фамилия", Map("placeholder" -> "Фамилия", "error-messages" -> "Ошибка"))
@attrInput("given_name", "Имя", Map("placeholder" -> "Имя", "error-messages" -> "Ошибка"))
@attrInput("phone_number", "Номер мобильного телефона", Map("placeholder" -> "+7(999)9999999",
"error-messages" -> "reg.page.mobile.req.err.msg"))
@attrInput("email", "Адрес электронной почты", Map("placeholder" -> "name@example.com", "error-
messages" -> "reg.page.email.req.err.msg", "input-type" -> "mail"))
@passwordsInput
@agreement
@attrExpr("sub", "BIP-${&random(4)}")
@submitButton
```

Пример отображения указанного шаблона в интерфейсе веб-приложения «Регистрация

пользователя» представлен на рис. 80.

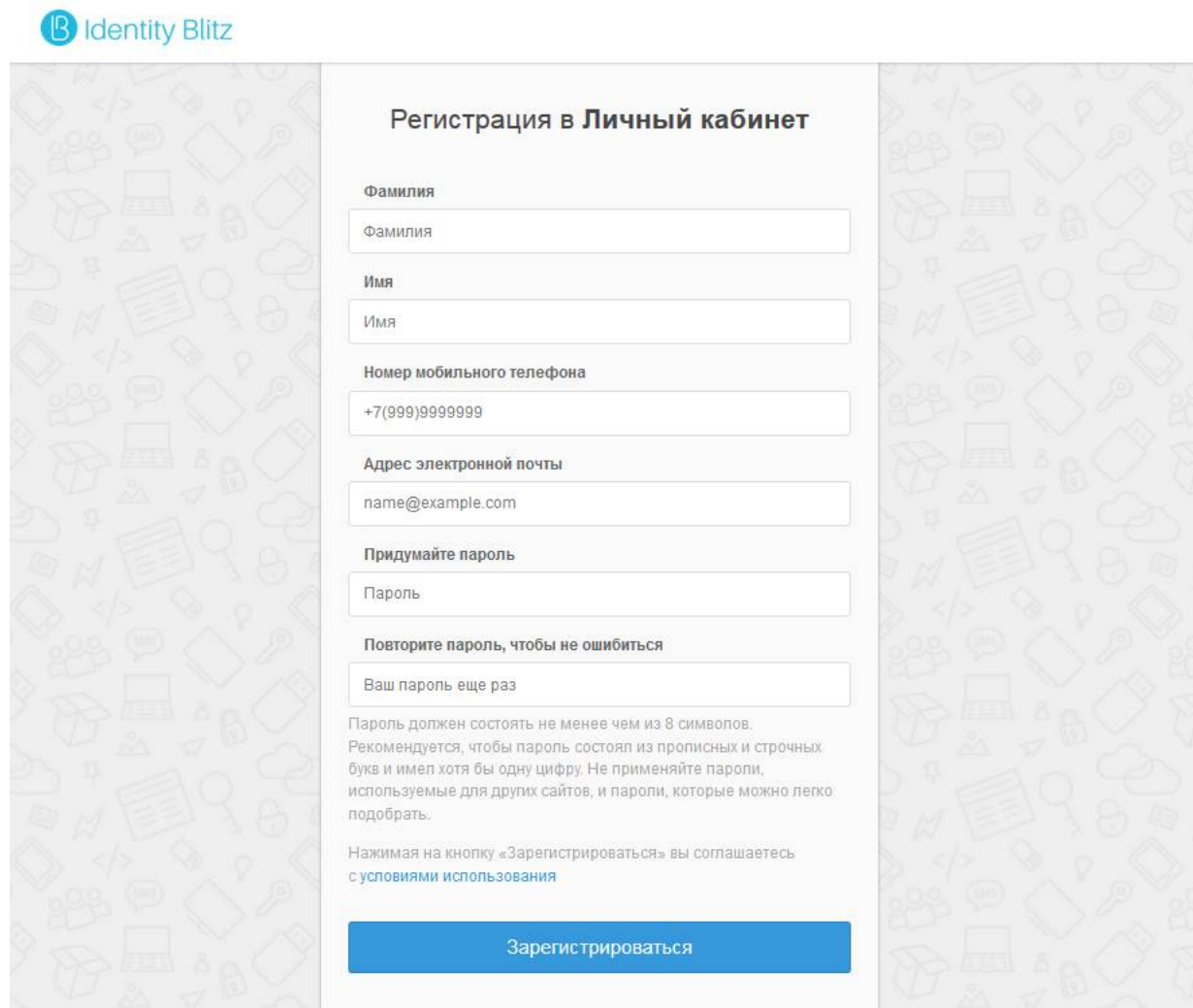


Рисунок 80 – Пример отображения регистрационной формы

Для добавления на форму регистрации выпадающего списка для выбора значений атрибута из справочника необходимо:

1. Создать на сервере Blitz Identity Provider директорию `/etc/blitz-config/custom_messages/dics`;
2. Создать файл `/etc/blitz-config/custom_messages/dics/dic_name` с содержимым справочника (вместо `dic_name` указать имя справочника, например, `company_id`).

Пример файла `company_id` для выпадающего справочника выбора компании:

```
001=Тестовая компания 1
002=Тестовая компания 2
003=Тестовая компания 3
```

Число в справочнике будет записываться в значение атрибута. Строка в справочнике будет показываться пользователю на форме регистрации.

3. проверить владельца директории `dics` и файлов справочников в ней. Владелец должен быть `blitz:blitz`.

```
chown -R blitz:blitz /etc/blitz-config/custom_messages/dics
```

4. в конфигурационном файле `blitz.conf` в блок `blitz.prod.local.idp.messages` добавить блок `dics`. В настройке `names` перечислить все имена справочников (для каждого справочника должен быть создан свой файл со значениями справочника). Например:

```
"dics" : {
  "dir" : "custom_messages/dics",
  "names" : [
    "company_id"
  ]
}
```

5. Перезапустить приложение `blitz-registration`.
6. В консоли управления в шаблоне страницы регистрации добавить строку с заполнением атрибута из справочника:

```
@attrInput("company", msg("Компания"), Map("dic" -> "company_id", "dic-default" -> "0", "sort" -> "key"))
```

7.2.2. 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. 81.

Рисунок 81 – Скриншот настроек сервиса регистрации

7.2.3. 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`.

7.2.4. 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. 16.2.2). Такой способ рекомендуется применять, если правила использования размещены на внешнем ресурсе, например, в виде отдельной веб-страницы.

7.3. Личный кабинет

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

- посмотреть или изменить данные своей учетной записи;
- посмотреть последние события безопасности (например, события входа);
- сменить пароль;
- посмотреть и настроить способы подтверждения входа (двухфакторной аутентификации);
- посмотреть и настроить ключи безопасности;
- 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;
- посмотреть события безопасности;

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

7.3.1. Отображение атрибутов пользователя

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

Пример этого блока представлен на рис. 82.

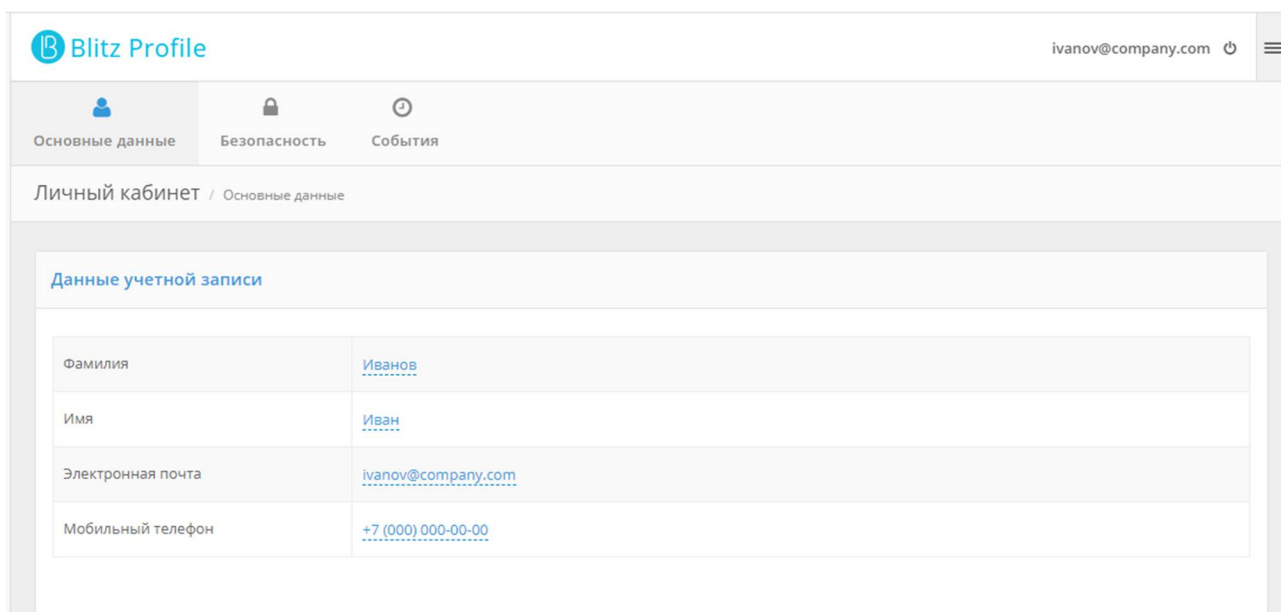


Рисунок 82 – Личный кабинет: данные учетной записи

Отображение данных пользователя определяется HTML-шаблоном. Шаблон представляет собой текстовый файл, который компилируется с помощью шаблонизатора Twirl³⁵. В шаблоне необходимо разместить функции, позволяющие пользователю в Личном 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)

³⁵ См.: <https://github.com/playframework/twirl>

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. 16.2.2 документа. Рекомендуется использовать файлы сообщений при необходимости поддержки мультиязычности.

Примеры функций:

Отображение атрибута `email`:

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

Отображение атрибута `phone_number` с возможностью его редактировать:

```
@editAsText("phone_number", "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 рис. 83.

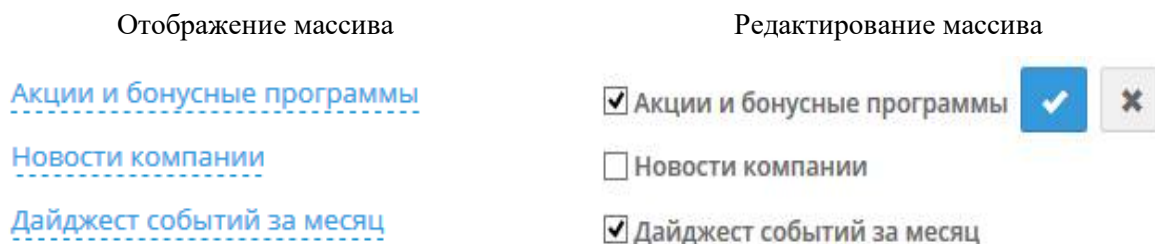


Рисунок 83 – Личный кабинет: массив строк (в режиме отображения и редактирования)

7.3.2. Дополнительные параметры

В качестве дополнительных параметров (см. Рисунок 84) можно задать:

- шаблон приветствия – информацию, которая отображается в правом верхнем углу Личного кабинета. Допустимо использовать строки подстановки. Например, `${family_name} ${given_name}` позволит отобразить фамилию и имя пользователя;

- URL для перехода после успешного выхода из Личного кабинета;
- период отображаемых пользователям событий аудита (в календарных месяцах от текущей даты);
- шаблон отображения геоданных в событиях (см. п. 16.1.31). Шаблон можно составить из следующих элементов, содержащих сведения о стране, регионе, городе и координатах: `${ip_ctr}`, `${ip_st}`, `${ip_ct}`, `${ip_lng}`, `${ip_lat}`, `${ip_rad}`
- доступные пользователям функции, т.е. функции, которые могут быть задействованы пользователем из Личного кабинета. Возможно включить или выключить следующие функции:
 - смена пароля;
 - управление ключами безопасности;
 - 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;
 - привязка ключей безопасности.

Настройки

Шаблон приветствия
Привет, \${email-}!
Отображается в правом верхнем углу Личного кабинета. Используйте строки подстановки для формирования приветствия. Например, "Привет, \${name}"

URL для перехода после успешного выхода
http://company.com
URL, на который пользователь будет перенаправлен в случае инициирования процедуры выхода из приложения после успешного выхода

Глубина просмотра аудита
3
Кол-во полных календарных месяцев просмотра событий

Шаблон отображения геоданных в событиях
"\${ip_ctr}, \${ip_st}, \${ip_ct}", \${ip_lng}", \${ip_lat}", \${ip_rad}"
Отображается в событиях. Используйте строки подстановки для формирования приветствия. Например, "\${ip_ctr}, \${ip_st}, \${ip_ct}"

Доступные пользователям функции

- ☒ Смена пароля
- ☒ Управление ключами безопасности
- ☒ Просмотр и привязка социальных сетей
- ☒ Просмотр устройств доступа
- ☒ Просмотр и отзыв разрешений
- ☒ Просмотр событий
- ☒ Привязка HOTP-генераторов
- ☒ Привязка TOTP-генераторов
- ☒ Настройка входа по коду подтверждения
- ☒ Настройка push-аутентификации
- ☒ Привязка ключей безопасности

Отмена Сохранить

Рисунок 84 – Настройка дополнительных параметров Личного кабинета

7.4. 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 (см. Рисунок 85). 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' (Access Recovery) settings page. The page title is 'Восстановление доступа'. Below the title is the section 'Настройки сервиса восстановления' (Service recovery settings). The settings are organized into several sections:

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

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

Рисунок 85 – 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. 4.5).

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 (см. Рисунок 86). Настройки поставщиков каждого из типов описаны далее в подразделах.

Подключенные внешние поставщики идентификации			
Название поставщика	Уникальное название	Тип поставщика	
Google	google_1	google	
Apple ID	apple_1	apple	
Яндекс	yandex_1	yandex	
Mail ID	mail_1	mail	
Facebook*	facebook_1	facebook	
Tinkoff ID	tcs_1	tcs	
VK	vk_1	vk	
Одноклассники	ok_1	ok	
ЕСИА	esia_1	esia	
Сбер ID	sbrf_1	sbrf	
Цифровой профиль ЕСИА	esiadp_1	esiadp	

[Добавить поставщика](#)
Google
Apple
Яндекс
Mail ID
Facebook
Тинькофф ID
ВКонтакте
Одноклассники
ЕСИА
ЦП ЕСИА
Сбер ID
Blitz Identity Provider
СУДИР

Рисунок 86 – Вид экрана настройки поставщиков идентификации

8.1. Вход через Apple ID

Для конфигурирования входа через Apple ID следует выполнить следующие шаги в разделе «Поставщики идентификации» консоли управления:

1. Добавить поставщика, имеющего тип **Apple 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.

Базовые настройки Apple

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 87 – Базовые настройки поставщика идентификации Apple ID

4. Перейти в «Apple Developer Account»³⁶ в раздел «Certificates, Identifiers & Profiles» (см. Рисунок 88)³⁷, в котором выполнить следующие операции:
 - в окне «Certificates, Identifiers & Profiles» выбрать в правом верхнем углу фильтр «App IDs». Кнопкой «+» рядом с «Identifiers» создать новый «App ID» (см. Рисунок 89):
 - выбрать тип **App**;
 - задать «Description». Он будет отображаться пользователю в окне подтверждения входа по Apple ID;
 - в «Bundle ID» задать идентификатор вида **com.company.login** на основе используемого в Blitz Identity Provider домена;
 - в «Capabilities» отметить «Sign In with Apple», нажать рядом кнопку Edit и проверить, что выбрано «Enable as a primary App ID»;
 - будет предложено завершить настройку – это все описано в последующих пунктах. Пока нужно нажать «Register».

Certificates, Identifiers & Profiles

Certificates	Identifiers +	🔍 App IDs ▾
Identifiers	NAME ▾	IDENTIFIER
Devices	BlitzIdentityProvider	com.identityblitz.blitzidp
Profiles		
Keys		
More		

Рисунок 88 – Отображение списка App IDs

³⁶ У компании должна быть действующая подписка Apple Developer ID.

³⁷ См.: <https://developer.apple.com/account/resources/identifiers/list>

Certificates, Identifiers & Profiles

< All Identifiers

Register an App ID

Back Continue

Platform

iOS, macOS, tvOS, watchOS

App ID Prefix

Y2B5234KDQ (Team ID)

Description

You cannot use special characters such as @, &, *, ' ', ", -, .

Bundle ID

☒ Explicit ☐ Wildcard

We recommend using a reverse-domain name style string (i.e., com.domainname.appname). It cannot contain an asterisk (*).

Capabilities

App Services

ENABLED	NAME
☐	Access WiFi Information ⓘ
☐	App Attest ⓘ

Рисунок 89 – Регистрация нового App ID

- в окне «Certificates, Identifiers & Profiles» выбрать в правом верхнем углу фильтр «Services App IDs». Кнопкой «+» рядом с «Identifiers» создать новый «Services App ID» (см. Рисунок 90):
 - задать «Description». Он будет отображаться пользователю в окне подтверждения входа по Apple ID;
 - задать «Identifier». Рекомендуется задать в виде `com.company.login` на основе используемого в Blitz Identity Provider домена. Позже созданный Identifier нужно будет ввести в настройках Blitz Identity Provider в качестве `client_id` в настройку «Идентификатор клиента (Service ID)»;
 - нажать «Register»;
 - выбрать созданный «Service ID». В его настройках поставить чекбокс «ENABLED» и нажать «Configure» (см. Рисунок 91);
 - в открывшемся окне проверить, что в «Primary App ID» указывается созданный ранее «App ID» (см. Рисунок 92);
 - в «Domains and Subdomains» через запятую перечислить домены, используемые Blitz Identity Provider;
 - в «Return URLs» перечислить URL возврата через запятую и с указанием `https`. Нужно указать URL, образцы которых Blitz Identity Provider показывает в настройках подключения Apple ID (см. Рисунок 94), например:

```
https://login.company.com/blitz/login/externalIdps/callback/apple/apple_1/false
https://login.company.com/blitz/profile/social/externalIdps/callbackPopup/apple/apple_1
```

- подтвердить задание настроек, нажав последовательно «Confirm»,

«Done», «Continue», «Save» в последующих экранах;

Certificates, Identifiers & Profiles

[< All Identifiers](#)

Register a Services ID

[Back](#) [Continue](#)

Description

You cannot use special characters such as @, &, *, ' , " , - , .

Identifier

We recommend using a reverse-domain name style string (i.e., com.domainname.appname). It cannot contain an asterisk (*).

Рисунок 90 – Регистрация нового Services App ID

Certificates, Identifiers & Profiles

[< All Identifiers](#)

Edit your Services ID Configuration

[Remove](#) [Continue](#)

Description

You cannot use special characters such as @, &, *, ' , " , - , .

Identifier

com.identityblitz.blitzidp-services

ENABLED	NAME
☒	Sign In with Apple

[Configure](#)

Рисунок 91 – Редактирование конфигурации Services App ID

Web Authentication Configuration

Use Sign in with Apple to let your users sign in to your app's accompanying website with their Apple ID. To configure web authentication, group your website with the existing primary App ID that's enabled for Sign in with Apple.

Primary App ID 1 App ID

BlitzIdentityProvider (Y2B5234KDQ.com.identityblitz.blit... [X](#) [v](#)

Website URLs [+](#)

Provide your web domain and return URLs that will support Sign in with Apple. Your website must support TLS 1.2 or higher. All Return URLs must be registered with the https:// protocol included in the URI string. After registering new website URLs, confirm the list you'd like to add to this Services ID and click Done. To complete the process, click Continue, then click Save.

[v](#)

Domains and Subdomains

demo.identityblitz.com [v](#)

Return URLs

https://demo.identityblitz.com/blitz/login/externall... [v](#)

https://demo.identityblitz.com/blitz/profile/social/e... [v](#)

[Cancel](#) [Done](#)

Рисунок 92 – Регистрация доменов и разрешенных адресов возврата для Services App ID

- в меню «Keys» (см. Рисунок 93) создать ключ для «Sign In with Apple». Это можно сделать только однократно, так что рекомендуется созданный ключ где-то сохранить. В Blitz Identity Provider в настоящий момент этот ключ не используется и не понадобится, но он должен быть создан и сохранен на будущее.

Certificates, Identifiers & Profiles

[← All Keys](#)

Register a New Key Continue

Key Name

You cannot use special characters such as @, &, *, ' , ", ~, . ,

ENABLE	NAME	DESCRIPTION	
☐	Apple Push Notifications service (APNs)	Establish connectivity between your notification server and the Apple Push Notification service. One key is used for all of your apps. Learn more	
☐	DeviceCheck	Access the DeviceCheck and AppAttest APIs to get data that your associated server can use in its business logic to protect your business while maintaining user privacy. Learn more	
☐	MapKit JS	Use Apple Maps on your websites. Show a map, display search results, provide directions, and more. Learn more ⓘ There are no identifiers available that can be associated with the key	Configure
☐	Media Services (MusicKit, ShazamKit)	Access the Apple Music catalog and make personalized requests for authorized users, and check audio signatures against the Shazam music catalog. ⓘ There are no identifiers available that can be associated with the key	Configure
☒	Sign in with Apple	Enable your apps to allow users to authenticate in your application with their Apple ID. Configuration is required to enable this feature. ⓘ This service must have one identifier configured.	Configure
☐	ClassKit Catalog	Publish all of your ClassKit app activities to teachers creating Handouts in Apple Schoolwork. Learn more	

Рисунок 93 – Регистрация ключа

- Перейти в консоль управления Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (см. Рисунок 94), которые включают в себя:
 - идентификатор клиента (Service ID), полученный в Apple Developer Account;
 - правила, которые будут использоваться для идентификации учетной записи в Apple ID и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Apple ID. Например, правило `email=${email}` означает, что атрибут `email` будет сопоставляться с атрибутом `email` в Apple ID;
 - 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 Apple 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 Apple ID, в Blitz Identity Provider. Например, правило `email=${email}` означает, что атрибут с именем `email` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи Apple ID (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через Apple ID данный атрибут будет обновлен в хранилище Blitz Identity Provider.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

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. 4.5).

Настройки поставщика идентификации Apple

Безопасность

Используйте настройки вашего [Apple Developer Account](#) для заполнения указанных ниже параметров. Не забудьте сохранить в настройках указанные URL перенаправления.

URL перенаправления (Return URLs) `http(s)://bip-dev1.reaxoft.ru/blitz/login/externalids/callback/apple/apple_1/false http(s)://bip-dev1.reaxoft.ru/blitz/profile/social/externalids/callbackPopup/apple/apple_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 клиента (Service ID)

Отмена Удалить Сохранить

Связывание учетных записей

Базовая настройка Расширенная настройка

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

email = \${email} ✕

+ 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
email	= \${email} ✕	☐

+ Добавить атрибут

Отмена Сохранить

Рисунок 94 – Дополнительные настройки поставщика идентификации Apple

8.2. 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 95 – Базовые настройки поставщика идентификации Google

4. Перейти в «Диспетчер API Google» (см. Рисунок 96)³⁸, 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.

³⁸ См.: <https://console.developers.google.com>

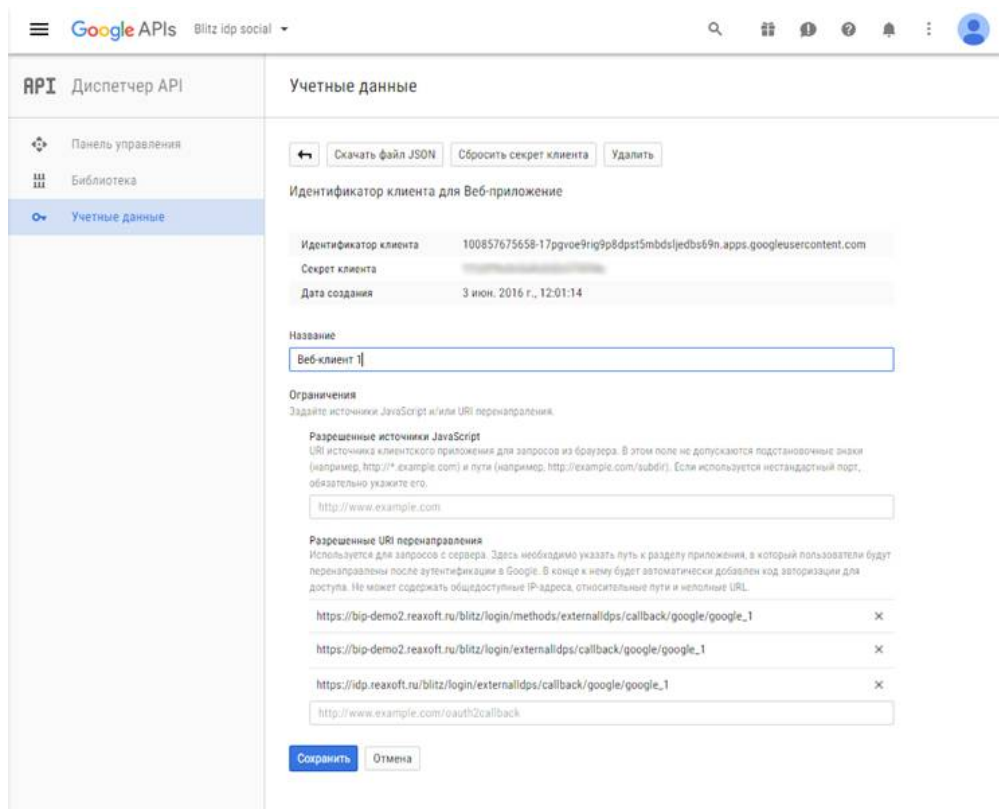


Рисунок 96 – Настройки в Диспетчере API Google

5. Перейти в консоль управления Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (см. Рисунок 97), 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 Google³⁹;
 - правила, которые будут использоваться для идентификации учетной записи в Google и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Google. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${given_name} ${family_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `given_name` и `family_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 Google,

³⁹ См.: <https://developers.google.com/+/web/api/rest/oauth#authorization-scopes>

- 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 `email=${email}` означает, что атрибут с именем `email` 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.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

8. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Базовые настройки Google

Идентификатор поставщика

google_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

Google

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

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)

https://demo.company.com/blitz/login/externaldps/callback/google/google_1/false

https://demo.company.com/blitz/profile/social/externaldps/callbackPopup/google/google_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 клиента (Client ID)

*****.apps.googleusercontent.com

Секрет клиента (Client secret)

Изменить значение

Разрешения

Запрашиваемые разрешения

email

profile

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](#)

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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

email

=

\$(email)

✖

+ 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) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=BJP-$(&random(4))` позволит присвоить атрибуту `uid` значение `BJP-xxxxxx`, где `xxxxxx` - случайное сгенерированная величина (набор цифр и букв латинского алфавита).

Атрибут

email

=

Правило

\$(email)

Мастер

☐

✖

+ Добавить атрибут

Рисунок 97 – Дополнительные настройки поставщика идентификации Google

8.3. 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.

Базовые настройки Яндекс Настройки поставщика идентификации Яндекс

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

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

Далее

Рисунок 98 – Базовые настройки поставщика идентификации Яндекс

4. Перейти в приложение «Яндекс.ОAuth»⁴⁰, 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 (см. Рисунок 97), которые включают в себя:
 - идентификатор клиента (ID приложения), полученный в приложении Яндекс.ОAuth;
 - пароль приложения, полученный в приложении Яндекс.ОAuth;

⁴⁰ См.: <https://oauth.yandex.ru/>

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

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Базовые настройки Яндекс

Идентификатор поставщика

yandex_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

Яндекс

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

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 Яндекс.

URI перенаправления (Callback URI)

http(s)://demo.company.com/blitz/login/externaldps/callback/yandex/yandex_1/false
http(s)://demo.company.com/blitz/profile/social/externaldps/callbackPopup/yandex/yandex_1

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

loginemail x logininfo x loginbirthday x

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](#)

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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

email

=

\$(email-)

x

+ 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} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - name и surname через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=61P-${&random(4)}` позволит присвоить атрибуту uid значение 61P-xxxxxx, где xxxxxx - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Пример атрибутов для маппинга

Атрибут	Правило	Мастер
email	= \$(email) x	☐ x

+ Добавить атрибут

Отмена

Сохранить

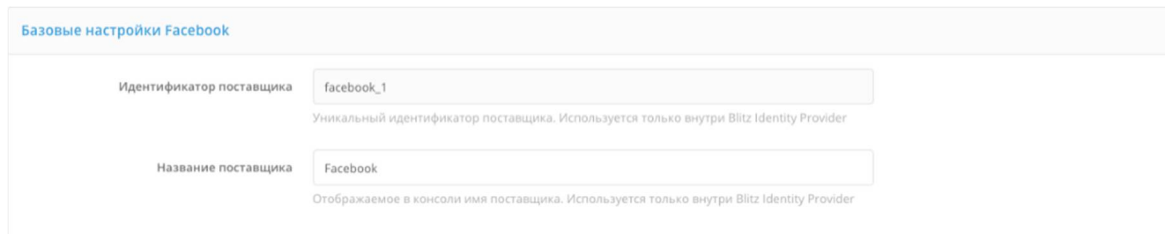
Рисунок 99 – Дополнительные настройки поставщика идентификации Яндекс

181

8.4. 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.



The screenshot shows a configuration interface titled 'Базовые настройки Facebook'. It contains two input fields. The first field is labeled 'Идентификатор поставщика' and contains the text 'facebook_1'. Below this field is a small note: 'Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider'. The second field is labeled 'Название поставщика' and contains the text 'Facebook'. Below this field is another small note: 'Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider'.

Рисунок 100 – Базовые настройки поставщика идентификации Facebook

4. Перейти в панель «Facebook для разработчиков» (см. Рисунок 101)⁴¹, 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?»

⁴¹ См.: <https://developers.facebook.com/apps/>

Рисунок 101 – Настройки в панели Facebook для разработчиков

5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (см. Рисунок 102), 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 Facebook⁴²;
- 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 `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Facebook. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${given_name} ${family_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `given_name` и `family_name` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило.

⁴² 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 `email=${email}` означает, что атрибут с именем `email` 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.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Базовые настройки Facebook*

Идентификатор поставщика: facebook_1
Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

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

Настройки поставщика идентификации Facebook*

Безопасность

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

Домен приложения: demo.company.com

URL-адреса для перенаправления OAuth:
[http\(s\)://demo.company.com/blitz/login/externalidps/callback/facebook/facebook_1/false](http(s)://demo.company.com/blitz/login/externalidps/callback/facebook/facebook_1/false)
[http\(s\)://demo.company.com/blitz/profile/social/externalidps/callback/Popup/facebook/facebook_1](http(s)://demo.company.com/blitz/profile/social/externalidps/callback/Popup/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): test_app

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

Разрешения и атрибуты

Запрашиваемые разрешения: public_profile x email x

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: id x name x email x

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.

