

Сервер аутентификации Blitz Identity Provider

Версия 5.0

РУКОВОДСТВО АДМИНИСТРАТОРА

СОДЕРЖАНИЕ

BB	ЗВЕДЕНИЕ				
1.	под	ОТОВКА К УСТАНОВКЕ	7		
	1.1.	Минимальные требования к развертыванию	7		
	1.2.	Рекомендуемые требования к развертыванию в кластере	8		
2	VCTA	HORKY	12		
2.	JCIA				
	2.1.	Установка JDК	12		
	2.2.	Установка мемсаснер	13		
	2.3.	Установка и настройка СУБД	14		
	2.3.1	Установка и настройка Couchbase Server			
	2.3.2	Установка и настройка PostgreSQL			
	2.4.	Установка и настройка сервера очередей RabbitMQ	16		
	2.5.	Установка приложений Blitz Identity Provider	17		
	2.6.	Настройка синхронизации файлов конфигурации	21		
	2.7.	Настройка веб-сервера	22		
	2.8.	Установка и настройка LDAP-каталога	23		
	2.9.	Вход в консоль управления	25		
	2.10.	Установка лицензионного ключа	26		
	2.11.	Управление учетными записями администраторов	27		
	2.12.	ПЕРЕЗАПУСК ПРИЛОЖЕНИЙ BLITZ IDENTITY PROVIDER	28		
3.	HACT	РОЙКА АТРИБУТОВ УЧЕТНЫХ ЗАПИСЕЙ	29		
	3.1.	Конфигурирование лоступных атрибутов			
	3.1.1	Настройка хранимых атрибутов			
	3.1.2	 Настройка вычисляемых атрибутов			
	3.1.3	 Настройка правил преобразования входных значений			
	3.1.4	 Настройка правил преобразования выходных значений			
	3.1.5	Настройка назначения атрибутов			
	3.2.	Полключение хранилиш атрибутов	34		
	3.2.1	Типы хранилиц			
	3.2.2	Годключение хранилиша по протоколу LDAP			
	3.2.3	Подключение к хранилишу по REST			
	3.2.4	Настройка внутреннего хранилиша			
4.	HACI	РОИКА СПОСОБОВ АУТЕНТИФИКАЦИИ	4/		
	4.1.	Настройка входа по логину и паролю	48		
	4.2.	Настройка входа с помощью средства электронной подписи	52		
	4.2.1	Настройка метода аутентификации в консоли управления	52		
	4.2.2	Использование и обновление плагина	54		
	4.3.	НАСТРОЙКА ВХОДА ЧЕРЕЗ ВНЕШНИЕ СЕРВИСЫ ИДЕНТИФИКАЦИИ	54		
	4.4.	Настройка входа с помощью прокси-аутентификации	55		
	4.5.	НАСТРОЙКА ВХОДА С ПОМОЩЬЮ СЕАНСА ОПЕРАЦИОННОЙ СИСТЕМЫ	56		
	4.5.1	Настройки контроллера домена (Kerberos-cepвepa)	57		
	4.5.2	Настройки в консоли управления Blitz Identity Provider	59		
	4.5.3	Настройки браузеров пользователей	61		
	4.5.4	Настройки запуска приложений Blitz Identity Provider	63		
	4.5.5	Настройки веб-сервера	63		
	4.6.	НАСТРОЙКА ВХОДА С ПОМОЩЬЮ КОДОВ ПОДТВЕРЖДЕНИЯ	63		
	4.7.	НАСТРОЙКА ВХОДА С ИЗВЕСТНОГО УСТРОЙСТВА	66		
			2		

	48	ПОЛТВЕРЖЛЕНИЕ ВХОЛА РАЗОВЫМ ПАРОЛЕМ НА ОСНОВЕ СОСТОЯНИЯ (НОТР)	66
	4.9	Полтвержление входа разовым паролем основе времени (тотр)	
	4.5.	Привязка устройств к учетным записям пользователей	
	4.10.	1 Приевруга аппаратицих брелокое	69
	4.10	 Привязка инпаратном орелоков Привязка мобильного приложения 	
	<i>4.10</i> .	2. Привязки мобилоного приложения.	71
	4.11. // 12	Коды подтверждения, отправляемые по электронной понте	71
	4.12.		74
	4.13.		75
5	ч. 14. DFГV	Пастролка влешлего метода а тептификации	
5.			
	5.1.	Создание учетной записи нового приложения	00
	5.2.	Haciponka Saivil и WS-Federation	55 ده
	5.2.1	л. Подимочение по SAML 1.0/1.1/2.0	ده ۸ ه
	5.2.2	и. Пооключение по wS-Federation	04 05
	5.2.5	. Настройка SAML-атриоутов	
	5.3.		8/
	5.5.1		8/
	5.3.2		
	5.3.3	5. Дооавление атриоутов в маркер иоентификации	93
	5.3.4	н. Настроика бинамической регистрации клиентов ОАит 2.0	
	5.4.	HACIPONKA KJINEHTA KEST-CEPBNCOB BLITZ IDENTITY PROVIDER	
6.	HAC	ТРОЙКА ПРОЦЕДУР ВХОДА В ПРИЛОЖЕНИЯ	99
	6.1.	Создание процедур входа	99
	6.2.	Примеры процедур входа	101
	6.2.1	. Принудительная двухфакторная аутентификация в приложение	
	6.2.2	2. Ограничение перечня доступных методов первого фактора	
	6.2.3	<i>В. Разрешить вход в приложение только при определенном значении атрибута у пользов</i>	ателя 103
7.	HAC	ТРОЙКА СЕРВИСОВ САМООБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ	105
	7.1.	Общие настройки	
	7.2.	Личный кабинет	107
	7.2.1	. Отображение атрибутов пользователя	107
	7.2.2	2. Дополнительные параметры	
	7.3.	РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ	109
	7.3.1	. Форма регистрации	
	7.3.2	2. Настройки сервиса регистрации	111
	7.3.3	В. Процедура регистрации	112
	7.3.4	4. Изменение текста условий использования	112
	7.3.5	5. Восстановление доступа	113
8.	BXO,	Д ЧЕРЕЗ ВНЕШНИЕ ПОСТАВЩИКИ ИДЕНТИФИКАЦИИ	114
	8.1.	Вход через Google	114
	8.2.	Вход через Яндекс	119
	8.3.	Вход через Гасевоок	
	8.4.	Вход через ВКонтакте	126
	8.5.	Вход через Одноклассники	130
	8.6.	Вход через Маіl ID	
	8.7.	Вход через Единую систему идентификации и аутентификации (ЕСИА)	
	8.8.	Вход через систему идентификации Сбербанка (Сбер ID)	142

8	3.9.	Вход через систему идентификации Mos ID (СУДИР)	146
8	3.10.	Вход через другую установку Blitz Identity Provider	149
9.	УПР	АВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЕЙ	153
ç	9.1.	Поиск учетных записей пользователей	154
ç	9.2.	Добавление учетных записей пользователей	154
9	9.3.	ГРОСМОТР И ИЗМЕНЕНИЕ АТРИБУТОВ ПОЛЬЗОВАТЕЛЕЙ	
	9.3.1	. Редактирование атрибутов пользователя	156
	9.3.2	Смена пароля пользователя	156
	9.3.3	Р. Просмотр и отвязка аккаунтов социальных сетей	157
	9.3.4	. Привязка устройств для проведения двухфакторной аутентификации по разовому паро	лю157
	9.3.5	. Привязка мобильного приложения Duo Mobile	158
	9.3.6	Б. Просмотр групп, в которые включен пользователь	159
	9.3.7	7. Просмотр прав	159
	<i>9.3.</i> 8	В. Просмотр и удаление выданных приложениям разрешений	160
10.	ПРО	СМОТР ГРУПП ПОЛЬЗОВАТЕЛЕЙ	161
11.	ПРО	СМОТР СОБЫТИЙ БЕЗОПАСНОСТИ	162
12.	HAC	ГРОЙКА УВЕДОМЛЕНИЙ И ОТПРАВКИ СООБЩЕНИЙ	163
-	12.1.	Настройка подключения к SMS-шлюзу	164
-	12.2.	Настройка подключения к сервису отправки рush-уведомлений	166
	12.3.	Настройка подключения к SMTP-шлюзу	168
13.	HAC	ГРОЙКА ВНЕШНЕГО ВИДА СТРАНИЦЫ ВХОДА	169
	13.1.	Редактирование шаблона по умолчанию	169
-	13.2.	Создание и изменение новых шаблонов с помощью конструктора	172
	13.3.	Создание и изменение новых шаблонов в ручном режиме	
14.	HAC	ТРОЙКИ ШЛЮЗА БЕЗОПАСНОСТИ	177
	14.1.	Настройка blitz-keeper	178
	14.2.	Создание правил доступа к сервисам	
	14.3.	Настройка правил обмена маркеров доступа	
15.	HAC	ТРОЙКИ КОНФИГУРАЦИОННЫХ ФАЙЛОВ	184
	15.1.	ФАЙЛ НАСТРОЕК BLITZ.CONF	184
	15.1.	1. Настройка парольных политик	185
	15.1	2. Ограничение количества одновременных проверок пароля пользователя	186
	15.1	3. Настройка времени отображения экрана логаута	
	15.1	4. Настройка вызова внешнего сервиса проверки электронной подписи	
	15.1	5. Настройка САРТСНА	187
	15.1	6. Настройка отправки событий в сервер очередей	189
	15.1	7. Запрос проверочного атрибута при восстановлении пароля	191
	15.1	8. Настройка хранения объектов в Couchbase Server	191
	15.1	9. Настройка домена Blitz Identity Provider	192
	15.1	10. Настройка справочника прав доступа	192
	15.1	11. Расширенные настройки подключения к хранилищам	193
	15.1	12. Блокирование неактивных пользователей	195
	15.1	13. Запрет повторного использования идентификатора удаленного пользователя	195
	15.1.	14. Настройка групп пользователей	195
	15.1	15. Вход через ЕСИА в режиме выбора сотрудника организации	196
-	15.2.	НАСТРОЙКИ ТЕКСТОВ ИНТЕРФЕЙСА	200

15.2.1.	Мультиязычность					
15.2.2.	Модификация текстовых сообщений веб-интерфейса					
15.2.3.	Модификация шаблонов писем и SMS-сообщений					
15.2.4.	Модификация сообщений для разных приложений					
15.3. Фа	ЙЛЫ НАСТРОЕК КОНСОЛИ УПРАВЛЕНИЯ					
15.3.1.	Настройка входа в консоль управления через SSO					
15.3.2.	Ограничение сессий					
15.3.3.	Настройка ролей и прав доступа в консоль управления					
16. РЕШЕНИ	Е ПРОБЛЕМ	212				
приложени	ПРИЛОЖЕНИЕ 1. ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ BLITZ IDENTITY PROVIDER					
ПРИЛОЖЕНИЕ 2. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ МЕР ЗАЩИТЫ ИНФОРМАЦИИ СОГЛАСНО ТРЕБОВАНИЯМ ФСТЭК						

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;
- вход с использованием сторонних поставщиков идентификации: вход с помощью аккаунтов социальных сетей, Единой системы идентификации и аутентификации (ЕСИА, Госуслуги), федеративный вход пользователей с использованием внешних поставщиков идентификации;
- 5. проверка прав доступа пользователей при входе в приложения;
- 6. проверка прав доступа пользователей и приложений при использовании RESTсервисов;
- 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.

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

1. Подготовка к установке

При развертывании 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.
- Приложения Blitz Identity Provider сервис аутентификации, приложение регистрации, приложение восстановления доступа, шлюз безопасности, консоль управления. Приложения регистрации, восстановления доступа, шлюз безопасности можно не устанавливать, если связанные с ними функции не планируется использовать.
- 3. СУБД. Можно использовать Couchbase Server или PostgreSQL.
- Хранилище учетных записей и паролей. Можно использовать LDAP-сервер, Microsoft Active Directory или любую (потребуется разработать коннектор) существующую систему хранения учетных записей и паролей.

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

1.1. Минимальные требования к развертыванию

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

Таблица 1

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

Минимальные требования к серверам для развертывания

Требования к сетевой связности:

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

Социальные сети	https://accounts.google.com
	https://graph.facebook.com
	https://oauth.yandex.ru
	https://oauth.vk.com
	https://account.mail.ru
	https://api.ok.ru
ЕСИА	https://esia-portal1.test.gosuslugi.ru
	https://esia.gosuslugi.ru
Сбер ID	https://online.sberbank.ru
СУДИР	https://login.mos.ru
	https://login-tech.mos.ru
	https://sudir.mos.ru
	https://sudir-test.mos.ru
к SMS-шлюзу (при	его использовании);

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

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

1.2. Рекомендуемые требования к развертыванию в кластере

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



Рисунок 2 – Развертывание в кластерной конфигурации

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

Таблица 2

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

Рекомендуемые требования к серверам для развертывания в кластере

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

Требуемые версии системного ПО:

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

Требования к сетевой связности:

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

² CM.: https://docs.couchbase.com/server/6.0/install/install-linux.html

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

 $^{{}^{4}\,}C{\tt M.:}\,https://docs.couchbase.com/server/current/install/deployment-considerations-lt-3nodes.html$

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

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

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

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

2. Установка

Для установки Blitz Identity Provider необходимо:

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

10. Настроить внешнее хранилище учетных записей (опционально).

2.1. Установка JDК

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

В качестве JDK рекомендуется использовать один из следующих:

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

Инструкция по установке OpenJDK 8 в CentOS и RHEL:

- Выполнить команду:

sudo yum install java-1.8.0-openjdk-devel

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

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

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

- открыть на редактирование файл java.security в директории /usr/lib/jvm/bellsoft-java8amd64/jre/lib/security;
- раскомментировать (или добавить) строку:

crypto.policy=unlimited

Инструкция по установке и настройке Oracle JDK 8:

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

 $^{^5\ {\}rm Cm.:}\ https://www.oracle.com/java/technologies/javase-jdk8-downloads.html$

- создать директорию под установку Oracle JDK 8:

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

– распаковать в созданную директорию дистрибутив Oracle JDK 1.8:

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

- Если версия Oracle JDK 1.8.0_151 и выше:
- открыть на редактирование файл java.security в директории /opt/oracle/jdk/jdk1.8.0_XXX/jre/lib/security;
- раскомментировать (или добавить) строку:

```
crypto.policy=unlimited
```

Если версия Oracle JDK 1.8.0_144 и ниже:

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

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

2.2. Установка memcached

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

Для установки memcached в CentOS и RHEL:

- выполнить команду:

yum install memcached

- после завершения установки добавить сервис memcached в автозапуск и запустить

сервис:

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

Для установки memcached в Astra Linux Special Edition:

```
- выполнить команду:
```

apt-get install memcached

- после завершения установки добавить сервис memcached в автозапуск и запустить

сервис:

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

⁶ CM.: https://www.oracle.com/java/technologies/javase-jce8-downloads.html

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

2.3. Установка и настройка СУБД

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

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

2.3.1. Установка и настройка Couchbase Server

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

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

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

Дистрибутив Couchbase Server можно загрузить здесь:

https://www.couchbase.com/downloads

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

После завершения установки добавить сервис Couchbase Server в автозапуск и

запустить сервис:

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

Проверить работоспособность сервиса, выполнив команду:

```
systemctl status couchbase-server
```

Далее необходимо:

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

./cb_init.sh

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

⁷ CM.: https://docs.couchbase.com/server/6.0/install/init-setup.html

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

- настроить резервное копирование БД, используя инструкцию⁸.

2.3.2. Установка и настройка PostgreSQL

Версия PostgreSQL должна быть 9.6.

В случае CentOS и RHEL необходимо установить PostgreSQL согласно инструкции: https://www.postgresql.org/download/linux/redhat/.

В случае Astra Linux Special Edition для установки PostgreSQL необходимо:

- выполнить команду:

apt-get install postgresql

- после завершения установки запустить сервис:

systemctl start postgresql

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

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

```
sudo -u postgres createdb blitzdb
su - postgres
psql
CREATE USER blitz WITH ENCRYPTED PASSWORD 'set-your-pwd';
GRANT ALL PRIVILEGES ON DATABASE blitzdb TO blitz;
GRANT ALL ON ALL TABLES IN SCHEMA public TO blitz;
ende on pasterner period d blitzdb f 001 init detabase priod
```

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

вместо set-your-pwd нужно вставить пароль, который будет использоваться для

подключения к PostgreSQL.

- настроить резервное копирование БД, используя инструкцию⁹.

2.4. Установка и настройка сервера очередей RabbitMQ

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

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

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

⁹ CM.: https://postgrespro.ru/docs/postgresql/9.6/backup-dump#backup-dump-all

- В случае Astra Linux Special Edition для установки RabbitMQ необходимо:
- выполнить команду:
- apt-get install rabbitmq-server
 - после завершения установки запустить сервис:

systemctl start rabbitmq-server

После завершения установки RabbitMQ в выбранной ОС необходимо войти в консоль

RabbitMQ (обычно, http://hostname:15672/) и выполнить следующие настройки:

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

2.5. Установка приложений Blitz Identity Provider

Blitz Identity Provider состоит из следующих приложений:

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

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

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

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

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

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

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

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

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

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

```
Your Blitz Identity Provider configured on domain: blitz-cert.loc
Your Blitz Identity Provider Console available on addresses:
   http://localhost:9001/blitz/console
   http://localhost:9001/blitz/console
Administration user credentials of Blitz Console:
   username - admin
   password - 50c2E6298B
Your can change user credentials at file - /usr/share/identityblitz/blitz-config/credentials
```

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

```
"internal-store-cb" : {
    "nodes" : [ CB_NODES ],
    "user" : "CB USERNAME",
    "password" : "CB PASSWORD"
}
```

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

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

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

отредактировать блок blitz.prod.local.idp.tasks (только при использовании СУБД



```
"tasks" : {
    "broker-rmq" : {
    "consumer" : {
             "poolSize" : 2
          },
          "exchange" : "RMQ EXCH NAME",
          "publisher" : {
               "ackTimeout" : 15,
               "channelsSize" : 8,
               "poolSize" : 2
          },
          "server" : {
    "host" : "RMQ_HOST",
    "port" : 5672
          },
"user" : {
              "password" : "RMQ_PASSWORD",
               "username" : "RMQ USERNAME"
          }
    },
    "executionRules" : [
         {
              "maxAttempts" : 2,
              "queue" : "default",
             "redeliveryDelayInSec" : 60
         }
    1,
    "queues" : [
         {
             "dequeueBatchSize" : 10,
             "dequeuePeriodInSec" : 30,
             "executorPoolSize" : 5,
             "name" : "default"
         }
    ]
```

}

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

- созданного пользователя на сервере очередей. Пароль следует указать в открытом виде, после запуска Blitz Identity Provider он будет зашифрован).
- отредактировать блок blitz.prod.local.idp.net, добавив в настройку trustedServers адреса подсетей серверов приложений Blitz Identity Provider:

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

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

}

[MEMCACHED] – указать хост и порт службы memcached (например, "ld-s-blitz1dev.ao.company:11211").