[Отмена](#) [Удалить](#) [Сохранить](#)

Связывание учетных записей

[Базовая настройка](#) [Расширенная настройка](#)

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) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=61P-$(random(4))` позволит присвоить атрибуту uid значение `61P-xxxxxx`, где `xxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

☒ 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

email = \$(email) [+ 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) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=61P-$(random(4))` позволит присвоить атрибуту uid значение `61P-xxxxxx`, где `xxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Атрибут: email = \$(email) [Мастер](#) [+ Добавить атрибут](#)

[Отмена](#) [Сохранить](#)

Рисунок 102 – Дополнительные настройки поставщика идентификации Facebook

8.5. 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.

The screenshot shows a web form titled 'Базовые настройки ВКонтакте'. It contains three input fields with labels and explanatory text below them:

- Идентификатор поставщика**: The input field contains 'vk_1'. Below it, the text reads: 'Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider'.
- Название поставщика**: The input field contains 'VK'. Below it, the text reads: 'Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider'.
- Версия**: The input field contains '5.131'.

Рисунок 103 – Базовые настройки поставщика идентификации ВКонтакте

4. Перейти в «Панель VK для разработчиков» (см. Рисунок 104)⁴³, 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).

⁴³ См.: <https://new.vk.com/dev>

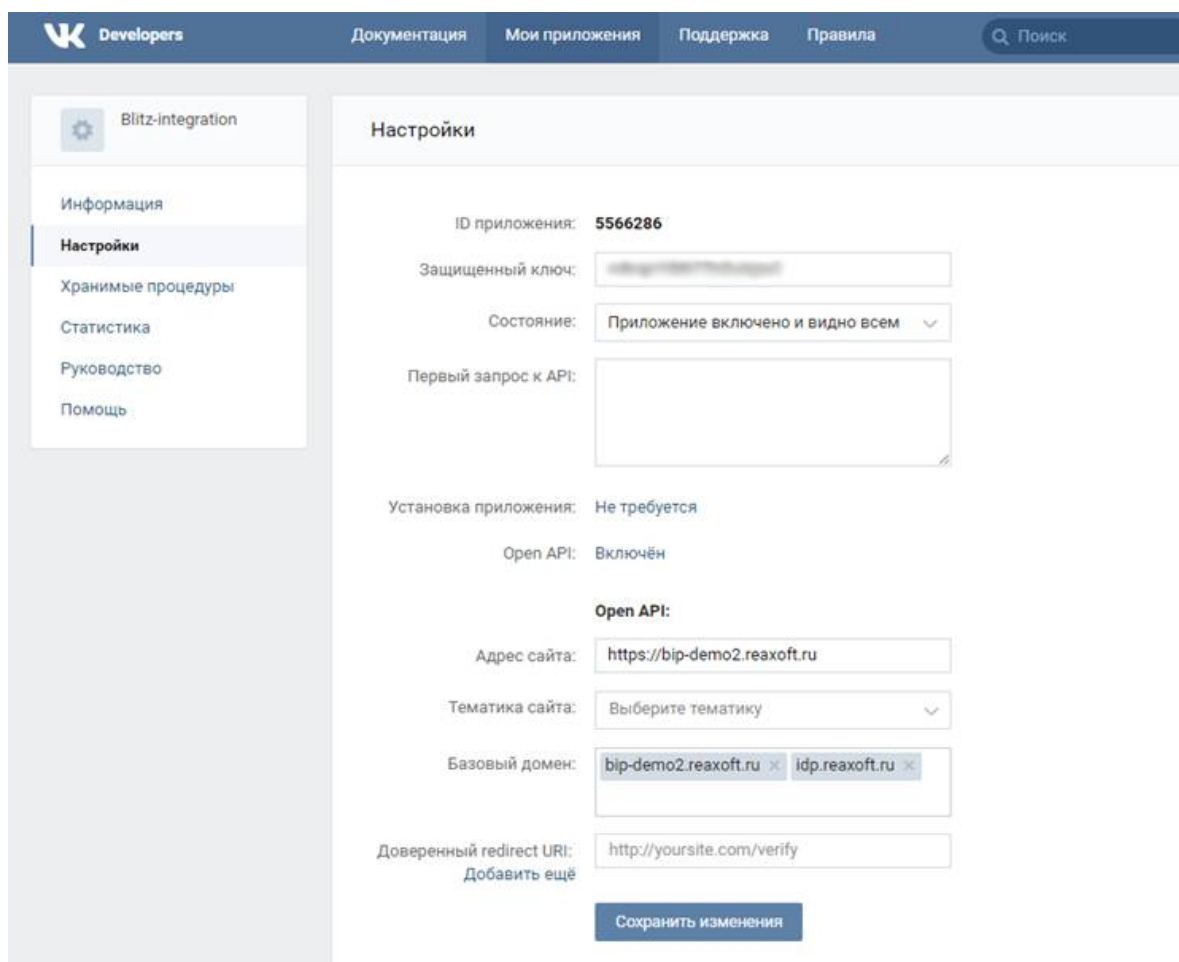


Рисунок 104 – Настройки в панели VK для разработчиков

5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (см. Рисунок 105), которые включают в себя:
 - ID приложения, полученный в панели VK для разработчиков;
 - защищенный ключ, полученный в панели VK для разработчиков;
 - запрашиваемые разрешения, предусмотренные в ВКонтакте⁴⁴;
 - правила, которые будут использоваться для идентификации учетной записи в ВКонтакте и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от ВКонтакте. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${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;

⁴⁴ 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 `email=${email}` означает, что атрибут с именем `email` 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.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п 4.5).

Базовые настройки ВКонтакте

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

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

5.52

Доверенные redirect URI

http(s)://demo.company.com/blitz/login/externalids/callback/vk/vk_1?false
 http(s)://demo.company.com/blitz/profile/social/externalids/callback/Popup/vk/vk_1

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

test

Защищенный ключ

Изменить значение

Разрешения

Запрашиваемые разрешения

email

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](#)

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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

email

=

\$(email)

✖

+ 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 формирования 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) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=81P-$(&random(4))` позволит присвоить атрибуту uid значение `81P-XXXXXX`, где `XXXXXX` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Атрибут

email

=

\$(email)

✖

+ Добавить атрибут

Отмена

Сохранить

Рисунок 105 – Дополнительные настройки поставщика идентификации ВКонтакте

189

8.6. 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 106 – Базовые настройки поставщика идентификации сети «Одноклассники»

4. Перейти на страницу «OAuth авторизация»⁴⁵, 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 (см. Рисунок 107), которые включают в себя:
 - ввод регистрационных данных приложения, полученных ранее:
 - название приложения (Application ID);
 - секретный ключ приложения;
 - публичный ключ приложения;

⁴⁵ 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} ${last_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `first_name` и `last_name` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт сети Одноклассники, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из Одноклассники, в Blitz Identity Provider. Например, правило `email=${email}` означает, что атрибут с именем `email` 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.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п 4.5).

Базовые настройки Одноклассники

Идентификатор поставщика

ok_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

Одноклассники

Отображаемое в консоли имя поставщика. Используется только внутри 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

https://demo.company.com/blitz/login/externaldps/callback/ok_1/false
https://demo.company.com/blitz/profile/social/externaldps/callbackPopup/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)

admin

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

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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

email

=

\$({email})

x

+ 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} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - name и surname через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=BP-${brandom(4)}` позволит присвоить атрибуту uid значение BP-xxxxxx, где xxxxxx - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Пример атрибутов для маппинга

Атрибут

email

=

\$({email})

x

+ Добавить атрибут

Отмена

Сохранить

Рисунок 107 – Дополнительные настройки поставщика идентификации сети Одноклассники

193

8.7. 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 108 – Базовые настройки поставщика идентификации Mail ID

4. Перейти на странице «Создание приложения» Mail.ru⁴⁶, 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 (см. Рисунок 109), которые включают в себя:
 - идентификатор клиента (ID приложения), полученный ранее;
 - секрет приложения, полученный ранее;
 - запрашиваемые разрешения (scope), например, **userinfo**;

⁴⁶ 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} ${last_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `first_name` и `last_name` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило.
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт Mail ID, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из Mail ID, в Blitz Identity Provider. Например, правило `email=${email}` означает, что атрибут с именем `email` 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.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Базовые настройки Mail ID

Идентификатор поставщика

mail_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

Mail ID

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

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)://demo.company.com/blitz/login/externaldps/callback/mail/mail_1/false
http(s)://demo.company.com/blitz/profile/social/externaldps/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

admin

Секрет приложения

Изменить значение

Разрешения

Запрашиваемые разрешения

userinfo

Для добавления разрешения введите его имя и нажмите Enter

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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

email

=

`$(email)`

✖

+ 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).

Пример атрибутов для маппинга

Атрибут	Правило	Мастер	
email	= <code>\$(email)</code>	☐	✖

+ Добавить атрибут

Отмена

Сохранить

Рисунок 109 – Дополнительные настройки поставщика идентификации Mail ID

197

8.8. 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 110 – 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 (см. п. 16.1.19).
5. Сертификат ключа необходимо зарегистрировать на Технологическом портале ЕСИА (см. следующий пункт).
6. Осуществить регистрацию информационной системы организации через Технологический портал ЕСИА⁴⁷, 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 (см. Рисунок 111);
 - сохранить данные и перейти к настройке сертификатов информационной системы;
 - загрузить сертификат для зарегистрированной информационной системы на Технологическом портал (см. Рисунок 112);

⁴⁷ 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

Проверочная система

Отображаемое название

Проверочная система

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

CHECKSYS

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

Проверочная система

URL системы

http://identityblitz.ru

+

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

RS256

▼

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

По умолчанию ▼

Время жизни access token, мин

60

min: 10; max: 180

Время жизни refresh token, мин

1051200

min: 60; max: 1051200

ОТВЕТСТВЕННЫЙ ЗА ЭКСПЛУАТАЦИЮ СИСТЕМЫ

ФИО

Иванов Иван Иванович

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

Сохранить

Отмена

Рисунок 111 – Добавление системы в Технологическом портале ЕСИА

199

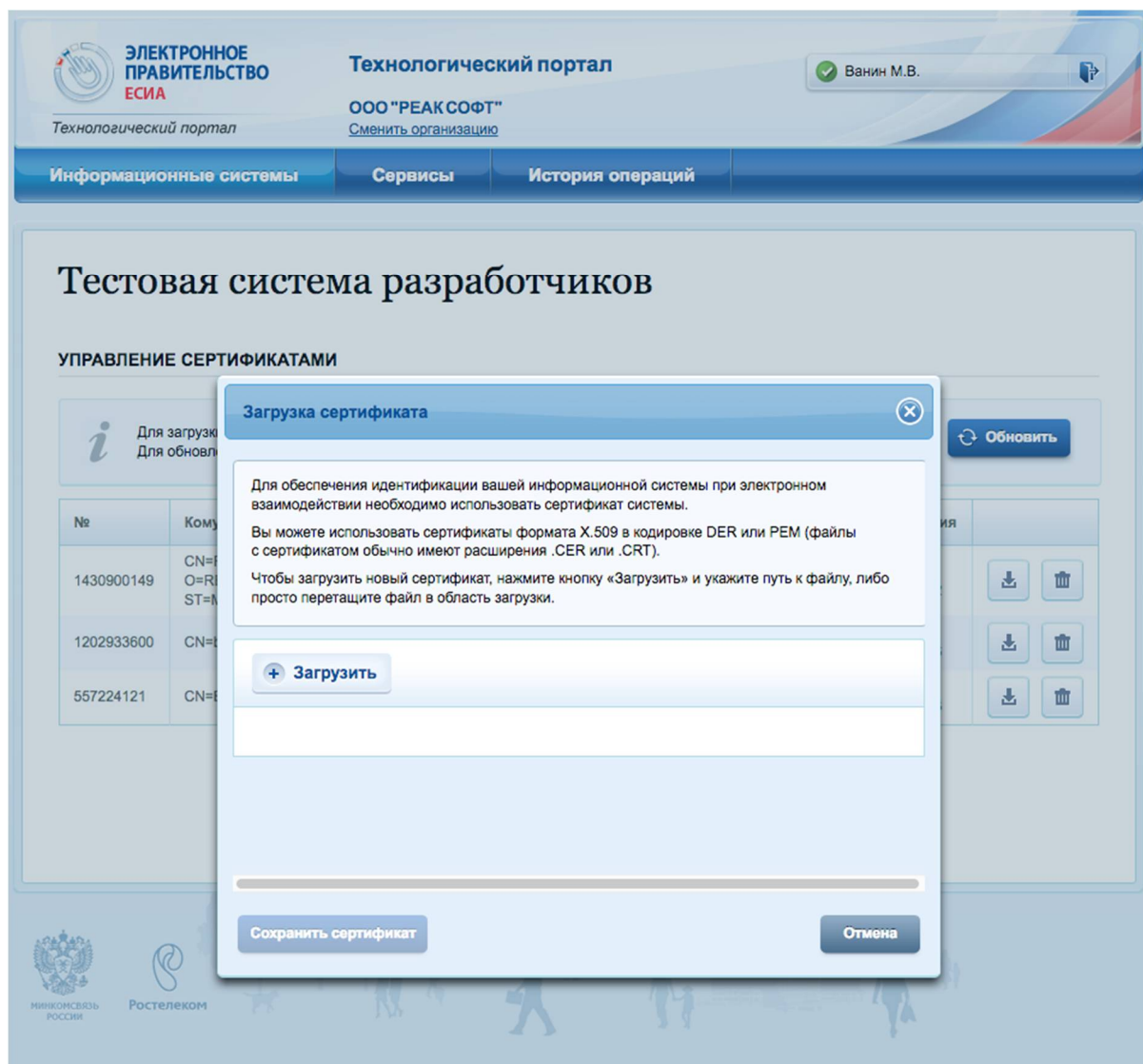


Рисунок 112 – Добавление сертификата системы в Технологическом портале ЕСИА

7. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (см. Рисунок 113), которые включают в себя:

- URL для авторизации – адрес обработчика ЕСИА, вызываемого из браузера, например, <https://esia-portal1.test.gosuslugi.ru/aas/oauth2/ac> (ТЕСТ ЕСИА) или <https://esia.gosuslugi.ru/aas/oauth2/ac> (ПРОД ЕСИА);
- URL для получения и обновления маркера – адрес обработчика ЕСИА, вызываемого с сервера Blitz Identity Provider для получения маркера доступа, например, <https://esia-portal1.test.gosuslugi.ru/aas/oauth2/te> (ТЕСТ ЕСИА) или <https://esia.gosuslugi.ru/aas/oauth2/te> (ПРОД ЕСИА);
- URL для получения данных – адрес обработчика ЕСИА, вызываемого с сервера Blitz Identity Provider для получения данных учетной записи, например, [https://esia-portal1.test.gosuslugi.ru/rs/prns/\\${prn_oid}](https://esia-portal1.test.gosuslugi.ru/rs/prns/${prn_oid}) (ТЕСТ ЕСИА) или [https://esia.gosuslugi.ru/rs/prns/\\${prn_oid}](https://esia.gosuslugi.ru/rs/prns/${prn_oid}) (ПРОД ЕСИА);

- мнемоника системы (client_id), указанная ранее в Технологическом портале ЕСИА;
- идентификатор ключа электронной подписи (alias) – идентификатор ключа электронной подписи, загруженный в хранилище Blitz Identity Provider⁴⁸. 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, 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;

⁴⁸ Хранилище, указанное в разделе keystore конфигурационного файла Blitz Identity Provider.

- 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 `email=${email}` означает, что атрибут с именем `email` 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 ЕСИА⁴⁹.

9. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

⁴⁹ См.: <https://identityblitz.ru/services/esia-integration>

Базовые настройки ЕСИА

Идентификатор поставщика

esia_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

ЕСИА

Отображаемое в консоли имя поставщика, используется только внутри Blitz Identity Provider

Настройки поставщика идентификации ЕСИА

Безопасность

Заполните данные для корректного взаимодействия Blitz Identity Provider с ЕСИА.

URL для авторизации

https://esia-portal1.test.gosuslug.ru/aas/oauth2/ac

URL для получения и обновления маркера

https://esia-portal1.test.gosuslug.ru/aas/oauth2/ta

URL для получения данных

https://esia-portal1.test.gosuslug.ru/rs/gms/\$gms_oid

Мнемоника системы (\$bent_id)

Идентификатор ключа электронной подписи (\$ksp)

Предварительно ключ электронной подписи должен быть загружен в хранилище, указанное в разделе ключи в конфигурационном файле 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 разрешение из доступного списка

Доступные разрешения

Запрашиваемые разрешения

contacts

openid

full_name

inn

mobile

snls

email

Для добавления разрешения введите его имя и нажмите Enter.
Укажите перечень разрешений (список), которые должны быть получены при обращении к поставщику идентификации.

Запрашиваемые данные пользователя

☒ Основные данные☒ Документы☒ Адреса☒ Контакты

Отмеченные ранее разрешения (список) должны позволить получить указанные данные

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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 `$(attr_name)`, где `attr_name` – это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `snls=$(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

phone_number

*

\$(mobile)

✖

+ добавить условие

OR

email

*

\$(email)

✖

+ добавить условие

OR

snls

*

\$(snls)

✖

+ 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 `$(attr_name)`, где `attr_name` – это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `snls=$(name) $(surname)` означает, что атрибут `Sn` будет формироваться из двух атрибутов – `name` и `surname` через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=ESIA2P-$(bentid(4))` позволит присвоить атрибуту `uid` значение `ESIA2P-xxxxxx`, где `xxxxxx` – случайно сгенерированная величина (выбор цифр и букв латинского алфавита).

Доступные атрибуты для mappings

Атрибут	Правило	Мастер
given_name	\$(firstName)	☐ ✖
family_name	\$(lastName)	☐ ✖
snls	\$(snls)	☐ ✖
inn	\$(inn)	☐ ✖
esialid	\$(oid)	☐ ✖
+ Добавить атрибут		

Отмена

Сохранить

Рисунок 113 – Дополнительные настройки поставщика идентификации ЕСИА

203

8.9. Вход через Цифровой профиль ЕСИА

Для конфигурирования входа через Цифровой профиль ЕСИА следует выполнить следующие шаги в разделе «Поставщики идентификации»:

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

Базовые настройки ЦП ЕСИА

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 114 – Базовые настройки поставщика идентификации ЦП 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 (см. п. 16.1.19).
5. Сертификат ключа необходимо зарегистрировать на Технологическом портале ЕСИА (см. следующий пункт).
6. Осуществить регистрацию информационной системы организации через Технологический портал ЕСИА⁵⁰, 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 (см. Рисунок 115);
 - сохранить данные и перейти к настройке сертификатов информационной системы;
 - загрузить сертификат для зарегистрированной информационной системы на Технологическом портал (см. Рисунок 116);

⁵⁰ 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

Проверочная система

Отображаемое название

Проверочная система

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

CHECKSYS

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

Проверочная система

URL системы

http://identityblitz.ru

+

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

RS256

▼

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

По умолчанию ▼

Время жизни access token, мин

60

min: 10; max: 180

Время жизни refresh token, мин

1051200

min: 60; max: 1051200

ОТВЕТСТВЕННЫЙ ЗА ЭКСПЛУАТАЦИЮ СИСТЕМЫ

ФИО

Иванов Иван Иванович

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

Сохранить

Отмена

Рисунок 115 – Добавление системы в Технологическом портале ЕСИА

205

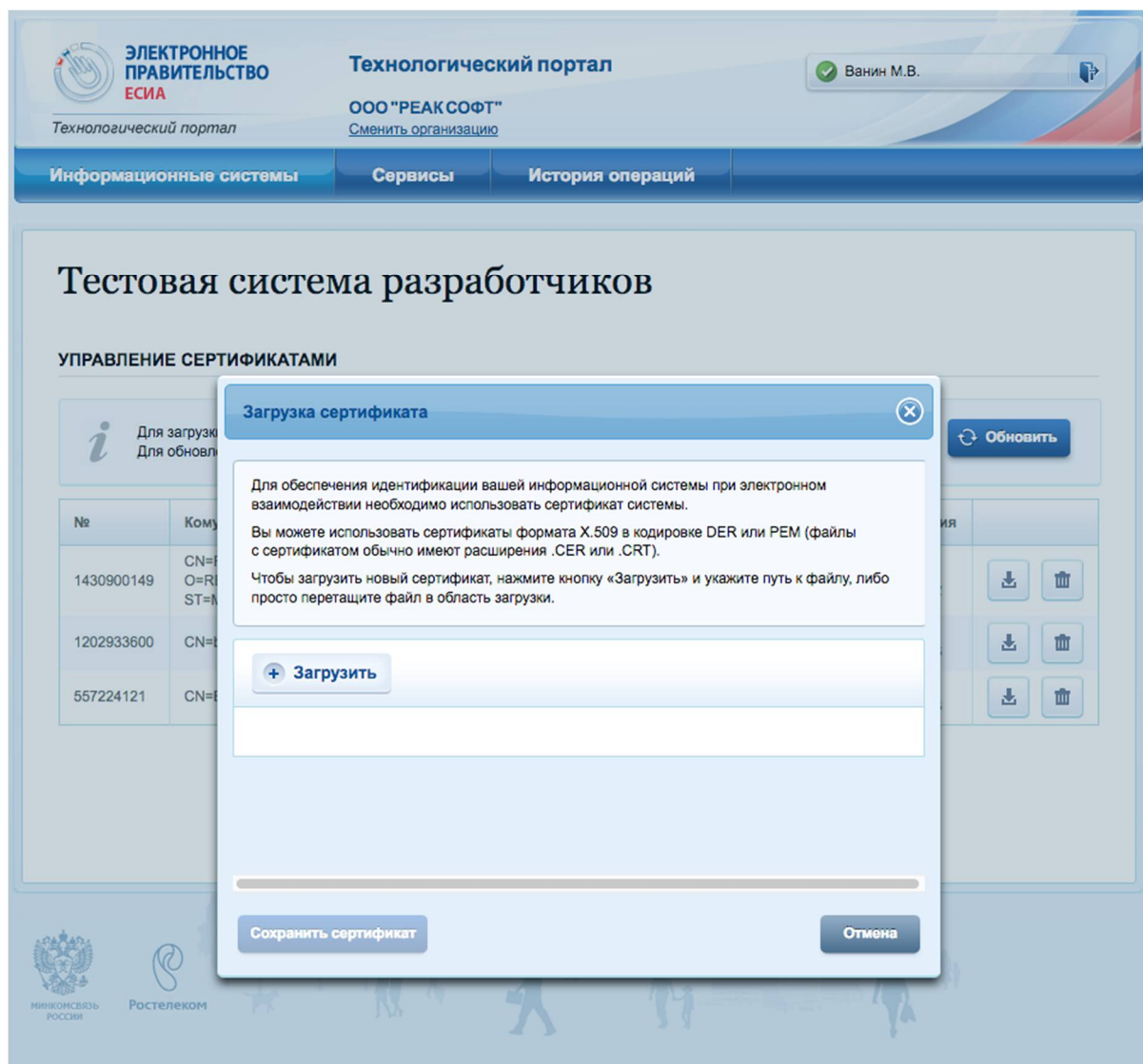


Рисунок 116 – Добавление сертификата системы в Технологическом портале ЕСИА

7. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (см. Рисунок 117), которые включают в себя:

- URL для авторизации – адрес обработчика ЕСИА, вызываемого из браузера, например, <https://esia-portal1.test.gosuslugi.ru/aas/oauth2/ac> (ТЕСТ ЕСИА) или <https://esia.gosuslugi.ru/aas/oauth2/ac> (ПРОД ЕСИА);
- URL для получения и обновления маркера – адрес обработчика ЕСИА, вызываемого с сервера Blitz Identity Provider для получения маркера доступа, например, <https://esia-portal1.test.gosuslugi.ru/aas/oauth2/te> (ТЕСТ ЕСИА) или <https://esia.gosuslugi.ru/aas/oauth2/te> (ПРОД ЕСИА);
- URL для получения данных – адрес обработчика ЕСИА, вызываемого с сервера Blitz Identity Provider для получения данных цифрового профиля, например, <https://esia-portal1.test.gosuslugi.ru/digital/api/public/v1> (ТЕСТ ЕСИА) или <https://esia.gosuslugi.ru/digital/api/public/v1> (ПРОД ЕСИА);

- мнемоника системы (client_id), указанная ранее в Технологическом портале ЕСИА;
- идентификатор ключа электронной подписи (alias) – идентификатор ключа электронной подписи, загруженный в хранилище Blitz Identity Provider⁵¹. Именно сертификат ключа этой электронной подписи должен быть загружен в Технологический портал ЕСИА;
- запрашиваемые разрешения – перечень запрашиваемых разрешений из ЕСИА;
- тип согласия – запрашиваемый в цифровом профиле тип согласия;
- срок действия согласия – количество минут, на которое запрашивается согласие;
- ответственное лицо – сотрудник организации, ответственный за обработку данных, полученных из цифрового профиля;
- запрашиваемые данные пользователя – необходимо отметить те данные, которые следует получать из цифрового профиля 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

⁵¹ Хранилище, указанное в разделе keystore конфигурационного файла Blitz Identity Provider.

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 `email=${email}` означает, что атрибут с именем `email` 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 ЕСИА⁵² с доступом к цифровому профилю.

9. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

⁵² См.: <https://identityblitz.ru/services/esia-integration>

Базовые настройки ЦП ЕСИА

Идентификатор поставщика

etsiap_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

Цифровой профиль ЕСИА

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

Настройки поставщика идентификации Цифровой профиль ЕСИА

Безопасность

Заполните данные для корректного взаимодействия Blitz Identity Provider с ЕСИА.

URL для авторизации

https://esia-portal1.test.gosuslugi.ru/aas/oauth2/ac

URL для получения и обновления маркера

https://esia-portal1.test.gosuslugi.ru/aas/oauth2/te

URL для получения данных

https://esia-portal1.test.gosuslugi.ru/digital/api/public/v1

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

passport_cert_desc x divorce_cert_desc x birth_cert_desc x history_passport_desc x

vehicles_desc x birthdate_desc x fullname_desc x its_desc x mobile_desc x email_desc x id_desc x

death_cert_desc x change_fullname_cert_desc x inn_desc x vehicles_reg_cert_desc x

drivers_license_desc x birthplace_desc x paternity_cert_desc x foreign_passport_desc x

snils_desc x addresses_desc x gender_desc x

Для добавления разрешения введите его имя и нажмите Enter

Укажите перечень разрешений (список), которые должны быть получены при обращении к поставщику идентификации.

Тип согласия

CREDIT

Обычно совпадает с целью, разрешенной организацией для запроса данных Цифрового профиля

Срок действия согласия

1440

Количество минут, на которое запрашивается согласие. Не может превышать максимальный срок действия, определенный для данного типа согласия.

Ответственное лицо

Петров П.П.

Сотрудник организации или организация, осуществляющие обработку данных (строка с ФИО или другой информацией)

Запрашиваемые данные пользователя

☒ Основные данные ☒ Паспорт гражданина РФ

Отменяемые ранее разрешения (срок) должны позволять получать указанные данные

Отмена Удалить Сохранить

Связывание учетных записей

Базовые настройки Расширенная настройка

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

Доступные атрибуты для подстановки

☒ 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

☒ Требуется ввод пароля, если учетная запись была идентифицирована

email

*

\${email}

✖

+ 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=\${id}-\${&random(4)} позволит присвоить атрибуту uid значение uid-xxxxxx, где xxxxxx - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Доступные атрибуты для подстановки

Атрибут

etsaid

=

Правило

\${oid}

Мастер

☒ ✖

+ Добавить атрибут

Отмена Сохранить

Рисунок 117 – Дополнительные настройки поставщика идентификации ЦП ЕСИА

209

8.10. 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.

Базовые настройки Сбер ID

Идентификатор поставщика: sbrf_1
Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

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

Рисунок 118 – Базовые настройки поставщика идентификации Сбер ID

4. Зарегистрировать приложение в системе Сбер ID. Для этого воспользоваться инструкцией, размещенной на официальном сайте этого поставщика идентификации⁵³. 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 (см. Рисунок 119), 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;
 - URL для получения данных – адрес, по которому происходит получение данных пользователя. Должен быть указан внутренний адрес сети, обращение через

⁵³ См.: <https://developer.sberbank.ru/doc/v1/sberbank-id/enrollsteps>

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 `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Сбер ID. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${given_name} ${family_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `given_name` и `family_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 банка;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту банка.

- правила сохранения атрибутов, полученных из Сбер ID, в Blitz Identity Provider. Например, правило `email=${email}` означает, что атрибут с именем `email` 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.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

8. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Базовые настройки Сбер ID

Идентификатор поставщика

sbrf_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

Сбер ID

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

Настройки поставщика идентификации Сбер ID

Безопасность

Для заполнения используйте данные, полученные при регистрации своей системы в Банке.

URI перенаправления (Redirect URI)

https://demo.company.com/blitz/login/externalidps/callback/sbrf/sbrf_1false
https://demo.company.com/blitz/profile/social/externalidps/callbackPopup/sbrf/sbrf_1

Адрес страницы, на которую будет перенаправлен ответ после успешной аутентификации в системе Банка.

URL для авторизации

https://online.sberbank.ru/CSAFront/oidc/sberbank_id/authorize.do

URL для получения и обновления маркера

https://sec.api.sberbank.ru/ru/prod/tokens/v2/oidc

URL для получения данных

https://sec.api.sberbank.ru/ru/prod/sberbankid/v2.1/userinfo

Client ID

admin

Client Secret

Изменить значение

Группы данных

Запрашиваемые группы данных

name x email x openid x birthdate x msnidoc x inn x mobile x

snls x gender x

Для добавления группы данных введите ее имя и нажмите Enter

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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 `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `Or=$(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

email

=

\$(email)

✖

+ 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 `$(attr_name)`, где `attr_name` - это имя атрибута, получаемого от поставщика идентификации. Вы можете указывать в одном правиле несколько атрибутов. Например, правило `Or=$(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).