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

```
"modules" : {
    "enabled" : ${play.modules.enabled}[
        "modules.JDECModule",
        "modules.JDECInternalStoreModule",
        "modules.JDECAuditStoreModule",
        "modules.RmqTaskModule"
    ]
}
```

В случае использования Couchbase Server в качестве СУБД нужно оставить блок

modules без изменений, а именно в следующем виде:

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

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

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

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

/usr/lib/jvm/java-1.8.0-openjdk для OpenJDK 8, /opt/oracle/jdk для Oracle JDK 8);

- путь к файлу blitz-keeper-thirdparty-5.Х.Х.tar.gz (только в случае установки сертифицированной версии).
- дождаться окончания установки приложения. Установка будет произведена в директорию /usr/share/identityblitz.
- добавить приложения в автозапуск на соответствующих им серверах и запустить их:

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

2.6. Настройка синхронизации файлов конфигурации

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

1. На сервере с консолью управления Blitz Console:

- установить rsync и incron:

```
sudo yum install rsync incron
```

или (для Astra Linux Special Edition)

```
sudo apt install rsync incron
```

- переключиться на пользователя blitz

sudo su - blitz

- сгенерировать ssh ключ командой (на все задаваемые утилитой вопросы

рекомендуется выбрать ответы по умолчанию):

ssh-keygen

- прочитать и сохранить для дальнейшего использования публичный ssh ключ:

cat /usr/share/identityblitz/.ssh/id rsa.pub

– открыть настройки incrontab:

```
incrontab -e
```

- в открывшемся окне редактора вставить следующее:

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

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

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

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

node_list="NODES_LIST"

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

в качестве значения node_list, вместо NODES_LIST, необходимо прописать список

hostname нод кластера Blitz (кроме ноды консоли управления Blitz Console).

- сделать файл /usr/share/identityblitz/scripts/config_sync.sh исполняемым:

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

- запустить incrontab, выполнив под пользователем root команду:

systemctl enable incrond systemctl start incrond

2. На остальных серверах приложений Blitz Identity Provider:

установить rsync:

sudo yum install rsync или (для Astra Linux Special Edition)

sudo apt install rsync

- переключиться в пользователя blitz:

sudo su - blitz

- выполнить следующий скрипт:

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

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

2.7. Настройка веб-сервера

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

1. Скорректировать блок настроек балансировки:

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

Параметры имеют следующие назначения:

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

```
2. Скорректировать блок настроек снятия TLS:
```

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

Параметры имеют следующие назначения:

- [BLITZ-SSL-CERT-FILE] путь (полное имя) к файлу с TLS-сертификатом сервера;
- [BLITZ-IDP-CONSOLE-NODE-01] путь (полное имя) к файлу с TLS-ключом сервера.
- 3. Следует учесть, что Blitz Identity Provider игнорирует заголовок X-Forwarded-Proto https, если в nginx X-Forwarded-For содержит более одного IP-адреса, например:

proxy_set_header X-Forwarded-For \$proxy_add_x_forwarded_for;

В этом случае рекомендуется использовать следующее значение директивы:

proxy_set_header X-Forwarded-For \$remote_addr;

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

2.8. Установка и настройка LDAP-каталога

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

Поддерживаются:

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

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

Для установки 389 Directory Server в CentOS и RHEL:

- выполнить команды установки:

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

- установить limits в соответствии с рекомендациями 389 Directory Server:

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

- инициализировать LDAP-каталог. Ответить на вопросы установщика.

setup-ds-admin.pl

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

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

- Для установки в Astra Linux Special Edition:
- выполнить команду установки и скрипт инициализации каталога:

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

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

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

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

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

chmod +x ldap init.sh ./ldap_init.sh

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

chmod +x ldap ssl.sh ./ldap ssl.sh

- После выполнения скрипта перезапустить LDAP-каталог:

systemctl restart dirsrv.target

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

chmod +x ldap_pwdpolicy.sh
./ldap_pwdpolicy.sh

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

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

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

systemctl restart dirsrv.target

2.9. Вход в консоль управления

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

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

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

Пости	
ЛОГИН	
🆀 Be	зедите логин
Парол	Ь
A BE	зедите пароль
	Войти

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.

Blitz Console ≡		admin O
Приложения	Консоль управления / Притожния	
 приложения приложения прочинки данных Аутентификация Процедуры входа Поставщики идентификация Сорвисы самообслуживания Пользователя Группы Аминистраторы SAML Outh 2.0 Макельска 	Консоль управления / Присожникя Подключенные приложения Добавьте приложения, которые должны использовать сервисы BBIz Identity Provider - проводить идентификацию и вутентификацию пользователей, а таске вызывать REST: сервисов. Для подискочения приложения необходино ввести данные о нем, а таске сконфигурировать один из доступных протоколов. Более подробная информация размещена в Руховодстве администратора и Руховодстве по интеграции. Добавьть приложения	
 Устройства Собщения Сообщения Внешний вид 		
	E 2021 OCO -PEAK CODT- Bu kcnomocystre Elitz Identity Provider Enterprise Edition, espons 5.0.0.27.08.2021-16.31.	

Рисунок 4 – Вид главного экрана консоли управления

2.10. Установка лицензионного ключа

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

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

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

О продукте	
Blitz Identity Prov версия 2.27.0.5575	ider Enterprise Edition
Посмотреть документацию	Сообщить об ошибке
Информация о лицензии	
Дата окончания действия лицензии	31.12.2019
Максимальное количество приложений	999
	Изменить пицичано

Рисунок 5 – Просмотр информации о лицензии

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

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

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

2.11. Управление учетными записями администраторов

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

Blitz Console					admin 😃
Приложения	Консе	оль управления / Администраторы			
🛢 Источники данных					
Ҟ Аутентификация	Аp	министраторы			
🕄 Процедуры входа					
👻 Поставщики идентификации		Логин	Роли	Пароль	
🗶 Сервисы самообслуживания		admin	× суперпользователь	Изменить пароль	×
曫 Пользователи			- Chicken and a		
😂 Администраторы		support	×администратор ТП	Изменить пароль	×
🗰 SAML					
Soluth 2.0		security	×администратор иь	изменить пароль	<u> </u>
🖣 Устройства		sysadmin	× системный администратор	Изменить пароль	×
📿 События					
💟 Сообщения				т создать учетную запись администр	атора
🖵 Внешний вид					
				Co	хранить

Рисунок 6 – Управление администраторами

В разделе «Администраторы» доступны следующие действия:

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

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

Таблица 3

Стандартные роли администраторов в Blitz Identity Provider

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

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

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

2.12. Перезапуск приложений Blitz Identity Provider

Для перезапуска приложений Blitz Identity Provider необходимо использовать команду: systemctl restart APP_NAME

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

Пример команды для перезапуска приложения сервиса аутентификации:

systemctl restart blitz-idp

3. Настройка атрибутов учетных записей

3.1. Конфигурирование доступных атрибутов

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

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

Конфигурирование атрибутов состоит из:

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

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

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

3.1.1. Настройка хранимых атрибутов

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

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

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

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

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

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

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

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

Хранимые атрибуты					
Определите атрибуты учетной записи пользователя. Для внешнем хранилище, в таком случае укажите правило п	і этого задайте <i>название</i> – уникальное имя реобразования в настройках этого хранил	і атрибута в системе ища.	е. Название атрибута	может отличаться	от его имени во
Таже выберите <i>тип значения</i> – тип данных атрибута.					
Укажите, какие атрибуты являются:					
 поисковыми (Поиск) - эти атрибуты будут учтены п следует предусмотреть индекс; обязательными (Обяз.) - эти атрибуты должны быт уникальными (Уник.) - эначения этих атрибутов до 	ои поиске учетной записи в разделе «Поль - заданы при регистрации пользователя и лжны быть уникальны в системе.	зователи», при испо не могут быть удал	ользовании внешнего ены в дальнейшем.	о хранилища по эт	им атрибутам
Наименование атрибута	Тип значения	Поиск	Обяз.	Уник.	
uid	String	V	V	•	×
surname	String	۷			×
name	String				×
mail	String	V		✓	×
mobile	String			•	×
					+ Добавить атрибут

Рисунок 7 – Пример настройки хранимых атрибутов

3.1.2. Настройка вычисляемых атрибутов

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

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

Примеры правил:

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

 $^{^{11}}$ Справку по поддерживаемым параметрам строк подстановки можно посмотреть здесь: http://tldp.org/LDP/abs/html/parameter-substitution.html

При необходимости определите вычисляемь Вычисляемому атрибуту может быть присво	ые атрибуты – укажите их <i>наимен</i> ено константное значение.	нование, тиі	п значения, а также настройте <i>правило вычисления</i> на осно	ве хранимых атрибутов.
Примеры настройки				
 Создать атрибут «Имя и фамилия» и сначала определите хранимые атри Создать атрибут «домен электроннс определите хранимый атрибут mail. Справку по поддерживаемым параметрам 	из хранимых атрибутов firstname ибуты firstname и lastname. Далее ой почты» из хранимого атрибута . Далее задайте вычисляемый атр и строк подстановки можно посм	<i>и lastname:</i> задайте вы а <i>mail:</i> рибут domai ютреть <u>здес</u>	числяемый атрибут fullname с правилом вычисления – \${fi in и определите его правило вычисления \${mail##*@} . b-	rstname} \${lastname}.
	-			
Наименование атрибута	Тип значения		Правило вычисления	
Наименование атрибута est	Тип значения String	v	Правило вычисления	×
Наименование атрибута est idGroup	Тип значения String Array of strings	>	Правило вычисления 1 \$(memberOf)	×

Рисунок 8 – Пример настройки вычисляемых атрибутов

3.1.3. Настройка правил преобразования входных значений

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

Пример решаемых задач:

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

Правила преобразования вхо	дных значений		
Эти правила позволяют пров выражений. Примеры настройки	ерять корректность формата ввода данных и обеспечивают сохра	нение данных в корректном формате. Правила задаются с помо	щью регулярных
Наименование атрибута	Декомпозиция	Компоновка	
mail	^(.+)@(.+).(.+)\$	\${0}	×
mobile	^(\+?)([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 выхо	одных значений			
Эти правила позволяют совери	шить дополнительные преобразования с вычисляемыми атрибут.	эми.		
Наименование атрибута	Декомпозиция		Компоновка	
adGroup	^(CN=39SU-ABCD-)(?!TEST- DEV-)(.*)\$	\${0-}		×
			+ /	обавить 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).
- Выражение, определяющее имя пользователя в консоли. Например, выражение \${surname} \${name} \${middlename-} 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 буде	т идентификатором в системе. Идентификатор должен быть уникальным и не меняться со временем.
Также можно указать, какие а	атрибуты используются:
 для определения забл в качестве адреса эле в качестве номера моб 	окированных учетных записей. Этот атрибут должен быть булевым (Boolean); стронной почты; ильного телефона
Можно также указать правил	ю, по которому будет формироваться имя пользователя для отображения в консоли
Идентификатор	uid 🗸
Признак блокировки	×
Имя пользователя в консоли	\${surname} \${name} \${middlename-}
Электронная почта	× mail
Мобильный телефон	× mobile
	Сохранить

Рисунок 11 – Конфигурирование назначения атрибутов

3.2. Подключение хранилищ атрибутов

3.2.1. Типы хранилищ

В качестве хранилищ атрибутов пользователей Blitz Identity Provider позволяет использовать:

- 1. Внешнее (подключенное) хранилище. В качестве 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).
- 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».

ранилища атрибутов		
Если все учетные записи предполагается хранить в Blitz Identity Provider, то достаточн хранилища (built-in). Если требуется подключить внешнее хранилище, нажмите на кно хранилище», выберите тип хранилища и настройте его.	ю одного внутреннего лку «Добавить новое	
bip-dldap01		
Idap: 389-DS		
bip-ddc01		
Idap: Microsoft Active Directory		
	Добавить новое хра	нилище

Рисунок 12 – Хранилища атрибутов

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

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

Тип хранилища	LDAP	~	
Хост	ldap.example.com		
Порт	636		
	Использовать SSL		

Рисунок 13 – Экран добавления хранилища учетных записей

3.2.2. Подключение хранилища по протоколу LDAP

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

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

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

¹³ Допустимо указать пользователя только с правами на чтение, если хранилище используется только для чтения.
указать настройки поиска – глубину поиска и максимальное число возвращаемых учетных записей (это влияет на число пользователей, отображаемых в разделе «Пользователи» консоли управления).

Параметры подключения к	LDAP хранилищу
Идентификатор	bip-dldap01
Описание	389 <u>Project</u>
Только для чтения	Her
Настройка соединения	Без балансировки DNS-балансировка
Хост	bip-dldap01
Порт	636
	☑ Использовать SSL
Настройка пула соединений	
Таймаут со	единения, мс 3000 Начальное количество соединений 10
Тайма	ут ответа, мс 3000 Максимальное количество соединений 10
Учетная запись для работы с	: хранилищем
Для корректной работы долх Provider, то необходимы пра	кна быть указана учетная запись с правами на чтение данных из хранилища. Если планируется изменение/добавление данных средствами Blitz Identity ва на запись
Пользователь(DN)	uid=reader,ou=sub,dc=reaxoft,dc=loc
Пароль	Изменить значение
Базовый DN	ou=sub,dc=reaxoft,dc=loc
Настройки поиска	
Глубина поиска	В базовом DN и в подчиненных ~
Максимальное количество записей, возвращаемых при	100
поиске	

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

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

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

- использовать специальные правила записи атрибутов в данный LDAP-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-}.

LDAP-каталоге. И	для чтения, и для записи	можно указать правила ра	збиения и правила пр	еобразования значений а	трибутов. Это позволяет:
 дать атрибуту sn, а в Blitz Io LDAP; 	ив системе другое названи lentity Provider необходим	ие, не совпадающее с его и 10 его использовать как su	именем в LDAP-катало urname , то выберите ат	ге. Например, если в LDAP рибут <mark>surname</mark> и укажите	-каталоге атрибут задан к sn в качестве его названі
 использовать формате +7(9 преобразован 	оспециальные правила за 99)1234567 в LDAP-катало ния +7 <mark>\${1-}\${2-</mark> }.	писи атрибутов в данный г без скобок, то для записи	LDAP-каталога. Напри 1 задайте правило раз(мер, если вы хотите сохра биения <mark>^\+7\(([0-9]{3})\)</mark>	нять мобильный телефон ([0-9]{7})\$ и правило
 использовать мобильного т можно испол 	, специальные правила чт елефона задан в формате ьзовать правило разбиен	тения атрибутов из данног +79991234567, а в Blitz Ide ия ^\+7([0-9]{3})([0-9]{7	o LDAP-каталога. Напр entity Provider использ })\$ и правило преобр	имер, если в LDAP-катало уется формат +7(999)12345 азования <mark>+7(\${1-})\${2-}</mark> ;	ге атрибут с номером 667, то для чтения из катал
Атрибут	Название в LDAP	Запи Правило разбиения	сь Правило преобразования	Чтен Правило разбиения	иие Правило преобразования
uid 🗸	userPrincipalName				
surname 🗸	sn				
	givenName				
name 🗸					
name 👻	mail				

Рисунок 15 – Настройка правил сопоставления атрибутов (фрагмент)

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

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

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

Параметры созда	ния новых пользовател	іей		
Для корректной параметры. При пользователя. С	работы создания пользов и формировании значений Списочное значение можно	ателя необходимо указать спе параметров можно использов о задать через запятую.	ецифичные для LDAP хранили ать строки подстановки из атן	ща рибутов
DN	uid=\${uid},ou=bip-demo2,o	u=sub,dc=dev,dc=reaxoft,dc=loc		
пользователей	Например, CN=\${mail},CN=t	users,DC=domain,DC=com		
Первоначальные атрибуты	Название	Формат	Значение	
Например: objectclass.	objectClass	Array of strings	r top,blitz-schema	×
			+ До	бавить атрибут

Рисунок 16 – Настройка параметров создания новых пользователей

3.2.3. Подключение к хранилищу по REST

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

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

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

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

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

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

Параметры REST-сервисов	
Идентификатор	rest_test
Описание	
Только для чтения	
Максимальное количество записей, возвращаемых при поиске	100
Перечень доступных атрибутов	x uid x surname x name x mail x mobile x objectGUID x logon_name x objectSID x memberOf x mobile_test x passport
Адреса REST-сервисов	
URL сервиса поиска пользователей	http://172.25.0.142:3000/search
	НПР метод запроса: GET. Параметр запроса: • rq1 — запрос в формате Resource Query Language (RQL). Формат ответа: 200 оК, список пользователей в формате JSON Array в кодировке UTF-8. Пример листинга
URL сервиса получения данных пользователя	http://172.25.0.142:3000/user/\${id}
	При указании URL необходимо использовать строку подстановки для идентификатора пользователя – \$(id) . HTTP метод запроса: GET. Формат ответа: 200 ОК, данные пользователя в формате 3SON в кодировке UTF-8. Если пользователь не найден: 400 Bad Request, код ошибки USER_NOT_FOUND в формате text/plain; charset=utf-8.
	пример листинга

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

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

3.2.3.1. Сервис поиска пользователей

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

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

¹⁵ https://github.com/kriszyp/rql

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

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

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

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

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

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

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

Пример запроса:

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

Пример ответа:

```
{
    "id": "ID123",
    "attrs": {
      "uid": "BIP123",
      "name": "Ivan",
      "surname": "Ivanov",
      "mail": "ivanov@test.org",
      "mobile": "+79991234567"
    }
  },
  {
    "id": "ID456",
    "attrs": {
      "uid": "BIP456",
      "name": "Elena",
      "surname": "Ivanova",
      "mail": "ivanova@test.org",
      "mobile": "+79997654321"
    }
  }
1
```

3.2.3.2. Сервис получения данных пользователя

В ряде случаев Blitz Identity Provider запрашивает данные конкретного пользователя. Сервис получения данных пользователя должен обрабатывать запросы методом GET, в котором в URL указывается атрибут id – внутренний идентификатор пользователя в подключенной базе данных. При задании URL этого сервиса необходимо использовать строку

подстановки для идентификатора пользователя – \${id}, например:

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

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

Пример запроса:

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

Пример ответа, если пользователь найден:

```
HTTP/1.1 200 OK
Date: Mon, 18 Jul 2016 12:28:59 GMT
Content-Type: application/json; charset=utf-8
{
    "id": "ID123",
    "attrs": {
        "uid": "BIP123",
        "name": "IVan",
        "surname": "IVanov",
        "mail": "ivanov@test.org",
        "mobile": "+79991234567"
    }
}
```

Ответ для случая, если пользователь не найден:

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

USER NOT FOUND

3.2.3.3. Сервис проверки логина и пароля

Сервис проверки логина и пароля должен обрабатывать запросы методом POST, в теле

которых указаны следующие параметры (в формате application/x-www-form-urlencoded):

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

В случае успеха сервис должен вернуть ответ 200 ОК.

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:

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 РИТ,

в теле которых указаны следующие параметры (в формате application/json):

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

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

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

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

Пример запроса:

```
PUT /users HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/json
Cache-Control: no-cache
{
    "password":"*******",
    "attrs": {
        "uid": "ivanov@test.org"
        "mail": "ivanov@test.org"
    }
}
```

Пример ответа (пользователь создан):

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

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

Пример ответа (учетная запись уже зарегистрирована):

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

USER ALREADY EXISTS:ivanov@test.org

3.2.3.6. Сервис изменения данных пользователя

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

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

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

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

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

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

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

Пример запроса:

```
POST /users/ID123 HTTP/1.1
Host: idstore.identityblitz.com
Content-Type: application/json
Cache-Control: no-cache
{
    "replaced": {
        "mail": "ivanov@domain.org"
    },
    "deleted": ["surname"],
    "password": "########"
}
```

Пример ответа:

```
HTTP/1.1 200 OK
Date: Mon, 18 Jul 2016 12:38:53 GMT
Content-Type: application/json; charset=utf-8
{
    "id": "ID123",
    "attrs": [
        "uid": "BIP123",
        "name": "Ivan",
        "email": "ivanov@domain.org"
]
```

```
}
```

3.2.3.7. Сервис удаления пользователя

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

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

В случае успеха сервис должен вернуть статус 200 ОК.

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.

Параметры встроенного хра	нклища	
Идентификатор	built-in	
Описание	Built-in store	
Только для чтения	Her v	
Максимальное количество записей, возвращаемых при	100	
поиске		
		Удалить Сохранить

Рисунок 18 – Настройка внутреннего хранилища

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

4. Настройка способов аутентификации

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

код по сеансу операционной системы		Логин и пароль
и входе будет использоваться текущий сеанс операционной системы		При входе в систему пользователю необходимо ввести логин и пароль
Перейти к конфигурации метода		Перейни к настройкам
редство электронной подлиси		Вход через внешние сервисы идентификации
и входе в систему попьзователю необходимо использовать средство электронной п и смарт-карту	одлиси	Для входа пользователь будет перенаправлен на внешний сервис идентификации. Пользователю потребуются дать согласне на передачу данных своей учетной записи в Biltz
Перейти к конфигурации метода		Identity Provider. Перейти к настройкам
код по разовой ссылке		Вход с известного устройства
код в систему осуществляется по специальной ссылке. Ссылка действует однократн чение ограниченного периода времени.	ю в	После услешного входа устройство запоминается. В течение определенного периода вход систему осуществляется автоматически
ирейти к настройкам		Сконфигурируйте метод для использования
одтверждение с помощью кода		
исле успешного первичного входа пользователю нужно ввести код из сообщения, пе номер мобильного телефона	ереданного	
арейти к настройкам		
райти к настройкам		Добавить внешений метод вутентифи
рейти к настройкам рой фактор		Добавить внешаний метод кутентифи
рой фактор зоовый пароль на основе секрета (НОТР)		Дебавить внешний метод аутентифи Разовый пароль на основе времени (ТОТР)
ройти к настройкам рой фактор азовый пароль на основе секрета (НОТР) эсле успециюто периичного входа пользователю кулко ввести код, стенерированный перияли-ким устройством - генеритором одноразовых паролей рафити к настройкам		Добавить внешний метод аутентифи Разовый пароль на основе времени (ТОТР) После успецного перанного входа пользователю нузно ввести код, стенерированный мобильных пригозничен или усройством Перейти к настройкам
рейти к настройкам рой фактор взоевый пароль на основе секрета (НОТР) осле услешито первичного вклада попьзователю иухию ввести код, стенерированный ихидильным устройством - генератором одноразовых паролей рейти к настройкам зо ризћ-аутентифи кация		Добавить внешений метод аутентнфи Разовый пароль на основе времени (ТОТР) После успециеного первичено входа пользователю нужно ввести код, стенерированный мобильным пригожением или устройством Перейти к настройкам
рейти к настройкам рой фактор азовый пароль на основе секрета (НОТР) сле успеционто перенного входа попьзователо кулоко веести код. стенерированный пройти к настройкам зо ризћ-ауттелтификация адперехдение входа с помецько мобильного приложения Duo Mobile - необходимо о вт-увадомление	а тветить на	Добавить внешний метод аутентифи Разовый пароль на основе времени (ТОТР) После услешного первичного входа пользователю нужно ввести код, стенерированный мобильным приложением или устройством Перейти к настройкам Вход с известного устройства Полелляет не требевать усиленную аутентификацию (второй фактор) при входе с извесстного устройства.
райти к настройкам рой фактор азовый пароль на основе секрета (НОТР) сле успешното периичного входа пользователю нужно ввести нод, стенерированный парейти к настройкам ио ризh-аутентификация праейти к конфигурации метода Парейти к конфигурации метода	а тветить ма	Добавиль, внешаний метод аутентифи Разовый пароль на основе времени (ТОТР) После успешного первичного входа пользователю нуюно ввести код. сгенерированный мобильным приложением или устройством Перейли к настройкам Вход с известного устройства Позволяет не требевать усиленную аутентификацию (второй фактор) при входе с известного устройства.
рейти к настройкам рейти к конфигурации метода рутверидение конфигурации метода рутверидение с помощью кода	а	Добавить внешаний метод аутентнфи Разовый пароль на основе времени (ТОТР) После успешного первичного входа пользеватело нукою ввести код. сгенерированный мобильным приложением или устройством Перейти к настройкам Вход с известного устройства Позволлет на требовать усиленную аутентнфикацию (второй фактор) при входе с известного устройства.
рейти к настройкам рой фактор азовый пароль на основе секрета (НОТР) сле услещного перинного входа попьзователю нулко ввести код. стенерированный паройи к настройкам ло ризh-аутентификация до ризh-аутентификация датеридение с помощью кодиа тарейти к конфитурации метода датеридение с помощью кодиа сле услешного перинного входа попьзователю нулко ввести нод из сообщения, ле номер мобильного телефона	а а тветить на преданного	Добавиль внешний метод аутентифи Разовый пароль на основе времени (ТОТР) После услешного первичного входа пользователю нужно ввести код, стенерированный моблильных протоженева или устройством Прейли к настройкам Вход с известного устройства Позволяет на требовать усиленную аутентификацию (второй фактор) при входе с известного устройства.

Рисунок 19 – Настройка способов аутентификации (фрагмент)

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

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

Общие настройки	
Уровень аутентификации по	Первый фактор 🗸
умолчанию	Укажите требование к аутентификации пользователей по умолчанию. Если указан вариант "первый и второй фактор", то по умолчанию все пользователи должны пройти двухфакторную аутентификацию.
Продолжительность сессии	3600
при безденствии пользователя	Укажите время (в секундах), в течение которого будет сохранена сессия при бездействии пользователя, т.е. при отсутствии переходов между разными припожениями
Максимальная	10800
продолжительность сессии	Укажите время (в секундах), в течение которого будет сохранена сессия независимо от наличия действий пользователя
Отображаемое имя	\${mail-5mobile}
пользователя	Отображается на странице входа при входе с известното устройства. Используйте строки подстановки для формирования имени. Например, "S[lastname] S[lirstname]"

Рисунок 20 – Общие настройки аутентификации

4.1. Настройка входа по логину и паролю

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

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

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

ход по логину и паролю				
Для корректной работы входа по паролю укажите, каким несколько альтернативных правил определения логина	м обра 1. Ввод	ізом должен і логина не ч	формироваться логин и какому атрибуту в источнике данных он соответству увствителен к perистру.	ет. Вы можете создать
Для создания правила используйте строки подстановки. сп в хранилище данных.	. Напр	имер, прави	ло cn=\${login} означает, что строка, введенная пользователем, будет сравн	иваться с атрибутом
Посмотреть строки подстановки				
sAMAccountName	\$	-	\${login}	×
				+ добавить условие
R				
mail	\$	-	\${login}	×
				+ добавить условие
			+ добавить	альтернативное правило
				Отмена Сохранить

Рисунок 21 – Настройка входа по логину и паролю

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

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

- выбрать опцию «Всегда проверять текущий пароль пользователя на соответствие парольной политике» или вписать имя некоторого заголовка в поле «Проверять при наличии НТТР заголовка» (в этом случае, если НТТР-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).

	Всегда проверять текущий пароль пользователя на соответствие парольной политике
Проверять при наличии	X-PP-Check
НТТР 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	Спосле указанного кол-ва неудачных попыток будет установлена временная
временной олокировки	блокировка пользователю на использование данного метода аутентификации
Длительность	
временной блокировки	Определяет длительность временной блокировки в минутах по истечению которых
	пользователь сново сможет использовать данный метод аутентификации

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

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

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

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

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

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

При включенной защите про	оисходит замедление процесса аутентификации. В этом случае после ввода пароля пользователь будет ожидать результата в течение периода,
определенного настроикои	«оремя задержи». предусмотрены следующие автоматические режимы защиты.
 на уровне системы в цело 	м. включается, если процент неуспешных аутентификации достигнет определенного порога (настроика «порог включения системной защиты»).
- на уровне пользователя. В	Зключается, если пользователь вводит подряд определенное количество неверных паролей (настройка «Порог включения пользовательской защиты»).
Защита	Автоматический режим на уровне пользователей
емя задержки, в секундах	3
Порог включения тользовательской защиты	5
рог включения системной защиты	40
Порог выключения системной защиты	30

Рисунок 23 – Настройка защиты от подбора пароля

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

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

Правила выбора хранилища атрибутов			
По умолчанию поиск пользователей для ау пользователя будет осуществляться в опре Можно задать несколько альтернативных п Для создания правила используйте строки Посмотреть строки подстановки	тентификации происходит во всех активнь еделенном хранилище. равил выбора хранилища. Это позволит ау подстановки.	ых хранилищах. В данном блоке можно настроить правила, при выполн утентифицировать одних пользователей по одному хранилищу, других	ении которых поиск - по другому.
Хранилище атрибутов		Правило соответствия	
main	not \${_rpld_}	^(.*)\$	×
		+ Доб	авить альтернативное условие
test_db ~	not \${_rpld_}	test_app	×
		+ Доб	авить альтернативное условие
			+ Добавить правило
			Отмена Сохранить

Рисунок 24 – Настройка правил выбора хранилища атрибутов

4.2. Настройка входа с помощью средства электронной подписи

4.2.1. Настройка метода аутентификации в консоли управления

При использовании для аутентификации средств электронной подписи необходимо:

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

При конфигурировании входа по электронной подписи можно также указать:

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

OCuper Lacrpointal	щие настройки Триравнять использование з цвухфакторную аутентификац Троверять, что сертификат п	этого метода к применению первого и второго ф цию опъзователя не отозван					
	Триравнять использование : цвухфакторную аутентификац Троверять, что сертификат п	этого метода к применению первого и второго ф цию опьзователя не отозван					
	Проверять, что сертификат п		актора. Если	1 опці	ия включена, то вход по электронной подписи будет означать, ч	то пользователь проц	іел
PARKAR COTTETTERS		onoodarennine oroodan					
passivial correterenses passivial correterenses passivial corret							
parana contractorem Ages coppectively padota is stoga no anertpointely nogrines yeasone, savise none gonenia curriteriations to ceptivelywara a second an arbeijationes in a ceptivelywara a spectro in a ceptivelywara. Contract Contract and C							
равила соответствия Для коррестной работы входа по элестронной подписи укажите, какие поля должны считываться из сертификата и каким атрибутам в источнике данных они о можете содать несолько альтеринион подписи укажите, какие поля должны считываться из сертификата и каким атрибутам в источнике данных они о можете содать сарти несолько альтеринион сарибутов спользуйте строки подстановки. Например, правило Синбраврест, со) означает, что атрибут SMP2C сертификата будет сравниваться с атрибутов CN в хранилице данных. Поскотреть строки подстановки mail						Отмена	Сохранит
равила соответствия Apr коррестной работы входа по электронной подписку укажите, какие поля должны считываться из сертификата и каким атрибутав в источняке данных он о можете создать несколько алектронной подписку укажите, какие поля должны считываться из сертификата и каким атрибута в источняке данных он о каке создать несколько алектронной подписку укажите, какие поля должны считываться из сертификата от каким атрибутая в источняке данных он о сертификата будет сравниваться с атрибутов используйте строки подстановки. Например, правило Синф (Subject, Co) означает, что атрибут заласе mail • • fgGBBECT.E) • • • * добавить али * * добавить алит создание учетной записи Балики учетной записи Создание учетной записи Создание учетной записи. Всли при входе по электронной подписки пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите, и будет созраннае лектронная почта из сертификату электронной подписи тими • • § Subject, E) Создавать учетную запись. Включите эту функцию и укажите, и • • Можето создань не найден по сертификату электронной подписи тими • • § Subject, E) • • • будивать цента ото пользователь не найден по сертификату электронной подписи • • • будивать учетную запись. Включите эту функцию и укажите, в создавать учетную запись. Включите эту функцию и укажите, • • • • робавить али • • • • фованть и и • • • • • • • • • • • • • • • • •							
Для корректной работы входа по электронной подписи укажите, какие поля должны считываться из сертификата и каким атрибутам в источнике данных они со иожете содать несклолко альтернативных правил. Для собланение считываные истизавения из сертификата априбутов используйте строки подстановки. Например, правило син-\$(\$ивл:ст.сл) означает, что атрибут зилах сертификата будет сравниваться с атрибутов CN в храннилице данных. Посмотреть строки подстановки mail	вила соответствия						
дите одолачения счи повелеми и сертификата а дирију ов использун с спроки подстанових, например, правило свез (завлест св.), озлачает, что а рикут завлес сертификата (ст. строки подстановки mail • • • \$(SUBJECT.E) • • добавить альт • добавить альт • содавить учетной записи Если при входе по электронной подписи пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите, Blitz Identity Provider должны формироваться из атрибутов сертификату электронной подписи Посмотреть строки подстановки 1 создавать учетную запись, если пользователь не найден по сертификату электронной подписи Атрибут • Правило валиси 1 создавать учетную запись, если пользователь не найден по сертификату электронной подписи паil • • • \$(SUBJECT.E) ии	Для корректной работы вх можете создать несколько	юда по электронной подписи укажите, какие г • альтернативных правил.	поля должн	ны сч	итываться из сертификата и каким атрибутам в источнике д	анных они соответс	гвуют. Вы
Поскотреть строки подстановки mail	сертификата будет сравни	ваться с атрибутом CN в хранилище данных.	строки под	стан	OBKN. HAILPINNED, ILPABUNO CN=\${SUBJECT.CN} OSHAHABI, HIO AT	PNOYI SUBJECT.CN	
mail • \$(SUBJECT.E) • • • • • • • • • • • • • <td>Посмотреть строки подста</td> <td>новки</td> <td></td> <td></td> <td></td> <td></td> <td></td>	Посмотреть строки подста	новки					
mail * \$(SUBJECT.E) * * * * * * * * * * * * * * *							
+ добавить альт - + добавить альт 	mail	✓ = \$	\${SUBJECT.E}			*	
задание учетной записи сли при входе по электронной подписи пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите. Віта Identity Provider должны формироваться из атрибутов сертификата. Используйте строки подстановки. Например, правило mail + {SUBJECT.E} Посмотреть строки подстановки Посмотреть строки подстановки Создавать учетную запись, если пользователь не найден по сертификата электронной подписи трибут Правило						+ добавит	ь условие
+ добавить альт сот сот сот сот сот сот сот со							
ота подавать учетную запись, если пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите, Bitz Identity Provider должны формироваться из атрибутов сертификата. Используйте строки подстановки. Например, правило msil+s{SuBJECT.E} означает, что будет сохранена электронная почта из сертификата. Используйте строки подстановки. Например, правило msil+s{SuBJECT.E} означает, что будет сохранена электронная почта из сертификата. Используйте строки подстановки. Например, правило msil+s{SuBJECT.E} означает, что будет сохранена электронная почта из сертификата. Используйте строки подстановки. Например, правило msil+s{SuBJECT.E} означает, что будет сохранена электронная почта из сертификата. Используйте строки подстановки. Например. правило msil+s{SuBJECT.E} означает, что будет сохранена электронная почта из сертификата. Используйте строки подстановки. Например. правило msil+s{SuBJECT.E} означает, что будет сохранена электронная почта из сертификата. Используйте строки подстановки. Например. правило msil+s{SuBJECT.E} означает, что будет сохранена электронная почта из сертификата. Используйте строки подстановки подстановк					+ A	обавить альтернатив	юе прави/
аздание учетной записи вздание учетной записи Если при входе по электронной подписи пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите, Віїс identity Provider должны формироваться из атрибутов сертификата. Используйте строки подстановки. Например, правило mail-s(SuBJECT.E) означает, что будет сохранена электронная почта из сертификата. Посмотреть строки подстановки Создавать учетную запись, если пользователь не найден по сертификату электронной подписи трибут трибут таll ин							
аздание учетной записи Если при входе по электронной подписи пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите, Blitz identity Provider должны формироваться из атрибутов сертификата. Используйте строки подстановки. Например, правило ==11=\${SUB3ECT,E} означает, что будет сохранена электронная почта из сертификата. Создавать учетную запись, если пользователь не найден по сертификату электронной подписи ктрибут mail mail f(SUBJECT,E) f(SUBJECT,E)						Отмена	Сохрани
радание учетной записи Если при входе по электронной подписи пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите, Bitz Identity Provider должны формироваться из атрибутов сертификата. Используйте строки подстановки. Например. правило mail=\$(SUBJECT.E) означает, что будет сохранена электронная почта из сертификата. Создавать учетную Запись, если пользователь не найден по сертификату электронной подписи создавать учетную запись, если пользователь не найден по сертификату электронной подписи атрибут mail mail f (SUBJECT.E) f (SUBJECT.E)							
задание учетной записи Если при входе по электронной подписи пользователь не найден, то можно для этого пользователя создать учетную запись. Включите эту функцию и укажите, Bltz identity Provider должны формироваться из атрибутов сертификата. Используйте строки подстановки. Например. правило mol1-s(SUBJECT.E) означает, что будет сохранена электронная почта из сертификата. Посмотреть строки подстановки создавать учетную запись, если пользователь не найден по сертификату электронной подписи атрибут mail mail mail mail mail mail mail mail							
Атрибут правило mail v v v v v v v v v v v v v v v v v v v	будет сохранена электроні Посмотреть строки подста	ная почта из сертификата. новки	ктронной по	одпис	и		
mail v = \$(SUBJECT.E)	оздавать учетную запись, ес	сли пользователь не наиден по сертификату элек					
mail v - \$(SUBJECT.E)	_оздавать учетную запись, ек рибут	сли пользователь не наиден по сертификату элек			Правило		
uid v = S(SUBJECT,E)	оздавать учетную запись, ек рибут	сли пользователь не наиден по сертификату элек		_	Правило		
	оздавать учетную запись, е рибут mail	сли пользователь не наиден по сертификату элек	>	=	Правило \$(SUBJECT.E)		
	оздавать учетную запись, ег рибут mail uid	сли пользователь не наиден по сертификату элен	>	-	Правило \$(SUBJECT.E) \$(SUBJECT.E)		
	создавать учетную запись, ег рибут mail uld	сли пользователь не наиден по сертификату элен	>	-	Правило \$(SUBJECT.E) \$(SUBJECT.E)	+ 00622	
	создавать учетную запись, ег рибут mail uld	сли пользователь не наиден по сертификату элен	>	-	Правило \$(SUBJECT.E) \$(SUBJECT.E)	+ Добае	атриб
т	создавать учетную запись, ек рибут mail uld	сли пользователь не наиден по сертификату элен	>	-	Правило \$(SUBJECT.E) \$(SUBJECT.E)	+ Добаг	жить атриб
	создавать учетную запись, ек рибут mail uld	сли пользователь не наиден по сертификату элен	>	-	Правило \$(SUBJECT.E) \$(SUBJECT.E)	+ Добає Отмена	з з
Intradiation	создавать учетную запись, ек рибут mail uld	сли пользователь не наиден по сертификату элен	v		Правило \$(SUBJECT.E) \$(SUBJECT.E)	+ Добае Отмена	алана Сохрани
h m haur m	создавать учетную запись, ек pибут mail uid	сли пользователь не наиден по сертификату элен	v		Правило \$(\$UBJECT.E) \$(\$UBJECT.E)	+ Добае Отмена	з з
Загрузите сертификаты удостоверяющих центров (СА), подтверждающих подлинность ключей электронной подписи пользователей.	создавать учетную запись, ек pибут mail uid ииd	сли пользователь не наиден по сертификату элен	Y	•	Правило \$(SUBJECT.E) \$(SUBJECT.E)	+ Добае Отмена	сохрани
ажите путь к сертификату для загрузки	оздавать учетную запись, ек рибут mail uld тификаты Загрузите сертификаты удо	сли пользователь не наиден по сертификату элен	у у х подлинно	= = = = = = = = = = = = = =	Правило \$(SUBJECT.E) \$(SUBJECT.E) ключей электронной подписи пользователей.	+ Добае Отмена	ить атриб
Обзор Загрузить	создавать учетную запись, ек рибут mail uid ии Загрузите сертификаты удо жите путь к сертификату до	сли пользователь не наиден по сертификату элек остоверяющих центров (СА), подтверждающи ия загрузки	у у	сто сто с	Правило \$(SUBJECT.E) \$(SUBJECT.E) Ключей электронной подписи пользователей.	+ Добае Отмена	Сохрани
-	оздавать учетную запись, ек рибут mall uid uid Загрузите сертификаты удо жите путь к сертификату дл	сли пользователь не наиден по сертификату элен остоверяющих центров (СА), подтверждающи ия загрузки 2бзор Загрузить	т т	=	Правило \$(SUBJECT.E) \$(SUBJECT.E) Ключей электронной подписи пользователей.	+ Добае Отмена	ить атриб
Период	оздавать учетную запись, ек рибут mail uld загрузите сертификаты уди жите путь к сертификаты уди	сли пользователь не наиден по сертификату элен остоверяющих центров (СА), подтверждающи ия загрузки 2030р Загрузить	у У	= =	Правило \$(SUBJECT.E) \$(SUBJECT.E) ключей электронной подписи пользователей.	+ Добае Отмена	Сохрани
Серийный номер Кому выдан Кем выдан Сонтостовереноший центо Сонтостовереноший ушето Сонтостовереноши у Сонтостовереноши у Сонтостовереноши у Сонтостовереноши у Сонтостовереноши у Сонтостовереноши у Сонтостоверено Сонтостоверено у СонтоС	оздавать учетную запись, ек рибут mail uid загрузите сертификаты удо жите путь к сертификаты удо ките путь к сертификату дл	сли пользователь не наиден по сертификату элен остоверяющих центров (СА), подтверждающи ия загрузки Обзор Загрузить Кому выдан СМ=Тестовый VII РТК (РТЛабс). ОЦ=Улостоволом	 <!--</td--><td></td><td>Правило \$(SUBJECT.E) \$(SUBJECT.E) \$(SUBJECT.E) Ключей электронной подписи пользователей. Ключей электронной подписи пользователей.</td><td>+ добае Отмена Период действия</td><td>х х</td>		Правило \$(SUBJECT.E) \$(SUBJECT.E) \$(SUBJECT.E) Ключей электронной подписи пользователей. Ключей электронной подписи пользователей.	+ добае Отмена Период действия	х х