Пример атрибутов для маппинга

Атрибут

email

=

\$(email)

Мастер

☐

✖

+ Добавить атрибут

Отмена

Сохранить

Рисунок 119 – Дополнительные настройки поставщика идентификации Сбер ID

213

8.11. Вход через систему идентификации Tinkoff ID

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

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

Базовые настройки Тинькофф ID

Идентификатор поставщика: tcs_1
Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

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

Рисунок 120 – Базовые настройки поставщика идентификации Tinkoff ID

4. Зарегистрировать приложение в системе Tinkoff ID. Для этого подать заявку на официальном сайте этого поставщика идентификации⁵⁴. По результатам регистрации вы должны иметь:
 - идентификатор клиента (Client ID);
 - секрет клиента (Client Secret).
5. Перейти в Blitz Identity Provider и заполнить настройки поставщика идентификации (см. Рисунок 121), которые включают в себя:
 - URL для авторизации – адрес, по которому должна инициироваться аутентификация, например: <https://id.tinkoff.ru/auth/authorize>;
 - URL для получения и обновления маркера – адрес, по которому происходит получение и обновление маркера доступа, например: <https://id.tinkoff.ru/auth/token>;
 - URL для получения данных – адрес, по которому происходит получение данных пользователя, например: <https://id.tinkoff.ru/userinfo/userinfo>;
 - URL для получения паспортных данных – адрес, по которому происходит получение паспортных данных пользователя, например: <https://business.tinkoff.ru/openapi/api/v1/individual/documents/passport>;
 - URL для получения данных о СНИЛС – адрес, по которому происходит

⁵⁴ См.: <https://www.tinkoff.ru/corporate/business-solutions/open-api/tinkoff-id/integration/>

получение СНИЛС пользователя, например:
<https://business.tinkoff.ru/openapi/api/v1/individual/documents/snils;>

- идентификатор клиента (Client ID);
- секрет клиента (Client Secret);
- запрашиваемые группы данных – перечень запрашиваемых групп данных из Tinkoff ID;
- правила, которые будут использоваться для идентификации учетной записи в Tinkoff ID и Blitz Identity Provider. Для создания правила следует использовать строки подстановки `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от Tinkoff ID. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${given_name} ${family_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `given_name` и `family_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 Tinkoff 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 банка;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту банка.

- правила сохранения атрибутов, полученных из Tinkoff ID, в Blitz Identity Provider. Например, правило `email=${email}` означает, что атрибут с именем `email` в Blitz Identity Provider будет заполняться значением из атрибута `email` учетной записи Tinkoff ID (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через Tinkoff ID данный атрибут будет обновлен в хранилище Blitz Identity Provider.

6. Сохранить данные в Blitz Identity Provider.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Базовые настройки Тинькофф ID

Идентификатор поставщика

tcs_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

Tinkoff ID

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

Настройки поставщика идентификации Тинькофф ID

Безопасность

Для заполнения используйте данные, полученные при регистрации своей системы в Банке.

URI перенаправления (Redirect URI)

http(s)://bip-dev1.rexsoft.ru/blitz/login/externaldps/callback/tcs/tcs_1/false http(s)://bip-dev1.rexsoft.ru/blitz/profile/social/externaldps/callback/Popup/tcs/tcs_1

Адрес страницы, на которую будет перенаправлен ответ после успешной аутентификации в системе Банка.

URL для авторизации

https://id.tinkoff.ru/auth/authorize

URL для получения и обновления маркера

https://id.tinkoff.ru/auth/token

URL для получения данных

https://id.tinkoff.ru/userinfo/userinfo

URL для получения паспортных данных

https://business.tinkoff.ru/openapi/api/v1/individual/documents/passport

URL для получения данных о СНИЛС

https://business.tinkoff.ru/openapi/api/v1/individual/documents/snils

Client ID

test

Client Secret

Изменить значение

Запрашиваемые данные пользователя

☒ Основные данные ☒ Паспорт ☒ СНИЛС

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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

email

▼

=

\$(email)

✖

+ 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) $(surname)` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=BIP-$(&random(4))` позволит присвоить атрибуту `uid` значение `BIP-XXXXXX`, где `XXXXXX` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Пример атрибутов для логина

Атрибут	Правило	Мастер	
email ▼	\$(email) ✖	☐	✖

+ Добавить атрибут

Отмена

Сохранить

Рисунок 121 – Дополнительные настройки поставщика идентификации Tinkoff ID

217

8.12. 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 122 – Базовые настройки поставщика идентификации СУДИР

4. Зарегистрировать приложение в системе СУДИР. Для этого подать заявку согласно инструкции, размещенной на официальном сайте этого поставщика идентификации⁵⁵. По результатам регистрации вы должны иметь:
 - идентификатор (client_id);
 - секрет (client_secret).
5. Перейти в Blitz Identity Provider и заполнить настройки поставщика идентификации (см. Рисунок 123), которые включают в себя:
 - URL для авторизации – адрес, по которому должна инициироваться аутентификация, например: <https://login.mos.ru/sps/oauth/ae> для внешнего контура СУДИР и <https://sudir.mos.ru/blitz/oauth/ae> для внутреннего;
 - URL для получения и обновления маркера – адрес, по которому происходит получение и обновление маркера доступа, например: <https://login.mos.ru/sps/oauth/te> для внешнего контура СУДИР и <https://sudir.mos.ru/blitz/oauth/te> для внутреннего;
 - URL для получения данных – адрес, по которому происходит получение данных пользователя, например: <https://login.mos.ru/sps/oauth/me> для внешнего контура СУДИР и <https://sudir.mos.ru/blitz/oauth/me> для внутреннего;
 - идентификатор (client_id);
 - секрет (client_secret);
 - запрашиваемые разрешения – перечень запрашиваемых разрешений, например, `openid` и `profile`;

⁵⁵ 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} ${LastName}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `FirstName` и `LastName` через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт СУДИР, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту СУДИР;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту СУДИР.
- правила сохранения атрибутов, полученных из СУДИР, в Blitz Identity Provider. Например, правило `email=${mail}` означает, что атрибут с именем `email` 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.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.5).

Базовые настройки СУДИР

Идентификатор поставщика

mos_1

Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider

Название поставщика

Mos ID

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

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 portalu Moskvy (mos.ru) можно посмотреть [здесь](#). Информация о работе с внутренним контуром СУДИР размещена [здесь](#).

Предопределенные ссылки возврата (redirect_url)

https://demo.company.com/blitz/login/externaldps/callback/mos/mos_1/false

https://demo.company.com/blitz/profile/social/externaldps/callbackPopup/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

https://login.mos.ru/spa/oauth/ae

URL для получения и обновления маркера

https://login.mos.ru/spa/oauth/te

URL для получения данных

https://login.mos.ru/spa/oauth/me

Идентификатор (client_id)

test

Секрет (client_secret)

Изменить значение

Разрешения

Запрашиваемые разрешения

openid

profile

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

guid

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовая настройка

Расширенная настройка

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

email

=

\$(mail)

✖

+ 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} ${surname}` означает, что атрибут CN будет формироваться из двух атрибутов - `name` и `surname` через пробел. Правило можно использовать для задания константного или вычисляемого значения. Например, правило `uid=Blitz-${random(4)}` позволит присвоить атрибуту `uid` значение `Blitz-xxxxxx`, где `xxxxxx` - случайно сгенерированная величина (набор цифр и букв латинского алфавита).

Атрибут	Правило	Мастер
email	= \$(mail) ✖	☐ ✖

+ Добавить атрибут

Отмена

Сохранить

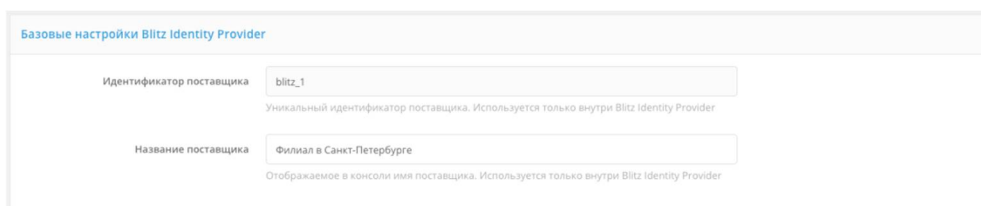
Рисунок 123 – Дополнительные настройки поставщика идентификации СУДИР

221

8.13. 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») или иного поставщика идентификации, поддерживающего OIDC, 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.



Базовые настройки Blitz Identity Provider

Идентификатор поставщика	blitz_1
Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider	
Название поставщика	Филиал в Санкт-Петербурге
Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider	

Рисунок 124 – 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 (см. Рисунок 125), 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 `${attr_name}`, где `attr_name` – это имя атрибута, получаемого от доверенного Blitz Identity Provider. Можно указывать в одном правиле несколько атрибутов. Например, правило `CN=${given_name} ${family_name}` означает, что атрибут `CN` будет сопоставляться с сочетанием двух атрибутов – `given_name` и `family_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 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 внешнего поставщика;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту внешнего поставщика.
- правила сохранения атрибутов, полученных из доверенного Blitz Identity Provider, в Blitz Identity Provider. Например, правило `email=${email}` означает, что атрибут с именем `email` 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.

Если возможностей, предоставляемых базовыми настройками сопоставления учетной записи внешнего поставщика идентификации с учетной записью Blitz Identity Provider и правил сохранения атрибутов в Blitz Identity Provider недостаточно, то можно нажать на вкладку «Расширенная настройка» и задать правила связывания учетных записей и сохранения атрибутов с помощью процедуры связывания, реализованной на языке Java.

7. В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п 4.5).

Базовые настройки Blitz Identity Provider

Идентификатор поставщика

Идентификатор поставщика. Используйте только внутри Blitz Identity Provider

Имя поставщика

Отображаемое в консоли имя поставщика. Используйте только внутри Blitz Identity Provider

Настройка поставщика идентификации Blitz Identity Provider

Безопасность

Для заполнения указанных параметров обратиться к администратору внешнего поставщика идентификации Blitz Identity Provider. Необходимая информация размещена в спецификации подключаемого приложения (по протоколу OAuth 2.0). Также перейдите администратору привязанной к нему OID-параметризации.

Предопределенный источник информации (userinfo_url)

https://demo.company.com/blitz/authorize/oauth2/callback/blitz_oidcfalse

https://demo.company.com/blitz/profile/oauth2/callback/blitzoidcfalse

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

URL для информации

https://demo.company.com/blitz/oauth2

URL для получения и обновления маркера

https://demo.company.com/blitz/oauth2/*

URL для получения данных

https://demo.company.com/blitz/oauth2/me

Идентификатор (blitz_id)

test_blitz

Секрет (secret_secret)

Изменить значение

Разрешения

Запрашиваемые разрешения

openid

profile

Для добавления разрешений соедините это имя с именем scopes. Укажите в параметре (разрешений (scopes), 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 ирибут внешнего поставщика идентификации, который будет использоваться для связи учетной записи в Blitz Identity Provider.

Идентификатор

oid

Отмена

Удалить

Сохранить

Связывание учетных записей

Базовые настройки

Расширенная настройка

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 сопоставления с учетной записью поставщика идентификации. Для создания пароля используйте строки подстановки: \${user_name}, где user_name - это имя атрибута, получаемого от поставщика идентификации. Вы можете указать в одном правиле несколько атрибутов. Например, правило: cn=\${name} \$({surname}), означает, что атрибут CN будет формироваться из двух атрибутов: name и surname через пробел.

☒ При первом входе пользователя через поставщика идентификации, если учетная запись не была идентифицирована

☐ Для пароля должно быть найдено только одно учетная запись, по заданным правилам соответствия

☒ Проверять ввод пароля: если учетная запись была идентифицирована

name

=

\$(name)

✖

+ добавить условие

+ добавить альтернативное правило

Атрибуты

Укажите, каким образом должны формироваться атрибуты, используемые в Blitz Identity Provider, на основе данных, полученных от поставщика идентификации. Для формирования каждого атрибута должно быть составлено свое правило. Для создания правила используйте атрибуты и обозначения: \${attr_name}, где attr_name - это имя атрибута, получаемого от поставщика идентификации. Вы можете указать 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 как одного или нескольких значений. Например, правило: cn=\${name} \$({surname}) \${email} означает, что атрибут CN будет формироваться из трех атрибутов: name и surname через пробел, и email. \${email} - случайное значение из набора цифр и букв латинского алфавита.

Атрибут

name

=

\$(name)

✖

Мастер

☐

+ Добавить атрибут

Отмена

Сохранить

Рисунок 125 – Настройки подключения к внешнему поставщику идентификации Blitz Identity Provider

225

9. Управление учетными записями пользователей

В разделе «Пользователи» консоли управления доступны следующие операции:

- поиск учетных записей пользователей;
- добавление учетной записи пользователя;
- просмотр и редактирование атрибутов учетной записи пользователя;
- изменение пароля учетной записи пользователя;
- просмотр и отвязка учетных записей внешних поставщиков идентификации;
- привязка устройств для проведения двухфакторной аутентификации;
- просмотр групп, в которые включен пользователь, управление членством пользователя в группах;
- просмотр и удаление устройств пользователя;
- просмотр, привязка, удаление ключей безопасности пользователя;
- просмотр прав учетной записи пользователя, назначение и отзыв прав;
- просмотр разрешений, выданных пользователем приложениям;
- удаление учетной записи пользователя.

Общий вид страницы управления данными пользователей представлен на рисунке 126.

Пользователи

Иванов

Создать учетную запись пользователя...

Учетные записи пользователей

389-дс: ВР-***** Иванов Иван Иванович, ivanov@company.com	Данные пользователя	События безопасности
	sub ВР-***** family_name Иванов given_name Иван middle_name Иванович email ivanov@company.com phone_number +7(000)0000000 locked Нет	

Сохранить

Рисунок 126 – 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.

Также доступны:

- кнопка копирования ссылки на найденного пользователя – при ее нажатии ссылка на пользователя копируется в буфер обмена;
- ссылка «События безопасности» для быстрого перехода к просмотру событий безопасности за текущий день, в которых найденный пользователь фигурирует в качестве объекта доступа.

9.2. Добавление учетной записи пользователя

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» (*)).

Рисунок 127 – Создание учетной записи пользователя

9.3. Просмотр и изменение атрибутов пользователя

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, устройства пользователя, ключи безопасности и др.

The screenshot shows a web interface for managing users. At the top, there's a search bar with 'Иванов' entered and a 'Найти' button. Below the search bar, there's a link 'Создать учетную запись пользователя...'. The main section is titled 'Учетные записи пользователей' and contains a list of users. One user is highlighted: '389-ds: BIP-*****' and 'Иванов Иван Иванович, ivanov@company.com'. To the right of this list is a tabbed interface. The 'Данные пользователя' tab is active, showing fields for 'sub' (BIP-*****), 'family_name' (Иванов), 'given_name' (Иван), 'middle_name' (Иванович), 'email' (ivanov@company.com), 'phone_number' (+7(000)0000000), and 'locked' (Нет). There is a 'Сохранить' button at the bottom right of this section. Below the user details is a 'Смена пароля' section with a 'Новый пароль' field, a 'Сгенерировать пароль' checkbox, and an 'Изменить' button.

Рисунок 128 – Просмотр информации о пользователе (фрагмент)

На карточке пользователя можно совершать следующие операции:

- редактировать атрибуты пользователя;
- изменять пароль;
- просматривать перечень привязанных учетных записей внешних поставщиков идентификации, отвязывать внешние учетные записи;
- изменять требуемый уровень аутентификации для пользователя;
- привязывать или удалять устройства для проведения аутентификации: генераторы разовых паролей (см. п. 9.3.4) 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 запомненные устройства и браузеры пользователя;
- просматривать, добавлять и удалять ключи безопасности пользователя;
- 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 129 – Смена пароля

9.3.3. Просмотр и отвязка привязанных учетных записей внешних поставщиков идентификации

В блоке «Привязанные учетные записи внешних систем» можно посмотреть перечень аккаунтов внешних поставщиков идентификации (социальных сетей, банков, ЕСИА, Mos ID

и др.), 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 связь с внешней учетной записью.

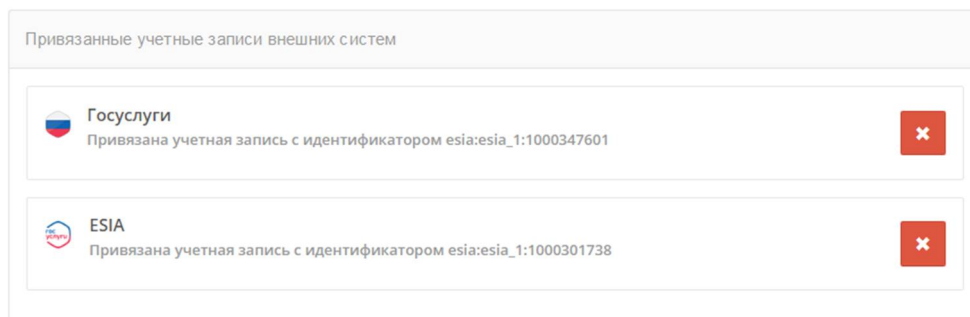


Рисунок 130 – Просмотр информации о пользователе:
привязанные учетные записи внешних поставщиков

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 HOTP/TOTP генератор по серийному номеру (см. Рисунок 131) либо привязать к учетной записи по QR-коду мобильное приложение, осуществляющее выработку TOTP-кодов (см. Рисунок 132).

A screenshot of a web form titled "Генератор паролей на основе секрета (HOTP)" (HOTP-based password generator). The form contains three input fields: "Серийный номер" (Serial number) with a placeholder "Серийный номер устройства генерации разовых паролей" (Serial number of the one-time password generation device), "Пароль 1" (Password 1), and "Пароль 2" (Password 2). At the bottom right of the form is a blue button labeled "Привязать" (Link).

Рисунок 131 – Привязка HOTP-устройства по серийному номеру администратором

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: NAWGF7K7DXV75DH25FCMBOSBUPVJ2CQG
Секрет закодирован в Base32 кодировке

Сохранить

Рисунок 132 – 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.

Приложение Duo Mobile (QR-код)

Сосканируйте QR-код с помощью приложения Duo Mobile пользователя и нажмите "Сохранить":

duo://KOj14IDEE556dm8Rq6ac-YXBpLWFIMTZIMDhjLmR1b3NIY3VyaXR5LmNvbQ

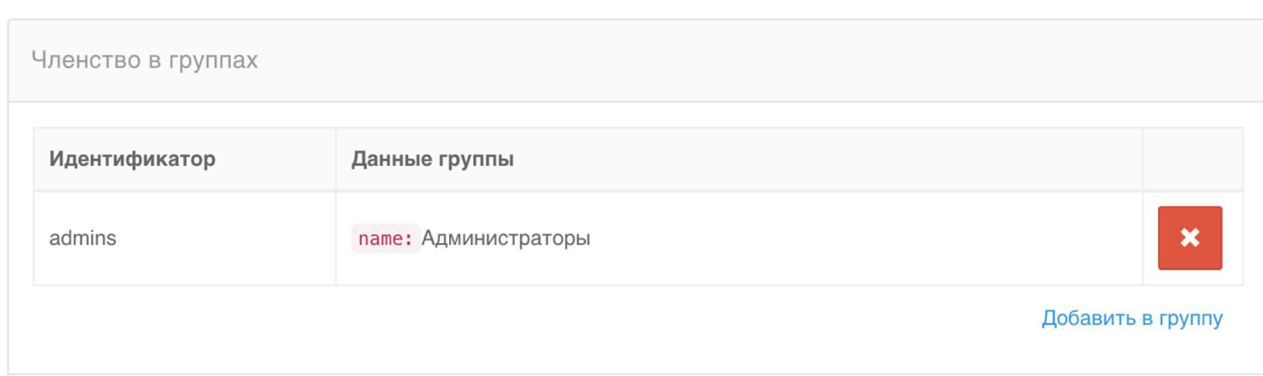
Сохранить

Рисунок 133 – Привязка мобильного приложения Duo Mobile

9.3.6. Просмотр групп, в которые включен пользователь, управление членством пользователя в группах

Если пользователь включен в группы, то эта информация будет отображена в блоке «Членство в группах» (см. Рисунок 134). По каждой группе будут отображены следующие данные:

- идентификатор группы;
- значения атрибутов группы.

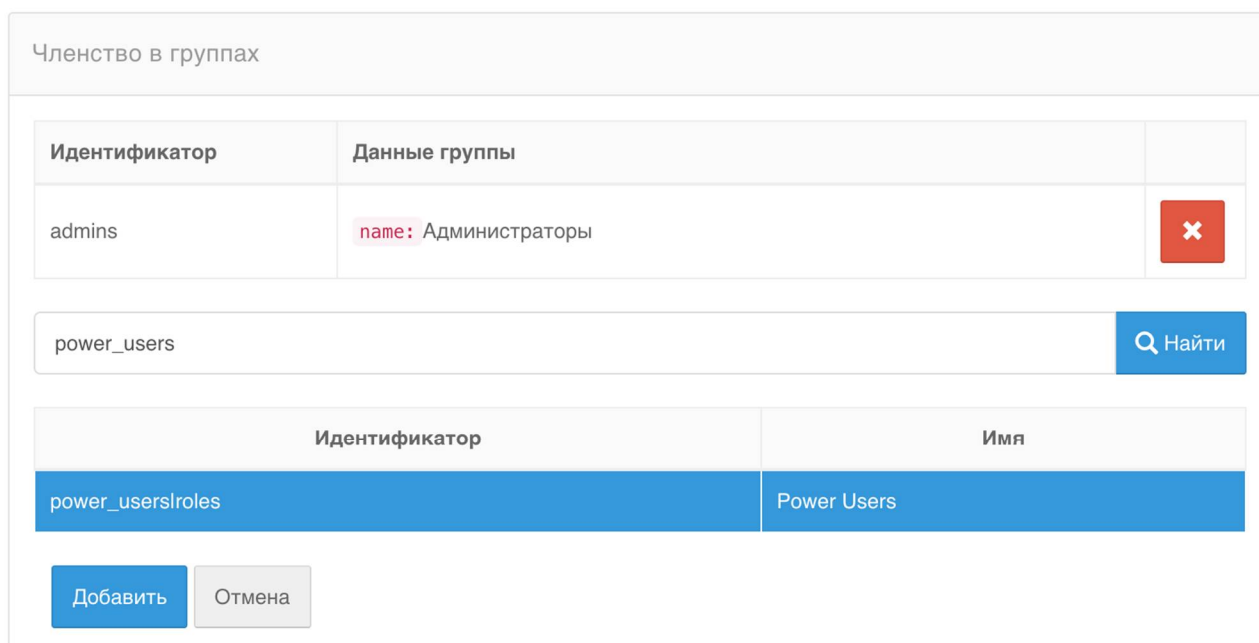


Идентификатор	Данные группы	
admins	name: Администраторы	

[Добавить в группу](#)

Рисунок 134 – Просмотр групп пользователя

Можно исключить пользователя из группы с помощью кнопки удаления или добавить пользователя в другую группу с помощью ссылки «Добавить в группу» (см. Рисунок 135). Для добавления пользователя в группу нужно будет ввести значение атрибута, идентифицирующего группу, нажать кнопку «Найти», выбрать подходящую группу из списка найденных, и нажать кнопку «Добавить».



Идентификатор	Данные группы	
admins	name: Администраторы	

power_users  [Найти](#)

Идентификатор	Имя
power_usersroles	Power Users

[Добавить](#) [Отмена](#)

Рисунок 135 – Добавление пользователя в группу

9.3.7. Просмотр прав, назначение и отзыв прав

Если в отношении пользователя есть права со стороны приложений или других учетных записей, то это будет отображено в блоке «Права в отношении пользователя» (см. Рисунок 136). Если пользователь имеет права в отношении объектов, например, других учетных записей, то это будет отображено в блоке «Права пользователя в отношении объектов» (см. Рисунок 137).

Каждое право характеризуется следующими параметрами:

- идентификатор объекта;
- имя;
- право.

Права субъектов в отношении пользователя			
Идентификатор	Имя	Право	
test-system	test-system	Назначать права	

[Назначить права](#)

Рисунок 136 – Просмотр прав других субъектов в отношении пользователя

Права пользователя в отношении объектов			
Идентификатор	Имя	Право	
_blitz_profile	custom.app.name._blitz_profile	Менять пароль	
_blitz_profile	custom.app.name._blitz_profile	rights.right.SUPPORT	
isergeev@domain.com	Сергеев Иван Петрович	rights.right.TEST	
_blitz_console	custom.app.name._blitz_console	Назначать права	

[Назначить права](#)

Рисунок 137 – Просмотр прав пользователя в отношении объектов

Отозвать право доступа можно с помощью кнопки удаления рядом с правом доступа (см. Рисунок 138 и Рисунок 139). Назначить право доступа можно с помощью ссылки «Назначить права». При этом надо будет выбрать назначаемое право доступа из списка, тип субъекта (пользователь или приложение) или объекта (пользователь, группа или приложение), найти и выбрать субъекта/объекта.

Права субъектов в отношении пользователя

Права отсутствуют

Право:

Тип субъекта:

Поиск субъекта:

Идентификатор	Имя
test-app	test-app

Рисунок 138 – Назначение другим субъектам прав к учетной записи пользователя

Права пользователя в отношении объектов

Идентификатор	Имя	Право	
_blitz_profile	custom.app.name._blitz_profile	Менять пароль	✕
_blitz_profile	custom.app.name._blitz_profile	rights.right.SUPPORT	✕
isergeev@domain.com	Сергеев Иван Петрович	rights.right.TEST	✕
_blitz_console	custom.app.name._blitz_console	Назначать права	✕

Право:

Тип объекта:

Поиск объекта:

Идентификатор	Имя
6c02de61-909f-49d6-9bc4-4edb7d021c18	Иванов Александр
854436f6-af58-4a3f-8cb7-c2c441eb4a76	Иванов Сергей

Рисунок 139 – Назначение пользователю прав к объектам

9.3.8. Просмотр и удаление запомненных устройств и браузеров

Администратор имеет возможность просмотреть устройства и браузеры, с которых пользователь осуществлял вход с использованием своей учетной записи (см. Рисунок 140).

Описание устройств включает:

- признак того, запомнена ли на устройстве сессия входа и является ли устройство доверенным. Признак кодируется с помощью цвета:
 - серый – на устройстве не запомнена сессия входа и устройство не является доверенным;
 - желтый – на устройстве не запомнена сессия входа, но устройство является доверенным;
 - синий – на устройстве запомнена сессия входа, но устройство не является доверенным;
 - зеленый – на устройстве запомнена сессия входа и устройств является доверенным.
- имя и версия операционной системы устройства, определенные на основе UserAgent;
- имя и версия браузера, определенные на основе UserAgent;
- дата и время последнего входа с данного устройства и браузера;
- IP-адрес пользователя, который был определен при последнем входе с данного устройства и браузера.

Устройства пользователя				
Устройство	Браузер	Последний вход	Последний IP адрес	
 macOS 10.15.7	Chrome 100	04.05.2022 16:05	172.25.0.1	
 macOS 10.15.7	Yandex 22	27.04.2022 16:04	37.144.36.99	
 macOS 10.15.7	Chrome 100	25.04.2022 20:04	212.46.18.101	

Рисунок 140 – Просмотр и удаление запомненных устройств и браузеров пользователя

9.3.9. Управление ключами безопасности

Администратор имеет возможность просмотреть перечень ключей безопасности (Passkey, WebAuthn, FIDO2, U2F), зарегистрированных для учетной записи пользователя (см. Рисунок 141). Для каждого ключа безопасности указаны:

- имя ключа;
- дата и время регистрации ключа;
- область применения (для Passkey и FIDO2 – для входа и для подтверждения входа; для

U2F – только для подтверждения входа);

- дата и время последнего использования ключа.

Ключи безопасности пользователя				
Имя ключа	Добавлен	Область применения	Последнее использование	
Face ID на iPhone	28.10.2022 16:10	Для входа Для подтверждения входа	01.11.2022 14:11	

[Добавить ключ](#)

Рисунок 141 – Просмотр ключей безопасности пользователя

Администратор может зарегистрировать новый ключ безопасности с помощью ссылки «Добавить ключ» (см. Рисунок 142). В обычном сценарии использования ключи безопасности себе добавляет сам пользователь в момент входа (онбординг) или через личный кабинет.

Укажите название нового ключа

Имя ключа

Создать

Отмена

Рисунок 142 – Добавление ключа безопасности пользователя

Возможность добавления ключа администратором может быть полезна в следующих сценариях:

Администратор лично выдает пользователям аппаратный FIDO2/U2F ключ и привязывает его к учетной записи. Для доступа к приложениям компании используется двухфакторная аутентификация.

Администратору в целях технической поддержки нужна возможность войти под учетной записью пользователя. Сброс от учетной записи пароля доставит пользователю неудобства – вместо этого можно зарегистрировать ключ безопасности и использовать его для входа. Все действия по регистрации и удалению ключей безопасности регистрируются как события безопасности.

9.3.10. Просмотр и удаление выданных приложениям разрешений

Администратор имеет возможность просмотреть перечень разрешений, выданных пользователем приложениям (см. Рисунок 143). Каждое разрешение описывается:

- идентификатор приложения;
- перечень разрешений (scope);
- дата выдачи разрешений.

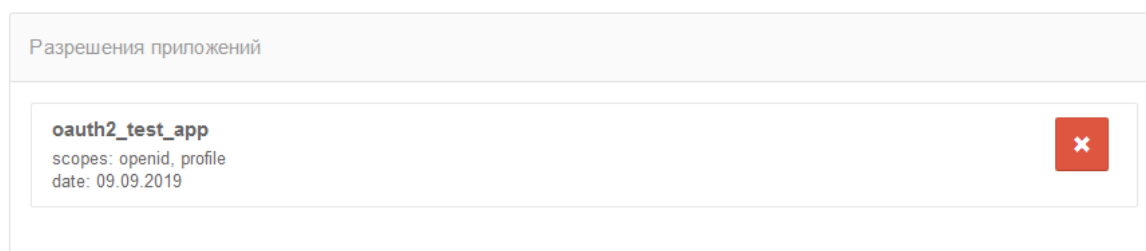


Рисунок 143 – Просмотр выданных разрешений

10. Управление группами пользователей

Если в Blitz Identity Provider настроена возможность работы с группами пользователей (см. п. 16.1.18), то в консоли управления появится раздел «Группы». В данном разделе можно осуществлять поиск групп по одному из сконфигурированных атрибутов, редактировать группы, создавать и удалять группы, управлять членством пользователей в группах.

По каждой найденной группе отображаются ее атрибуты (см. Рисунок 144). 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»).