Рисунок 25 – Настройка входа по электронной подписи

4.2.2. Использование и обновление плагина

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

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

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

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

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

4.3. Настройка входа через внешние сервисы идентификации

Возможен вход с использованием следующих внешних сервисов идентификации:

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

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

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

Вход через внешние сервисы идентификации Для добавления и настройки поставщиков идентификации используйте раздел консоли «Поставщики идентификации».							
Название поставщика	Уникальное название	Тип поставщика					
Google	google_1	google					
Яндекс	yandex_1	yandex					
Facebook	facebook_1	facebook					
VK	vk_1	vk					
Одноклассники	ok_1	ok					
Blitz	blitz_1	blitz					
ESIA	esia_1	esia					
Сбербанк ID	sbrf_1	sbrf					

Рисунок 26 – Включение необходимых внешних сервисов идентификации

4.4. Настройка входа с помощью прокси-аутентификации

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

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

Для корректной работы метода необходимо указать:

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

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

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

рокси-аутентификация				
Чтобы использовать данн пользователя. Метод при обнаружены, то будут исп	ый метод аутентификации, обязат меняется автоматически, если в НТ ользованы другие методы аутенти	ельно долже ТР-заголовка фикации	н быть настроен прокси-сервер, передаюш ах получены необходимые для идентифика	ий в НТТР-заголовках идентификационную информацию ции пользователя данные. Если заголовки не
ТТР-заголовки				
ребуемые НТТР-заголовки	X-SSL-Client-CERT × X-SSL-Client- Для добавления HTTP-заголоак	Serial x X-S а введите его	SL-Client-S-DN x X-SSL-Client-Mail x	
	Укажите названия НТТР-заголовков аутентификации пользователя. Если при любом наборе заголовков	, которые дол и заголовки не	жны присутствовать для проведения е указаны, то аутентификация будет возможна	
НТТР-заголовок с	X-SSL-Client-CERT			
пользователя	Заголовок, в котором передается се идентификация пользователя по ат	ртификат пол рибутам серті	ьзователя. Если указан, то возможна ификата	
Для корректной работы п альтернативных правил. Для обозначения заголов сравниваться с атрибутом Если насторено систыван	рокси-аутентификации укажите, ка ков используйте строки подстанов I сп в хранилище данных. ис стимичата из опревеленного з	кие НТТР-заг ки. Наприме	оловки соответствуют каким атрибутам в и p. правило cm=\$(HTTP_X_SSL_CLIENT_ON) о можио мастлонть правила соответствия по	сточнике данных. Вы можете создать несколько значает, что заголовок <u>HTTP_X_SSL_CLIENT_ON</u> будет дой голтификата и атрибитов в урадионние ваниску
используя строки подстан Посмотреть строки подста	ие се паряката из определенного з ювки. ановки для X509 сертификата.	aronoska, ro	иолно настроить правила соответствия по	лея сертнулкага п атрябутов в храплилице далнах,
mail	:		X-SSL-Client-Mail	×
				+ добавить условие
				+ добавить альтернативное правило
				Отмена Сохранита

Рисунок 27 – Настройка входа с помощью прокси-аутентификации

4.5. Настройка входа с помощью сеанса операционной системы

Способ входа с использованием сеанса операционной системы позволяет пользователям не проходить дополнительно идентификацию и аутентификацию в Blitz Identity Provider, если они ранее вошли со своего ПК в сеть организации и прошли идентификацию и аутентификацию в операционной системе (вошли в сетевой домен). Такие пользователи получат 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 контролера домена (Kerberos-сервера).
- 2. Настройки в консоли управления Blitz Identity Provider.
- 3. Настройки браузеров пользователей.
- 4. Настройки запуска приложений Blitz Identity Provider.
- 5. Настройки веб-сервера.

4.5.1. Настройки контроллера домена (Kerberos-сервера)

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

	kerbe	eros-se	so Prop	ertie	5		_
Organization M	ember Of	Passwo	ord Replica	ation	Dial-in	En	vironmen
Sessions Ren	note control	Ren	note Deskt	op Se	rvices Pro	file	COM+
General Addr	ess Acc	ount	Profile	Tel	ephones	D	elegation
User logon name:							
HTTP/SSO.EIS.	RU		@region.	.ru			~
User logon name	(pre-Windov	vs 2000)	:				10
REGION			krb-sso				
Unlock accou	nt						
Unlock account options:	nt os DES enc nt supports f	ryption ty Kerberos	vpes for thi : AES 128	s acco bit end	ount		^
Unlock account options:	nt os DES enc nt supports f nt supports f irre Kerberos	ryption ty Kerberos Kerberos	ypes for thi : AES 128 : AES 256 nentication	s acco bit eno	ount cryption. cryption.		~
Unlock account Account options: Use Kerber This account This account Do not reque Account expires	nt os DES enci nt supports f nt supports f irre Kerberos s	ryption ty Kerberos Kerberos : preauth	vpes for thi AES 128 AES 256 nentication	s acco bit eno bit eno	ount cryption. cryption.		
Unlock account Account options: Use Kerber This account This account Do not requ Account expires Never	nt os DES enc nt supports f nt supports f irre Kerberos	ryption ty Kerberos Kerberos : preauth	vpes for thi AES 128 AES 256 ventication	s acco bit eno bit eno	ount syption. syption.		~
Unlock accou Account options: Use Kerber This accou This accou Do not requ Account expires Never End of:	nt os DES enc nt supports h nt supports h ire Kerberos 13 сент	ryption ty Kerberos Kerberos : preauth ября 20	vpes for thi AES 128 AES 256 mentication	s acco bit eno	ount sryption. sryption.		× ×

Рисунок 28 – Свойства Kerberos

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

Пример настройки:



Рисунок 29 - Настройка политик шифрования

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

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

Параметры команды ktpass:

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

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

4.5.2. Настройки в консоли управления Blitz Identity Provider

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

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

При необходимости можно:

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

Настройки субъекта службы Kerberos (SPN)						
Загрузите файл таблицы ключей (keytab), сгенерированный для субъекта службы Kerberos HTTP/bip-dev1.reaxoft.loc						
Укажите путь к файлу ключей для загрузки						
Обзор Загрузить						
Файл ключей SPN	Субъект службы Kerberos					
bip-dev.keytab	HTTP/bip-dev1.reaxoft.loc@LAB.REAXOFT.LOC					

Рисунок 30 – Keytab-файл успешно загружен

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

Правила соответствия			
Для корректной работы входа по сеансу опе операционной системы. Вы можете создать Для создания правила используйте строки п сеанса операционной системы, будет сравн Посмотреть строки прастановки	рационной системы укажит несколько альтернативных юдстановки. Например, пра иваться с атрибутом userPr	re, каким атрибутам в источнике данных с правил. вило userPrincipalName=\${username}@\${ incipalName в хранилище данных.	оответствуют имя и домен пользователя из текущего сеанса domain} означает, что имя пользователя с доменом из
sAMAccountName	\$	\$(username)	×
			+ добавить условие + добавить альтернативное правило
			Отмена Сохранить

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

записи в хранилище

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

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

Дополнительные настрой	ки		
Время задержки перед запуском метода	5		
	Количество секунд, в течение которых пользователь может переключиться на другой метод аутентификации		
Время ожидания получения токена	5		
	Количество секунд ожидания получения токена. По окончанию периода возвращается сообщение об ошибке		
		Отмена	Сохран
		Officia	

Рисунок 32 – Дополнительные настройки

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

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

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

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

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

4.5.3. Настройки браузеров пользователей

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

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

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

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

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

Для Microsoft Internet Explorer нужно задать следующие настройки:

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

ternet C	Options						?	\times	2 4	ocal intr	ranet					
General	Security	Privacy C	ontent	Connectio	ons Pr	rograms	Advance	ed		<u>ا</u> ا	Use the settings be the local intranet z	low to de one.	efine whi	ch website	s are ind	cluded in
Select a	a zone to v	iew or chan	je securi	ty settings	i.					[Automatically de	etect intr	anet netv	vork		
6					6	0					Include all lo	ocal (intra	anet) site	s not listed	l in othe	r zones
Inte	ernet	Local intrane	t Trust	ted sites	Restrict	ted sites					Include all s	ites that	bypass th	e proxy se	erver	
											🗹 Include all n	etwork p	aths (UN	Cs)		
١	Local in This zor found o	n tranet ne is for all w n your intrar	ebsites t et.	hat are		S	ites		У	Vhat are	intranet settings?	Adv	anced	O	<	Cancel
									-							
Securit Allo	ity level for owed levels	this zone for this zon	e: All						L	ocal inte	ranet					×
Allo	ity level for owed levels (i	this zone for this zon dium-low Appropriate ntranet) Most conten Unsigned Ac Same as Me	e: All for webs : will be tiveX cor	iites on yo run withou ntrols will el without	ur local ut prom not be o	network npting you download	u Jed			ocal intr	You can add and this zone will use the sone will use the sone will use the sone will use the sone sone sone sone sone sone sone son	remove v the zone' ne:	vebsites f 's security	rom this z	one. All	× websites in
Allo	ity level for owed levels (i Enable P	this zone for this zon fium-low Appropriate ntranet) Most conten Unsigned Ac Same as Me rotected Moc	e: All for webs : will be tiveX cor dium leve e (require	ites on yo run witho ntrols will el without res restart	ur local ut prom not be o prompt	network npting you download ts ernet Exp	u ded blorer)		La A	Add this	You can add and i this zone will use i website to the zon dp.domain/ru/	remove v the zone' e:	vebsites f 's security	rom this z settings.	one. All	websites in
Securit Allo	ity level for wed levels (i (i Enable Pi	this zone s for this zon dium-low Appropriate ntranet) Most conten Unsigned Ac Same as Me rotected Moc	e: All for webs : will be t tiveX cor dium leve dium leve (requin Cus	ites on yo run witho ntrols will el without res restart stom level.	ur local ut prom not be o prompt ing Inte	network npting you download ts ernet Exp Defau	u ded blorer) It level			Add this https://i	ranet You can add and i this zone will use i website to the zon dp.domain ru/	remove v the zone' e:	vebsites f 's security	rom this z	one. All	× websites in <u>A</u> dd
Securit	ity level for owed levels (i (i Enable P	this zone for this zon dium-low Appropriate ntranet) Most conten Unsigned Ac Same as Me rotected Moc	e: All for webs : will be tiveX cor dium leve dium leve Cus	ites on yo run withon ntrols will el without res restart stom level. Reset al	ur local ut prom not be o prompt ing Inte I zones	network npting you download ts ernet Exp Defau to defau	i ded blorer) It level			Add this https://i	You can add and i this zone will use t website to the zon dp.domain[ru/ s:	remove v the zone' te:	vebsites f 's security	rom this z settings.	one. All	× websites in Add Remove
Securit Allo	ity level for owed levels (ii - - - - - - - - - - - - - - - - - -	this zone for this zon fium-low Appropriate ntranet) Most conten Unsigned Ac Same as Me rotected Moc	e: All for webs : will be i tiveX cor dium leve dium leve (requin Cus	ites on yo run withou trols will el without res restart stom level. Reset al your syste	ur local ut prom not be o prompl ing Inte I zones m admi	network npting you download ts ernet Exp Defau to defau inistrator.	i ded blorer) it level It level			Add this https://i	You can add and i You can add and i this zone will use i website to the zon dp.domain[ru/ ::	remove v the zone'	vebsites f	rom this z	one. All	> websites in Add Remove
Securit Allo	ity level for owed levels (i - - - - - - - - - - - - - - - - - -	this zone s for this zon fium-low Appropriate ntranet) Most conten Unsigned Ac Same as Me rotected Moc	e: All for webs : will be i tiveX cor dium leve de (requin Cus aged by y	ites on yo run withon htrols will el without res restart itom level. Reset al your syste K	ur local ut promp not be o prompt ing Inte I zones m admi Car	network npting you download ts ernet Exp Defau to defau inistrator.	u Jed blorer) It level It level	oly		Add this https://i Websites	ranet You can add and i this zone will use i website to the zor dp.domain/ru/ :: ::	remove v the zone" ee:	vebsites f 's security s:) for all	rom this z settings.	one. All	X websites in Add Remove
Securit Allo	ity level for wwed levels (i - - - - - - - - - - - - - - - - - -	this zone a for this zon fium-low Appropriate ntranet) Most conten Unsigned Ac Same as Me rotected Moc	e: All for webs tiveX cor dium leve (requin Cus aged by y	ites on yo run withou trols will el without res restart itom level. Reset al your syste K	ur local ut prom prompt ing Inte I zones m admi Car	network apting you download ts ernet Exp Defau to defau inistrator.	i ded blorer) it level it level	bly		Add this https://i	ranet You can add and i this zone will use i website to the zor dp.domain/ru/ :: ::	remove v the zone' ee: on (https	vebsites f 's security s:) for all	rom this z settings. sites in thi	one. All	× websites in Add