Группы

Профиль	Атрибут	Значение	
grps	id	newusers	Найти

[Создать группу...](#)

Группы пользователей

newusers

Данные группы

name: Новый пользователи [Сохранить](#)

Члены группы

Идентификатор	Имя пользователя	
6647dc35-0c4f-4054-a7e7-fae41b011b4f	Петров Иван	✕
18539368-f59f-4ef1-8f34-3389272fa8bd	Васильев Дмитрий	✕

[Добавить пользователя...](#)

[Удалить группу](#)

Рисунок 144 – Просмотр групп пользователей

Доступны возможности по редактированию атрибутов группы, удалению группы, включению пользователей в группу с помощью ссылки «Добавить пользователя...» (см. Рисунок 145), исключению пользователя из группы, созданию новых групп пользователей с помощью ссылки «Создать группу...» (см. Рисунок 146).

Члены группы

Идентификатор	Имя пользователя	
6647dc35-0c4f-4054-a7e7-fae41b011b4f	Петров Иван	
18539368-f59f-4ef1-8f34-3389272fa8bd	Васильев Дмитрий	

Найти

Идентификатор	Имя пользователя
a9072d2b-9e89-45a5-9447-d0d126ba0332	Иванов Александр
854436f6-af58-4a3f-8cb7-c2c441eb4a76	Иванов Сергей

Добавить

Отмена

Рисунок 145 – Включение пользователя в группу

Профиль ☒ grps

Идентификатор группы

name

Создать

Отмена

Рисунок 146 – Создание новой группы пользователей

11. Управление правами доступа

Для ведения справочника прав доступа в Blitz Identity Provider используется раздел «Права доступа» консоли управления (см. Рисунок 147). Права доступа могут использоваться для контроля доступа пользователей в приложения, для контроля вызова приложениями защищаемых REST-сервисов, а также могут быть запрошены и использованы приложениями для осуществления контроля доступа пользователя к функциям приложений.

Справочник прав доступа

Задайте права доступа, которые могут быть назначены пользователям, группам или приложениям.

Название	Описание	
SUPPORT		X
ADMIN		X
TEST	Проверочное право доступа	X
USER		X

[+ Добавить право доступа](#)

Сохранить

Рисунок 147 – Ведение справочника прав доступа

12. 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

Идентификатор субъекта

admin

Полный IP-адрес или маска

Название приложения

Период

09.02.2023 00:0009.02.2023 23:59

за сегодняза неделюза месяц

Группа событий

☐ Вход ☐ Выход ☐ Авторизация доступа

☐ Изменение аутентификационных данных

☐ Изменения учетной записи

☐ Операции с группами

☐ Отправка кодов подтверждения

☐ Администрирование

Протокол

☐ OAuth 2.0 ☐ SAML ☐ Другие

ПрименитьОчистить

ID процесса	Время	Событие	Субъект	Объект	Приложение	IP-адрес
 6b0d69b4...	09.02.2023 13:39:38	Выполнен вход	admin	admin	Консоль управления	176.213.69.7
 8f65709b...	09.02.2023 13:09:18	Выполнен вход	admin	admin	Консоль управления	212.46.18.101
 21ba5f91...	09.02.2023 13:09:00	Выполнен вход	admin	admin	Консоль управления	212.46.18.101

Рисунок 148 – Просмотр событий безопасности

13. Настройка уведомлений и отправки сообщений

Для задания настроек уведомлений и подключения к системам отправки сообщений используется раздел «Сообщения» консоли управления Blitz Identity Provider (см. Рисунок 149). 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, `${phone_number}` означает, что информация будет отправлена на телефон `phone_number`;
- 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;
 - добавление нового ключа безопасности;
 - удаление ключа безопасности.

Параметры каналов оповещений

SMS-сообщения
Настройка сервиса отправки SMS-сообщений

Push-уведомления
Настройка сервиса отправки push-уведомлений

Email-сообщения
Настройка SMTP-сервера

Уведомления

Настройте уведомления и пользователи будут оповещаться о различных событиях безопасности

Способы уведомления

Способ уведомления	Атрибут с контактом	
Электронная почта	\$(email-)	✖
SMS	\$(phone-number-)	✖

+ Добавить способ уведомления

Уведомлять пользователей о событиях

Тип события	Способы уведомления
Вход с неизвестного устройства	+ Электронная почта
Смена пароля	+ Электронная почта
Смена пароля в зависимой учетной записи	+ Электронная почта
Восстановление доступа	+ Электронная почта
Восстановление доступа в зависимой учетной записи	+ Электронная почта
Привязка учетной записи социальной сети	+ Электронная почта
Настройка метода двухфакторной аутентификации	+ Электронная почта
Изменение режима подтверждения входа	+ Электронная почта
Получение права менять пароль в зависимой учетной записи	+ Электронная почта
Предоставление права менять пароль	+ Электронная почта
Отзыв права менять пароль в зависимой учетной записи	+ Электронная почта
Отзыв предоставленного права менять пароль	+ Электронная почта
Регистрация учетной записи	+ Электронная почта
Добавление ключа безопасности	+ Электронная почта
Удаление ключа безопасности	+ Электронная почта

Сохранить

Рисунок 149 – Настройка уведомлений и подключения к системам отправки сообщений

13.1. 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» (см. Рисунок 150).

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=${phone_number}&mes=${message}&charset=utf-8`

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, `^ОК,+`

Шаблон ответа при ошибке: `^ERROR,+`
Регулярное выражение, определяющее наличие ошибки при отправке сообщения. Например, `^ERROR,+`

[Отмена](#) [Сохранить](#)

Рисунок 150 – 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=${phone_number}&mes=${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.

13.2. 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, `^ОК.+`

Шаблон ответа при ошибке

`.\\"errorCode\":[1-9].+`

Регулярное выражение, определяющее наличие ошибки при отправке сообщения. Например, `^ERROR.+`

Отмена

Сохранить

Рисунок 151 – Настройка интеграции с сервисом отправки push-уведомлений

13.3. 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» (см. Рисунок 152).

The screenshot shows the 'Настройка SMTP-сервера' (SMTP server configuration) page. It contains the following fields and controls:

- Хост** (Host): A text input field containing 'mail01.company.loc'.
- Порт** (Port): A text input field containing '25'.
- Использовать TLS** (Use TLS): A checkbox that is currently unchecked.
- Отправитель** (Sender): A text input field containing 'notif@company.com'. Below it is the label 'email-адрес отправителя' (sender email address).
- Логин** (Login): A text input field. Below it is the label 'Логин учетной записи для соединения с SMTP-сервером' (Login for connecting to the SMTP server). To the right of this field is a checked checkbox with the label 'Совпадает с адресом отправителя' (Matches sender address).
- Пароль** (Password): A text input field. To its right is a blue link labeled 'Изменить значение' (Change value).
- Buttons**: At the bottom right, there are two buttons: 'Отмена' (Cancel) and 'Сохранить' (Save).

Рисунок 152 – 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.

14. 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. 14.1).

Также имеется возможность:

- создавать и изменять новые шаблоны с помощью конструктора и назначать их разным приложениям (п. 14.2);
- создавать и изменять новые шаблоны в ручном режиме (п. 14.3).

14.1. 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

default

Название шаблона

Стандартный шаблон

Описание

Используется по умолчанию

Приложения

http://jira.rexsoft.ru/secure/Dashboard.jspa, oauth2_demo_app02, openschool, re

Сохранить

Внешний вид страницы входа

Тема

Светлая

Расположение основного блока

Слева

☒ По центру

Справа







Логотип

Загрузить логотип



Рекомендуемая высота логотипа 32px

Фоновый рисунок

Загрузить фоновый рисунок

Или выбрать из предложенных рисунков

Рисунок 1



Рисунок 2



Рисунок 3



Рекомендуемый размер файла не более 1MB

Настройка футера

Добавьте фрагмент HTML-кода для отображения в футере страницы входа.

1 Скопируйте сюда фрагмент HTML кода

Сохранить

Рисунок 153 – 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 154, 155, 156 приведены примеры страниц входа в результате стандартной настройки.

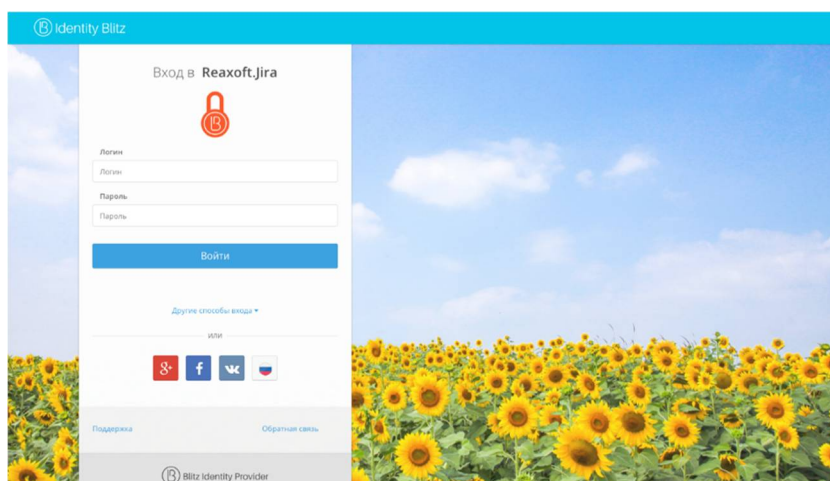


Рисунок 154 – Пример страницы входа с social login и дополнительным футером

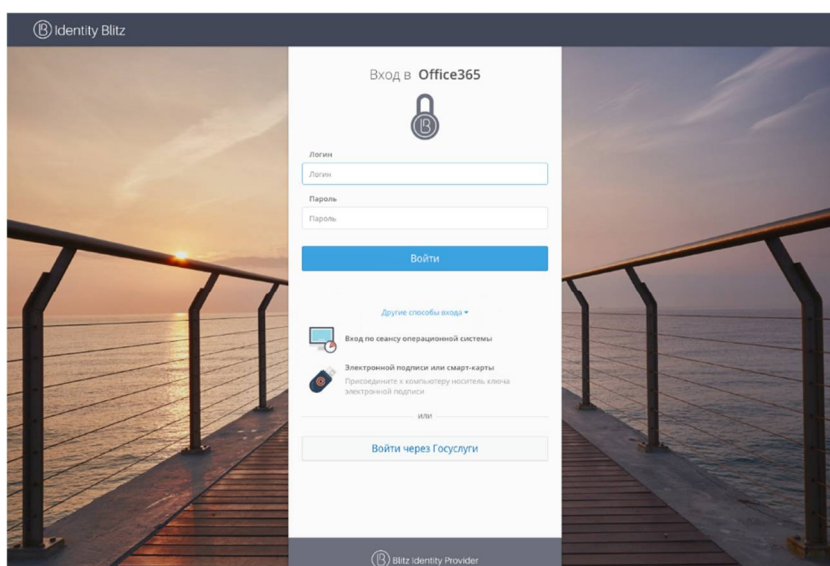


Рисунок 155 – Пример страницы входа в темном интерфейсе и с режимами входа по электронной подписи, сеансу операционной системы или через ЕСИА

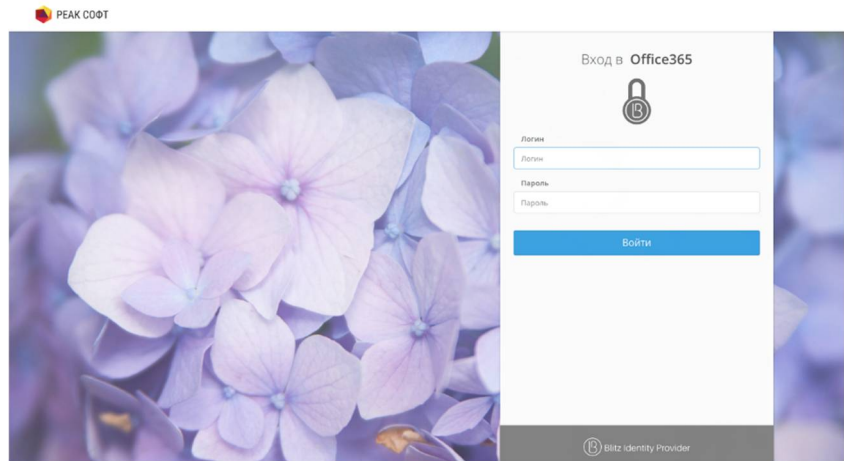


Рисунок 156 – Пример страницы входа в светлом интерфейсе, с логотипом в заголовке страницы и без специальных режимов входа

14.2. 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.

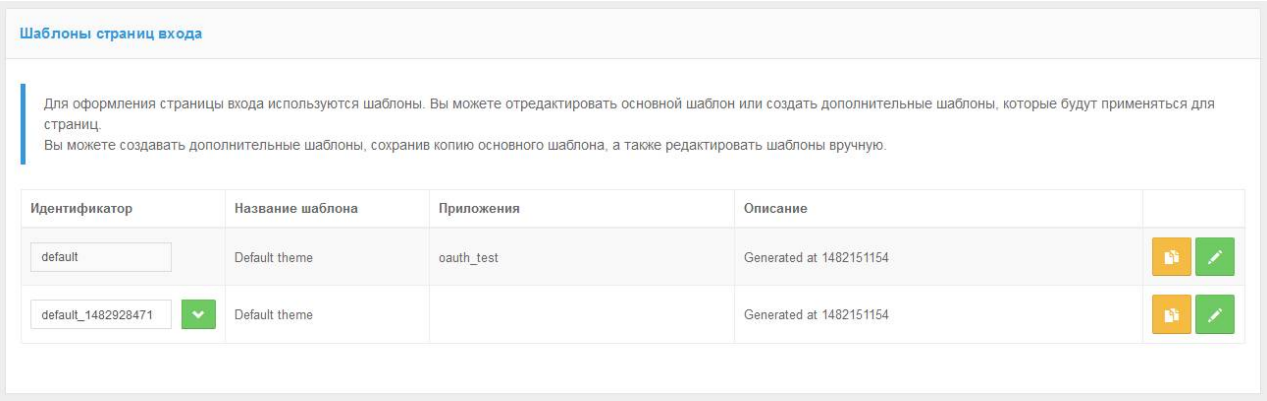


Рисунок 157 – Создание нового шаблона на базе существующего основного шаблона

Чтобы новый шаблон использовался при входе в некоторое приложение, необходимо в разделе «Приложения» перейти к редактированию нужного приложения и выбрать требуемый шаблон страниц.

Рисунок 158 – Назначение шаблона страницы входа приложению

14.3. 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 159);
- обратно заархивировать файлы шаблона, убедившись, что файл `meta.conf` находится в корневой директории.

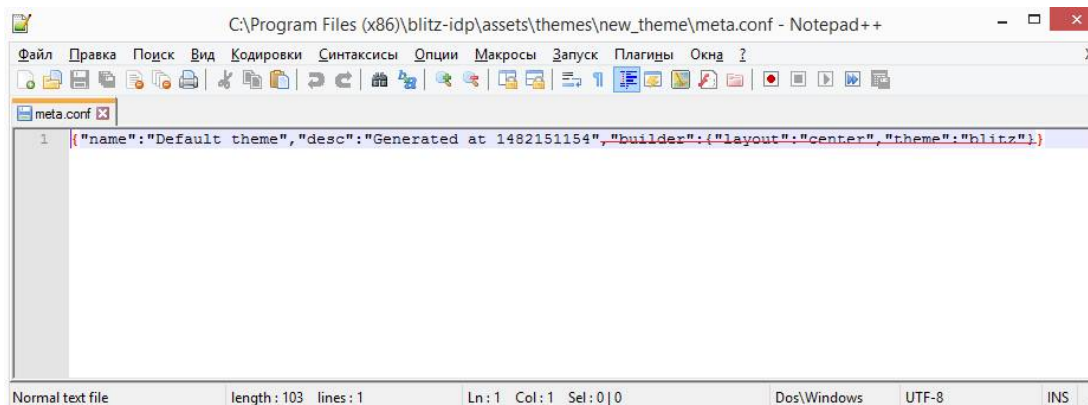


Рисунок 159 – Удаление параметра builder из файла meta.conf

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 Twirl⁵⁶.

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 `@fBuilder()` добавляет на страницу код основной формы аутентификации (пример основной формы приведен на рисунке 160). 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.

⁵⁶ См.: <https://www.playframework.com/documentation/2.5.x/ScalaTemplates>

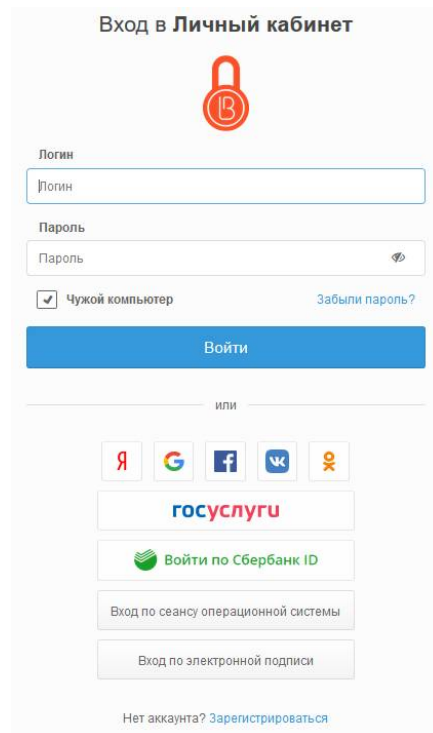


Рисунок 160 – Блок с основной формой аутентификации

Листинг простейшего шаблона приведен ниже:

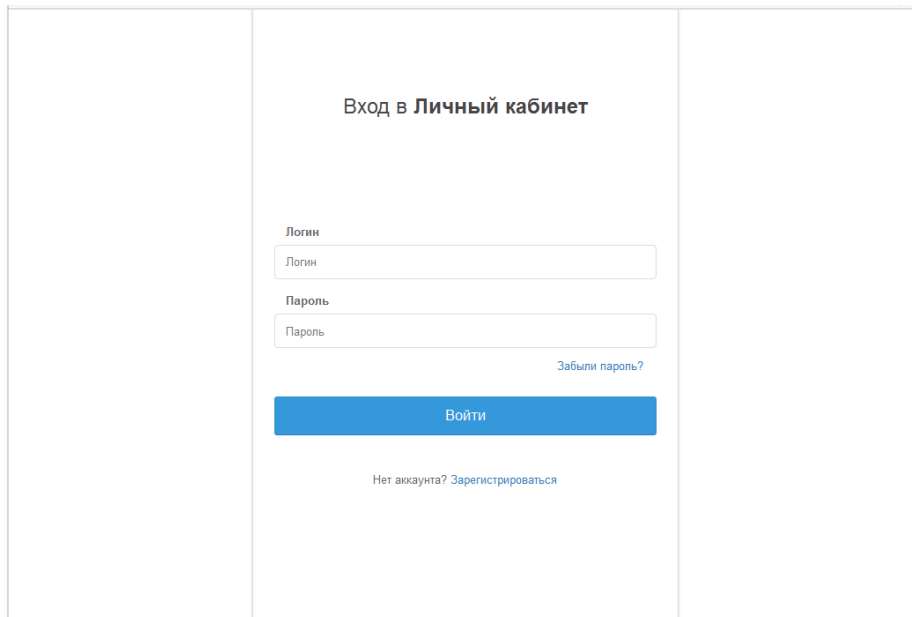
```
@(headers: Html, form: Html, scripts: Html, path: String)(implicit request: RelyingPartyRequest[_],
messages: Messages)

<!DOCTYPE html>
<html>

<head>
  @headers
</head>

<body>
  <div id="main">
    <section id="content_wrapper">
      @fBuilder()
    </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 161.



Вход в Личный кабинет

Логин

Пароль

[Забыли пароль?](#)

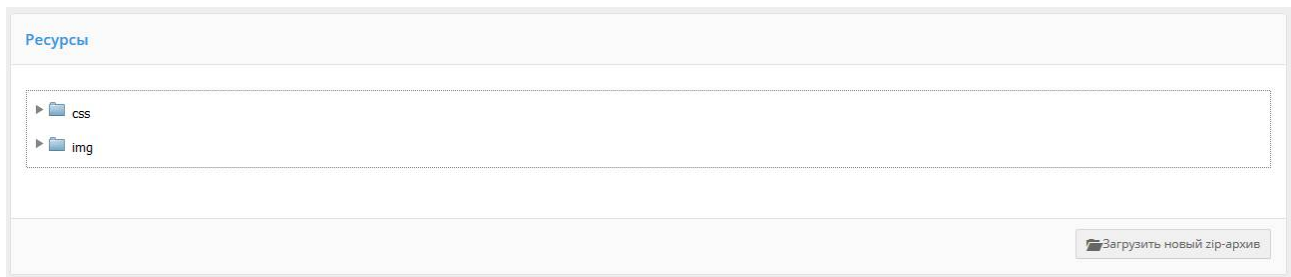
Войти

[Нет аккаунта? Зарегистрироваться](#)

Рисунок 161 – 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.



Ресурсы

- css
- img

[Загрузить новый zip-архив](#)

Рисунок 162 – Внешний вид: доступные ресурсы

15. 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 Exchange⁵⁷. Иллюстрация взаимодействия приведена на схеме (см. Рисунок 163).



Рисунок 163 – 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.

15.1. Настройка blitz-keeper

Настройка blitz-keeper осуществляется путем редактирования конфигурационного файла `blitz-keeper.conf`, расположенного в каталоге `/etc/blitz-keeper`.

⁵⁷ 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.

15.2. 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;

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.

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. 16.1.18).

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.

15.3. 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. 15.2). 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.

16. 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. 4.4.2, п. 7, п. 14);
- `custom_messages/*` – строки пользовательского интерфейса (см. п. 16.2);
- `devices/*` – вспомогательные каталоги для обработки загрузки HOTP и TOTP устройств (см. п. 4.15.1);
- `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. 15);
- `blitz.conf` – основной файл конфигурации (см. п. 16.1);
- `boot.conf` – настройки путей к конфигурационным файлам;
- `console.conf` – настройки консоли управления (см. п. 16.3);
- `credentials` – учетные записи администраторов консоли управления (см. п. 16.3.3);
- `play.conf` – настройки серверов приложений (см. п. 2.1.5 и п. 16.1.14);
- `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. 15);
- `blitz-keeper-log4j.xml` – настройки журналирования событий и ошибок.

16.1. 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.audit` – настройки регистрации событий безопасности;
- `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 хранилище учетных записей;
- `blitz.prod.local.idp.stores` – настройки основной СУБД;
- `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 логута;
- `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;
- `blitz.prod.local.idp.webAuthn` – настройки ключей безопасности;
- `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`.

16.1.1. 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  
}
```

16.1.2. Отключение функции смены пароля при входе

Если Blitz Identity Provider подключен к хранилищу учетных записей, в которое разрешена запись (хранилище не в режиме «Только для чтения»), то при входе пользователя с учетной записью из этого хранилища, если парольная политика потребует от пользователя смены пароля, то пользователю будет показан экран изменения пароля (с просьбой ввести старый и новый пароль). Иногда отображение экрана смены пароля при входе не желательно. Отключить экран можно с помощью задания в конфигурационном файле `blitz.conf` в разделе `blitz.prod.local.idp.login.methods.password` следующего блока настроек:

```
"changePasswordMode": {  
  "type": "except_for",  
  "idStores": ["ldap1", "ldap2"]  
}
```

В настройке `idStores` нужно перечислить идентификаторы тех хранилищ учетных записей, для которых пользователю не должна предлагаться смена пароля при входе.

16.1.3. Настройка внешнего валидатора атрибута

Если возможностей, предоставляемых правилами преобразования входных значений с помощью регулярных выражений (см. п. 3.1.3) недостаточно для реализации требуемой бизнес-логики проверки допустимости значения атрибута, то для атрибута можно запрограммировать и настроить использование внешнего валидатора.

Для этого нужно создать программу с внешним валидатором и собрать ее в JAR-файл.

Созданный JAR-файл нужно скопировать на серверы с приложениями Blitz Identity Provider. Адрес размещения JAR-файлов прописать в Java-опцию `extensionsDir`.

Пример:

```
export JAVA_OPTS="${JAVA_OPTS} -DextensionsDir=/usr/share/identityblitz/extensions"
```

В блоке настроек атрибутов `blitz.prod.local.idp.id-attrs.attrsMeta` в блок описания атрибута, для которого нужно включить проверку через внешний валидатор, необходимо добавить в блоке `source` блок `validators`:

- в настройке `className` прописать адрес Java-класса, реализующего имплементацию интерфейса `AttributeValidator` из Blitz JDK;
- в блоке `conf` прописать настройки, передающиеся в валидатор.

Пример настроек:

```
"id-attrs" : {
```

```

    "attrsMeta" : [
      {
        {
          "class" : "verified-mobile",
          "format" : "string",
          "name" : "phone_number",
          "realmed" : false,
          "required" : false,
          "searchable" : true,
          "source" : {
            "validators" : [
              {
                "className" : "validator.MobileValidator",
                "conf" : {
                  "conf1" : "value1"
                }
              }
            ],
            "type" : "idStore"
          },
          "unique" : false
        },
        ...
      ]
    ]
  }
}

```

16.1.4. Настройка транслятора атрибута

С атрибутом можно ассоциировать транслятор, описывающий правила преобразования атрибута при чтении из LDAP-каталога и при записи в LDAP-каталог. В блоке настроек хранения атрибута в разделе настроек соответствия атрибутов `blitz.prod.local.idp.id-stores.list.mappingRules` в блоке описания атрибута, для которого нужно включить транслятор, необходимо добавить блок `translator` с настройкой `className`, в которой указать имя Java-класса, реализующего алгоритм трансляции. Java-класс должен реализовывать имплементацию интерфейса `LdapAttributeTranslator` из Blitz JDK

При необходимости настроить транслятор для атрибута `objectGUID` из LDAP-каталога Active Directory, чтобы этот атрибут представлялся не в байтовом виде, а в форме строки GUID, можно использовать встроенный в Blitz Identity Provider Java-класс `com.identityblitz.idp.store.ldap.core.translator.ObjectGUIDTranslator`.

Пример настройки:

```

"id-stores" : {
  "list" : [
    {
      ...
      "mappingRules" : [
        ...
        {
          "name" : "objectGUID",
          "storeAttr" : "objectGUID",
          "translator" : {
            "className" :
              "com.identityblitz.idp.store.ldap.core.translator.ObjectGUIDTranslator"
          }
        },
        ...
      ]
    },
    ...
  ]
}

```

При использовании самостоятельно разработанного транслятора необходимо создать программу с внешним транслятором и собрать ее в JAR-файл. Созданный JAR-файл нужно

скопировать на серверы с приложениями Blitz Identity Provider. Адрес размещения JAR-файлов прописать в Java-опцию `extensionsDir`.

Пример:

```
export JAVA_OPTS="${JAVA_OPTS} -DextensionsDir=/usr/share/identityblitz/extensions"
```

16.1.5. 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 логат. 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  
}
```

16.1.6. 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 >"  
}
```

16.1.7. Настройка вызова плагина электронной подписи

Для задания нестандартных настроек вызова плагина электронной подписи при запросе входа пользователем по электронной подписи необходимо в конфигурационном файле в разделе `blitz.prod.local.idp.login.methods.x509` необходимо создать блок настроек `plugin` с переопределенными настройками вызова плагина:

```
"plugin" : {  
  "allModulesEnabled" : false,  
  "capi" : {  
    "providers" : [  
      {  
        "name" : "Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider",  
        "pinMode" : 1  
      },  
      {  
        "name" : "Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider",  
        "pinMode" : 1  
      },  
      {  
        "name" : "Infotecs Cryptographic Service Provider",  
        "pinMode" : 1  
      }  
    ]  
  }  
}
```

```

        "pinMode" : 1
    },
    {
        "name" : "Signal-COM GOST R 34.10-2012 (512) Cryptographic Provider",
        "pinMode" : 1
    },
    {
        "name" : "Signal-COM CPGOST Cryptographic Provider",
        "pinMode" : 1
    },
    {
        "name" : "Signal-COM GOST R 34.10-2012 (256) Cryptographic Provider",
        "pinMode" : 1
    }
],
"stores" : []
},
"modules" : [
    "capi",
    "Aladdin R.D. Unified JaCarta",
    "ISBC ESMART",
    "Rutoken",
    "SafeNet"
]
}

```

В блоке конфигурации можно убрать лишние модули из `modules` и `providers`, чтобы ограничить перечень доступных средств электронной подписи. Также для используемых провайдеров можно настроить режим ввода пин-кода согласно документации на плагин⁵⁸.

16.1.8. 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",

```

⁵⁸ См.: https://identityblitz.ru/products/smart-card-plugin/documentation/?ref=p_pl#document-9


```

        "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**;
 - **by_brute_force_protection** – CAPTCHA отображается, если Blitz Identity Provider обнаружил подбор пароля к конкретной учетной записи или массовый подбор пароля ко всем учетным записям.

При использовании режима `by_brute_force_protection` требуется дополнительно создать в блоке `blitz.prod.local.idp.password` блок настроек `bruteForceProtection` со следующими настройками:

- `disabled` – выключена или нет защита (true/false);
- `captcha` – использовать ли тест CAPTCHA при срабатывании защиты (true/false);
- `delay` – время задержки входа в секундах (применяется, если выключено использование CAPTCHA);
- блок `system` в настройке `thresholds` – если необходима защита на уровне системы (защита от перебора на разные логины). Задаются настройки:
 - `minAttemptsToActivate` – минимальное кол-во прошедших входов для включения механизма защиты на основе статистики системы (по умолчанию 100 входов);
 - `timeWindowInMin` – временное окно сбора статистики по соотношению успешных и неуспешных входов в минутах, должно быть четным (по умолчанию 100 минут);
 - `failedAttemptsPercent`, настройка `turnOff` – порог выключения автоматической защиты, в процентах;
 - `failedAttemptsPercent`, настройка `turnOn` – порог включения автоматической защиты, в процентах.
 - `forced` – включить принудительно защиту для всех (true/false).
- блок `system` в настройке `thresholds` – если необходима защита на уровне отдельных пользователей (защита от подбора пароля на конкретного пользователя). Задаются настройки:
 - `ttlInSec` – период, за который накапливается счетчик неуспешных входов по пользователю в секундах (по умолчанию 3600 секунд);
 - `failedAttempts`, настройка `turnOn` – количество ошибочных входов за период, после которого для учетной записи включится защита.

Пример настроек блока `bruteForceProtection` (включена только защита на уровне пользователя):

```
"bruteForceProtection" : {  
  "delay" : 0,  
  "captcha" : true,  
  "disabled" : false,  
  "thresholds" : {  
    "user" : {  
      "failedAttempts" : {  
        "turnOn" : 5  
      },  
      "ttlInSec" : 3600  
    }  
  }  
}
```

Пример настроек `bruteForceProtection` (включена защита на уровне пользователя и на уровне системы):

```
"bruteForceProtection" : {
  "disabled": false,
  "delay" : 0,
  "captcha" : true,
  "thresholds" : {
    "system" : {
      "minAttemptsToActivate": 1000,
      "timeWindowInMin": 180,
      "failedAttemptsPercent" : {
        "turnOff" : 20,
        "turnOn" : 30
      },
      "forced" : false
    },
    "user" : {
      "ttlInSec": 3600,
      "failedAttempts" : {
        "turnOn" : 5
      }
    }
  }
}
```

В случае использования в качестве CAPTCHA сервиса Google reCAPTCHA v3⁵⁹ необходимо:

- задать следующие настройки в `blitz.prod.local.idp.captcha`:

```
"captcha" : {
  "reCAPTCHA" : {
    "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" : {
```

⁵⁹ См.: <https://developers.google.com/recaptcha/docs/v3>

```
"_name" : "X-Captcha-Check",
"_value" : "true",
"_type" : "on_header",
"type" : "always_on"
},
"enabled" : true,
"initJs" : "require(['/blitz/assets/blitz-common/javascripts/recaptcha_v3.js', 'captcha-conf'],
function(captcha, conf){ captcha(conf);});",
"name" : "reCAPTCHAav3"
}
```

Для добавления CAPTCHA на страницу подтверждения привязки учетной записи пользователя к учетной записи из внешнего поставщика идентификации необходимо задать следующие настройки в `blitz.prod.local.idp.externalIdps.captcha`:

```
"captcha" : {
  "mode" : {
    "_name" : "X-Captcha-Check",
    "_value" : "true",
    "_type" : "on_header",
    "type" : "always_on"
  },
  "enabled" : true,
  "initJs" : "require(['/blitz/assets/blitz-common/javascripts/recaptcha_v3.js', 'captcha-conf'],
function(captcha, conf){ captcha(conf);});",
  "name" : "reCAPTCHAav3"
}
```

Для добавления CAPTCHA на страницу регистрации пользователей необходимо задать следующие настройки в `blitz.prod.local.idp.provisioning.registration.captcha`:

```
"captcha" : {
  "mode" : {
    "_name" : "X-Captcha-Check",
    "_value" : "true",
    "_type" : "on_header",
    "type" : "always_on"
  },
  "enabled" : true,
  "initJs" : "require(['/blitz/assets/blitz-common/javascripts/recaptcha_v3.js', 'captcha-conf'],
function(captcha, conf){ captcha(conf);});",
  "name" : "reCAPTCHAav3"
}
```

Для добавления CAPTCHA на страницу восстановления пароля необходимо задать следующие настройки в `blitz.prod.local.idp.provisioning.recovery.captcha`:

```
"captcha" : {
  "mode" : {
    "_name" : "X-Captcha-Check",
    "_value" : "true",
    "_type" : "on_header",
    "type" : "always_on"
  },
  "enabled" : true,
  "initJs" : "require(['/blitz/assets/blitz-common/javascripts/recaptcha_v3.js', 'captcha-conf'],
function(captcha, conf){ captcha(conf);});",
  "name" : "reCAPTCHAav3"
}
```

16.1.9. Настройка отправки событий в сервер очередей

В сервер очередей могут быть отправлены следующие события:

- регистрация пользователя (`USER_REGISTERED`);
- 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 (только для сообщений `USER_REGISTERED` и `USER_PASSWORD_SET`), в параметре `encCertificate` следует указать псевдоним ключа электронной подписи (в стандартном хранилище ключей `BlitzIdPKeystore.jks`), которым следует шифровать пароли в сообщениях.

16.1.10. Настройка использования сервера очередей в качестве брокера сообщений

В Blitz Identity Provider для обработки асинхронных задач применяется встроенный брокер сообщений, использующий для отслеживания задач базу данных.

При большой интенсивности запросов к Blitz Identity Provider может быть целесообразным использование сервера очередей RabbitMQ в качестве брокера сообщений. Для этого нужно в консоли RabbitMQ (обычно, `http://hostname:15672/`) 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.

После настройки RabbitMQ необходимо скорректировать настройки в `blitz.conf` – в блоке `blitz.prod.local.idp.tasks` установить `broker-type` в значение `rmq` и задать настройки подключения к RabbitMQ в блоке `broker-rmq`:

- в параметре `exchange` задать имя `blitz-tasks-exh`;
- в параметре `queue` в блоке `executionRules` и в параметре `name` в блоке `queues` задать имя `blitz-tasks`;
- в параметре `username` в блоке `user` задать имя пользователя (`blitz`);
- в параметре `password` в блоке `user` задать пароль пользователя в открытом виде – после запуска Blitz Identity Provider пароль будет зашифрован;
- в параметрах `host` и `port` блока `server` указать адрес и порт подключения к RabbitMQ;
- при необходимости скорректировать остальные параметры, определяющие размер пула соединений (`poolSize`), количества каналов (`channelSize`), время ожидания отклика от сервера очередей (`ackTimeout`);

- при необходимости скорректировать настройки брокера обработки задачи, определяющие количество попыток (`maxAttempts`) повторной обработки задач в случае ошибки, время между попытками (`redeliveryDelayInSec`), размер обрабатываемой пачки сообщений (`dequeueBatchSize`), период проверки очереди (`dequeuePeriodInSec`), количество обработчиков (`executorPoolSize`):

Пример конфига приведен ниже:

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

16.1.11. 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"
  ]
}

```

16.1.12. 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"
  },
  ...
}

```

16.1.13. Настройка времени хранения объектов в базе данных

Можно настроить для данных аудита ограничение по сроку хранения записей в базе данных (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
  },
  ...
}

```

Можно настроить для данных об устройствах ограничение по сроку хранения записей в базе данных. Для этого нужно в блоке `blitz.prod.local.idp.login` добавить настройки:

- `uaActiveTtlInSec` – время хранения записи об устройстве (в секундах), с которым связана долгосрочная сессия пользователя или которое пользователь при входе отметил

в качестве доверенного. Если настройка не задана, то информация о таком устройстве хранится в течение года с последнего входа с этого устройства;

- `uaInactiveTtlInSec` – время хранения записи об остальных устройствах (в секундах). Если настройка не задана, то информация о таком устройстве хранится в течение 5 суток.

Пример настроек:

```
"login": {  
  ...  
  "uaActiveTtlInSec": 2678400,  
  "uaInactiveTtlInSec": 432000,  
  ...  
}
```

16.1.14. 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 изменить в `blitz.prod.local.idp.lang` в блоке `portal-lang-cookie` значение настройки `domain` (см. п. 16.2.1):

Пример фрагмента конфигурационного файла:

```
"lang" : {  
  ...  
  "portal-lang-cookie" : {  
    "domain" : "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",  
  ...  
}
```

Изменить домен и путь Blitz Identity Provider в файлах `/blitz-config/saml/conf/relying-party.xml`, `/blitz-config/saml/metadata/idp-metadata.xml`.

Пример изменения настроек в `relying-party.xml`:

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>  
<ns18:RelyingPartyGroup ...>  
  <ns18:AnonymousRelyingParty  
    provider="https://demo.identityblitz.com/blitz/saml"  
    defaultSigningCredentialRef="IdPCredential"/>  
  <ns18:DefaultRelyingParty  
    provider="https://demo.identityblitz.com/blitz/saml"  
    defaultSigningCredentialRef="IdPCredential">  
    ...  
  </ns18:DefaultRelyingParty>  
  ...  
</ns18:RelyingPartyGroup>
```

Пример изменения настроек в `idp-metadata.xml`:

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor ... entityID="https://demo.identityblitz.com/blitz/saml">
  <IDPSSODescriptor ...>
    ...
    <ArtifactResolutionService
      Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML1/SOAP/ArtifactResolution"
      index="1"/>
    <ArtifactResolutionService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/SOAP/ArtifactResolution"
      index="2"/>
    <SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/Redirect/SLO"
      ResponseLocation="https://demo.identityblitz.com/blitz/saml/profile/SAML2/Redirect/SLO"/>
    <SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Plain-Redirect"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/Redirect/Plain/SLO"
      ResponseLocation="https://demo.identityblitz.com/blitz/saml/profile/SAML2/Redirect/Plain/SLO"/>
    <SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/SOAP/SLO" />
    ...
    <SingleSignOnService
      Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
      Location="https://demo.identityblitz.com/blitz/saml/profile/Shibboleth/SSO"/>
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/POST/SSO"/>
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/POST-SimpleSign/SSO"/>
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/Redirect/SSO"/>
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Plain-Redirect"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/Redirect/Plain/SSO"/>
  </IDPSSODescriptor>
  <AttributeAuthorityDescriptor ...>
    ...
    <AttributeService
      Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML1/SOAP/AttributeQuery"/>
    <AttributeService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://demo.identityblitz.com/blitz/saml/profile/SAML2/SOAP/AttributeQuery"/>
    ...
  </AttributeAuthorityDescriptor>
</EntityDescriptor>
```

16.1.15. 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"  
  },  
  ...  
}
```

16.1.16. 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`).

16.1.17. 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
  }
}
```

16.1.18. 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, используемого 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.

16.1.19. Настройка контейнера ключей для работы с ЕСИА и Цифровым профилем

Запросы на аутентификацию через внешние поставщики идентификации ЕСИА и ЦП ЕСИА должны быть подписаны электронной подписью с использованием контейнера ключей с алгоритмами ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. Для использования в Blitz Identity Provider необходим файловый контейнер ключа электронной подписи в формате криптопровайдера КриптоПро CSP (версия 4.0 или выше). Для получения контейнера ключей необходимо обратиться в аккредитованный удостоверяющий центр. В случае если контейнер ключей выпускается удостоверяющим центром на физический носитель, то важно указать, что контейнер ключей должен быть выпущен с экспортируемым закрытым ключом, чтобы его можно было использовать в Blitz Identity Provider.

После получения в аккредитованном удостоверяющем центре контейнера ключей его необходимо импортировать в хранилище ключей, используемое Blitz Identity Provider. Для этого можно или обратиться в техническую поддержку Blitz Identity Provider или воспользоваться следующей инструкцией:

1. Установить на ПК криптопровайдер КриптоПро CSP⁶⁰ (версия 4.0 и новее) и установить закрытый ключ электронной подписи в реестр Windows. Для этого выполнить шаги:
 - запустить КриптоПро CSP;
 - выбрать вкладку «Сервис» и нажать на кнопку «Посмотреть сертификаты в контейнере» (см. Рисунок 164):

⁶⁰ См.: <https://cryptopro.ru/>

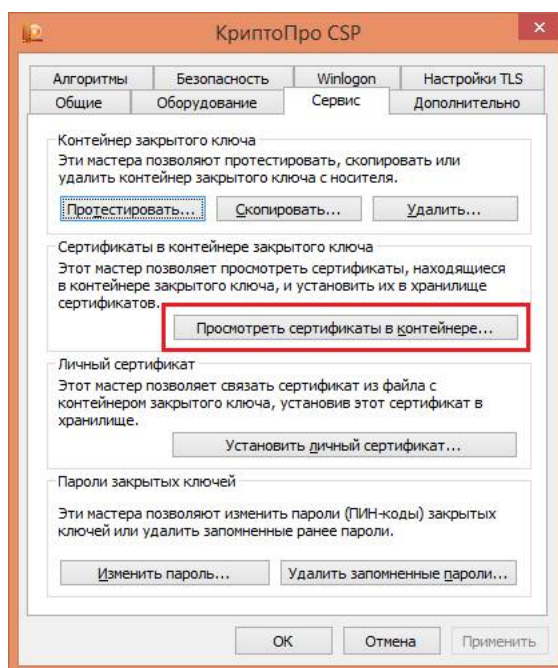


Рисунок 164 – Просмотр сертификатов в контейнере ключей

- нажать на кнопку «Обзор» (см. Рисунок 165):

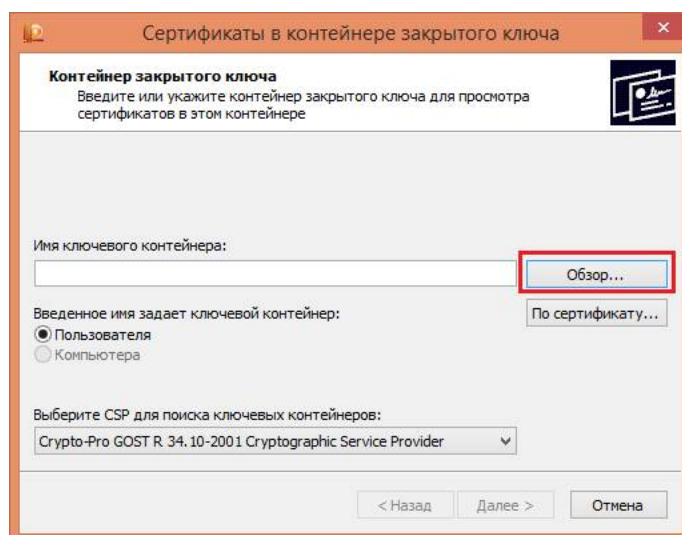


Рисунок 165 – Просмотр сертификатов в контейнере ключей (продолжение)

- выбрать контейнер с ключом ГОСТ Р 34.10-2012 (см. Рисунок 166):

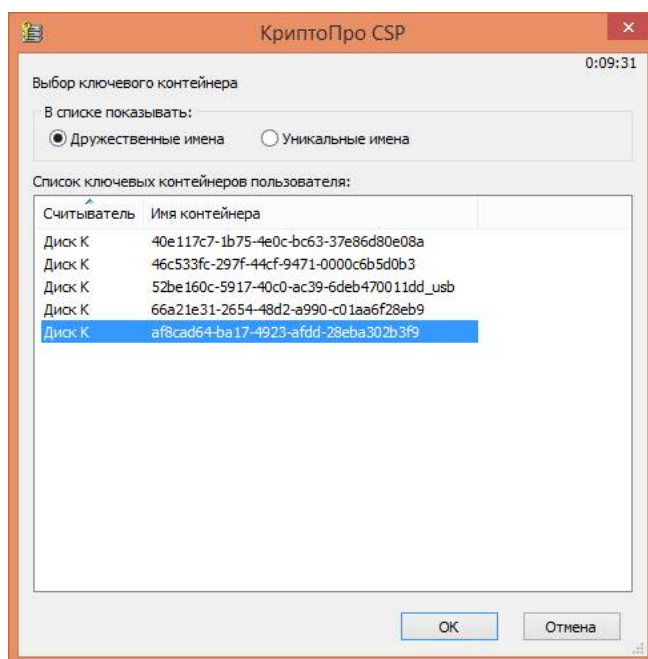


Рисунок 166 – Выбор контейнера ключа

- в открывшемся окне убедиться, что выбран нужный ключевой контейнер (см. Рисунок 167) и нажать далее:

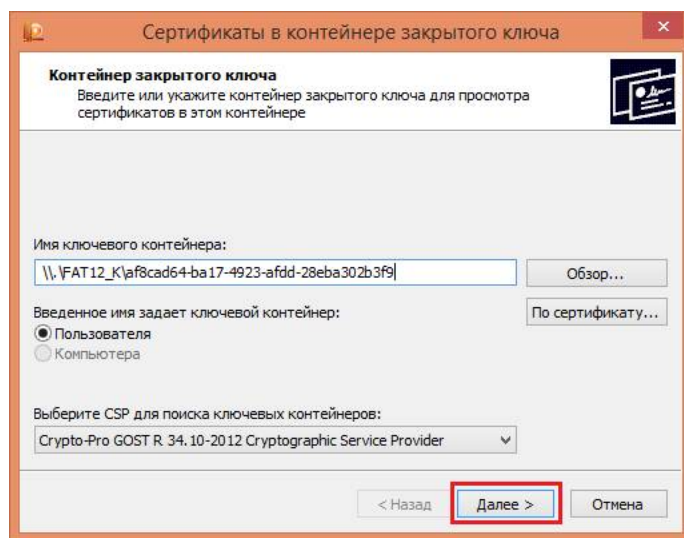


Рисунок 167 – Проверка выбранного контейнера ключа

- в окне со свойствами сертификата (см. Рисунок 168) нажать на кнопку «Установить»:

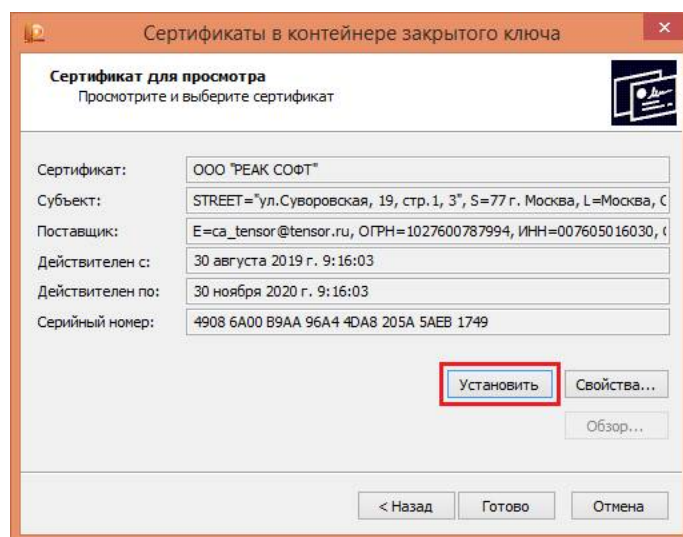


Рисунок 168 – Установка сертификата в реестр

- сообщение «Сертификат был установлен в хранилище «Личные» текущего пользователя» свидетельствует об успешном сохранении.
2. Экспортировать ключ КриптоПро из хранилища Windows в PKCS#12. Для этого приобрести и запустить утилиту **P12FromGostCSP**⁶¹. Нужна специальная версия утилиты – рекомендуется проконсультироваться с технической поддержкой Blitz Identity Provider.

После запуска утилиты выполнить шаги:

- выбрать сертификат (см. Рисунок 169):

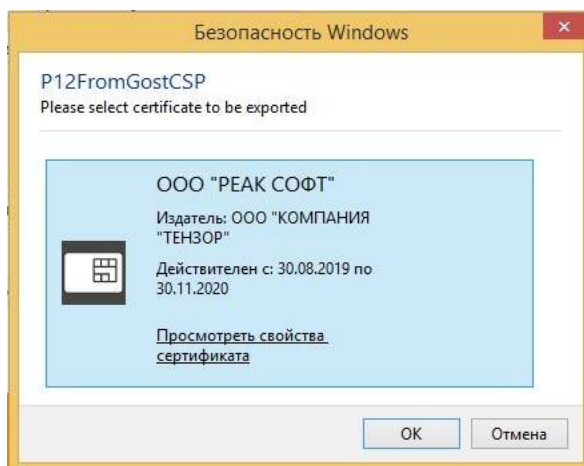


Рисунок 169 – Выбор сертификата

- задать пароль от создаваемого контейнера PKCS#12 (см. Рисунок 170):

⁶¹ См.: http://soft.lissi.ru/ls_product/utills/p12fromcsp/

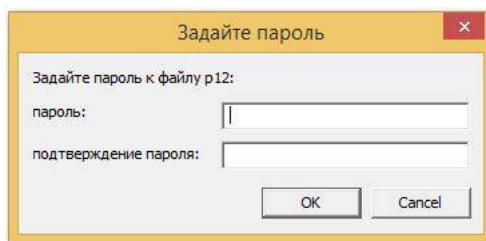


Рисунок 170 – Задание пароля от контейнера PKCS12

- указать файл (см. Рисунок 171) для сохранения PKCS#12. В качестве расширения обязательно указать `.pfx`.

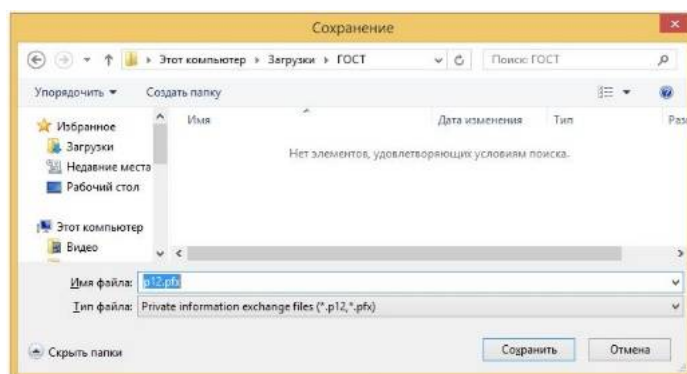


Рисунок 171 – Сохранение файла с контейнером PKCS#12

3. Установить на ПК окружение Java (JRE) версии 8.
4. Импортировать ключ из PKCS#12 в BKS-хранилище с помощью бесплатной утилиты `gost-keytool`⁶².

В этой операции используются параметры:

- `srckeystore` – путь к файлу PKCS#12;
- `srcstorepass` – пароль от контейнера PKCS#12 (был задан на шаге 2);
- `srcalias` – имя ключа в контейнере PKCS#12. Нужно указать значение `csp_exported`;
- `srckeypass` – пароль к ключу в контейнере PKCS#12. Нужно указать то же самое значение, что и для параметра `srcstorepass`;
- `destkeystore` – путь к файлу BKS `esia-gost.bks`;
- `deststoretype` – тип хранилища. Нужно указать значение `BKS`;
- `deststorepass` – пароль к хранилищу BKS;
- `destalias` – имя (alias) ключа в BKS, например, `gost2012`;
- `destkeypass` – пароль к ключу в BKS. Нужно указать то же самое значение, что и для параметра `deststorepass`.

⁶² См.: <https://identityblitz.ru/wp-content/uploads/2019/11/gost-keytool.zip>

Пример вызова операции импорта ключа из PKCS#12 в BKS:

```
java -cp gost-keytool.jar:bcprov-jdk15on-1.62.jar ru.reaxoft.gost.Keytool import_pkcs12 --srckeystore file.pfx --srcstorepass 1 --srcalias csp_exported --srckeypass 1 --destkeystore esia-gost.bks --deststoretype BKS --deststorepass 2 --destalias gost2012 --destkeypass 2
```

5. Скопировать созданное BKS хранилище на сервер с установленной консолью управления (blitz-console) в каталог `/usr/share/identityblitz/blitz-config/`. Дать права пользователю `blitz` на файл контейнера командой:

```
chown blitz:blitz /usr/share/identityblitz/blitz-config/esia-gost.bks
```

6. Из текущего хранилища ключей `BlitzIdPKeystore.jks` экспортировать ключи в созданное BKS хранилище. Для этого выполнить следующие шаги на сервере с консолью управления blitz-console:

- экспорт ключей из JKS хранилища в PKCS#12 хранилище:

```
keytool -importkeystore -srckeystore BlitzIdPKeystore.jks -destkeystore BlitzIdPKeystore.p12 -srcstoretype JKS -deststoretype PKCS12 -deststorepass <ПАРОЛЬ ОТ JKS ХРАНИЛИЩА>
```

- импорт ключей из PKCS#12 хранилища в BKS хранилище:

```
keytool -importkeystore -srckeystore BlitzIdPKeystore.p12 -srcstorepass <ПАРОЛЬ P12> -srcstoretype pkcs12 -destkeystore <ПУТЬ К BKS хранилищу> -deststorepass <ПАРОЛЬ BKS ХРАНИЛИЩА> -deststoretype bks -providerclass org.bouncycastle.jce.provider.BouncyCastleProvider -providerpath /usr/share/identityblitz/blitz-console/lib/org.bouncycastle.bcprov-jdk15on-1.62.jar
```

7. Переключить Blitz Identity Provider на работу с новым хранилищем:

- в файле `blitz.conf` скорректировать блок настроек `blitz.prod.local.idp.keystore` следующим образом:

```
{
  "keystore" : {
    "password" : "<ПАРОЛЬ BKS ХРАНИЛИЩА>",
    "path" : "esia-gost.bks",
    "type" : "BKS"
  }
}
```

- перезапустить приложения Blitz Identity Provider.

16.1.20. 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. 8.8) 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 172).

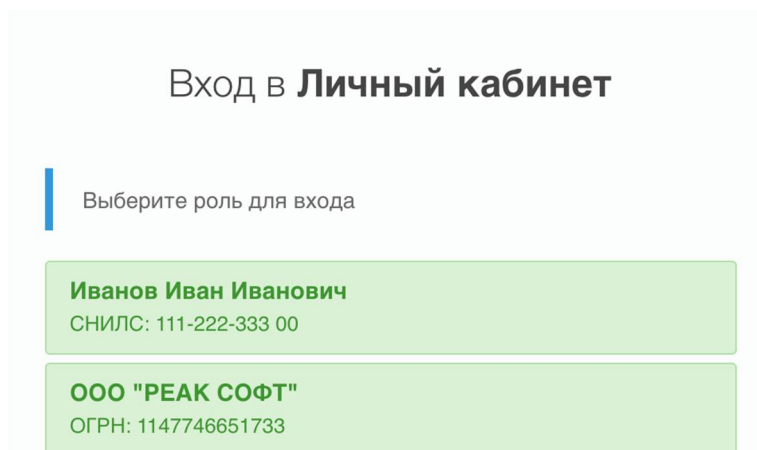


Рисунок 172 – Пример страницы выбора режима входа через ЕСИА

- 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. 16.1.18) и вход через ЕСИА (см. п. 8.8). 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" : "${org.agencyType-}"
    },
    {
        "attr" : "org_agencyterrrange",
        "master" : true,
        "value" : "${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_addrs",
  "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"
          }
        ]
      }
    ]
  }
}
```

```
}  
  }  
  },  
  ...  
  ]  
}  
}
```

16.1.21. Настройка аутентификации по ключам безопасности (WebAuthn, Passkey, FIDO2, U2F)

Blitz Identity Provider позволяет использовать для идентификации и аутентификации ключи безопасности (WebAuthn, Passkey, FIDO2, U2F) (см. п. 4.12 и п. 4.20). Для этого нужно создать блок настроек `blitz.prod.local.idp.webAuthn` со следующими настройками:

- `credentialsDiscoveryMode` – схема поиска привязанных к учетной записи ключей безопасности. Возможные значения настройки:
 - `SERVER` (используется по умолчанию) – сервер передает браузеру список привязанных к учетной записи ключей безопасности после предварительной идентификации пользователя (для этого при входе по ключу безопасности пользователь предварительно вводит свой логин);
 - `CLIENT` – браузер самостоятельно запрашивает у пользователя выбор ключа безопасности среди ключей, зарегистрированных для домена Blitz Identity Provider. При таком режиме ключи безопасности регистрируются с дополнительным параметром `requireResidentKey=TRUE`. Данный режим не рекомендуется к использованию, так как пока не все браузеры поддерживают работу в этом режиме и умеют отображать пользователю запрос на выбор ключа безопасности;
- настройка `attachmentOnly` в блоке настроек `authenticator` – указывает фильтр для типов аутентификаторов. При отсутствии настройки фильтрация не применяется. Возможные значения фильтрации:
 - `cross-platform` – разрешить использование кроссплатформенных ключей безопасности (устройства, подключаемые по USB, NFC или Bluetooth);
 - `platform` – разрешить использование встроенных в платформу ключей безопасности (Passkey, ПИН-код, Touch ID, Face ID, Windows Hello).
- `callTimeoutMs` – определяет максимальное время ожидания обработки вызова обращения к ключу безопасности. Рекомендуется задавать таймаут не менее 60 секунд. Значение настройки задается в миллисекундах;
- блок настроек `rp`, содержащий настройку с именем домена (`id`), на который будут привязываться ключи безопасности (домен должен совпадать с доменом, используемым Blitz Identity Provider, или вышестоящим доменом) и настройку с

- именем организации или приложения (**name**);
- блок настроек **trustedStores**, содержащий тип (**type**), файловый путь (**path**) и пароль (**password**) доступа к контейнеру ключей, использующемуся для проверки подписи аттестационных объектов, формируемых при регистрации ключей безопасности. Контейнер ключей автоматически обновляется при установке новых версий Blitz Identity Provider и содержит актуальные корневые и промежуточные сертификаты TPM модулей, FIDO, а также сертификаты Apple и Google, необходимые для проверки подписи аттестационных объектов. При необходимости ограничить ключи безопасности до устройств определенных производителей нужно удалить из контейнера ключей лишние корневые и промежуточные сертификаты;
 - блок настроек **user**, содержащий отображаемое имя пользователя **displayName**, задаваемое как фрагмент подстановки из атрибутов учетной записи пользователя (например, **\${given_name} \${family_name}**) и имя пользователя **name**, показываемое ему при выборе ключа безопасности, также задаваемое как фрагмент подстановки из атрибутов учетной записи пользователя;
 - **acceptedKeysAlgorithms** – настройка, содержащая список принимаемых алгоритмов ключей: **-7** (ECDSA P-256 + SHA-256) и **-257** (RSASSA + SHA-256);
 - **normalCounterDistance** – настройка, позволяющая задействовать возможности ключей безопасности по защите от атак клонирования ключа безопасности. Некоторые FIDO2 и U2F устройства обладают встроенными счетчиками подписей и передают при аутентификации текущий счетчик на сервер. Blitz Identity Provider в таком случае будет проверять, что разница между текущим значением счетчика аутентификации в ключе и сохраненным счетчиком аутентификации на сервере не больше заданного в настройке значения.

Пример настроек:

```
"webAuthn" : {
  "acceptedKeysAlgorithms" : [
    -7,
    -257
  ],
  "_authenticator" : {
    "_attachmentOnly" : "platform"
  },
  "callTimeoutMs" : 60000,
  "credentialsDiscoveryMode" : "SERVER",
  "normalCounterDistance" : 1,
  "rp" : {
    "id" : "company.com",
    "name" : "AUTH-SYSTEM"
  },
  "trustedStores" : [
    {
      "password" : "*****",
      "path" : "webAuthn-trusted-ca.jks",
      "type" : "jKS"
    }
  ]
},
```



```
"user" : {  
  "displayName" : "${given_name-} ${family_name-}",  
  "name" : "${email-}"  
}
```

16.1.22. Блокирование перебора кодов подтверждения

При прохождении аутентификации такими способами как «Подтверждение с помощью кода», «Подтверждение с помощью электронной почты», «Разовый пароль на основе секрета (НОТР)», «Разовый пароль на основе времени (ТОТР)», а также при восстановлении пароля пользователь вводит коды подтверждения. Blitz Identity Provider контролирует число отправок кодов подтверждения и число неуспешных попыток ввода кода подтверждения (из SMS, email, генератора кодов) по каждому методу проверки в разрезе учетных записей. При 10 попытках включается временная блокировка использования метода на 15 минут. При необходимости можно изменить настройки по умолчанию для каждого из методов. Для этого нужно у метода аутентификации в блоке `blitz.prod.local.idp.login.methods` в разделе соответствующего метода аутентификации и в блоке `blitz.prod.local.idp.provisioning.recovery` (для восстановления пароля) задать в настройке `tempLockAfter` максимальное число попыток, а в настройке `tempLockForMin` время блокировки в минутах. Блокировки запоминаются в оперативной памяти Blitz Identity Provider –при перезапуске всех серверов Blitz Identity Provider блокировки снимаются. Также блокировки подбора кодов подтверждения на учетной записи снимаются в случае сброса пароля пользователя. Для отключения функции можно поставить в `0` значение настройки `tempLockForMin`.