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

Security Settings - Local Intranet Zone	×
Settings	
 Enable Allow websites to prompt for information using scripted windows Disable Enable Enable XSS filter Disable Enable Scripting of Java applets Disable Enable Scripting of Java applets Disable Enable Prompt User Authentication Automatic logon only in Intranet zone Automatic logon with current user name and password Prompt for user name and password 	
Reset custom settings	
Reset to: Medium-low (default) ~ Reset	
OK Cancel	

Рисунок 34 – Настройки Internet Explorer для Kerberos – включение

встроенной идентификации

Для Mozilla Firefox нужно задать следующие настройки:

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

4.5.4. Настройки запуска приложений Blitz Identity Provider

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

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

4.5.5. Настройки веб-сервера

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

Рекомендуемые значения буферов для nginx приведены ниже:

proxy buffer size 16k; proxy buffers 4 16k; proxy_busy_buffers_size 16k; client_body_buffer_size 16K; client_header_buffer_size 16k; client_max_body_size 8m; large_client_header_buffers 2 16k;

4.6. Настройка входа с помощью кодов подтверждения

Можно использовать отправляемые в мобильное приложение push-уведомления или

SMS-сообщения для проверки:

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

Для использования кодов подтверждения необходимо:

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

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

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

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

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

Подтверждение о	с помощью кода			
Первый фактор	Второй фактор			
Для корректной атрибуту в источ логина. Ввод ло Для создания п введенная поль Посмотреть стр	идентификации пользов ннике данных он соответ гина не чувствителен к р завила используйте стро зователем, будет сравни хоки подстановки	ателя укажи ствует. Вы м егистру. ки подстано ваться с атр	ите, каким образом дол можете создать нескол овки. Например, прави рибутом <mark>см</mark> в хранили	лжен формироваться логин и какому ько альтернативных правил определения ло cn=\${login} означает, что строка, ще данных.
mobile			\${login}	×
				+ добавить условие
				+ добавить альтернативное правило
Тараметры кодоі	з подтверждения			
Длина	6			
	Количество символов в к	оде подтвер	ждения	
Время действия	120			
	Количество секунд, посло перестает действовать. Н	е которого ко Чеобходима	од подтверждения отправка нового кода	
Количество	3			
попыток	Количество неудачных по Если количество попытон нового кода	опыток ввода к превышено	а кода подтверждения. о, требуется отправка	
способы отправи Настройте спосо	ки кода обы отправки кодов подт	верждения.	Если будет выбрано (Золее одного способа, то первый будет
рассматриватьс Отправлять	я как основной, а осталы	ные как рез	ервные. Атрибут с контактом	
Push-уведомлен	ие	~	\${mobile}\${guid}	×
SMS		~	\${mobile-}	×
				+ Добавить способ отправки
				Отмена Сохранить
Ірофили настро	йки метода			
Для каждого фа использованы д Преобразовать	ктора используется свой ля единого профиля. в единый профиль	профиль. Е	3 результате преобразо	ования настройки текущего профиля будут

Рисунок 35 – Настройки входа с помощью кода подтверждения

4.7. Настройка входа с известного устройства

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

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

Вход с известного устр	ойства
Длительность запоминания устройства	 Приравнять использование этого метода к применению первого и второго фактора. Если опция включена, то вход с известного устройства будет означать, что пользователь прошел двухфакторную аутентификацию 30 Количество дней, в течение которого пользователю не потребуется повторный вход с известного устройства. Изменение будет доступно после перезапуска приложения.
	Отмена Сохранить

Рисунок 36 – Настройка входа с известного устройства

4.8. 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 RFC4226 «HOTP: An HMAC-Based One-Time Password Algorithm»¹⁶.

Для использования НОТР необходимо:

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

¹⁶ Cm.: https://tools.ietf.org/html/rfc4226

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

ля корректной работы в етода указываются при	хода с помощью разового пароля, стенерированного методом НОТР, необходимо указать привязке устройства к учетной записи пользователя (см. раздел "Пользователи").	базовые настройки метода. Специфические настройки
цопустимое отклонение	10	
	Количество последующих кодов, которые могут быть введены для успешного входа	
Отклонение для	100	
Chinapananadan	Величина диапазона, в пределах которого будет произведен поиск кодов при выполнении синхронизации	

Рисунок 37 – Настройки НОТР-аутентификации

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

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

4.9. Подтверждение входа разовым паролем основе времени (ТОТР)

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

Password Algorithm»¹⁷. В качестве таковых могут быть:

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

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

- Допустимое отклонение при проверке кода (количество предыдущих / последующих кодов). По умолчанию оба значения равны 1: пользователь при входе может ввести как текущий код подтверждения, так и следующий или предыдущий (т.е. сгенерированный в соседних временных интервалах). Такая необходимость может возникнуть, например, для компенсации возможной незначительной рассинхронизации серверного времени и времени на TOTP-устройствах пользователей.
- 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.
- Ссылки на приложения-генераторы разовых паролей. Следует указать ссылки на приложения, которые рекомендуется использовать пользователям. Эти ссылки будут предложены пользователю в веб-приложении «Личный кабинет».

¹⁷ Cm.: https://tools.ietf.org/html/rfc6238

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

Разовый пароль на основе	времени (ТОТР)	
Для корректной работы вх указываются при привязке	ода с помощью разового пароля, сгенерированного методом ТОТР, необходимо указать б а устройства к учетной записи пользователя (см. раздел "Пользователи").	азовые настройки метода. Некоторые настройки метода
Допустимое отклонение	1	
(вперед)	Количество последующих по времени кодов, которые могут быть введены для успешного входа	
Допустимое отклонение	1	
(назад)	Количество предыдущих по времени кодов, которые могут быть введены для успешного входа	
 Настройка отображения ге	нераторов разовых паролей	
Атрибут с именем	mail	
пользователя	Имя пользователя будет отображаться в генераторе разовых паролей после привязки	
Название единой системы	Blitz IDP	
	Название системы будет отображаться в генераторе разовых паролей после привязки	
Ссылки на приложения - ге	нераторы разовых паролей	
Укажите для каждой ОС, ка предложено загрузить при	кие мобильные приложения рекомендуется использовать для генерации разовых пароле гложение для данной ОС.	й. Если ссылка не указана, то пользователям не будет
iOS	http://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8	
Android	https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2	
Windows Mobile	https://www.microsoft.com/ru-ru/store/apps/authenticator/9wzdncrfj3rj	
		Отмена Сохранить

Рисунок 38 – Общие настройки ТОТР-аутентификации

4.10. Привязка устройств к учетным записям пользователей

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

4.10.1. Привязка аппаратных брелоков

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

Загрузите файл с данн к своей учетной записи	ыми генераторов одноразовых пар и, указав его серийный номер.	оолей. После загрузки поль:	зователи смогут само	стоятельно привязать НОТ	Р/ТОТР-генерато
Название генератора					
Формат данных	YubiKey Traditional CSV	•			
Файл с данными			Обзор		
	Загрузить				
груженные генерато	ры				
агруженные генераторы	История загрузок				
		_			

Рисунок 39 – Загрузка файлов с описаниями устройств генерации кодов

Для выполнения загрузки файла нужно задать имя для загружаемый 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).

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

После загрузки файла следует:

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

ве времени (ТОТР)	
Серийный номер устройства генерации разовых паролей	
	Поивязать
	Серийный номер устройства генерации разовых паролей

Рисунок 40 – Привязка аппаратного ТОТР-генератора

4.10.2. Привязка мобильного приложения

Для привязки мобильного приложения следует:

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

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

Генератор паролей на осн	ове времени (ТОТР)	
Название генератора	GoogleAuthenticator	
Алгоритм шифрования	SHA1 Y	
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	NAWGF7K7DXV75DH2SFCMBOSBUPVJ2CQG	
		Сохранить

Рисунок 41 – Привязка мобильного приложения, генерирующего ТОТР-коды

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

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

Для этого необходимо:

- настроить и включить метод аутентификации «Подтверждение с помощью кода».
 Необходимо задать:
 - длину кода подтверждения;
 - время его действия;
 - количество допустимых попыток;

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

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

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

При необходимости перейти к единым настройкам следует перейти по ссылке «Преобразовать в единый профиль» в блоке «Профили настройки метода».
Первый фактор	Второй фактор			
араметры кодо	в подтверждения			
Длина	6	гержления		
	Количество символов в коде под	Борлдония		
Время действия	120 Количество секунд. после которо	го код подтверждения		
	перестает действовать. Необход	има отправка нового кода		
Количество	3			
nonbrok	Количество неудачных попыток в Если количество попыток превыц нового кода	вода кода подтверждения. цено, требуется отправка		
пособы отправ Настройте спос рассматриватьс	ки кода обы отправки кодов подтвержден я как основной, а остальные как	ния. Если будет выбрано бол резервные.	пее одного способа, то г	первый будет
пособы отправ Настройте спос рассматриватьс Отправлять	ки кода обы отправки кодов подтвержден я как основной, а остальные как	ния. Если будет выбрано бол резервные. Атрибут с контактом	тее одного способа, то г	первый будет
пособы отправ Настройте спос рассматриватьс Отправлять Push-уведомлен	ки кода обы отправки кодов подтвержден я как основной, а остальные как ие	ния. Если будет выбрано бол резервные. Атрибут с контактом \${mobile}\${guid}	ве одного способа, то г	первый будет
пособы отправ Настройте спос рассматриватьс Отправлять Push-уведомлен SMS	ки кода обы отправки кодов подтвержден я как основной, а остальные как ие ~	ния. Если будет выбрано бол резервные. Атрибут с контактом \${mobile}\${guid} \${mobile-}	ве одного способа, то п	первый будет
пособы отправ Настройте спос рассматриватьс Отправлять Push-уведомлен SMS	ки кода обы отправки кодов подтвержден я как основной, а остальные как ие	ния. Если будет выбрано бол резервные. Атрибут с контактом \${mobile}\${guid} \${mobile-}	тее одного способа, то г	первый будет
пособы отправ Настройте спос рассматриватьс Отправлять Push-уведомлен SMS	ки кода обы отправки кодов подтвержден я как основной, а остальные как ие	ния. Если будет выбрано бол резервные. Атрибут с контактом \${mobile}\${guid} \${mobile-}	тее одного способа, то г + Добавить Отм	первый будет
пособы отправ Настройте спос рассматриватьс Отправлять Push-уведомлен SMS	ки кода обы отправки кодов подтвержден я как основной, а остальные как ие	ния. Если будет выбрано бол резервные. Атрибут с контактом \${mobile}\${guid} \${mobile-}	тее одного способа, то г + Добавитъ Отм	первый будет
пособы отправ Настройте спос рассматриватьс Отправлять Ризh-уведомлен SMS	ки кода обы отправки кодов подтвержден ие	ния. Если будет выбрано бол резервные. Атрибут с контактом \${mobile}\${guid} \${mobile-}	тее одного способа, то п + Добавитъ Отм	первый будет

Рисунок 42 – Настройки кодов подтверждения для двухфакторной аутентификации

4.12. Коды подтверждения, отправляемые по электронной почте

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

Для этого 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. 12.3).

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

Іодтверждение (с помощью электронной почты		
араметры кодо	в подтверждения		
Длина	6		
	Количество символов в коде подтверждения		
Время действия	300		
	Количество секунд, после которого код подтверждения перестает действовать. Необходима отправка нового кода		
Количество	10		
попыток	Количество неудачных попыток ввода кода подтверждения. Если количество попыток превышено, требуется отправка нового кода		
араметры отпра	звки		
Атрибут с	\${mail-}		
контактом	Выражение, по которому будет формироваться адрес электронной почты для отправки кода подтверждения		
		Отмена	Сохрани

Рисунок 43 – Настройки кодов подтверждения, отправляемых по электронной почте

4.13. Подтверждение входа с помощью Duo Mobile

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

Для этого необходимо выполнить настойки на стороне сервиса Duo Security:

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

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

- сконфигурировать метод аутентификации «Duo push-аутентификация» (см. рис. 44).
 Необходимо указать:
 - параметры учетной записи Duo (имя хоста, интеграционный и секретный ключ);
 - параметры взаимодействия:
 - имя пользователя (задается с помощью строки подстановки) это имя будет отображено в Duo Mobile в качестве имени учетной записи;
 - время действия кода активации (в секундах) время, в течение которого действителен код привязки (QR-код);
 - данные для отображения в приложении информация, отображаемая пользователю в Duo Mobile в виде «ключ: значение». Здесь можно передать значение пользовательского атрибута или какое-то фиксированное значение. В качестве значения также можно указать строку \${app} – это позволит отобразить имя приложения, куда пользователь входит;
 - ссылки на загрузку приложения Duo Mobile.
- включить метод «Duo push-аутентификации» в разделе «Аутентификация».

¹⁹ Cm.: https://duo.com/product/multi-factor-authentication-mfa/duo-mobile-app

²⁰ Cm.: https://signup.duo.com/

²¹ Cm.: https://admin.duosecurity.com/

для использова	ния push-аутентификации	ı от Duo Sec	urity необходимо:		
- зарегистриров	ать учетную запись на сай	йте Duo;			
- войти в панел	ь администратора и перей	іти в раздел	Applications;		
- нажать на Pro	tect an Application, среди п	риложений	найти Auth API. После	этого нажать на Protect this Applica	ition
чтобы получить	свой интеграционный и се	екретный кл	юч, а также имя хоста		
етная запись					
Имя хоста (API hostname)	api-ab16e08c.duosecurity.	com			
нтеграционный	•••••	•			
тюч (integration key)					
екретный ключ	•••••				
(secret key)					
араметры взаим	юдействия				
Шаблон имени	\${mail}				
пользователя	Строка подстановки, опред	еляющая им:	я пользователя в		
	запросе на вход. Например	o, "\${mail}"			
ремя действия	86400				
сода активации					
анные для отоб	Время (в секундах), в течен привязки (штрихкод) ражения в приложении	ние которого	действителен код		
анные для отоб При аутентифиі виде "ключ: зна Имя = \${name}	Время (в секундах), в течен привязки (штрихоход) ражения в приложении кации может быть передан чение". Задайте необходим \${surname} позволит перед	ние которого на информа мые ключи и дать ключ и	действителен код ция, которая будет от их значения, использ мя со значением из ат	ображена в мобильном приложени уя строки подстановки. Например, грибутов паme и surname.	ИВ
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан чение". Задайте необходия \${surname} позволит перед	ние которого на информа мые ключи и дать ключ и	действителен код ция, которая будет от их значения, использ кя со значением из а	ображена в мобильном приложени уя строки подстановки. Например, грибутов <mark>пате</mark> и <mark>surname</mark> .	ИВ
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользовател:	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан нение". Задайте необходим \${surname} позволит перед	ние которого на информа мые ключи и дать ключ и =	действителен код ция, которая будет от и их значения, использ мя со значением из ат \${name}	ображена в мобильном приложени уя строки подстановки. Например, грибутов name и surname.	ИВ
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользовател: Вход в:	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан нение". Задайте необходим \${surname} позволит перед	ние которого на информа мые ключи и дать ключ и = =	действителен код ция, которая будет от и их значения, использ мя со значением из ат \${name} Blitz IDP PROD	ображена в мобильном приложени уя строки подстановки. Например, грибутов name и surname. Х	и в
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользовател: Вход в:	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан чение". Задайте необходим §{surname} позволит перед роки подстановки	ние которого на информа мые ключи и дать ключ и = =	действителен код ция, которая будет от и их значения, использ мя со значением из ат \${name} Blitz IDP PROD	ображена в мобильном приложени уя строки подстановки. Например, грибутов name и surname. Х + Добав	ИТЬ
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользовател: Вход в:	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан нение". Задайте необходим §{surname} позволит перед	ние которого на информа мые ключи и дать ключ и = =	действителен код ция, которая будет от и их значения, использ мя со значением из ат \${name} Blitz IDP PROD	ображена в мобильном приложени уя строки подстановки. Например, грибутов name и surname. Х + Добави	ить
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользовател: Вход в:	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан нение". Задайте необходим §(surname): позволит перед роки подстановки	ние которого на информа мые ключи и дать ключ и = =	действителен код ция, которая будет от их значения, использ мя со значением из ат \${name} Blitz IDP PROD	ображена в мобильном приложени уя строки подстановки. Например, грибутов name и surname. Х + Добав	ИТЬ
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользователя Вход в: сылки на прило	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан- нение". Задайте необходим §(surname): позволит перед роки подстановки а жения - Duo Mobile кдой OC, какие мобильные	ние которого на информа мые ключи и дать ключ и дать ключ и = = =	действителен код ция, которая будет от и их значения, использ мя со значением из ат \${name} Blitz IDP PROD	ображена в мобильном приложени уя строки подстановки. Например, грибутов name и surname.	ить
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользовател: Вход в: Вход в: Сылки на прило Укажите для каз Если ссылка не	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан- нение". Задайте необходим §(surname): позволит перед роки подстановки а жения - Duo Mobile кдой OC, какие мобильные указана, то пользователян	ние которого на информа мые ключи и дать ключ и дать ключ и = = = =	действителен код ция, которая будет от и их значения, использ мя со значением из ат \${name} Blitz IDP PROD	ображена в мобильном приложени уя строки подстановки. Например, грибутов name и surname.	ить
анные для отоб При аутентифии виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользователя Вход в: Сылки на прило Укажите для каз Если ссылка не IOS	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан- чение". Задайте необходия у(surname) позволит перед- юки подстановки а жения - Duo Mobile кдой OC, какие мобильные указана, то пользователян https://itunes.apple.com/ru	ние которого на информа мые ключи и дать ключ и адать ключ и = = = = =	действителен код ция, которая будет от их значения, использ ка со значением из ат \${name} Blitz IDP PROD вlitz IDP PROD	ображена в мобильном приложени уа строки подстановки. Например, грибутов name и surname.	ить
анные для отоб При аутентифии виде "ключ: зна имя = \${name} Посмотреть стр Имя пользовател: Вход в: Сылки на прило Укажите для каз Если ссылка не iOS Android	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан- нение". Задайте необходия у(surname) позволит перед юки подстановки а жения - Duo Mobile кдой ОС, какие мобильные указана, то пользователян https://itunes.apple.com/ru https://play.google.com/sta	ние которого на информа мые ключи и дать ключ и дать ключ и = = = = = = = = = =	действителен код ция, которая будет от их значения, использ кма со значением из ат \${name} Bitz IDP PROD Bitz IDP PROD Bitz IDP PROD ipeдложено загрузить bile/id422663827 ils?id=com.duosecurity.	ображена в мобильном приложени уа строки подстановки. Например, грибутов name и surname.	и в в
анные для отоб При аутентифи виде "ключ: зна Имя = \${name} Посмотреть стр Имя пользовател: Вход в: Вход в: Зылки на прило Укажите для каз Если ссылка не iOS Android Nindows Mobile	Время (в секундах), в течен привязки (штрихкод) ражения в приложении кации может быть передан- чение". Задайте необходия §(surname) позволит перед- юки подстановки а жения - Duo Mobile кдой ОС, какие мобильные указана, то пользователян https://itunes.apple.com/ru https://play.google.com/stu	ние которого на информа мые ключи и дать ключ и дать ключ и = = = = = = = = = = - - - - - - - - -	действителен код ция, которая будет от их значения, использ кма со значением из ат \${name} Вitz IDP PROD Вitz IDP PROD вitz IDP PROD is рекомендуется испо предложено загрузить bile/id422663827 ils?id=com.duosecurity.	ображена в мобильном приложени уя строки подстановки. Например, грибутов name и surname.	И В