Пример настроек:

```
"login" : {  
  ...  
  "methods" : {  
    ...  
    "sms" : {  
      "profiles" : {  
        "1" : {  
          ...  
          "tempLockAfter" : 10,  
          "tempLockForMin" : 15  
        },  
        "2" : {  
          ...  
          "tempLockAfter" : 10,  
          "tempLockForMin" : 15  
        }  
      }  
    },  
    "email" : {  
      ...  
      "tempLockAfter" : 10,  
      "tempLockForMin" : 15  
    }  
    "hotp" : {  
      ...  
      "tempLockAfter" : 10,  
      "tempLockForMin" : 15  
    },  
    "totp" : {  
      ...  
      "tempLockAfter" : 10,  
      "tempLockForMin" : 15  
    }  
  }  
}
```

```

    },
    ...
  },
  ...
  "provisioning" : {
    "recovery" : {
      ...
      "tempLockAfter" : 10,
      "tempLockForMin" : 15
    },
  },
}

```

16.1.23. Включение режима запоминания множества учетных записей

Сервер аутентификации Blitz Identity Provider поддерживает режим мультивхода, в котором запоминает несколько учетных записей пользователей, использующих для входа одни и те же устройство и браузер. Это может быть полезно, когда у пользователя может быть сразу несколько учетных записей от сервиса, и должна быть предусмотрена возможность переключения между этими учетными записями без необходимости делать логат. Это также может быть полезно для семейных сервисов, когда с одного и того же устройства и браузера с сервисом могут работать разные члены семьи и допустимо, чтобы переключение между учетными записями членов семьи выполнялось без логата из этих учетных записей.

Для включения режима мультивхода необходимо в блок настроек `blitz.prod.local.idp.login` добавить раздел `mus` со следующими настройками:

- `plural` – в случае значения `true` включает в Blitz Identity Provider режим мультивхода;
- `widget` – блок настроек, определяющий отображение карточки пользователя на экране выбора учетной записи пользователя из списка запомненных. Настройка `displayName` определяет верхнюю отображаемую строку в карточке пользователя (например, можно настроить вывод имени и фамилии пользователя). Настройка `displayId` определяет нижнюю отображаемую строку в карточке пользователя (например, можно настроить вывод адреса электронной почты, номера телефона или логина учетной записи). Настройка `showIcon` определяет, необходимо ли отображать в карточке пользователя аватар, составленный из букв первой строки `displayName`.

Пример настройки:

```

"login" : {
  ...
  "mus" : {
    "plural" : true,
    "widget" : {
      "displayName" : "${given_name-} {family_name-}",
      "displayId" : "${phone_number-}",
      "showIcon" : true
    }
  },
  ...
}

```

Можно настроить маскирование отображаемых в карточке пользователя сведений. Для этого необходимо использовать функцию `maskInMiddle(savedFirstChars, savedLastChars,`

replacer). Пример настройки для задания маскированного отображения номера телефона: `${phone_number&maskInMiddle(3,3,)}`

16.1.24. Настройки сервиса OIDC Discovery

Blitz Identity Provider автоматически публикует сервис OIDC Discovery⁶³ в соответствии с заданными в Blitz Identity Provider настройками. В составе сервиса можно прописать адрес документации на OIDC сервис. Чтобы задать свой адрес документации, необходимо в блоке настроек `blitz.prod.local.idp.oauth` прописать настройку `serviceDocumentationUrl` со значением адреса ссылки на документацию.

16.1.25. Изменение адресов вызовов внешних поставщиков идентификации

При внедрении Blitz Identity Provider может возникнуть потребность настроить вызовы с серверов Blitz Identity Provider обработчиков внешних поставщиков идентификации не напрямую, а через прокси сервер. В этом случае есть необходимость изменить стандартные адреса обработчиков внешних поставщиков идентификации на адреса, зарегистрированные на прокси сервере. Чтобы скорректировать адреса обработчиков, необходимо изменить значения настроек `authUri`, `tokenUri`, `dataUri` в соответствующих блоках настроек внешних поставщиков идентификации в `blitz.prod.local.idp.federation`.

Пример настроек для входа через внешний поставщик Google:

```
"federation" : {
  "points" : {
    "google" : [
      {
        ...
        "authUri" : "https://accounts.google.com/o/oauth2/auth",
        "tokenUri" : "https://accounts.google.com/o/oauth2/token",
        "dataUri" : "https://www.googleapis.com/oauth2/v1/userinfo?alt=json",
        ...
      },
      ...
    ]
  }
}
```

16.1.26. Настройка внешнего SAML поставщика входа

Blitz Identity Provider позволяет настроить вход через внешний поставщик идентификации, работающий по протоколу SAML 2.0.

Для этого необходимо в блоке настроек `blitz.prod.local.idp.federations` создать внешний поставщик `saml` со следующими настройками:

- `name` – системное имя внешнего поставщика идентификации;
- `humanReadableName` – описание внешнего поставщика идентификации;
- `clientId` – имя поставщика услуг (EntityId), присвоенное Blitz Identity Provider при

⁶³ См.: <https://tools.ietf.org/html/rfc8414>

регистрации во внешнем SAML поставщике идентификации;

- `signAuthnReq` – определяет, должен ли Blitz Identity Provider подписывать SAML-запрос, отправляемый внешнему поставщику идентификации;
- `checkAssertionSign` – определяет, необходимо ли проверять подпись SAML-утверждений, полученных от внешнего поставщика идентификации (для ПРОД-сред обязательно необходимо включать проверку подписи);
- блок `credentials` с настройками доступа к ключевому контейнеру, используемому для подписывания запросов к поставщику идентификации SAML. Настраивается опционально, в случае если для взаимодействия с внешним поставщиком идентификации требуется использовать отдельный контейнер ключей. Если настройка не задана, то ключи будут браться из основного keystore, настроенного в блоке `blitz.prod.local.idp.keystore` (при этом в качестве `alias` будет использоваться имя поставщика идентификации из настройки `name`). Задаются настройки:
 - `alias` – имя ключа в контейнере;
 - `keystore` – блок настроек, содержащий тип контейнера (`type`), который может быть JCEKS или BKS, а также путь к контейнеру (`path`) и пароль к контейнеру (`password`);
- `idpMetaPath` – путь к файлу, в котором хранятся метаданные внешнего поставщика идентификации (XML-файл с метаданными IDP);
- блок настроек `userMatching` – задает правила сопоставления учетных записей:
 - в настройке `type` – признак, что используется базовая (значение `builder`) настройка связывания учетных записей;
 - в настройке `mapping` – правила сопоставления учетных записей из внешнего SAML-поставщика идентификации учетным записям в Blitz Identity Provider;
 - в настройке `matchingRules` – правила переноса SAML-утверждений из внешнего поставщика идентификации в атрибуты учетной записи в Blitz Identity Provider;
 - `requireLogInToBind` – признак «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»;
 - `strictMatching` – признак «Требовать ввод пароля, если учетная запись была идентифицирована»;
 - `uniqueMatching` – признак «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия».

Пример настроек внешнего поставщика идентификации:

```
"federation" : {  
  "points" : {  
    "saml" : [  

```

```

{
  "name" : "demo-idp",
  "humanReadableName" : "External SAML IDP",
  "clientId" : "login.company.com",
  "signAuthnReq" : true,
  "checkAssertionSign" : true,
  "_credentials" : {
    "alias" : "demo-idp",
    "keyStore" : {
      "password" : "*****",
      "path" : "demo-idp-key.jks",
      "type" : "JCEKS"
    }
  },
  "idpMetaPath" : "demo-idp-metadata.xml",
  "userMatching" : {
    "type" : "builder",
    "mapping" : [
      {
        "attr" : "urn:saml:mail",
        "master" : false,
        "value" : "${email}"
      }
    ],
    "matchingRules" : [
      [
        {
          "attr" : "urn:saml:mail",
          "value" : "${email}"
        }
      ]
    ],
    "requireLogInToBind" : false,
    "strictMatching" : false,
    "uniqueMatching" : false
  }
},
...
}

```

После создания настроек внешнего поставщика необходимо включить его в списке доступных внешних поставщиков идентификации. Для этого в блок настроек `blitz.prod.local.idp.login` в перечень методов аутентификации (`methods`) в список внешних поставщиков входа `externalIdps` добавить внешний поставщик с `fedPoint`, соответствующий настроенному. Пример настройки для включения внешнего поставщика идентификации с типом `saml` и именем `demo-idp`:

```

"login" : {
  ...
  "methods" : {
    ...
    "externalIdps" : {
      "idps" : [
        ...
        {
          "fedPoint" : "saml:demo-idp"
        },
        ...
      ],
      ...
    },
    ...
  },
  ...
}

```

Настроить логотип для кнопки входа через внешний поставщик входа согласно инструкции в п. 16.2.4.

16.1.27. Настройка внешнего поставщика входа СУДИС

Blitz Identity Provider позволяет настроить вход через внешний поставщик идентификации СУДИС.

Для этого необходимо в блоке настроек `blitz.prod.local.idp.federations` создать внешний поставщик `sudis` со следующими настройками:

- `name` – системное имя внешнего поставщика идентификации;
- `humanReadableName` – описание внешнего поставщика идентификации;
- `clientId` – имя поставщика услуг (EntityId), присвоенное Blitz Identity Provider при регистрации в СУДИС;
- блок `credentials` с настройками доступа к ключевому контейнеру, используемому для подписывания и шифрования запросов к СУДИС. Должно использоваться ПО CMSServer, дистрибутив которого предоставляет поставщик СУДИС.

Задаются настройки:

- `endpoint` – адрес сервера CMSServer;
- `fingerprint` – SHA1 хэш сертификата IDP СУДИС. Указывается в формате `{SHA1}значение`;
- `recipientKey` – идентификатор ключа СУДИС (значение `cn` из `subject` сертификата СУДИС);
- `senderKey` – идентификатор ключа Blitz Identity Provider, используемого для подписания запросов к СУДИС и расшифрования ответов (значение `cn` из `subject` сертификата Blitz Identity Provider, зарегистрированного в СУДИС);
- `idpEntityId` – EntityID СУДИС;
- `sidAttrName` – имя атрибута, используемого в качестве идентификатора учетной записи в СУДИС;
- `ssoServiceLocation` – адрес обработчика запроса запросов на аутентификацию в СУДИС;
- `sloServiceResponseLocation` – адрес ответа на запросы логаута, инициированные в СУДИР из СУДИС;
- `sloServiceLocation` – адрес обработчика логаута в СУДИС при инициировании логаута из СУДИР в СУДИС;
- блок настроек `userMatching` – задает правила сопоставления учетных записей:
 - в настройке `type` – признак, что используется базовая (значение `builder`) настройка связывания учетных записей;
 - в настройке `mapping` – правила сопоставления учетных записей из внешнего

SAML-поставщика идентификации учетным записям в Blitz Identity Provider;

- в настройке `matchingRules` – правила переноса SAML-утверждений из внешнего поставщика идентификации в атрибуты учетной записи в Blitz Identity Provider;
- `requireLogIntoBind` – признак «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»;
- `strictMatching` – признак «Требовать ввод пароля, если учетная запись была идентифицирована»;
- `uniqueMatching` – признак «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия».

Пример настроек внешнего поставщика идентификации:

```
"federation" : {
  "points" : {
    "sudis" : [
      {
        "clientId" : "<ENTITY_ID BLITZ>",
        "credentials" : {
          "endpoint" : "http://<CMS_HOST>:<CMS_PORT>",
          "fingerprint" : "{SHA1}<FINGERPRINT SUDIS CERT>",
          "recipientKey" : "<SUDIS_KEY SUBJECT.CN>",
          "senderKey" : "<BLITZ_KEY SUBJECT.CN>"
        },
        "humanReadableName" : "SUDIS",
        "idpEntityId" : "http://...",
        "name" : "sudis",
        "sidAttrName" : "oid",
        "ssoServiceLocation" : "http://.../idp/profile/SAML2/POSTGOST/SSO",
        "sloServiceLocation" : "http://.../idp/Logout",
        "sloServiceResponseLocation" : "http://.../idp/profile/SAML2/Redirect/SLO",
        "userMatching" : {
          ...
        }
      }
    ]
  }
}
```

После создания настроек внешнего поставщика необходимо включить его в списке доступных внешних поставщиков идентификации. Для этого в блок настроек `blitz.prod.local.idp.login` в перечень методов аутентификации (`methods`) в список внешних поставщиков входа `externalIdps` добавить внешний поставщик с `fedPoint`, соответствующий настроенному. Пример настройки для включения внешнего поставщика идентификации с типом `sudis` и именем `sudis`:

```
"login" : {
  ...
  "methods" : {
    ...
    "externalIdps" : {
      "idps" : [
        {
          "fedPoint" : "sudis:sudis"
        },
        ...
      ],
      ...
    },
    ...
  },
  ...
}
```

16.1.28. Включение режима регистрации незавершенных попыток входа

В Blitz Identity Provider все события фиксируются по факту окончания вызывавшего их процесса. Для большинства событий это нормально, так как процессы краткосрочные.

Среди всех регистрируемых событий есть важные события, связанные с входом пользователей. Если вход произошел успешно, то в самом конце процесса входа регистрируется событие безопасности, в котором указывается, кто, куда и когда вошел, какие методы аутентификации были задействованы, IP-адрес, UserAgent и много других деталей.

В зависимости от сделанных при внедрении настроек процесс входа может быть устроен сложно. Не всегда будет достаточно только ввести логин и пароль, и нужно будет дополнительно пройти подтверждение входа или в процессе входа пользователь будет взаимодействовать со вспомогательными приложениями (pipes), например, актуализировать контакт, настраивать Passkey или отвечать на вопрос, доверяет ли он устройству/браузеру. Если пользователь в какой-то момент этого процесса перестанет продолжать вход, то процесс входа не завершится, и как следствие, событие аудита о таком незавершенном входе не создастся. В зависимости от того, в какой момент это случится, это может быть проблемой безопасности. Например, если пользователь просто открыл страницу входа и не стал вводить логин и пароль, то фиксация такого события в журнале безопасности не представляет особого интереса. А вот если пользователь ввел правильные логин и пароль, но попал на экран подтверждения входа, который не стал проходить, то такое событие безопасности было бы хорошо зафиксировать. Возможно, злоумышленник перебирал пароль и смог успешно его подобрать, но не смог пройти проверку второго фактора аутентификации. Событие безопасности позволило бы узнать о такой ситуации, если бы оно было записано и анализировалось.

Для включения регистрации событий неуспешных (незавершенных) входов необходимо в блоке настроек `blitz.prod.local.idp.login` добавить параметры:

- `postponeEnabled` – значение `true`, если механизм включен;
- `postponeTtl` – время в секундах, после истечения которого регистрируется отложенное событие аудита, если вход не был завершен.

В случае если для обработки задач используется RabbitMQ, то для основной очереди задач необходимо сделать дополнительную очередь с названием `<название основной очереди>-postpone` и задать для нее следующие аргументы:

```
x-dead-letter-exchange = <используемый exchange>
x-dead-letter-routing-key = <основная очередь>
```

Так же для созданной очереди необходимо настроить binding на используемый exchange.

16.1.29. Настройка передачи событий безопасности в файл или Kafka

В Blitz Identity Provider можно настроить регистрацию событий безопасности в один или несколько приемников. Настройка задается в блоке настроек `blitz.prod.local.idp.audit`. Необходимо задать следующие настройки:

- `emitters` – определяет список приемников записей аудита. По каждому приемнику заполняется блок настроек:
 - `type` – тип приемника. Возможные значения:
 - `audit-store` – запись производится в СУБД;
 - `log` – запись производится в логгер `logback`;
 - `kafka` – запись производится на сервер очередей Kafka.
 - `enabled` – необязательная настройка – определяет, включен или нет приемник;
 - `include` – необязательная настройка – перечисляются типы событий безопасности (см. таблицу 6), по которым осуществляется запись в приемник. Если настройка не указана, то пишутся все события безопасности;
 - `exclude` – необязательная настройка – перечисляются типы событий безопасности (см. таблицу 6), которые не должны записываться в приемник. Если настройка не указана, то никакие события не исключаются. Если настройка указана вместе с `include`, то сначала список событий определяется настройкой `include`, а потом из него исключаются события, указанные в `exclude`. Рекомендуется не использовать совместно обе настройки `include` и `exclude`, а применять только что-то одно;
 - `logger` – необязательная настройка – указывается только для приемника с типом `log`. Позволяет определить имя логгера. Если настройка не задана, то запись производится в логгер с именем `AUDIT`;
 - `name` – необязательная настройка – указывается для приемников с типами `log` и `kafka`. Указывает имя приемника, так как для этих типов приемников можно настроить несколько приемников. Если настройка не задана, то используются `log` и `kafka` в качестве имен приемников;
 - `bootstrapServers` – обязательная настройка для приемника с типом `kafka` – указывается список адресов для первоначального подключения к кластеру Kafka;
 - `topic` – обязательная настройка для приемника с типом `kafka` – название топика Kafka, в который должно отправляться событие;
 - `securityProtocol` – необязательная настройка для приемника с типом `kafka` – в случае использования подключения по SASL может не указываться. При подключении по

SSL в настройке должно быть указано значение **SSL**;

- **sasl** – необязательный блок настроек для приемника с типом **kafka** – задает параметры подключения при использовании SASL-аутентификации для подключения к Kafka:
 - **jaasConfig** – строка подключения, в которой можно использовать параметры подстановки из **secureParams**;
 - **mechanism** – значение **PLAIN**;
 - **secureParams** – блок с параметрами, которые будут зашифрованы в конфигурационном файле при запуске сервера.

Пример блока:

```
"sasl" : {
  "jaasConfig" : "org.apache.kafka.common.security.plain.PlainLoginModule required
username=\"alice\" password=\"${pswd}\"",
  "mechanism" : "PLAIN",
  "secureParams" : {
    "pswd" : "Содержимое зашифруется при запуске",
  }
},
```

- **ssl** – необязательный блок настроек для приемника с типом **kafka** – задает параметры SSL для подключения к Kafka:
 - **enabledProtocols** – строки со списком включенных протоколов;
 - **keyStore** – блок настроек с параметрами доступа к ключевому контейнеру Blitz Identity Provider. Содержит настройки **type**, **path**, **password**;
 - **trustedStore** – блок настроек с параметрами доступа к контейнеру с доверенными сертификатами. Содержит настройки **type**, **path**, **password**;
 - **keyPassword** – необязательная настройка – пароль для доступа к ключу;

Пример блока:

```
"securityProtocol" : "SSL",
"ssl" : {
  "enabledProtocols" : ["TLSv1.2,TLSv1.3"],
  "keyStore" : {
    "password" : "CHANGE-ME",
    "path" : "/etc/blitz-config/bip-dlapp01-1.jks",
    "type" : "JKS"
  },
  "trustedStore" : {
    "password" : "CHANGE-ME",
    "path" : "/etc/blitz-config/ca.jks",
    "type" : "JKS"
  },
  "keyPassword": "CHANGE-ME"
},
```

- **tuning** – необязательный блок настроек для приемника с типом **kafka** – задает опциональные настройки **producer** для взаимодействия с Kafka. Имена параметров необходимо указывать с точкой как в документации Kafka⁶⁴.

Пример блока:

⁶⁴ См.: <https://kafka.apache.org/documentation/#producerconfigs>

```
"tuning": {  
  "client.id": "BlitzKafka"  
}
```

- **emitAtLeastOneOf** – необязательная настройка – указывается список приемников, достаточно записи событий в любой из которых, чтобы операция считалась успешной;
- **emitToAllOf** – необязательная настройка – указывается список приемников, по которым обязательно должно быть получено подтверждение успешной записи события, чтобы операция считалась успешной. Если настройки **emitAtLeastOneOf** и **emitToAllOf** не заданы, то обязательно подтверждение от всех настроенных приемников;
- **emitTimeoutInSec** – необязательная настройка – определяет максимальное время отклика от приемника в ответ на запроса записи события. Если настройка не задана, то ожидание 60 секунд.

Пример настроек записи аудита одновременно в лог, в СУБД и в Kafka:

```
"audit": {  
  "emitters": [  
    {  
      "type": "log",  
      "name": "users-log",  
      "enabled": true,  
      "logger": "AUDIT",  
      "exclude": ["admin_added", "admin_pswd_changed", "admin_removed", "admin_roles_changed",  
        "config_changed"]  
    },  
    {  
      "type": "log",  
      "name": "admins-log",  
      "enabled": true,  
      "logger": "AUDITADMIN",  
      "include": ["admin_added", "admin_pswd_changed", "admin_removed", "admin_roles_changed",  
        "config_changed"]  
    },  
    {  
      "type": "audit-store",  
      "enabled": true  
    },  
    {  
      "type": "kafka",  
      "enabled": true,  
      "name": "kafka",  
      "include": ["login"],  
      "bootstrapServers": ["infra-kfk01:9443"],  
      "topic": "blitz_audit",  
      "securityProtocol": "SSL",  
      "ssl": {  
        "enabledProtocols": ["TLSv1.2,TLSv1.3"],  
        "keyStore": {  
          "password": "CHANGE-ME",  
          "path": "/etc/blitz-config/bip-app01.jks",  
          "type": "JKS"  
        },  
        "trustedStore": {  
          "password": "CHANGE-ME",  
          "path": "/etc/blitz-config/ca.jks",  
          "type": "JKS"  
        }  
      }  
    }  
  ],  
  "emitAtLeastOneOf": ["users-log", "admins-log", "kafka"],  
  "emitToAllOf": ["audit-store"],  
  "emitTimeoutInSec": 30  
}
```

При регистрации аудита в лог можно настроить логгер с помощью файла конфигурации `logback.xml`⁶⁵. Пример настройки логгера **AUDIT** в файле конфигурации `logback.xml`:

```
...
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
  <file>${dir.logs}/audit-${app.name}.log</file>
  <encoder>
    <pattern>%date - [%level] -[%file:%line] - %message%n%xException{20}</pattern>
  </encoder>
  <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
    <fileNamePattern>${dir.logs}/archive/audit-${app.name}_%d{yyyy-MM-dd}.log.gz</fileNamePattern>
    <maxHistory>90</maxHistory>
    <totalSizeCap>5GB</totalSizeCap>
  </rollingPolicy>
</appender>

<logger name="AUDIT" additivity="false">
  <appender-ref ref="AUDIT" />
</logger>
...
```

Пример записей в логге:

```
2022-11-22 14:03:01,576 - [INFO] - [LoggerEventEmitterDriver.scala:32] -
{"ip":"172.25.0.1","timestamp":1669114981529,"id_store":"ldap01","authnDone":"true","process_id":"fe
25a9b5-bdea-433b-86f9-42c96c197acd","user_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36","lp_id":"test-
system","client_auth_method":"redirectUri","type":"login","object_id":"BIP-
123456","protocol":"OAuth","subject_id":"BIP-
123456","auth_methods":"webAuthn","session_id":"1fedbc79-4cc1-429f-bf62-d475d2617be2"}
2022-11-22 14:03:41,593 - [INFO] - [LoggerEventEmitterDriver.scala:32] -
{"ip":"172.25.0.1","timestamp":1669115021586,"id_store":"ldap01","authnDone":"false","process_id":"b
8f3ae70-7163-45b4-97af-cbd880aelf7d","user_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36","lp_id":"test-
system","client_auth_method":"redirectUri","type":"login","object_id":"BIP-
123456","protocol":"OAuth","subject_id":"BIP-
123456","auth_methods":"webAuthn","session_id":"1fedbc79-4cc1-429f-bf62-d475d2617be2"}
```

Набор атрибутов записи может отличаться в зависимости от типа события безопасности и особенностей процесса входа. Назначения атрибутов в записи аудита приведены в таблице ниже:

Таблица 6

Назначение атрибутов в записи аудита

Атрибут	Назначение и возможные значения
<code>type</code>	Тип события безопасности: <code>admin_added</code> – добавлен администратор <code>admin_pswd_changed</code> – изменен пароль администратора <code>admin_removed</code> – удален администратор <code>admin_roles_changed</code> – изменены роли администратора <code>app_password_changed</code> – задан пароль для приложения <code>attribute_changed</code> – добавлен, изменен или удален атрибут <code>attribute_confirmed</code> – атрибут подтвержден <code>auth</code> – выполнена аутентификация (при OAuth 2.0 Resource Owner Password Credentials) <code>auth_failed</code> – ошибка аутентификации <code>auth_req</code> – запрос на аутентификацию <code>authz_granted</code> – выдано OAuth-разрешение <code>authz_rejected</code> – отказано в выдаче OAuth-разрешения

⁶⁵ См.: <https://logback.qos.ch/documentation.html>

Атрибут	Назначение и возможные значения
	- <code>authz_revoked</code> – отозвано OAuth-разрешение - <code>bind_ext_account</code> – учетная запись привязана к внешней - <code>config_changed</code> – изменены настройки конфигурации - <code>duo_put</code> – мобильное приложение Duo Mobile привязано - <code>duo_remove</code> – мобильное приложение Duo Mobile отвязано - <code>grant_right</code> – назначение прав доступа - <code>group_attr_changed</code> – у группы пользователей изменен или удален атрибут - <code>group_registered</code> – группа пользователей создана - <code>group_removed</code> – группа пользователей удалена - <code>hotp_attached</code> – привязан HOTP-генератор - <code>hotp_detached</code> – отвязан HOTP-генератор - <code>internal_user_deleted</code> – учетная запись удалена - <code>locked_methods_changed</code> – изменен список заблокированных методов аутентификации - <code>login</code> – выполнен вход - <code>login_failed</code> – ошибка входа - <code>login_stopped</code> – неуспешный вход - <code>logout</code> – выполнен выход - <code>logout_req</code> – запрос на выход - <code>member_added</code> – пользователь включен в группу пользователей - <code>member_removed</code> – пользователь исключен из группы пользователей - <code>need_password_change</code> – установлен признак необходимости смены пароля - <code>recovery</code> – доступ к учетной записи восстановлен - <code>recovery_fail</code> – восстановление доступа не выполнено - <code>recovery_req</code> – выполнен запрос на восстановление доступа - <code>registration</code> – учетная запись зарегистрирована - <code>registration_req</code> – выполнен запрос на регистрацию - <code>required_factor_changed</code> – изменен режим аутентификации пользователя - <code>reset_user_password</code> – пароль установлен администратором - <code>revoke_right</code> – отзыв прав доступа - <code>send_email_code</code> – код подтверждения отправлен на email - <code>send_push_code</code> – код подтверждения отправлен в Push - <code>send_sms_code</code> – код подтверждения отправлен по SMS - <code>token_exchange_failed</code> – отказано в обмене маркера доступа - <code>token_exchanged</code> – произведен обмен маркера доступа - <code>token_granted</code> – выдан маркер доступа - <code>totp_attached</code> – привязан TOTP-генератор - <code>totp_detached</code> – отвязан TOTP-генератор - <code>unbind_ext_account</code> – учетная запись отвязана от внешней - <code>user_locked</code> – учетная запись заблокирована - <code>user_password_changed</code> – изменен пароль пользователя - <code>user_unlocked</code> – учетная запись разблокирована - <code>web_authn_reg_key</code> – добавлен ключ безопасности - <code>web_authn_revoke_key</code> – удален ключ безопасности

Атрибут	Назначение и возможные значения
<code>alt_pswd_cause</code>	Причина, по которой пользователя просили сменить пароль Возможные значения: <code>password_expired</code> - пароль просрочен <code>password_reset</code> - пароль нужно сменить при первом входе <code>password_policy_violated</code> - пароль не соответствует парольной политике
<code>attr_name</code>	Имя установленного, удаленного или измененного атрибута.
<code>auth_methods</code>	Содержит список пройденных пользователем методов аутентификации. Возможные значения: <code>password</code> – парольная аутентификация <code>spnego</code> – вход с помощью сеанса ОС <code>x.509</code> – вход с помощью средства электронной подписи <code>qrCode</code> – вход по QR-коду <code>webAuthn</code> – вход или подтверждение входа с помощью ключей безопасности <code>css</code> – автоматический вход по результатам регистрации пользователя или восстановления пароля <code>sms</code> – одноразовый пароль по SMS <code>email</code> – одноразовый пароль по email <code>hotp</code> – второй фактор аутентификации с помощью аппаратного брелока <code>totp</code> – второй фактор аутентификации с помощью программного TOTP-генератора кодов подтверждения <code>externalIdps:<type>:<name></code> – вход с помощью внешнего поставщика идентификации (соцсети или ЕСИА) <code>userApp</code> – вторичная аутентификация в мобильном приложении <code>outside_%NAME%</code> – внешний метод входа с именем <code>%NAME%</code> Наличие перед методом префикса <code>cls:</code> означает, что вход был выполнен с помощью долгосрочной сессии, а ранее при первичном входе использовались те методы входа, что перечислены после <code>cls:</code>
<code>auth_soft_id</code>	Приложение-аутентификатор (при входе по QR-коду)
<code>authnDone</code>	Проводилась ли аутентификация при этом входе
<code>captcha_passed</code>	Признак, что при входе спрашивалась CAPTCHA
<code>client_auth_method</code>	Способ аутентификации вызвавшего Blitz Identity Provider приложения: <code>internal</code> – для событий, вызванных внутренними приложениями Blitz Identity Provider <code>x.509</code> – для событий, вызванных SAML-приложениями, при условии, что SAML-запрос пришел подписанным <code>Basic</code> – для приложений, вызывающих REST-сервисы, использующие Basic-авторизацию <code>redirectUri</code> – для приложений, которые идентифицировали себя в URL (например, указали свой <code>client_id</code> в URL-параметре), но чья аутентификация не проводилась (достоверно не известно, что это действительно вызывает Blitz Identity Provider именно

Атрибут	Назначение и возможные значения
	это приложение) - Bearer – использование access_token для аутентификации мобильным приложением с динамическими client_id/client_secret
dcId	Динамический client_id
device	ID устройства
deviceFingerprint	Отпечаток устройства
dTyp	Тип устройства (при динамической регистрации)
email	Адрес электронной почты
entry_point	Тип интерфейса, использованного для регистрации пользователя: - WEB – при регистрации из веб-приложения Blitz Identity Provider - REST – при регистрации через REST-сервисы Blitz Identity Provider
error	Ошибка (при неуспешных событиях)
ext_account_id	Идентификатор внешней учетной записи
ext_account_name	Имя внешнего поставщика идентификации
ext_account_type	Тип внешнего поставщика идентификации
failed_method	Указывает, какой метод аутентификации не смог пройти пользователь
group_id	Идентификатор группы пользователей
group_profile	Идентификатор профиля использования групп пользователей
id_store	Хранилище учетной записи
ip	IP адрес пользователя
lp_id	Идентификатор приложения (EntityId для SAML или client_id для OIDC), вызвавшего Blitz Identity Provider.
mobile	Номер мобильного телефона
module	Идентификатор измененного блока настроек
new_attr_value	Новое значение установленного или измененного атрибута
new_factor	Новое значение признака, указывающего на необходимость проверки второго фактора аутентификации
new_roles	Роли, добавленные учетной записи администратора
oauth_scopes	Список разрешений, которые выдал или отозвал пользователь
object_id	Идентификатор объекта операции (пользователь, по которому

Атрибут	Назначение и возможные значения
	выполнялась операция)
old_attr_value	Прежнее значение удаленного или измененного атрибута
old_factor	Прежнее значение признака, указывающего на необходимость проверки второго фактора аутентификации
old_roles	Роли, отозванные у учетной записи администратора
origin_app	Идентификатор приложения, инициировавшего регистрацию пользователя или восстановление пароля
process_id	Идентификатор процесса
protocol	Протокол взаимодействия приложения с Blitz Identity Provider. Возможные значения: - SAML – для SAML и WS-Federation - OAuth – для OpenID Connect и OAuth 2.0 - simple – для прокси-аутентификации - internal – для входа в Личный кабинет (_blitz_profile)
pswd_changed	Признак, что рекомендовалась смена пароля
pswd_tmp_locked	Признак, что была временная блокировка
recovery_contact	Указанный при восстановлении контакт (email или номер мобильного телефона)
recovery_type	Тип восстановления пароля: email или mobile
right_name	Название права доступа
roles	Роли учетной записи администратора
session_id	Уникальный идентификатор сессии пользователя. Позволяет коррелировать все события пользователя, выполненные им в рамках общей пользовательской сессии.
subject_id	Идентификатор субъекта операции (пользователь, который вызвал операцию)
tags	Метка назначенного или отозванного права доступа
timestamp	Дата и время события. Например, 2022-11-04T17:49:58.384+0300
tried_old_pswd	Признак того, что была попытка входа с паролем из сохраненной истории паролей (предыдущим паролем)
used_login	Логин, использованный при входе
user_agent	Данные о пользовательском устройстве (UserAgent)
wa_key_id	Идентификатор ключа безопасности
wa_key_name	Имя ключа безопасности

Атрибут	Назначение и возможные значения
withDelay	Включалась задержка при входе

16.1.30. Изменение системных имен полей ввода логина и пароля

По умолчанию Blitz Identity Provider на странице ввода логина и пароля называет поля ввода логина и пароля идентификаторами `login` и `password`. При внедрении Blitz Identity Provider при миграции с существующей системы входа, в которой использовались другие названия полей, может существовать требование, что нужно сохранить в Blitz Identity Provider прежние используемые названия полей. Это может быть полезно, так как некоторые браузеры, сохранившие логины и пароли пользователей, и использующие их для автоподстановки, смогут продолжать осуществлять автоподстановку сохраненных значений и при переключении системы входа на использование Blitz Identity Provider, при условии сохранения домена страницы входа и названия полей на странице входа.

Для установки требуемых названий полей ввода логина и пароля необходимо в блок настроек `blitz.prod.local.idp.password` добавить следующие настройки:

- `loginInputName` – идентификатор поля ввода логина на странице входа;
- `passwordInputName` – идентификатор поля ввода пароля на странице входа.

Пример настроек:

```
"password" : {
  ...
  "loginInputName" : "j_username",
  "passwordInputName" : "j_password",
  ...
}
```

16.1.31. Настройка использования базы геоданных

Можно подключить к Blitz Identity Provider базу данных в формате `mmdb`⁶⁶ с геоданными. В этом случае Blitz Identity Provider при регистрации событий безопасности, а также при запоминании устройств и браузеров пользователя дополнительно к сохранению IP-адреса будет записывать соответствующие IP-адресу данным о стране, регионе и городе, а также широту, долготу и радиусу точности, полученные из базы геоданных.

Сохраненные геоданные будут показываться администратору в консоли управления. Также можно включить отображение геоданных пользователю в «Личном кабинете» и включить их в тексты уведомлений, отправляемых по SMS или email.

Для подключения базы данных с геоданными необходимо выложить на серверах с Blitz Identity Provider файл формата `mmdb` с базой данных, а также создать блок настроек

⁶⁶ См.: <https://www.maxmind.com/en/geoip2-databases>

`blitz.prod.local.idp.geoIp` со следующими настройками в блоке `driver`:

- `type` – тип базы с геоданными. Поддерживается только тип `geoIp2-db`;
- `path` – путь на сервере к файлу с базой геоданных в формате `mmdb`.

Пример настроек:

```
"geoIp": {
  "driver": {
    "type": "geoIp2-db",
    "path": "geoIp/GeoIP2-City.mmdb"
  }
}
```

16.1.32. Настройки вспомогательных приложений (pipes)

Можно настроить, чтобы при входе Blitz Identity Provider показал пользователю объявление. При этом пользователю могут быть показаны одна или две кнопки, а выбор пользователя можно будет проанализировать в процедуре входа.

Для настройки отображения пользователю объявления нужно:

- создать процедуру входа на основе стандартной (см. п. 6.2.8);
- в конфигурационном файле `blitz.conf` добавить раздел `blitz.prod.local.idp.built-in-pipes`, в котором назначить вспомогательному приложению с типом `info` идентификатор `id` и тип объявления `type`. Возможны следующие типы объявлений:
 - `news` – отображается одна кнопка
 - `agreement` – отображается две кнопки.
- настроить тексты кнопок и объявления (см. п. 16.2.7).

Пример конфигурации вспомогательных приложений `info` с идентификаторами `alarm` и `user_agreement`:

```
"built-in-pipes": {
  "info": [
    {
      "id": "alarm",
      "type": "news"
    },
    {
      "id": "user_agreement",
      "type": "agreement"
    }
  ]
}
```

Можно настроить, чтобы при входе Blitz Identity Provider показал пользователю окно выбора из списка значений и сохранил результат выбора в атрибуте в учетной записи пользователя.

Для настройки отображения пользователю списка значений нужно:

- создать процедуру входа на основе стандартной (см. п. 6.2.11);
- в конфигурационном файле `blitz.conf` добавить раздел `blitz.prod.local.idp.built-in-pipes`, в котором назначить вспомогательному приложению с типом `choice` идентификатор `id` и имя атрибута `claim`, в который необходимо сохранять результат выбора.

- настроить тексты кнопок и объявления (см. п. 16.2.7).

Пример конфигурации вспомогательного приложения `choice`:

```
"built-in-pipes": {  
  "choice": [  
    {  
      "id": "select_value",  
      "claim": "role"  
    }  
  ]  
}
```

16.1.33. Одновременное использование нескольких СУБД

В Blitz Identity Provider можно настроить одновременное использование СУБД Couchbase Sever и СУБД PostgreSQL для хранения разных типов объектов. Для этого необходимо в блоке настроек `blitz.prod.local.idp.stores` задать следующие настройки:

- `default_type` – используемая по умолчанию СУБД. Возможные значения: `cb` – Couchbase Server, `jdbc` – PostgreSQL или иная реляционная СУБД с поддержкой JDBC;
- `list-of-types` – идентификаторы классов объектов Blitz Identity Provider и используемые для размещения соответствующих им объектов СУБД (`cb` или `jdbc`). Включать в настройку нужно только те классы объектов, которые размещаются в СУБД, отличной от указанной в `default_type`. Доступны следующие классы объектов:
 - `user-store` – атрибуты учетных записей;
 - `access-token-store` – маркеры безопасности;
 - `refresh-token-store` – маркеры обновления;
 - `id-ext-store` – привязки внешних поставщиков идентификации;
 - `device-code-store` – коды подтверждения для OAuth 2.0 Device Authorization Grant;
 - `access-list-store` – выданные пользователем разрешения приложениям;
 - `blitz-action-store` – коды подтверждения контактов (sms, email);
 - `oath-token-store` – привязки HOTP и TOTP генераторов разовых паролей;
 - `oath-load-proc-store` – история загрузок описаний аппаратных HOTP и TOTP генераторов разовых паролей;
 - `confirmation-request-store` – запросы разовых паролей;
 - `reg-context-store` – контекст регистрации пользователей;
 - `reg-context-storef` – контекст регистрации пользователей;
 - `id-store-maker` – встроенное хранилище идентификаторов пользователей;
 - `rev-ctx-store` – контекст восстановления паролей пользователей;
 - `db-client-store` – динамические клиенты;
 - `db-client-storef` – динамические клиенты;
 - `initial-token-store` – IAT маркеры;

- `user-agent-store` – устройства (браузеры) пользователей;
 - `web-authn-key-store` – ключи безопасности;
 - `audit-store` – события безопасности;
 - `task-store` – асинхронные задачи.
- `utils` – перечень модулей с утилитами, необходимых для используемого типа СУБД: `modules.CouchbaseModule` – для Couchbase Server, `modules.JDBCModule` – для PostgreSQL.

Пример настроек совместного использования двух СУБД:

```
"stores" : {
  "default-type" : "jdbc",
  "list-of-types" : {
    "access-token-store" : "cb",
    "refresh-token-store" : "cb",
    "user-agent-store" : "cb"
  },
  "utils" : [
    "modules.CouchbaseModule",
    "modules.JDBCModule"
  ]
}
```

16.2. Настройки текстов интерфейса

16.2.1. 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 (см. Рисунок 173).

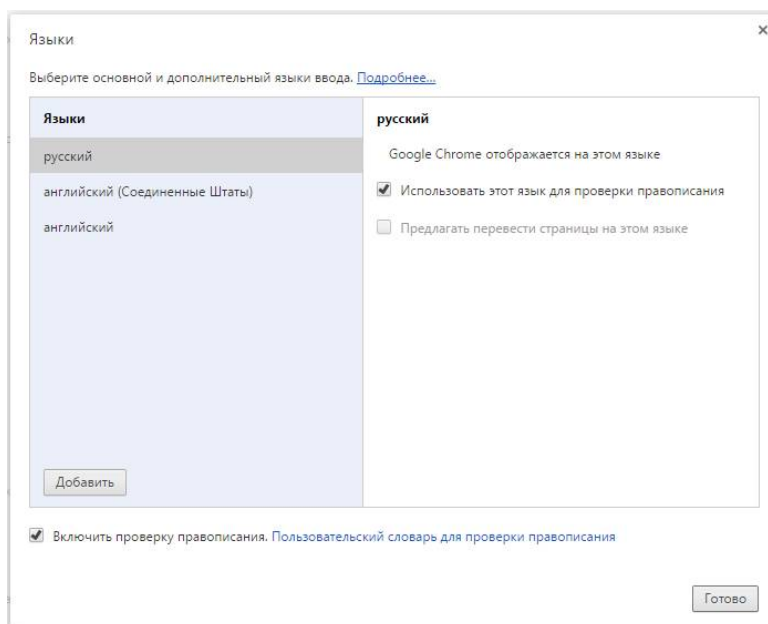


Рисунок 173 – Настройка языка для браузера Chrome

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:

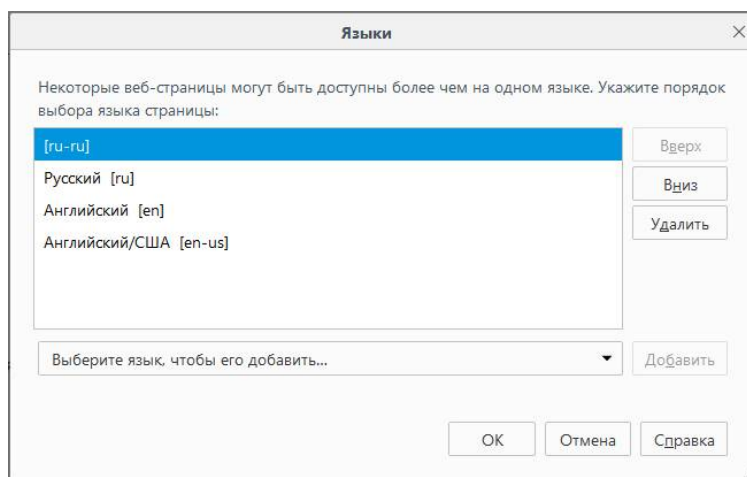


Рисунок 174 – Настройка языка для браузера Firefox

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" : "blitzling"  
  }  
}
```

Таким образом, например, если применение английского языка интерфейса не требуется, то его можно удалить из параметра `languages`.

16.2.2. 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.

16.2.3. 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. 16.2.2 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 почте. 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 7

Типы сообщений из группы «информирование» (notif)

Тип сообщения	Описание	Параметры
<code>login_unknown_device</code>	Информирование пользователя о входе с неизвестного устройства	– <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>ua.name</code> – имя устройства

Тип сообщения	Описание	Параметры
		- <code>app.id</code> – идентификатор приложения - <code>app.name</code> – имя приложения - <code>ip</code> – IP-адрес - <code>ip.country</code> – страна - <code>ip.state</code> – регион - <code>ip.city</code> – город - <code>ip.lat</code> – широта - <code>ip.lng</code> – долгота - <code>ip.radius</code> – радиус окрестности - <code>device.type</code> – тип устройства - <code>device.mkey</code> – собранный ключ для сообщений, правило формирования: <code>s"\$deviceType.\$osName.\$osVer"</code> - <code>os.name</code> – имя операционной системы - <code>os.ver</code> – версия операционной системы - <code>os.mkey</code> – собранный ключ для сообщений, правило формирования: <code>s"\$osName.\$osVer"</code> - <code>event.time</code> – время события (в unixtime). В шаблоне сообщения можно использовать следующие функции форматирования: - <code>[\$(<ATTR>&dic(<MSG_KEY_PREFIX>,<PARAM_SUBSTITUTION>)]</code> – получение значения из строки; - <code>[\$(<ATTR>&formatUnixTime(dd MMMM YYYY г.,ru,GMT))]</code> – форматирование даты и времени, где <code>dd MMMM YYYY г.</code> – шаблон в формате <code>SimpleDateFormat</code>, <code>ru</code> – локаль (опционально), <code>GMT</code> – таймзона (опционально)
<code>link_social_network</code>	Информирование пользователя о присоединении к социальной сети	- <code>fp.humanReadableName</code> – название внешнего поставщика идентификации - атрибуты пользователя
<code>change_pwd</code>	Информирование пользователя о смене пароля	- атрибуты пользователя

Тип сообщения	Описание	Параметры
<code>changed_pwd_to_object</code>	Информирование о смене пароля в зависимой учетной записи	– атрибуты зависимой учетной записи с префиксом <code>obj.</code>
<code>access_recovery</code>	Информирование пользователя о восстановлении пароля	– атрибуты пользователя
<code>access_recovery_by_object</code>	Информирование о восстановлении пароля в зависимой учетной записи	– атрибуты зависимой учетной записи с префиксом <code>obj.</code>
<code>set_2factor_auth</code>	Информирование пользователя о назначении второго фактора аутентификации	– <code>method</code> – код метода аутентификации – <code>method.msg</code> – имя метода аутентификации, полученное через строку <code>msg(message.method.name.\$[method])</code> – атрибуты пользователя
<code>granted_access_to</code>	Информирование субъекта о предоставлении доступа к объекту	– <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	– <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	– <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	– <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	– <code>entryPoint</code> – канал регистрации – <code>appId</code> – приложение – <code>requesterId</code> – приложение – атрибуты пользователя

Пример строки:

```
message.notif.login_unknown_device.email.body=Уважаемый пользователь!<br><br>Мы обнаружили, что вы вошли в систему с нового устройства ${event.time&formatUnixTime(dd MMMM YYYY г., ru, GMT)}:<br>${device.mkey&dic(dics.devices,os.ver)}, браузер ${ua.name&dic(dics.browsers)}<br>Если вы не совершали это действие, обратитесь к администратору.
```

Таблица 8

Типы сообщений из группы «регистрация» (reg)

Тип сообщения	Описание	Параметры
vrf_code	Отправка кода подтверждения контакта при регистрации	- code – код подтверждения - link – ссылка для подтверждения (только для email) - req.ip – IP-адрес - req.userAgent – userAgent пользователя - cfg.domain – домен - атрибуты пользователя из контекста регистрации с префиксом attrs.
set_pwd_link	Отправка ссылки на смену пароля при регистрации (только для канала email)	- link – ссылка на страницу смены пароля - req.ip – IP-адрес - req.userAgent – userAgent пользователя - cfg.domain – домен - атрибуты пользователя из контекста регистрации с префиксом attrs.
generated_pwd	Отправка назначенного при регистрации пароля (только для канала SMS)	- pwd – сгенерированный пароль - req.ip – IP-адрес - req.userAgent – userAgent пользователя - cfg.domain – домен - атрибуты пользователя из контекста регистрации с префиксом attrs.

Таблица 9

Типы сообщений из группы «восстановление доступа» (recovery)

Тип сообщения	Описание	Параметры
vrf_code	Отправка кода подтверждения контакта при восстановлении доступа	- code – код подтверждения - link – ссылка для подтверждения (только для email)

Таблица 10

Типы сообщений из группы «аутентификация» (auth)

Тип сообщения	Описание	Параметры
vrf_code	Отправка кода подтверждения мобильного номера (каналы: SMS/push)	code – код подтверждения

Таблица 11

Типы сообщений из группы «личный кабинет» (profile)

Тип сообщения	Описание	Параметры
vrf_code	Отправка кода подтверждения контакта при изменении его в Личном кабинете	– attr.msg – наименование атрибута в форме профиля – attr – код атрибута – link – ссылка для подтверждения (только для email) – code – код подтверждения

Таблица 12

Типы сообщений из группы «программный интерфейс» (api)

Тип сообщения	Вариации	Описание	Параметры
vrf_code	– \$attr.\$rpId – отдельно для данного приложения и атрибута – \$attr – отдельно для данного атрибута	Отправка кода подтверждения контакта через API	– code – код подтверждения – link – ссылка (только для email) – attr.value – новый контакт (email или мобильный номер) – attr – код атрибута контакта

16.2.4. Настройка логотипов кнопок входа через внешние поставщики идентификации

В Blitz Identity Provider можно изменить логотипы, отображаемые на кнопках входа через внешние поставщики идентификации (социальные сети) на странице входа и кнопок привязок внешних поставщиков идентификации в личном кабинете.

Для настройки нужно создать в директории custom_messages в файле messages строки, имена которых соответствуют следующим паттернам:

- для страницы входа – meth-logo.\${type}.\${name}
- для личного кабинета – social-icon.\${type}.\${name}

В \${type} указывается тип внешнего поставщика идентификации, в \${name} – имя поставщика идентификации. Значения берутся из настроек (см. п. 8).

В значении строк указываются имена <icon class>, присваиваемые кнопкам.

Примеры строк:

```
social-icon.saml.demo-idp=saml-demo
social-icon.esia.esia_1=esia
meth-logo.saml.demo-idp=meth-saml-demo
meth-logo.esia=meth-esia
```

16.2.5. Модификация имен устройств и браузеров

В Blitz Identity Provider можно настроить имена устройств (операционных систем) и

браузеров с точностью до версий. Для этого в нужно создать в директории `custom_messages` в файле `messages` строки, имена которых соответствуют следующим паттернам:

- для браузеров – `dics.browsers.<name>`. Поддерживаются определение следующих браузеров для подстановки в `<name>`: Firefox, Opera, Chrome, Safari, IE, Edge, Yandex, Sputnik, unknown.
- для устройств (операционных систем) – `dics.devices.<typ>.<os>.<ver>`. В качестве `<typ>` можно указывать: kindle, mobile, tablet, iphone, windowsPhone, pc, ipad, playStation, unknown. В качестве `<os>` можно указывать: Android, iOS, WindowsPhone, Windows, macOS, Linux, ChromeOS, unknown. Если для `<os>` и `<ver>` не определена частная строка, то берется более общая строка.

Примеры строк:

```
dics.browsers.Firefox=Firefox Browser
dics.browsers.Opera=Opera
dics.browsers.Chrome=Google Chrome
dics.browsers.Safari=Safari
dics.browsers.IE=Internet Explorer
dics.browsers.Edge=Microsoft Edge
dics.browsers.Yandex=Яндекс.Браузер
dics.browsers.Sputnik=Спутник
dics.devices.mobile=Мобильное устройство
dics.devices.mobile.Android=Android
dics.devices.mobile.Android.10=Android 10
dics.devices.mobile.Android.9=Android 9
dics.devices.tablet=Планшет
dics.devices.iphone=iPhone
dics.devices.iphone.iOS.14=iPhone (iOS {0})
dics.devices.pc.macOS=macOS {0}
dics.devices.pc.macOS.13=macOS Ventura {0}
dics.devices.pc.macOS.12=macOS Monterey {0}
dics.devices.pc.macOS.11=macOS Big Sur {0}
dics.devices.pc.macOS.10.15=macOS Catalina {0}
dics.devices.pc.macOS.10.14=macOS Mojave {0}
dics.devices.pc.macOS.10.13=macOS High Sierra {0}
dics.devices.pc.macOS.10.12=macOS Sierra {0}
dics.devices.pc.Windows.8=Windows 8
dics.devices.pc.Windows.10=Windows 10
dics.devices.pc.Windows.11=Windows 11
```

16.2.6. 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. 16.2.2). 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.

16.2.7. Настройка сообщений вспомогательных приложений (pipes)

В Blitz Identity Provider можно настроить сообщения вспомогательного приложения, выпускающего ключ безопасности (Passkey, WebAuthn, FIDO2) при входе пользователя. Можно настроить разные тексты сообщений в зависимости от устройств (операционных систем), используемых пользователем. Для этого в нужно создать в директории `custom_messages` в файле `messages` строки, имена которых соответствуют следующим паттернам:

- `pipes.conf.webAuthn.addKey.<message-path>.<device-type>.<os>`;
- `login.outside.flow.error.internal.webAuthn.addKey.<device-type>.<os>`.

В качестве `<message-path>` указывается имя строки (см. ниже пример). В качестве `<device-type>` указывается тип устройства: `mobile`, `tablet`, `iphone`, `pc`, `ipad`. В качестве `<os>` можно указывать: `Android`, `iOS`, `Windows`, `macOS`, `Linux`, `ChromeOS`. Если для `<device-type>` и `<os>` не определена частная строка, то берется более общая строка.

Примеры строк:

```
pipes.conf.webAuthn.addKey.page.title.pc.macOS=Вход по Touch ID  
pipes.conf.webAuthn.addKey.head.title.pc.macOS=Вход по Touch ID  
pipes.conf.webAuthn.addKey.info.pc.macOS=Использовать Touch ID или пароль компьютера Mac для входа в приложения?
```

```
pipes.conf.webAuthn.addKey.finishInfo.pc.macOS=Вход по Touch ID для учетной записи настроен. Нажмите
кнопку "Продолжить"
pipes.conf.webAuthn.addKey.name.pc.macOS=Touch ID на Mac
login.outside.flow.error.internal.webAuthn.addKey.pc.macOS=Произошла ошибка при настройке входа по
Touch ID на Mac

pipes.conf.webAuthn.addKey.page.title.pc.Windows=Вход через Windows Hello
pipes.conf.webAuthn.addKey.head.title.pc.Windows=Вход через Windows Hello
pipes.conf.webAuthn.addKey.info.pc.Windows=Использовать PIN-код компьютера, распознавание лица или
отпечатка пальца для входа в приложения?
pipes.conf.webAuthn.addKey.finishInfo.pc.Windows=Вход через Windows Hello для учетной записи
настроен. Нажмите кнопку "Продолжить"
pipes.conf.webAuthn.addKey.name.pc.Windows=Windows Hello
login.outside.flow.error.internal.webAuthn.addKey.pc.Windows=Произошла ошибка при настройке входа
через Windows Hello

pipes.conf.webAuthn.addKey.page.title.iphone.iOS=Вход по Face ID
pipes.conf.webAuthn.addKey.head.title.iphone.iOS=Вход по Face ID
pipes.conf.webAuthn.addKey.info.iphone.iOS=Использовать Face ID или Touch ID телефона для входа в
приложения?
pipes.conf.webAuthn.addKey.finishInfo.iphone.iOS=Вход через Face ID для учетной записи настроен.
Нажмите кнопку "Продолжить"
pipes.conf.webAuthn.addKey.name.iphone.iOS=Face ID на iPhone
login.outside.flow.error.internal.webAuthn.addKey.iphone.iOS=Произошла ошибка при настройке входа
через Face ID

pipes.conf.webAuthn.addKey.page.title.ipad.iOS=Вход по Touch ID
pipes.conf.webAuthn.addKey.head.title.ipad.iOS=Вход по Touch ID
pipes.conf.webAuthn.addKey.info.ipad.iOS=Использовать Touch ID планшета для входа в приложения?
pipes.conf.webAuthn.addKey.finishInfo.ipad.iOS=Вход через Touch ID для учетной записи настроен.
Нажмите кнопку "Продолжить"
pipes.conf.webAuthn.addKey.name.ipad.iOS=Touch ID на iPad
login.outside.flow.error.internal.webAuthn.addKey.ipad.iOS=Произошла ошибка при настройке входа
через Touch ID

pipes.conf.webAuthn.addKey.page.title.mobile.Android=Вход по распознаванию лица или отпечатка пальца
pipes.conf.webAuthn.addKey.head.title.mobile.Android=Вход по распознаванию лица или отпечатка пальца
pipes.conf.webAuthn.addKey.info.mobile.Android=Использовать распознавание лица или отпечатка пальца
для входа в приложения?
pipes.conf.webAuthn.addKey.finishInfo.mobile.Android=Вход через распознавание лица или отпечатка
пальца для учетной записи настроен. Нажмите кнопку "Продолжить"
pipes.conf.webAuthn.addKey.name.mobile.Android=Smart Lock на Android
login.outside.flow.error.internal.webAuthn.addKey.mobile.Android=Произошла ошибка при настройке
входа через через распознавание лица или отпечатка пальца

pipes.conf.webAuthn.addKey.page.title=Вход по ключу безопасности
pipes.conf.webAuthn.addKey.head.title=Вход по ключу безопасности
pipes.conf.webAuthn.addKey.info=Использовать ключ безопасности FIDO2 для входа в приложения?
pipes.conf.webAuthn.addKey.finishInfo=Вход через ключ безопасности для учетной записи настроен.
Нажмите кнопку "Продолжить"
pipes.conf.webAuthn.addKey.name=FIDO2
```

В Blitz Identity Provider можно настроить тексты для вспомогательного приложения, показывающего пользователю сообщение при входе в приложение. Для этого нужно определить в директории `custom_messages` в файле `messages` строки для настроенных в `blitz.prod.local.idp.built-in-pipes.info` приложений с их `{id}` вспомогательного приложения.

Пример строк:

```
pipes.info.head.title.{id} - название вкладки
pipes.info.page.title.{id} - заголовок вспомогательного приложения
pipes.info.message.{id} - текст сообщения
pipes.info.read.{id} - название кнопки (для вспомогательных приложений с типом "news")
pipes.info.agree.{id} - название 1-й кнопки (для вспомогательных приложений с типом "agreement")
pipes.info.disagree.{id} - название 2-й кнопки (для вспомогательных приложений с типом "agreement")
```

В Blitz Identity Provider можно настроить тексты для вспомогательного приложения, запрашивающего у пользователя при входе выбор значения из списка и сохраняющего результат выбора в атрибут учетной записи. Для этого нужно определить в директории `custom_messages` в файле `messages` строки для настроенных в `blitz.prod.local.idp.built-in-pipes.choice` приложений с их `{id}` вспомогательного приложения.

Пример строк:

```
pipes.choice.head.title.{id} - название вкладки
pipes.choice.page.title.{id} - заголовок вспомогательного приложения
pipes.choice.info.{id} - текст информации под заголовком
pipes.choice.button.{id}.{choiceId} - текст на кнопке выбора
pipes.choice.skip - текст на кнопке пропуска
```

В Blitz Identity Provider можно настроить тексты для вспомогательного приложения, запрашивающего у пользователя при входе в приложение ввод значения атрибута. Для этого нужно определить в директории `custom_messages` в файле `messages` строки, соответствующие следующему паттерну – `pipes.act.attr. <message-path>.common.<attr-name>`.

В качестве `<message-path>` указывается имя строки (см. ниже пример). В качестве `<attr-name>` указывается имя атрибута.

Примеры строк (в случае заполнения атрибута `family_name`):

```
pipes.act.attr.page.title.common.family_name=Подтверждение фамилии
pipes.act.attr.head.title.common.family_name=Подтверждение фамилии
pipes.act.attr.info.confirm.common.family_name=В учетной записи указана ваша фамилия?<br>Проверьте и
нажмите кнопку <b>Подтвердить</b>.
pipes.act.attr.info.enter.common.family_name=В учетной записи не указана фамилия.<br>Введите и
нажмите кнопку <b>Подтвердить</b>.
pipes.act.attr.label.common.family_name=Фамилия
pipes.act.attr.msg.required.msg.common.surname=Введите фамилию
```

16.3. Файлы настроек консоли управления

Консоль управления настраивается с помощью файлов `console.conf` и `credentials`. Далее в подразделах описаны возможные настройки.

16.3.1. 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/пароллю учетных записей, заведенных в разделе «Администраторы» (см. п. 2.1.12);
- режим входа через SSO;
- гибридный режим входа, когда администратор может войти как по логину/пароллю 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 (см. Рисунок 175); `credentials` – вход только по логину и паролю из настроек консоли управления (см. Рисунок 3); если параметр не задан, то доступны оба варианта на выбор пользователя (см. Рисунок 176).

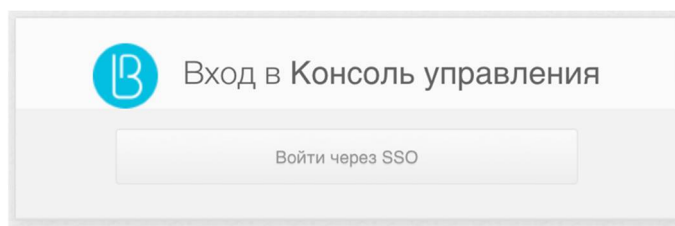


Рисунок 175 – Окно входа в консоль при включенном режиме SSO

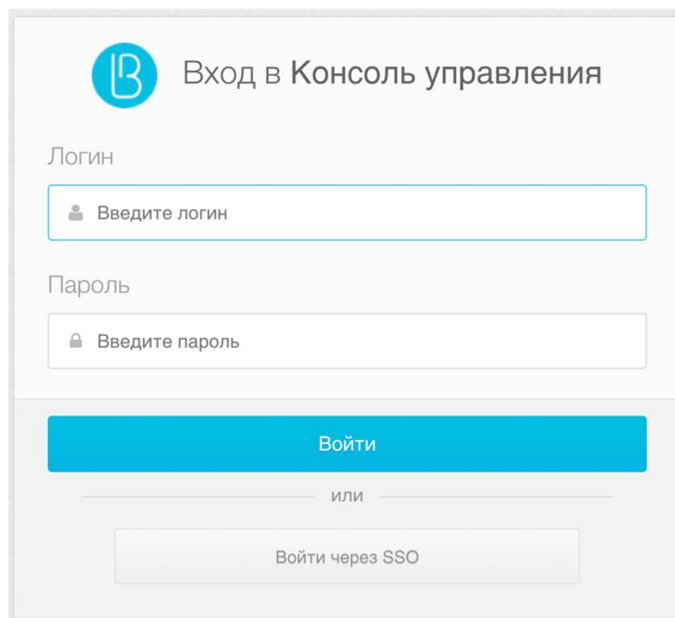


Рисунок 176 – Окно входа в консоль при всех включенных режимах входа

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`.

16.3.2. 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. 6.2.6).

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,
  ...
}
```

16.3.3. Настройка ролей и прав доступа в консоль управления

Стандартные роли администраторов описаны в п. 2.1.12. 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. 16.2). 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:

Таблица 13

Права доступа консоли управления Blitz Identity Provider

Право доступа	Доступные разделы консоли управления
<code>w_app</code>	«Приложения»
<code>w_system</code>	«Источники данных», «Аутентификация», «Процедуры входа», «Поставщики идентификации», «SAML», «OAuth 2.0», «Устройства», «Сообщения»
<code>w_ui</code>	«Сервисы самообслуживания», «Внешний вид»
<code>w_admin</code>	«Администраторы», «События»
<code>w_user</code>	«Пользователи», «Группы», «Права доступа»
<code>r_user</code>	«Пользователи» (только просмотр), «Группы» (только просмотр), «Права доступа» (только просмотр)
<code>r_audit</code>	«События» (только просмотр)

17. 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 обращении указать используемую версию Blitz Identity Provider.