Рисунок 44 – Настройки Duo push-аутентификации

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

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

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

- 1. Выбрать способ подтверждения входа «Подтверждение с помощью мобильного приложения Duo Mobile».
- 2. Установить на смартфон приложение Duo Mobile и отсканировать QR-код, а также нажать «Подтвердить».
- После проверки этот метод аутентификации будет добавлен пользователю.
 В консоли управления администратор должен:
- 1. Найти необходимого пользователя.
- 2. Перейти к блоку «Приложение Duo Mobile (QR-код)» и нажать на кнопку «Привязать Duo Mobile».
- 3. Попросить пользователя отсканировать QR-код с помощью мобильного приложения Duo Mobile.

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



Рисунок 45 – Инициирование push-аутентификации



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

4.14. Настройка внешнего метода аутентификации

Blitz Identity Provider позволяет разработчикам при внедрении добавить поддержку своего собственного метода аутентификации. Для этого нужно разработать приложение, peanusyющее логику аутентификации, и подключить этого приложение к Blitz Identity Provider. В Blitz Identity Provider для этого конфигурируется метод аутентификации «Внешний метод аутентификации». Можно peanusoвать 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:

- 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;

- соокіе безопасности название соокіе, в которой будет передаваться идентификатор сессии из внешнего метода.
- 2. На стороне внешнего метода необходимо предусмотреть обработку запросов на аутентификацию и определение применимости согласно документу «Руководству по интеграции».

Добавление вне	шнего метода аутентификации			
Идентификатор	first			
	Уникальное название (идентификатор) внешнего метода аутентификации. Будет использоваться в том числе и в аудите			
URL сервиса	https://extmethod.test.net]		
	Адрес основного сервиса внешнего метода аутентификации. Принимает на вход текущую информацию о процессе аутентификации и возвращает НТТР-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. Еспи 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			
Соокіе безопасности	Вт Название cookie, в которой будет передаваться идентификатор сессии из внешнего метода			
Удалить			Отмена	Обновить

Рисунок 47 – Пример настройки внешнего метода

5. Регистрация приложений

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

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

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

Подключенные приложения	
Sharepoint http://auth2.microsoft.com/adfs/services/trust	× .
JIRA http://jira.reaxoft.ru/secure/Dashboard.jspa	× .
Office 365 urn:federation:MicrosoftOnline	× .
	Добавить приложение

Рисунок 48 – Главный экран настройки приложений

5.1. Создание учетной записи нового приложения

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

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

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

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

Новое приложение		
Идентификатор (entityID,	Укажите идентификатор приложения	
client_id)	Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entitylD) и OAuth (соответствует client_id).	
Название	Укажите название приложения	
	Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider.	
Домен	Укажите домен приложения	
		Отмена Сохраните

Рисунок 49 – Базовые настройки приложения

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

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

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

дентификатор (entityID или	test_app
client_id)	Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (coorsercrayer entryID) и OAuth 2.0 (coorsercrayer client_id).
Название	Тестовое приложение
	Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider
Домен	test.ru
	Ссылка на стартовую страницу приложения, например, http://testdomain.ru/. При TLS-ayreнmeфикации приложения проверяется, что в сергификате приложения указан именно этот домен
Ключ шифрования	*
идентификаторов	Если ключ задан, то идентификатор пользователя для приложения будет зашифрован с использованием данного ключа. Значение ключа можно выбрать на списка. Также можно назначить новый ключ, для этого введите его в строке поиска и нажмите Enter
Шаблон страниц	default ~
	Шаблон страниц определяет внешний вид страниц входа. Если шаблон не указан, то используется шаблон по умогчанию.
ефиксы ссылок возврата	Для добавления нового URL введите его и нажмите Enter
при выходе	Список URL используется для проверки ссылок возврата (post_logout_redirect_uri). Если в запросе на выход указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в выходе будет отказано

Рисунок 50 – Выбор шаблона страницы входа и настройка логаута

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

Протоколы
SAML OAuth 2.0 Simple REST
Протокол SAML не сконфигурирован. Сконфигурировать

Рисунок 51 – Настройка протоколов подключения

Поддерживаются следующие протоколы подключения:

- SAML для подключения приложений по SAML 1.0, 1.1, 2.0 и WS-Federation для идентификации и аутентификации пользователей;
- ОAuth 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 ргоху-сервера, если приложение не поддерживает возможности подключения по SAML/OIDC;
- REST для подключения приложений, использующих REST-сервисы Blitz Identity Provider по регистрации/изменению учетных записей, управлению устройствами аутентификации пользователей.

Если организация планирует разработку или доработку собственных приложений для

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

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

5.2. Настройка SAML и WS-Federation

5.2.1. Подключение по SAML 1.0/1.1/2.0

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

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

Протоколы			
SAML OAuth 2.0 Simpl	e REST		
Метаданные	Стрыть с файловой системы (?xml version="1.0" encoding="UIF-8"?> cmd:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:blitz="urn:blitz:shibboleth:2.0:mdetx" xmlns:blitz="urn:blitz:shibboleth:2.0:mdetx" cmd:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:mdetx" xmlns:blitz="urn:blitz:shibboleth:2.0:mdetx" cmd:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="fals" <cmd:keydescriptor use="signing"> <cmd:keydescriptor use="signing"> <cmd:keydescriptor use="signing"> <cds:ks09data> <cds:ks09certificate> MHICfzcCadegCCQDUgTYycEA+TANBgkqhkiG9w0BAQUFADCBgzELMAkGA1UEBhMC UUUXDANBgWTMAdydBkivc2NVdEPMA0GA1UEBwwGTW9zY293MRAwDgYDVQCKDAdS ZWF4b220MREwDwYDVQQLDAhzemF5dHNldjEQMA4GA1UEAwwHdGVzdC1zcDEbMBkG CSqGSIb3DgEJARYMGGVzdEB0ZNNOLJ1MB4XDTEOMTIMIZSONTEONVOXDTIONTIV <cd></cd></cds:ks09certificate></cds:ks09data></cmd:keydescriptor></cmd:keydescriptor></cmd:keydescriptor>	e" protocolSupp	ortEnumeration="urn:oasis:names:t
SAML профиль	SAML 2.0	Web SSO Profile	WS-Federation Passive Requestor Profile
Подписывать утверждения	always 🗸		
Шифровать утверждения	правило подписи зник-утверждении (sign assentions) пever Правило шифрования SAML-утверждений (Encrypt assertions)		
Шифровать идентификаторы (Namelds)	never v		
	 Включить передачу SAML-утверждений о пользователе в специальном блоке Attribute Statement 		
Атрибуты пользователя Определите, какие атрибуты по	льзователя должны передаваться в приложения и с какими названиями		
SAML-атрибут		Передавать	
LogonName		· •	×
transientId		· •	×
			+ Добавить
			Сохранить

Рисунок 52 – Настройки протокола SAML для приложения

5.2.2. Подключение по WS-Federation

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

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

- указать время жизни утверждений в ответе. Необходимо использовать формат ISO 8601 для указания продолжительности периода²², например, РТ5М – 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	e REST			
Метаданные	Cmppure c dawnosod currensu ((mdi EntityDescriptor xmlnsimd="urn:casis:namestc:SAML:2.0:metadata" (xmlns:saml="urn:casis:names:tc:SAML:2.0:metadata" (xmlns:saml="urn:casis:names:tc:SAML:2.0:metadata" (xmlns:saml="urn:casis:names:tc:SAML:2.0:metadata" (xmlns:saml="urn:casis:names:tc:SAML:2.0:metadata" (xmlns:saml="urn:casis:names:tc:SAML:2.0:metadata" (xml:SPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0:bir (xml:SPSSODescriptor) (xml:SPSSODescriptor) (xml:SPSSODescriptor) (xml:SPSSODescriptor)	/sf-prp dings:1	1.0:protocol"> TTP-POST-wsignin"	
SAML профиль	SAN	/IL 2.0 W	eb SSO Profile WS-Federa	tion Passive Requestor Profile
Подписывать утверждения	always v			
Время жизни утверждений	травило подписи SAML-утверждении (Sign assertions) РТ5М Время жизни утверждений в ответе в формате ISO 8601. Например, РТ5М - 5 минут.			
	☑ Включить передачу SAML-утверждений о пользователе в специальном блоке Attribute Statement			
Атрибуты пользователя Определите, какие атрибуты пол	льзователя должны передаваться в приложения и с какими названиями			
SAML-атрибут			Передавать	
transientId		*		×
upn		~	•	×
				+ Добавить
				Сохранить

Рисунок 53 – Настройки протокола WS-Federation для приложения

5.2.3. Настройка SAML-атрибутов

Для регистрации SAML-атрибутов пользователя в Blitz Identity Provider используется

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

раздел «SAML» консоли управления (Рисунок 54).

Для добавления нового SAML-атрибута необходимо:

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

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

риоуты Определите, какие атрибуты пользователя из хранилища могут переда	ваться в SAML-прилс	жения (поставщики услуг) в виде SAML-атрибутов	
DИСК			Q Найти
UserID	Свойства SAML	-атомбута	
UserMail		(
eduPersonPrincipalName	Название	UseriD	
um:blitzemail	Источник	uid	*
urn:blitz:upn		Сохранить	
um:blitz:givenName			
umblitzish			
urn:blitz:role	Кодировщик		
+ Добавить новый SAML-атрибут	Тип	SAML2String	~
	Название	um:blitz:userid	
	Короткое	userid	
	название		
	Формат имени	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	~
		Удалить	
	Кодировщик		
	Тип	SAML2StringNameID	~
	Название	umblitzuserid	
	Формат имени	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	~
		Удалить	
		+ доби	авить кодировщик
		Удал	ить SAML-атрибут

Рисунок 54 – Создание SAML-атрибутов

5.3. Настройка OAuth 2.0 и OpenID Connect 1.0

5.3.1. Настройка приложения

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

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

умолчанию будет переадресован пользователь после прохождения авторизации (redirect_uri);

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

1		
(client_secret)	Camanauli mana mananana ana ini di si si si	
	ссеринальных конст нарыжительных протизовного (совет) "960161). Если указак то именно этот Секрет должен инстатьзоваться подплоченным приложением при обращения к Bitz Identity Provider	
ополнительный		
cesper	Пополнительный секретный ключ подключаемого припожения	
(cuent_secret)	(client_secre). Если указан, то может использоваться в качеств апьтернативы к основному секрету	
редопределенная ссылка возврата	Введите предопределенный redirect_uri	
(redirect_uri)	URL, на который по умотнанию будет переадресован попьзователь после прохождения авторизации (redirect_un)	
Префиксы	http://localhost = https://sudir.reaxoft.ru =	
скоток возврата	https://yandex.ru =	
	Для добашления нового префикса введите его и нажмите En	
	Профинск используется для проверов ссылок позврата (rodecct_m). Если в запросе на вутитьтификацие уизазная ссылка возврата и она не соответствует не одному из указанных профиксов, то в аутентификацие будет отказано	
Допустимые	*biltz_change_paseword *auto_data_update *usr_grps	
разрешения	*blitz_groups *native *blitz_user_rights *openid	
	<pre>* profile * blitz_rm_rights * esia * blitz_api_user_chg</pre>	
	×bltz_api_sys_users ×bltz_api_sys_users_chg	
	= blitz_api_user	
	Разрешения (scope), которые будут доступны приложение.	
Разрешения по	* openid * profile	
умолчанию	Разрешения (scope), которые будут по умолчанию выданы	
	прыпокинево после авторизация. Если вначения по умотнанию не ухазаны, то в запросе необходина тако прописать требуемые разрешения.	
	Не требовать от пользователя согласие на предоставление	доступа к данным о себе
	Обязательное использование Preof Key for Code Exchange (RFC 7636) для Authorization code gr
Meroz	client secret basic	1
утентификации при обл	Усазанный метод аутентификации должны использовать по пол	E.
и обращения к ервису выдачи маркеров	указанные менад ву сентерикацие дакает на нашавшается при обращении к сорвику въдачи маркеров (token endpoint). При пустом значения доступна все метода	
Допустимые	= um:leff.params:oauth:grant-type.device_code	
grant type	<pre>* refresh_token * client_credentials * implicit</pre>	
	* authorization_code * password	
	Список grant type, которые будут доступны припожению. При пустом списке доступны все grant type	
Roperson	unde utiken uid teken udeuke onde	
response type		
	Снаков теретане туре, которые оудуг доктупны инстансу прытожнени при обращении к URL авторизации (аибиотаtion endpoint). При пустим списки доступны все response type.	
Время жизни маркера доступа		
	Задается каличество секунд через которое кад доступа будет и действителен. Если не задан, то берется из общек настроек.	0
Режим выдачи	offline	
маркеров доступа по умолчанию	Рекоми выдани мартиров достуга (access_token), если явно не указан в запросе. При online-рекоме не выдается мартер обновления (refresh_token)	
Время жизни	36000	
маркера обнояления	Задаятся количноство свяунд через которое код обновления будет на действителен. Если не задан, то берется из общих настроек.	
Добавляемые в	* esia_email * esia_lastName * esia_firstName	
маркер	« esia_mobile » org_oid » esia_inn » org_unit	
(id_token)	« esia_snils » org_title » org_OGRNIP » org_state	
утверждения	* esia_passport * org_INN * org_shortName	
	* org_OGRN * org_name * esia_middleName	
	* esia_birthPlace	
	<pre>x org_fullName = x org_city = x org_type = x org_id x enia_hirthDate</pre>	
	Дополнительные утверждения (claim), которые будут	
	добавлены в маркер идентификации (id_token).	
vice Authorizati	on Grant	
Формат	[0-9](3,3]-[0-9](3,3]-[0-9](3,3]	
иньзовательского кода	Формат указывается в виде шаблена на основе регулярного	
	мерикания, по которний ироисходит пенерация пользовательского лода для превезии устройства. Например. [0-9][2-3]-[0-9][2-3]	
Время жизни	300	
льзовательского кода	Задается колянество секунд через которое пользоватальский код будат не действителен. Если не задан, то берется из общих настроек.	
Ссылка на	https://test.ru/device	
страницу внода	Если соцпка не задана, то она формисиется автоматически	
опьзовательского кода		
пьзовательского кода	🗁 Добавлять в URL пользовательский код	
мьзовательского кода	ල් Добалить a URL попьзовательский код	

Рисунок 55 – Настройки протоколов OAuth 2.0 и OIDC для приложения

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

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

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

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

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

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

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

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

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

5.3.2. Общие настройки OAuth 2.0

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

Свойства					
URL с метаданными Blitz Identity Provider	/sps/oauth/.well-known/openid-configuration При подслючении приложений по OpenID Connect в настройках этих приложений может потребоваться указать эту ссылку на файп с метаданными поставщика идентификации				
URL для авторизации	/sps/oauth/ae На данный URL (authorization endpoint) должен быть направлен запрос на прове пользователя	дение авторизации			
URL для получения и обновления маркера	/sps/oeuth/te На данный URL (token endpoint) должен быть направлен запрос на получение или обновление маркера доступа				
Время жизни маркера доступа, сек	3600				
Формат маркера доступа	opaque	~			
	Аутентификация систем-клиентов с использованием Proxy TLS. Для аутенти Proxy TLS должно быть настроено взаимодействие через прокси-сереер и о установление двустороннего TSL-соединения. В поле Common Name (CN) с должен быть указан домен системы	ыкацык систем по беспечено эртификата системы			
Device Authorization Grant					
Время жизни пользовательского кода в секундах	300				
Минимально разрешенный интервал опроса статуса кода привязки устройства в секундах	ю разрешенный 1 опроса статуса жи устройства в секундах				
Настройка зсорез					
Укажите разрешения (scope получены по этим разрешен	r), которые могут быть запрошены системами (приложениями). При необ ниям	одимости укажите, какие атрибуты пользователя из хр	анилища могут быть		
Название разрешения	Описание	Атрибуты пользователя	Системный		
blitz_change_password	Смена пароля				
userinfo	Основные данные профиля пользователя	×given_name ×email ×sub ×name ×family_name			
native	Получение свя-куюн				
blitz_api_user	Получение всех атрибутов				
			+ Добавить scope		
			Сохранить		

Рисунок 56 – Задание общих настроек OAuth 2.0 / OIDC

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

- «URL с метаданными Blitz Identity Provider» по этой ссылке размещены динамически обновляемые настройки (метаданные) Blitz Identity Provider²⁴. Разработчики приложений могут не прописывать все указанные ниже URL в конфигурации своего приложения, а использовать в настойках единую ссылку на эти метаданные;
- «URL для авторизации» адрес обработчика OAuth 2.0 Authorization Endpoint для запросов через браузер на получение кода авторизации;
- «URL для получения и обновления маркера» адрес обработчика OAuth 2.0 Token
 Endpoint для получения маркеров безопасности (access_token, id_token, refresh_token).
 При необходимости можно:
- изменить «Время жизни маркера доступа», используемое по умолчанию при выпуске маркеров для всех приложений;
- указать «Формат маркера доступа», используемый по умолчанию при выпуске маркеров для всех приложений: строка (opaque) или JWT;
- отметить опцию «Аутентификация систем-клиентов с использованием Proxy TLS». В этом случае должно быть настроено взаимодействие приложений с Blitz Identity Provider через прокси-сервер с установкой двустороннего TSL-соединения. В поле «Common Name (CN)» сертификата системы должен быть указан домен системы подключаемого приложения.