При необходимости повысить уровень логирования необходимо в конфигурационном файле `/usr/share/identityblitz/blitz-config/blitz.conf` в блоке `logger` изменить уровни логирования. По умолчанию выставлены следующие уровни логирования:

```
"levels" : {
  "ROOT" : "TRACE",
  "application" : "TRACE",
  "com.couchbase.client" : "INFO",
  "com.couchbase.service" : "INFO",
  "com.couchbase.endpoint" : "INFO",
  "com.couchbase.node" : "INFO",
  "com.couchbase.tracing" : "INFO",
  "com.identityblitz" : "TRACE",
  "com.identityblitz.idp" : "TRACE",
  "com.identityblitz.idp.events" : "TRACE",
  "com.identityblitz.idp.flow.dynamic" : "TRACE",
  "com.identityblitz.idp.flow.dynamic.extend" : "TRACE",
  "com.identityblitz.idp.task.processing" : "DEBUG",
  "com.identityblitz.login-framework" : "TRACE",
  "com.identityblitz.login-framework.ldap-timings" : "INFO",
  "com.identityblitz.login.store" : "TRACE",
  "com.identityblitz.idp.rabbitmq" : "INFO",
  "com.identityblitz.play.memcached" : "INFO",
  "com.identityblitz.play.memcached.RefreshableMemcachedConnection" : "INFO",
  "com.unboundid.ldap.sdk" : "TRACE",
  "org.asynchttpclient.netty" : "TRACE",
  "org.opensaml" : "INFO",
  "org.opensaml.util.resource" : "INFO",
  "play" : "TRACE",
  "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
	OpenID Connect RP-Initiated Logout 1.0	да	да	да
	OpenID Connect Front-Channel Logout 1.0	нет	да	да
	OpenID Connect Back-Channel Logout 1.0	нет	да	да
	RFC 8693 "OAuth 2.0 Token Exchange"	нет	да	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
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 и 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
	Запоминание на устройстве нескольких пользователей. Возможность сменить текущую учетную запись пользователя без необходимости логаута	нет	опция	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 (reCAPTCHA или иной сервис, выбранный Заказчиком);	нет	да	да
	– временное блокирование входа по паролю учетной записи при выявленных попытках перебора	нет	да	да
	– замедление входа пользователя (задержка входа, решение браузером вычислительно сложной задачи – Proof of Work)	нет	да	да
	Предупреждение пользователя о попытке входа с паролем, который был недавно изменен	да	да	да
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	Apple ID, 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	да	да
	Вход через ЕСИА в режиме цифрового профиля	нет	опция	да
	Вход через Сбер ID и Tinkoff ID	нет	опция	да
	Вход через Mos ID (СУДИР)	нет	да	да
	Вход через внешний поставщик идентификации с поддержкой OIDC	нет	да	да
	Вход через внешний поставщик идентификации с поддержкой SAML	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
	Возможность программирования собственного алгоритма привязки учетных записей и сопоставления атрибутов	нет	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 WebAuthn, Passkey, FIDO2	Вход с помощью платформи-независимых ключей безопасности FIDO2	нет	да	да
	Вход с помощью платформи-зависимых ключей безопасности Passkey / FIDO2 – Windows Hello (пин-код, отпечаток пальца), Passkey, пароль или Touch ID от MacBook, Passkey, Face ID или Touch ID от смартфона или планшета с iOS или Android	нет	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 8.1/10/11, macOS 10.13/10.14/10.15/11/12/13, Linux Debian 9, Mint 19, Ubuntu 18	нет	да	да
	Поддерживаемые браузеры: Chrome, Firefox, Yandex	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 и сертификата встроенными возможностями ПО	нет	да	да
	Возможность проверки действительности подписи и 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
	Подтверждение входа ключом безопасности WebAuthn, Passkey, FIDO2	нет	да	да
	Подтверждение входа ключом безопасности U2F	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 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
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
	Информирование приложений о произведенном едином логауте через браузер (front channel)	нет	да	да
	Информирование приложений о произведенном едином логауте через сервер (back channel)	нет	да	да
Контроль доступа				
	Проверка правил доступа при входе пользователя в приложения. Проверка наличия у пользователя прав доступа, членства в группах пользователей, наличия атрибутов с требуемыми значениями	да	да	да
	Проверка правил доступа при вызове приложениями защищаемых REST-сервисов через шлюз безопасности Blitz Keeper (API Security Gateway)	нет	опция	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, Mos ID, соц.сети, банки) 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
	Проверка CAPTCHA (reCAPTCHA или иной сервис, выбранный Заказчиком)	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
	Дополнительные проверки при восстановлении пароля от учетной записи, для которой включена двухфакторная аутентификация	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
	Проверка CAPTCHA (reCAPTCHA или иной сервис, выбранный Заказчиком)	да	да	да
Действия с учетной записью в момент входа	Возможность в момент входа задать номер телефона (если отсутствует) в учетной записи или подтвердить актуальность телефона (если наступил срок необходимости подтверждения актуальности)	нет	да	да
	Возможность в момент входа задать адрес электронной почты (если отсутствует) в учетной записи или подтвердить актуальность адреса электронной почты (если наступил срок необходимости подтверждения актуальности)	нет	да	да
	Возможность в момент входа выпустить Passkey (настроить вход по Face ID / Touch ID)	нет	да	да
	Возможность показать пользователю объявление	нет	да	да
	Возможность запросить у пользователя согласие	нет	да	да
	Возможность запросить у пользователя заполнение текстового атрибута	нет	да	да
	Возможность запросить у пользователя выбор значения из списка значений	нет	да	да
	Возможность построить собственный бизнес-процесс взаимодействия с пользователем в момент входа в приложение (например, вывести пользователю информационное сообщение в каких-то ситуациях или запросить что-то вести)	нет	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
	Сопоставление IP-адресам геоданных в событиях и уведомлениях (БД в формате mmdb с геоданными предоставляет Заказчик)	нет	да	да
	Интерфейс администратора для поиска/просмотра событий безопасности	да	да	да
	Запись событий безопасности: в БД, в лог-файл, в Kafka	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, правила контроля доступа)	да	да	да
	– настройка атрибутов пользователей и сопоставление атрибутов хранилищам 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, запомненных браузеров пользователя, сброс пароля, блокирование/разблокирование учетной записи, управление ключами безопасности, управление членством в группах пользователей, назначение/отзыв прав доступа)	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. 16.3.1). 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. 16.1.17) и блокирование неактивных учетных записей (см. 16.1.16)
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. 4.1). 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. 8.8, п. 8.11, п. 8.13)
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. 6.2.4). Для использования функций работы с группами пользователей настроить группы пользователей (см. п. 16.1.18). 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. 11), разрешения (см. п. 5.3.2), установить разрешения приложений (см. п. 5.3.1), настроить шлюз безопасности (см. п. 15), настроить атрибуты пользователей (см. п. 3) и группы пользователей (см. п. 16.1.18), процедуры входа в приложения (см. п. 6).

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. 2.1.12), 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. 4.3)
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. 16.2)
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. 7.3.2)
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	Настроить политику ограничения числа параллельных сеансов (см. п. 16.3.2, п. 6.2.6)
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. 17)
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. 2.1.3)
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)

Приложение 3. Методика проверки основных параметров и характеристик ПО

№ пункта ТУ	Требование технических условий	Методика проверки
2.1.1.1	ПО «Blitz Identity Provider» должно осуществлять идентификацию и аутентификацию пользователей и администраторов ПО «Blitz Identity Provider». К внутренним пользователям относятся пользователи и администраторы, выполняющие свои функции в соответствии с инструкциями и которым в ПО «Blitz Identity Provider» присвоены учетные записи. Аутентификация осуществляется с использованием паролей, аппаратных средств, одноразовых паролей, или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств. В ПО «Blitz Identity Provider» должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа с правами администраторов и с правами пользователей с использованием сети связи общего пользования, в том числе сети Интернет, а также для локального доступа с правами администраторов и с правами пользователей. Идентификация осуществляется по идентификатору (имени учетной записи), связанному с учетной записью пользователя или администратора ПО «Blitz Identity Provider». ПО «Blitz» должно осуществлять идентификацию и аутентификацию приложения-клиента. Идентификация приложений-клиентов в ПО «Blitz Identity Provider» обеспечивается по логическим именам (client_id). Аутентификация приложений-клиентов в ПО «Blitz Identity Provider» обеспечивается с использованием протокола OAuth 2.0 с помощью проверки присвоенного приложению-клиенту пароля (client_secret) (мера защиты ИАФ.1).	Проверить, что идентификация и аутентификация пользователей работает в соответствии с заданными (см. п. 4) в системе настройками. Выполнять проверки в части используемых в конкретной установке методами идентификации и аутентификации. Проверить, что для администраторов консоли управления настроен вход через Blitz (см. п. 16.3.1) и настроено прохождение двухфакторной аутентификации при удаленном доступе (см. п. 6). Проверить, что работает функция задания для подключаемых приложений client_id и client_secret (см. п. 5)
2.1.1.2	ПО «Blitz Identity Provider» должно обеспечивать функции формирования администратором идентификатора, который однозначно идентифицирует пользователя и (или) приложение-клиента, присвоение идентификатора пользователю и (или) приложению-клиенту, предотвращение повторного использования идентификатора пользователя в течение установленного администратором периода времени, блокирование идентификатора пользователя после установленного оператором времени неиспользования. (мера защиты ИАФ.3).	Проверить, что настроены запрет на повторное использование идентификатора после удаления учетной записи (см. п. 16.1.17) и блокирование неактивных учетных записей (см. п. 16.1.16). Проверить, что невозможно создать учетную запись с идентификатором, который ранее использовался – для этого попробовать создать учетную запись через консоль управления (см. п. 9.2).
2.1.1.3	ПО «Blitz Identity Provider» должно осуществлять возможность изменения администратором аутентификационной информации (средств аутентификации), заданной их изготовителями и используемой при внедрении ПО «Blitz Identity Provider», генерации средств аутентификации пользователям, установления характеристик пароля: – задание минимальной сложности пароля с определяемыми администратором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов; – задание минимального количества измененных символов при создании новых паролей; – задание максимального времени действия пароля (срок, не позже которого пользователь должен сменить пароль); – задание минимального времени действия пароля (срок, в течение которого данный пароль не должен быть использован повторно); – запрет на использование пользователями определенного администратором числа последних использованных паролей при создании новых паролей. ПО «Blitz Identity Provider» должно обеспечивать: – блокирование (прекращение действия) и замену утерянных, скомпрометированных или поврежденных средств аутентификации;	Проверить, что нельзя установить пользователю пароль (см. п. 9), который не соответствует настроенной парольной политике (см. п. 4.1).

	– для паролей – сброс пароля админом, самостоятельное восстановление (замена) утерянного пароля пользователем; – для НОТР и ТОТР генераторов одноразовых паролей – удаление администратором привязанного к пользователю прежнего генератора, привязка нового генератора; – для SMS-кодов и email-кодов – замена в профиле пользователя номера мобильного телефона и/или адреса email на актуальные; – для входа с помощью внешних систем (ЕСИА и др.) – удаление администратором или пользователем связи учетной записи пользователя с учетной записью во внешней системе входа. – назначение необходимых характеристик средств аутентификации (в том числе механизма паролей), обновление аутентификационной информации (замена средств аутентификации); – защиту аутентификационной информации от неправомерных доступа к ней и модифицирования; – единую аутентификацию при доступе пользователей в подключенные к ПО «Blitz Identity Provider» приложения-клиенты (мера защиты ИАФ.4).	
2.1.1.4	ПО «Blitz Identity Provider» должно осуществлять защиту обратной связи при вводе аутентификационной информации. Защита обратной связи в процессе аутентификации должна обеспечиваться исключением отображения действительного значения аутентификационной информации. Вводимые символы пароля должны отображаться условными знаками «*» (мера защиты ИАФ.5).	Проверить, что во всех полях, предназначенных для ввода пароля (страница входа, страницы настроек в консоли управления), при вводе пароля отображаются символы маскирования.
2.1.1.5	ПО «Blitz Identity Provider» должно осуществлять однозначную идентификацию и аутентификацию пользователей, не являющихся администраторами (внешних пользователей). К внешним пользователям, относятся все пользователи информационной системы, не указанные в ИАФ.1 в качестве внутренних пользователей. ПО «Blitz Identity Provider» должно обеспечивать однозначную идентификацию и аутентификацию пользователей для всех видов доступа. ПО «Blitz Identity Provider» должно осуществлять идентификацию и аутентификацию внешних пользователей в том числе следующими способами: – с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977. – с использованием системы управления доступом к информационным ресурсам и системам города Москвы. – с использованием внешних систем входа сторонних организаций, построенных с использованием ПО «Blitz Identity Provider» (мера защиты ИАФ.6).	Проверить, что работает вход через настроенные внешние поставщики идентификации (см. п. 8.8, п. 8.11, п. 8.13). Для этого на странице входа нажать кнопку входа через соответствующий внешний поставщик и ввести данные от учетной записи внешнего поставщика.
2.1.2.1	ПО «Blitz Identity Provider» должно обеспечивать следующие функции управления учетными записями пользователей, в том числе внешних пользователей: – определение типа учетной записи (внутреннего пользователя, внешнего пользователя, временная); – объединение учетных записей в группы (при необходимости); – подтверждение верификации пользователя (факта проверки личности пользователя) при заведении учетной записи пользователя; – заведение, активация, блокирование и уничтожение учетных записей пользователей; – изменение учетных записей пользователей; – блокировка временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе. ПО «Blitz Identity Provider» должно обеспечить поддержку управления учетными записями пользователей администратором. Должно обеспечиваться автоматическое блокирование временных учетных записей по окончании установленного периода времени для их использования (мера защиты УПД.1).	Проверить в консоли управления (см. п. 9), что по атрибутам пользователей можно различать внешние, внутренние и временные учетные записи. Для различия используются настроенные атрибуты (см. п. 3). Проверить вход с использованием тестовых учетных записей различного типа в приложения – убедиться, что вход работает в соответствии с заданными настройками политики доступа пользователей в приложения (см. п. 6). Проверить, что для временных учетных записей настроены правила блокирования входа по истечению срока действия записей (см. п. 6.2.4). Для тестовой временной учетной записи установить истекший срок действия (см. п. 9), и убедиться, что вход такой учетной записью в приложения станет невозможным. При использовании функций работы с группами пользователей проверить, что для включенных в группы учетных записей отображается их членство в группах (см. п. 9).

2.1.2.2	ПО «Blitz Identity Provider» должно осуществлять: – дискреционный метод управления доступом субъектов доступа к объектам доступа: – Субъектами доступа выступают пользователи, идентифицируемые с использованием идентификатора пользователя и идентификатора группы/организации, в которую включен пользователь. Объектами доступа выступают защищаемые с использованием подсистемы шлюза безопасности (blitz_keeper) сервисы, идентифицируемые своими URL и HTTP-методами (GET/POST/PUT/DELETE). Приложения запрашивают в Blitz Identity Provider идентификацию/аутентификацию пользователя, и получают в результате маркер доступа (access_token). С использованием маркера доступа приложения вызывают защищаемые сервисы. Вызов осуществляется через подсистему шлюза безопасности (blitz_keeper). Подсистема шлюза безопасности осуществляет проверку настроенных в Blitz Identity Provider правил доступа, описывающих, каким субъектам доступа (пользователям) какие объекты доступа (сервисы) разрешено вызывать. Если нет разрешений на вызов сервиса, то подсистема шлюза безопасности возвращает приложению ошибку доступа. – Субъектами доступа выступают приложения, идентифицируемые с использованием идентификатора приложения (client_id), присвоенного приложению при регистрации в Blitz Identity Provider и аутентифицируемые с помощью секрета приложения (client_secret). Объектами доступа выступают защищаемые с использованием подсистемы шлюза безопасности (blitz_keeper) сервисы, идентифицируемые своими URL и HTTP-методами (GET/POST/PUT/DELETE). ПО «Blitz Identity Provider» позволяет определить произвольный набор типов доступа (разрешений scope), позволяющих выразить операции с защищаемым сервисом, разрешенные приложению. Приложения запрашивают в Blitz Identity Provider маркер доступа (access_token) с определенным набором разрешений. С использованием маркера доступа приложения вызывают защищаемые сервисы. Вызов осуществляется через подсистему шлюза безопасности (blitz_keeper). Подсистема шлюза безопасности осуществляет проверку заданных в Blitz Identity Provider правил доступа, описывающих, каким субъектам доступа (приложениям) какие объекты доступа (сервисы) разрешено вызывать. Если нет разрешений на вызов сервиса или маркер доступа получен без необходимого набора разрешений (scope), то подсистема шлюза безопасности возвращает приложению ошибку доступа. – Субъектами доступа выступают приложения, идентифицируемые с использованием идентификатора приложения (client_id), присвоенного приложению при регистрации в Blitz Identity Provider и аутентифицируемые с помощью секрета приложения (client_secret). Объектами доступа выступают учетные записи пользователей (совокупность атрибутов пользователя). Приложения запрашивают в Blitz Identity Provider идентификацию/аутентификацию пользователя и определенный набор разрешений (scope), и получают в результате маркер доступа (access_token). Затем приложения запрашивают в Blitz Identity Provider получение данных о пользователе и получают только тот набор данных, который соответствует заданным в Blitz Identity Provider правилам доступа (перечню разрешенных приложению разрешений (scope) и связанным с разрешениями атрибутам пользователя). – ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа. Предусмотрены следующие возможности назначения пользователем ролей и управления доступом на основе ролей: – В качестве ролей можно использовать группы доступа. Blitz Identity Provider предоставляет программные интерфейсы для создания/изменения/удаления групп доступа, включения/исключения	Проверить на тестовых учетных записях, что вход в приложения осуществляется в соответствии с заданными настройками прав доступа (см. п. 15.2). Модифицируя через браузер запрос приложения на получение кода авторизации к серверу проверить, что если в запрос добавить неразрешенное (см. п. 5.3.1) приложению разрешение (см. п. 5.3.2), то Blitz вернет приложению ошибку. Проверить, что вызов защищаемых шлюзом безопасности сервисов (см. п. 15) проходит успешно только при соответствии запроса установленным правилам доступа. Проверить, что вход пользователей в приложения работает в соответствии с настроенными при внедрении правилами ограничения доступа, основанными на проверке атрибутов пользователей (см. п. 3) или членства в группах пользователей (см. п. 16.1.18) или иных заданных в процедуре входа в приложения условиях (см. п. 6).

	чения пользователей в группы доступа. В настраиваемых в Blitz Identity Provider правилах доступа пользователей к защищаемым сервисам можно настраивать разрешение на доступ к сервисам только пользователям, включенным в определенные группы доступа. – В качестве ролей можно использовать значение выбранного атрибута учетной записи пользователя. Blitz Identity Provider позволяет настроить атрибут (например, role) и описать правила доступа пользователя к защищаемому сервису на основании проверки наличия у пользователя атрибута (role) с определенным значением; – В качестве ролей можно использовать назначаемые пользователям полномочия (rights). Blitz Identity Provider позволяет определить список полномочий (rights), предоставляет сервисы назначения/отзыва пользователям полномочий относительно приложения (отражает наличие у пользователя роли в приложении) или группы пользователей (отражает наличие у пользователя роли в организации, если группа пользователей используется для описания организаций). Правила доступа пользователей к защищаемым сервисам могут быть описаны так, чтобы осуществлять проверку наличия у пользователей определенных полномочий (ролей) для возможности вызова указанных сервисов. ПО «Blitz Identity Provider» должно обеспечивать: – управление доступом субъектов (пользователей) при входе в приложения-клиенты; – управление доступом субъектов (пользователей и приложений-клиентов) к защищаемым с использованием подсистемы шлюза безопасности сервисам (предоставляемым защищаемыми приложениями API) (мера защиты УПД.2).	
2.1.2.3	ПО «Blitz Identity Provider» должно предоставлять сервисы для назначения, хранения, отзыва пользователям полномочий (ролей). Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с УПД.2 (мера защиты УПД.4).	Проверить работоспособность сервисов изменения атрибутов, включения и исключения пользователей в группы, назначения и отзыва прав доступа (см. «Руководство по интеграции»)
2.1.2.4	ПО «Blitz Identity Provider» должно обеспечивать назначение прав и привилегий пользователям (через редактирование их атрибутов или через использование сервисов назначения/отзыва полномочий rights)), приложениям (через определение разрешений приложений – матрицы разрешений score), и администраторам. Доступ к объектам доступа с учетом минимально необходимых прав и привилегий обеспечивается в соответствии с УПД.2 (мера защиты УПД.5).	Проверить работоспособность функции назначения роли администратору (см. п. 2.1.12), управления атрибутами пользователей (см. п. 9), назначения права доступа с использованием сервисов (см. «Руководство по интеграции»)
2.1.2.5	ПО «Blitz Identity Provider» должно ограничивать количество неуспешных попыток входа в приложения-клиенты за период времени, установленный администратором, а также обеспечивать блокирование учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа. Ограничение количества неуспешных попыток входа должно обеспечиваться в соответствии с ИАФ.4 ПО «Blitz Identity Provider» должно обеспечивать автоматическое блокирование учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа за установленный период времени с возможностью разблокирования только администратором или самим пользователем при прохождении им процедуры восстановления пароля (мера защиты УПД.6).	Проверить, что при последовательных попытках ввода неправильного пароля учетная запись временно блокируется в соответствии с заданными настройками (см. п. 4.3)
2.1.2.6	ПО «Blitz Identity Provider» должно обеспечивать возможность отображения пользователю в виде сообщения («окна») при его входе в приложение-клиент (до завершения процесса аутентификации) о том, что в информационной системе реализованы меры защиты информации, а также о том, что при работе в информационной системе пользователем должны быть соблюдены установленные оператором правила и ограничения на работу с информацией. Успешное завершение входа в приложение-клиент осуществляется только после подтверждения пользователем ознакомления с предупреждением (мера защиты УПД.7).	Проверить, что при входе нового пользователя в приложение отображается экран запроса согласия пользователя (см. п. 5.3.1, п. 5.3.2, п. 16.2)
2.1.2.7	ПО «Blitz Identity Provider» должно обеспечивать (после успешного входа пользователя) оповещение	Проверить, что в приложении личного кабинета пользователь

	пользователя о дате и времени предыдущего входа в информационную систему от имени этого пользователя, количестве неуспешных попыток входа, зафиксированных с момента последнего успешного входа в информационную систему; об изменениях сведений, относящихся к учетной записи пользователя (в том числе изменении прав доступа), произведенных за период времени не менее, чем с момента предыдущего успешного входа в информационную систему (мера защиты УПД.8).	видит в аудите события безопасности по своей учетной записи (см. п. 7.3.2)
2.1.2.8	ПО «Blitz Identity Provider» должно обеспечивать возможность ограничить число параллельных сеансов доступа для каждой учетной записи пользователя. Для пользователей можно ограничить число активных параллельных (одновременных) сеансов (сессий) максимально разрешенным одним сеансом. Должна обеспечиваться возможность задать отдельно ограничение для привилегированных учетных записей (администраторов) и для обычных (непривилегированных) пользователей (мера защиты УПД.9).	Проверить, что невозможна параллельная работа пользователя одновременно в нескольких сеансах, в случае если настроена соответствующая политика ограничения числа параллельных сеансов (см. п. 16.3.2, п. 6.2.6)
2.1.2.9	ПО «Blitz Identity Provider» должно осуществлять блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в ПО «Blitz Identity Provider» или по запросу пользователя (инициированию логута). Блокирование сеанса доступа пользователя обеспечивает временное приостановление работы пользователя с ПО «Blitz Identity Provider». Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса. После блокировки сеанса, на устройстве отображения (мониторе) не должна отображаться информация сеанса. Блокирование сеанса доступа пользователя в ПО «Blitz Identity Provider» сохраняется до прохождения пользователем повторной идентификации и аутентификации в соответствии с ИАФ.1. ПО «Blitz Identity Provider» обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя до 5 минут (мера защиты УПД.10).	Проверить, что при неактивности пользователя его сеанс входа завершается после настроенного периода неактивности (см. п. 4)
2.1.3.1	ПО «Blitz Identity Provider» должно осуществлять регистрацию и хранение следующих событий безопасности: – вход (выход), а также попытки входа субъектов доступа в приложения-клиенты; – результаты проверки прав доступа приложений к сервисам при вызове приложениями защищаемых сервисов через подсистему шлюза безопасности; – регистрация учетных записей пользователей; – изменение атрибутов учетных записей пользователей; – изменение аутентификационной информации учетных записей пользователей (изменение/сброс/восстановление пароля, настроек двухфакторной аутентификации, привязок учетных записей внешних систем входа); – блокирование/разблокирование/удаление учетной записи пользователя. Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с РСБ.2. ПО «Blitz Identity Provider» должно регистрировать события, связанные с действиями от имени привилегированных учетных записей (администраторов), события, связанные с изменением привилегий учетных записей (мера защиты РСБ.1).	Проверить в консоли управления отображение событий безопасности с различными типами событий (см. п. 11).
2.1.3.2	ПО «Blitz Identity Provider» должно регистрировать следующий состав и содержание информации о событиях безопасности: – типа события безопасности; – даты и времена события безопасности; – идентификационная информация источника события безопасности;	Проверить в консоли управления состав сведений в зарегистрированных событиях безопасности для различных типов событий (см. п. 11).

	– результат события безопасности (успешно или неуспешно); – субъекты доступа (пользователь и приложение-клиент), связанные с данным событием безопасности. При регистрации входа субъектов доступа содержание информации должно дополнительно включать идентификатор, предъявленный при попытке доступа. При регистрации попыток доступа приложений-клиентов к защищаемым сервисам содержание регистрационных записей должно включать дату и время попытки доступа к сервису с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (приложения-клиента), URL запрашиваемого защищаемого сервиса. При изменении администратором конфигурации ПО «Blitz Identity Provider» обеспечивается запись предыдущего набора настроек с пометкой информации о том, какой администратор и когда изменил конфигурацию. Записываемой информации должно быть достаточно для отслеживания действий привилегированных пользователей в ПО «Blitz Identity Provider» (мера защиты РСБ.2).	
2.1.3.3	ПО «Blitz Identity Provider» должно обеспечивать сбор, запись и хранение информации о событиях безопасности (мера защиты РСБ.3).	Проверить в консоли управления отображение событий безопасности (см. п. 11).
2.1.3.4	ПО «Blitz Identity Provider» должно предупреждать администратора о сбоях при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти (мера защиты РСБ.4).	Проверить, что события функционирования в системе фиксируются в журналах событий (см. п. 17)
2.1.3.5	ПО «Blitz Identity Provider» должно предоставлять администратору возможность просмотра записей событий безопасности, подлежащих регистрации в соответствии с РСБ.1 (мера защиты РСБ.5).	Проверить в консоли управления отображение событий безопасности (см. п. 11).
2.1.3.6	ПО «Blitz Identity Provider» должно осуществлять синхронизацию системного времени с NTP-сервером (мера защиты РСБ.6).	Проверить в консоли управления (см. п. 11), что зарегистрированное в событиях безопасности время по проверочным действиям (например, тестовому входу в приложение) соответствует точному времени события.
2.1.3.7	ПО «Blitz Identity Provider» должно обеспечивать защиту информации о событиях безопасности. Доступ к записям аудита должен предоставляться администраторам (просмотр записей аудита всех пользователей), и пользователям (просмотр только собственных записей аудита). Должно предусматриваться резервное копирование записей регистрации (аудита) (мера защиты РСБ.7).	Проверить, что регулярно создаются файлы с резервными копиями СУБД (см. п. 2.1.3)
2.1.3.8	ПО «Blitz Identity Provider» должно предоставлять возможность просмотра информации о действиях отдельных пользователей в информационной системе (мера защиты РСБ.8).	Проверить в консоли управления отображение событий безопасности (см. п. 11).