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

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

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

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

атрибуты, передаваемые по этому разрешению²⁵.

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

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

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

5.3.3. Добавление атрибутов в маркер идентификации

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

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

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

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

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

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

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

Таблица 4

п				1			
Inusion	TOTILI IV		ID CONTI	di i i como		D TOIMTO DI LIOU	ΠΛΠΠΙΛΗ
	линных.	попучиемых	M < (`PIII M	шикити	кпнии	электнонной	11()/III//I//
TIPHNEP	динила	moory meenibin	my copin	w	110110 100	Juncici pomnon	подписи
1 1		•	1	1		1	

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

Пример добавляемой в конфигурационный файл структуры:

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

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

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

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

Таблица 5

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

Пример данных, получаемых из ЕСИА

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"
    }
]
```

1

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

Например, следующая запись позволяет определить атрибут custom_attr: "sessionClaims" : ["custom_attr"

5.3.4. Настройка динамической регистрации клиентов OAuth 2.0

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

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

Протоколы	Протоколы				
SAML OAuth 2.0 Simpl	SAUL Oludh 20 Simple REST				
Для корректной работы про	пишите эти ссылки в настройках приложения, в которое будет осуществляться вжод				
URL для авторизации	/sps/cauth/an				
	На данный URL (authorization endpoint) дотжен быть направлен запрос на проекдение авторизации пользователя				
URL для получения и /ses/ceuth/te					
обновления маркера	На данный URL (token endpoint) допжен быть направлен запрос на получение или обновление маркера доступа				
		Статический клиент	Динамические клиенты		

Рисунок 57 – Включение динамической регистрации клиентов

Указать базовые настройки динамической регистрации клиентов:

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

авторизации экземпляров приложения при их регистрации.

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

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

приложения;

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

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

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

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

Настройки динамической регистрации клиентов				
Разрешить динамическую регистрацию клиентов				
Идентификатор приложения	oauth2_test_app			
(software_id)	Используется для регистрации динамических клиентов			
Допустимые к прямой передаче утверждения	*Tirri yczpołiczea (device_type)			
	Эти утверждения допускается указывать в запросе на регистрацию п	инстанса приложения		
		Изменить		
Подписание метаданных пр	иложения			
Подпишите метаданные пр	иложения (software_statement). Эти метаданные передаются в	качестве утверждения в запросе на	регистрацию инстанса приложения	
Версия приложения	2			
	Версия приложения в метаданных должна соответствовать версии в	в первичном маркере		
Префиксы ссылок возврата	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			
Допустимые разрешения	× openid × profile			
	Разрешения (scope), которые будут доступны приложению.			
Истод аутентификации при обращении к сервису выдачи маркеров Client secret basic Указанный метод аутентификации должен использоваться инстансом приложения при обращении к сервису выдачи маркеров (token endpoint)				
Допустимые значения grant	× authorization_code × client_credentials			
type	Список grant type, которые будут доступны инстансу приложения			
Допустимые значения	× code × token			
response type	Список response type, которые будут доступны инстансу приложения авторизации (authorization endpoint)	я при обращении к URL		
Сгенерировать				
Первичные маркеры				
Первичные маркеры исполь	зуются для авторизации инстансов приложения при их регистр	рации		
Идентификатор		Дата создания	Версия ПО	
LP5fobUKu5uPhnZBew2qheePdw sSrHuXisPMWNb5a_gQ8jmg	V5pA_Y2XsJdr5ybNG4QBKF8xqW3epqpbZROE8-	04.06.2019 16:11:34	1	×
			Версия ПО	Выпустить

Рисунок 58 – Настройки динамической регистрации клиентов

5.4. Настройка клиента REST-сервисов Blitz Identity Provider

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

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

- «Пароль» будет использоваться при НТТР Вазіс 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-ауте	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 59 – Настройка приложения для работы с REST-сервисами

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

6. Настройка процедур входа в приложения

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

6.1. Создание процедур входа

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

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 60 – Экран настроек процедур входа

Создание процедуры входа включает в себя следующие шаги:

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

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

дентификатор процесса	ProfileAccess	
	и дентнфикатор процесса должен быть корректинам Јача-идентнфикатором. Java-класк, описывающий процесс входа, будет иметь такое же название.	
Описание	Процедура входа в Личный Кабинет	
	При необходимости укажите комментарий, описывающий особенности и назначение процесса.	.A.
Приложения	» Личный кабинет	
	Список приложений, для которых будет применяться данная процедура входа. Если приложения не указань, то процедура будет считаться глобальной, и применяться в тех случаяи, когда нет процедура для инсеретного приложения. При этом одновременно активированы мяжет быть только одна глобальная процедура, а также не должно быть коллисаний при определении процедуры входа для определенного приложения.	

Рисунок 61 – Экран создания новой процедуры входа

- Написание исходного кода процедуры (Рисунок 62). Для успешной работы процедуры входа необходимо написать на языке Java класс, реализующий необходимый интерфейс Strategy. Вся контекстная информация о пользователе, о текущем состоянии процедуры аутентификации и т.д. доступна в объекте Context. Процедура состоит из двух блоков, которые определяют:
 - действия, предпринимаемые на начальном этапе процесса аутентификации. В этом блоке, например, можно определить, при каких случаях авторизовать пользователя в приложение в режиме SSO (если пользователь ранее был аутентифицирован);
 - действия, предпринимаемые после первичной аутентификации пользователя. В этом блоке, например, можно определить, какие методы двухфакторной аутентификации при каких условиях использовать.
- 3. После написания кода необходимо нажать на кнопку «Компилировать». При наличии ошибок некорректные фрагменты кода будут выделены цветом и подписаны ошибки.
- 4. Если компиляция прошла успешно, можно сохранить процедуру.
- 5. Сохраненную процедуру можно активировать для этого следует нажать на кнопку «Активировать» в шапке соответствующей процедуры.
- 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 удается 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 (secondraforall). 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				
<pre>package com.identitybiltz.idp.flow.dynamic; import jawa.lang.*; import jawa.math.*; import com.identitybiltz.idp.login.authn.flow.Context; import com.identitybiltz.idp.login.authn.flow.StrategyState; import com.identitybiltz.idp.login.authn.flow.StrategyState; import com.identitybiltz.idp.login.authn.flow.StrategyState; import com.identitybiltz.idp.login.authn.flow.StrategyState; import com.identitybiltz.idp.login.authn.flow.StrategyState; import com.identitybiltz.idp.login.authn.flow.StrategyState.*; import com.identitybiltz.idp.login.authn.flow.StrategyState.*; import com.identitybiltz.idp.login.authn.flow.StrategyState.*; public class SecondFAtorAll implements Strategy { private final Logger = LoggeFfactory.getLogger("com.identitybiltz.idp.flow.dynamic"); goverride public StrategyState.Boxet ctx) { return StrategyState.LOGOUT_THEN_MORE(new String[]()); import istate.com.out_THEN_MORE(new String[]()); if (cx.justComplemedFactor) = 2) return StrategyState.BOOEN(); else return StrategyState.BOOEN(); is call strategyState.BOOEN();</pre>				
Компилировать Сохранить				

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

6.2. Примеры процедур входа

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

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

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

6.2.1. Принудительная двухфакторная аутентификация в приложение

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

```
@Override public StrategyState begin(final Context ctx) {
 if(ctx.claims("subjectId") != null) {
  // if the user is already authenticated, then we check the number of factors passed
   if (ctx.sessionTrack().split(",").length < 2)</pre>
     return StrategyState.MORE(new String[]{});
    else
     return StrateqyState.ENOUGH();
  }
  ^{\prime\prime} // if he is not authenticated or passed less than 2 factors, then we require passing 2FA
 else
   return StrategyState.MORE(new String[]{});
@Override public StrategyState next(final Context ctx) {
 // if the user has passed one auth factor, then we require a second one; if more than one - we
sign in to the application
 if(ctx.justCompletedFactor() == 1)
   return StrategyState.MORE(new String[]{});
 else
   return StrategyState.ENOUGH();
}
```

6.2.2. Ограничение перечня доступных методов первого фактора

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

- password вход по логину и паролю;
- х509 вход по электронной подписи;
- externalIdps вход через внешние поставщики идентификации (социальные сети, ЕСИА);
- spnego вход по сеансу операционной системы;
- sms вход по коду подтверждения из SMS-сообщения;
- knownDevice вход по известному устройству.

```
@Override public StrategyState begin(final Context ctx) {
  if(ctx.claims("subjectId") != null)
    return StrategyState.ENOUGH();
  else
    return StrategyState.MORE(new String[]{"password","x509"});
@Override public StrategyState next(final Context ctx) {
 if(ctx.justCompletedFactor() == 1)
    return StrategyState.MORE(new String[]{});
 else {
   String reqFactor = ctx.userProps("requiredFactor");
   if (regFactor == null)
     return StrategyState.ENOUGH();
    else {
     if(Integer.valueOf(reqFactor) < ctx.justCompletedFactor())</pre>
       return StrategyState.ENOUGH();
     else
```

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

```
}
}
```

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

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

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

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

Пример упрощенного варианта процедуры – допуск пользователя в приложение при

условии, что адрес его электронной почты paвeн ivanov@company.ru:

```
@Override public StrategyState begin(final Context ctx) {
 if(ctx.claims("subjectId") != null){
  // if user has been authenticated, than check his email
   if("ivanov@company.ru".equals(ctx.claims("mail")))
     return StrategyState.ENOUGH();
   else
     return StrategyState.DENY;
  1
 else
   // if user has not been authenticated, than ask him to authenticate
   return StrategyState.MORE(new String[]{});
@Override public StrategyState next(final Context ctx) {
  // after attribute validation we should check is the 2FA required or not
 if(!"ivanov@reaxoft.ru".equals(ctx.claims("mail")))
   return StrategyState.DENY;
 String reqFactor = ctx.userProps("requiredFactor");
 if(reqFactor == null)
   return StrategyState.ENOUGH();
 else {
   if(Integer.valueOf(reqFactor) < ctx.justCompletedFactor())</pre>
     return StrategyState.ENOUGH();
   else
     return StrategyState.MORE(new String[]{});
 }
}
```

7. Настройка сервисов самообслуживания пользователей

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

- 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.
- Веб-приложение «Регистрация пользователей». При включении становится доступен переход со страницы входа на форму самостоятельной регистрации (ссылка «Нет аккаунта? Зарегистрироваться»).
- 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 самооб	служивания	
Регистрация		Восстановление доступа
Самостоятельная Перейти к настрой	регистрация пользователей. кам	Самостоятельное восстановление доступа посредством отправки ссылки на адрес электронной почты или кода подтверждения в SMS-сообщении. Перейти к настройкам
Личный кабинет		
Возможность реда усиленную аутенти безопасности. Перейти к настрой	ктировать свои данные, включить кфикацию, изменить настройки кам	
Общие настройкі	1	
регистрации пол мобильного тели	подтверждения, отправляемого в SN	к учетной записи, а также при изменении номера Личный кабинет.
Длина	6	
	Число символов в коде подтверждения	
Время действия	300 Количество секунд, после которого код пери	естает действовать
Количество попыток	3 Количество неудачных попыток ввода кода Если количество попыток превышено, треб нового кода	подтверждения. уется отправка
Параметры кода	подтверждения, отправляемого по з	лектронной почте
Длина	6	
	Число символов в коде подтверждения	
Время действия	3600 Количество секунд, после которого код пери	естает действовать
		Сохранить

Рисунок 63 – Сервисы самообслуживания и их общие настройки

В подразделах осуществляется настройка каждого сервиса самообслуживания в отдельности.

7.2. Личный кабинет

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

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

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

7.2.1. Отображение атрибутов пользователя

На основной странице Личного кабинета отображается блок с данными учетной записи. Пример этого блока представлен на рис. 64.

🕑 Blitz Profil	kgavrilov@reaxoft.ru	ወ		
В Основные данные	С Безопасность	Особытия		
Личный кабинет / Основные данные				
Данные учетной записи				
Фамилия		Гаврилов		
Имя		Константин		
Электронная почт	а	kgavrilov@reaxoft.ru		

Рисунок 64 – Личный кабинет: данные учетной записи

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

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

кабинете вводить и редактировать данные о себе.

В шаблоне доступны следующие функции:

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

В этих функциях используются следующие параметры:

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

Примеры функций:

Отображение атрибута mail:

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

Отображение атрибута mobile с возможностью его редактировать:

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

Отображение булевого атрибута info с возможностью его редактировать:

@editAsBoolean("info", "Подписка")

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

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

Пример отображения массива строк в интерфейсе Личного кабинета представлен

на рисунке 65.
Отображение массива

Редактирование массива

Акции и бонусные программы Новости компании Дайджест событий за месяц Акции и бонусные программы
 Новости компании
 Дайджест событий за месяц

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

7.2.2. Дополнительные параметры

В качестве дополнительных параметров можно задать:

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

7.3. Регистрация пользователей

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

7.3.1. Форма регистрации

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

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

Пример шаблона для регистрации:

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

Пример отображения указанного шаблона в интерфейсе веб-приложения «Регистрация

пользователя» представлен на рис. 66.

B Identity Blitz		
	Регистрация в Личный кабинет	
	Фамилия	
	Фамилия	
	Имя	
	Имя	
	Номер мобильного телефона	
	+7(999)9999999	
	Адрес электронной почты	
	name@example.com	
	Придумайте пароль	
	Пароль	
	Повторите пароль, чтобы не ошибиться	
	Ваш пароль еще раз	
	Пароль должен состоять не менее чем из 8 символов.	
	Рекомендуется, чтобы пароль состоял из прописных и строчных букв и имел хотя бы одну цифру. Не применяйте пароли.	
	используемые для других сайтов, и пароли, которые можно легко	
	подобрать.	
	Нажимая на кнопку «Зарегистрироваться» вы соглашаетесь	
	с условиями использования	
	Зарегистрироваться	

Рисунок 66 – Пример отображения регистрационной формы

7.3.2. Настройки сервиса регистрации

В качестве настроек можно задать:

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

Скриншот фрагмента страницы настроек регистрации представлен на рис. 67.

Настройки сервиса регистрации	
Хранилище для учетной записи	bip-dldap01
Условия для успешной регистрации	х Писпользовать условия из процедуры регистрации
Укажите атрибуты (помимо обязательных), которые должны быть заполнены для успешной регистрации учетной записи	+ Добавить альтернативное условие
URL внешнего сервиса регистрации	
	Отмена Сохранить

Рисунок 67 – Скриншот настроек сервиса регистрации

7.3.3. Процедура регистрации

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

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

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

7.3.4. Изменение текста условий использования

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

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

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

7.3.5. Восстановление доступа

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

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

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

Восстановление доступ	a
Настройки сервиса вос	тановления
Возможные контакты восстановления доступа	× moile × mail Задайте список атрибутов пользователя, соответствующих возможным контактам пользователя
Возможные атрибуты для поиска	× mail × mobile × snils × login Задайте список атрибутов пользователя, по которым будет осуществляться поиск пользователя Составляться поиск пользователя
🗸 Проверя	ть наличие пользователей, имеющих право менять пароль в найденной учетной записи
🗸 Включи	ь дополнительную проверку для учетных записей с настроенной двухфакторной аутентификацией
Список методов	× email × totp × sms Задайте список методов, которые могут быть использованы для дополнительной проверки
	Отмена Сохранить

Рисунок 68 – Восстановление доступа

8. Вход через внешние поставщики идентификации

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

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

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

Подключенные внешние поставщики ид	ентификации		
Название поставщика	Уникальное название	Тип поставщика	
Google	google_1	google	1
Яндекс	yandex_1	yandex	1
Mail ID	mail_1	mail	1
Facebook	facebook_1	facebook	1
ВКонтакте	vk_1	vk	1
Одноклассники	ok_1	ok	1
Blitz	blitz_1	blitz	1
Госуслуги	esia_1	esia	1
Сбербанк ID	sbrf_1	sbrf	1
Добавить поставщик	a Google Яндекс Mail ID	Facebook ВКонтакте Одноклассники	ECMA C6ep ID Blitz Identity Provider

Рисунок 69 – Вид экрана настройки поставщиков идентификации

8.1. Вход через Google

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

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

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

Базовые настройки Google	
Идентификатор поставщика	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

Рисунок 70 – Базовые настройки поставщика идентификации Google

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

²⁷ CM.: https://console.developers.google.com

	Диспетчер API	Учетные	данные							
¢	Панель управления	to Cka	чать файл JSON	Сбросить секрет клиента	Удалить					
Ш	Библиотека	Идентифии	атор клиента дл	ия Веб-приложение						
	Учетные данные	1.5 S								
		Идентифик	атор клиента	100857675658-17pgvoe9ri	9p8dpst5mbdsl	edbs69n.app	s.googles	isercont	ent.com	
		Секрет кли	ента	9 mon 2016 = 12-01-14						
		Mara costo		3 BOR. 201010 12 12 01 14						
		Название								_
		Paspewer URI victovi (vanpusse	ные источники Java чика клиентского при р. http://*.example.com	iScript иложения для запросов из брау п) и пути (например, http://exan	зера. В этом поле iple.com/subdir). I	не допускаю Если использу	тся подста ется неста	новочны ндартны	е знаки И порт,	
		обязател	но укажите его.							
		Paspewer Intro-//w Paspewer Vicnoris ay nepekanp discryna. I https://	но укажите ero. www.example.com ные URI перенаправ ется для запрособ с авлены после аутент не может содержать i bip-demo2.reaxoft.rx	алення сервера. Здесь необладимо ука ификации в Google. В конце к и общедоступные IP-адроса, отно u/blitz/login/methods/externa	ать путь к разде ему будет автома сительные пути и Ildps/callback/g	ту приложени гически добак неполные UR oogle/google	я, а хотор: ілен код а L.	ий польз вторизац	ователи і ин для	будут
		odisaten http://w Paspeue Kenonsay nepenang docryna.i https://	но укажите ero. www.example.com ные URI перенаправ ется для запросов с с запены после аутент le может содержать i aip-demo2.reaxoft.rc aip-demo2.reaxoft.rc	ілёния зервера. Здесь необхадимо ука «фикация в Google. В конце а н общедоступные IP-адреса, отне u/blitz/login/methods/externa u/blitz/login/externalidps/call	аать путь к разде жу будет автома сительные пути и lidps/callback/g back/google/goo	ty приложени гически добас неполные UP oogle/google ogle_1	я, а хотор: влен код а L. 	ий польз вторизац	обатели і ин для	fygyt × ×
		odisaten http://w Paspewer Vicnonay nepenanp goctyna.i https://i https://	но укажите ero. www.example.com ные URI перенаправ ется для запросов с с залены после аутентъ в мажет содержать и ар-demo2.reaxoft.re ap-demo2.reaxoft.re dp.reaxoft.ru/biltz/6	аления герерал. Здесь необходимо ука фихация в Google. В конце к и общедоступные IP-адреса, отно u/blitz/login/methods/externa u/blitz/login/externalldps/call login/externalldps/callback/g	batь путь к разде ewy будет ватома ckrtchsweid bytw i lidps/callback/g back/google/go	ty приложени пически добас неполные UP oogle/google ogle_1	я, в хотори bheir код а L	ий польз вторизац	ователи і ин для	Gygyt × × ×

Рисунок 71 – Настройки в Диспетчере API Google

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

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

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

езопасность						
Используйте раздел "Учетные данные перенаправления.	" Диспетчера API Google	для :	заполнения указанных ниже параметров. Не забудьте сохра	анить в "Учетных да	нных" указанны	ae UF
URI перенаправления (Redirect URI)	http(s)://sudir.reaxoft.ru/s http(s)://sudir.reaxoft.ru/s	ps/log ps/pro	gin/externalldps/callback/google/google_1/false ofile/social/externalldps/callbackPopup/google/google_1			
	Эти ссылки должны быть корректной обработки ре если вы используете зац	ь прог зульт цище	писаны в настройках поставщика идентификации для атов аутентификации пользователя. Используйте схему https, нное соединение.			
Идентификатор клиента (Client ID)	test					
Секрет клиента (Client secret)	Изменить значение					
зрешения						
Запрашиваемые разрешения	email x profile x					
	Для добавления разреш Укажите перечень разре поставщику идентифика	ения і шениі ции, Г	введите его имя и нажмите Enter й (scope), которые должны быть получены при обращении к Теречень доступных разрешений Google			
дентификация учетных записей Укажите правила соответствия учетны с помощью этих правил будет осущест идентификации. Для создания правила используйте ст указывать в одном правиле несколько пате и surname через пробел.	х записей Biltz Identity Pro вляться поиск учетной з роки подстановки \${attr атрибутов. Например, п	ovide aпис <u>nam</u> равил	r и поставщика идентификации. При первом входе пользов и в Blitz Identity Provider для ее последующего связывания с е}, где attr_name - это имя атрибута, получаемого от поста по CN=\${name} \${surname} означает, что атрибут CN будет (ателя через поставь : учетной записью п авшика идентификаг формироваться из д	цика идентифи оставщика ции. Вы может цвух атрибутов	икаци е
аентификация учетных записей Укажите правила соответствия учетны с помощью этих правил будет осущест идентификации. Для создания правила используйте стр указывать в одном правиле несколько пате и surname через пробел. Предлагать пользователю ввести логин и Для привязки должна быть найдена тольк 2 Требовать ввод пароля, если учетная зап	х записей Biltz Identity Pri вляться поиск учетной з роки подстановки \${attr атрибутов. Например, п паропь для привязки, если ю одна учетная запись по : ись была идентифицирован	ovide аапис аа равил и учет задан	г и поставщика идентификации. При первом входе пользов и в Biliz Identity Provider для ее последующего связывания с e}, где attr_name - это имя атрибута, получаемого от поста по CN-\${name} \${surname} означает, что атрибут CN будет о ная запись не была идентифицирована ным правилам соответствия	ателя через поставц : учетной записью п авшика идентификац формироваться из д	цика идентифи оставщика ции. Вы может вух атрибутов	икаци е
 дентификация учетных записей Укажите правила соответствия учетны с помощью этих правил будет осущест идентификации. Для создания правила используйте стр указывать в одном правиле несколько пате и surname через пробел. Предлагать пользователю ввести логин и Для привязки должна быть найдена толы д Требовать ввод пароля, если учетная зап mail 	х записей Biltz Identity Pri твляться поиск учетной з роки подстановки \${attr атрибутов. Например, п пароль для привязки, если ю одна учетная запись по : ись была идентифицирован	оvide: апис а равил и учет задан на	r и поставщика идентификации. При первом входе пользов и в Blitz Identity Provider для ее последующего связывания с e}, где attr_name - это имя атрибута, получаемого от поста по CH=\${name} \${surname} означает, что атрибут CN будет о ная запись не была идентифицирована ным правилам соответствия = email	ателя через поставь : учетной записью п авшика идентификаг формироваться из д	цика идентифи оставщика ции. Вы можети вух атрибутов	икаци е
 дентификация учетных записей Укажите правила соответствия учетны с помощью этик правил будет осущест идентификации. Для создания правила используйте ст указывать в одном правиле несколько пате и sumame через пробел. Предлагать пользователю ввести логин и Для привязки должна быть найдена тольк Требовать ввод пароля, если учетная зап mail 	х записей Biltz Identity Pr вляться поиск учетной з роки подстановки \${attr атрибутов. Например, п пароль для привязки, если ю одна учетная запись по з ись была идентифицирован	оvide: апис пами равил азадан на	г и поставщика идентификации. При первом входе пользов и в Bilitz Identity Provider для ее последующего связывания с e}, где attr_name - это имя атрибута, получаемого от поста по CN=\${name} \${surname} означает, что атрибут CN будет с ная запись не была идентифицирована ным правилам соответствия = email	ателя через постави ; учетной записью п авшика идентификал формироваться из д + добавить г	цика идентифи оставщика ции. Вы может вух атрибутов (вух атрибутов + добавить усл	икаці е -
антификация учетных записей Укажите правила соответствия учетны с помощью этих правил будет осущест идентификации. Для создания правила используйте ст указывать в одном правиле несколько пате и surname через пробел. Предлагать пользователю ввести логин и Для привязки должна быть найдена тольк Требовать ввод пароля, если учетная зап mail	х записей Biltz Identity Pri твляться поиск учетной з роки подстановки \${attr атрибутов. Например, п пароль для привязки, если ю одна учетная запись по : ись была идентифицирован	руіdе апис равил задан на	г и поставщика идентификации. При первом входе пользов и в Biltz Identity Provider для ее последующего связывания с e}, где attr_name - это имя атрибута, получаемого от поста по CH=\${name} \${surname} означает, что атрибут CN будет с ная запись не была идентифицирована ным правилам соответствия = email	ателя через постави : учетной записью п авшика идентификац формироваться из д + добавить и	цика идентифи оставщика ции. Вы можети вух атрибутов вух атрибутов + добавить усл альтернативное	икаци е -
 дентификация учетных записей Укажите правила соответствия учетны с помощью этих правил будет осущест идентификации. Для создания правила используйте ст указывать в одном правиле несколько пате и surname через пробел. Предлагать пользователю ввести логин и Для привязки должна быть найдена тольк Требовать ввод пароля, если учетная зап mail рибуты Укажите, каким образом должны форм формирования каждого атрибута долж Для создания правила используйте об 	х записей Biltz Identity Prn твляться поиск учетной з роки подстановки \${attr атрибутов. Например, п пароль для привязки, если о одна учетная запись по : ись была идентифицирован ись была идентифицирован со одна учетная сли спо ись была сво по содна сво по содана сво сво по содана сво сво по содана сво сво сво по содана сво сво сво сво сво сво по содана сво	оуіdе апис равил задан на Сольз оавил , где	r и поставщика идентификации. При первом входе пользов и в Biltz Identity Provider для ее последующего связывания с e}, где attr_name - это имя атрибута, получаемого от поста по CH=\${name} \${surname} означает, что атрибут CN будет с ная запись не была идентифицирована ным правилам соответствия = email вуемые в Biltz Identity Provider, на основе данных, получаемь о. attr_name - это имя атрибута, получаемого от поставщика	ателя через поставц ; учетной записью п авшика идентификац формироваться из д + добавить ; « «х от поставщика ид идентификации. Вы	цика идентифи оставщика ции. Вы может вух атрибутов + добавить усл альтернативное ентификации.	икаци е - прави Для ввать
 дентификация учетных записей Укажите правила соответствия учетны с помощью этих правил будет осущест идентификации. Для создания правила используйте ст указывать в одном правиле несколько пате и surname через пробел. Предлагать пользователю ввести логин и Для привязки должна быть найдена толы Требовать ввод пароля, если учетная зап mail укажите, каким образом должны форм формирования каждого атрибута долж Для создания правила используйте об одном правиле несколько атрибутов. Н через пробел. 	х записей Biltz Identity Pri твляться поиск учетной з роки подстановки \${attr атрибутов. Например, п пароль для привязки, если ю одна учетная запись по : ись была идентифицирован ись была идентифицирован ись была сантифицирован быть создано свое пр означение \${attr_name} апример, правило си-s	оуіdе: памо памо задан на 	г и поставщика идентификации. При первом входе пользов и в Biliz Identity Provider для ее последующего связывания с e}, где attr_name - это имя атрибута, получаемого от поста по CII-\${name} \${surname} означает, что атрибут CN будет с ная запись не была идентифицирована ным правилам соответствия = email syeмые в Biliz Identity Provider, на основе данных, получаемы to. attr_name - это имя атрибута, получаемого от поставщика e; {surname} означает, что атрибут CN будет формироват племого значения. Например, правило uid=BIP-\${&random(d еличина (набор цифр и букв латинского алфавита).	ателя через поставы : учетной записью п авшика идентификац формироваться из д + добавить / 	цика идентифи оставщика ции. Вы можети вух атрибутов + добавить усл альтернативное сентификации. и можете указы ов – пате И su инть атрибуту и	повие - повие прави прави инd
 дентификация учетных записей Укажите правила соответствия учетны с помощью этих правил будет осущест идентификации. Для создания правила используйте ст указывать в одном правиле несколько пате и sumame через пробел. Предлагать пользователю ввести логин и Для привязки должна быть найдена толька Требовать ввод пароля, если учетная зап mail рибуты Укажите, каким образом должны форм формирования правила используйте об одном правиле несколько атрибута. Р через пробел. Правило можно использовать для зада значение втр-хохохох, где хохохох – и 	х записей Biltz Identity Pro вляться поиск учетной з роки подстановки \${attr атрибутов. Например, п паропь для привязки, если о одна учетная запись по : ись была идентифицирован ись была идентифицирован ись была свет по : означение \${attr_name} Например, правило си=\$ вния константного или вы случайно сгенерированн	очіdе апис равил задан на ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	r и поставщика идентификации. При первом входе пользов и в Blitz Identity Provider для ее последующего связывания с e; , где attr_name - это имя атрибута, получаемого от поста по CH=\${name} \${surname} означает, что атрибут CN будет о ная запись не была идентифицирована ным правилам соответствия = email email вуемые в Blitz Identity Provider, на основе данных, получаемо to. attr_name - это имя атрибута, получаемого от поставщика e; \${surname} означает, что атрибут CN будет формироват племого значения. Например, правило uid=вIP-\${Brandom(4 еличина (набор цифр и букв латинского алфавита).	ателя через поставц ; учетной записью п авшика идентифика; формироваться из д + добавить ; ых от поставцика ид идентификации. Вы ься из двух атрибуто ;)} позволит присво	цика идентифи оставщика ции. Вы может цвух атрибутов + добавить уси альтернативное центификации. и можете указы DB - пате И зи ить атрибуту и Мастер	якаци е - прави Для ивать ииd
 дентификация учетных записей Укажите правила соответствия учетны с помощью этих правил будет осущест идентификации. Для создания правила используйте ст указывать в одном правиле несколько пате и surname через пробел. Предлагать пользователю ввести логин и Для привязки должна быть найдена тольк Требовать ввод пароля, если учетная зап mail рибуты Укажите, каким образом должны форми формирования каждого атрибута долж Для создания правила используйте об одном правиле несколько атрибутов. Е через пробел. Правило можно использовать для зада значение втр-хососох, где хососох – ч Атрибут LastName 	х записей Biltz Identity Prr вляться поиск учетной з роки подстановки \${attr атрибутов. Например, п пароль для привязки, если о одна учетная запись по з ись была идентифицирован ись была идентифицирован ись была идентифицирован ись была создано свое пр означение \${attr_name} Например, правило civ=\$	очіdе: апис равил аадан на тольз равил , где (пале ая ве	г и поставщика идентификации. При первом входе пользов и в Biltz Identity Provider для ее последующего связывания с e;), где attr_name - это имя атрибута, получаемого от поста no CN=\${name} \${surname} означает, что атрибут CN будет о ная запись не была идентифицирована ным правилам соответствия = email email вуемые в Biltz Identity Provider, на основе данных, получаемы o, attr_name - это имя атрибута, получаемого от поставщика e;) \${surname} означает, что атрибут CN будет формироват племого значения. Например, правило uideBIP-\${&random(a еличина (набор цифр и букв латинского алфавита). Правило \${surame}	ателя через поставц ; учетной записью п авшика идентифика, формироваться из д + добавить ; ых от поставцика ид идентификации. Вы Бся из двух атрибуто ()) позволит присво	цика идентифи оставщика ции. Вы может вух атрибутов + добавить усл альтернативное сентификации. и можете указы ов - пате и su ить атрибуту и Мастер	икаци е - прави Для ввать главе

Рисунок 72 – Дополнительные настройки поставщика идентификации Google

8.2. Вход через Яндекс

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

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

Базовые настройки Яндекс Настройи	и поставщика идентификации Яндекс	
Идентификатор поставщика	yandex_172 Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider	
Название поставщика	Яндекс Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider	
		Далее

Рисунок 73 – Базовые настройки поставщика идентификации Яндекс

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

²⁹ См.: https://oauth.yandex.ru/

указанных выше доступов следует указать login:email, login:info и login:birthday;

- правила, которые будут использоваться для идентификации учетной записи в Яндекс и Blitz Identity Provider. Для создания правила следует использовать строки подстановки \${attr_name}, где attr_name – это имя атрибута, получаемого из 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 mail=\${default_email} означает, что атрибут с именем mail в Blitz Identity Provider будет заполняться значением из атрибута default_email учетной записи Яндекс (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно 120

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.
- В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.3).

езопасность						
Для заполнения используйте данн перенаправления, а также отмети	ные из приложения Янд «ть в разделе Доступы/	(ekc.) API	OAuth. H Яндекс.I	е забудьте сохранить в настройках приложения Паспорта данные, которые необходимо получа	а Яндекс.OAuth ул тъ от Яндекс.	казанные URI
JRI перенаправления (Callback URI)	http(s)://sudir.reaxoft.ru http(s)://sudir.reaxoft.ru /yandex_1	ı/sps ı/sps	/login/ex /profile/s	ternalldps/callback/yandex/yandex_1/false ocial/externalldps/callbackPopup/yandex		
	Эти ссылки должны бо	ыть п	рописань	в параметре Callback URI приложения		
	Яндекс.OAuth для кор Используйте схему ht	ррект tps, (ной обраб если вы и	отки результатов аутентификации пользователя. спользуете защищенное соединение.		
ID приложения	bf75d3b303ae474b957	3678	7b2633c8	1		
Пароль приложения	Изменить значение					
зрешения						
Запрашиваемые разрешения	login:email x lo	ogin:ir	ifo x	login:birthday x		
	Для добавления разро	ешен	ия введи	re его имя и нажмите Enter		
	Укажите перечень раз обращении к поставца	іреші (ику і	ений (sco) дентифи	ре), которые должны быть получены при кации. Перечень доступных для приложения		
	разрешений Яндекс					
тентификация учетных записеи						
записью поставщика идентифика. Для создания правила используйт можете указывать в одном правил двух атрибутов - name и surname v] Предлагать пользователю ввести лог	ге строки подстановки те несколько атрибутов через пробел. пин и пароль для привязки	\${at . Наг и, ес	tr_name} пример, п	, где attr_name - это имя атрибута, получаемог правило СN-\${name} \${surname} означает, что а я запись не была идентифицирована	о от поставшика атрибут СN будет	идентификации г формироватьс:
записько поставиция идентизириа. Пля создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч апредлагать пользователю ввести лог для привязки должна быть найдена тобовать ввод пароля, если учетная тобовать ввод пароля, если учетная	е строки подстановки не несколько атрибутов через пробел. гин и пароль для привязю только одна учетная запи в запись была идентифици	\${at . Наг и, ес: ись по	tr_name} пример, п пи учетна о заданнь ана	, где altr_name - это имя атрибута, получаемог правило CH-\$(name) \$(surname) означает, что а я запись не была идентифицирована м правилам соответствия	о от поставшика атрибут СN будет	идентификации формироватьс:
записько поставщика идентикрика. Для создания правила используйт оконсте указывать в одном правил двух атрибутов – пате и sumarre ч д Предлагать пользователю ввести по) Для привязки должна быть найдена :] Требовать веод пароля, если учетная mail	е строки подстановки пе несколько атрибутов через пробел. пин и паропь для привяжи только одна учетная запи я запись. была идентифиц	\${at: и. Наг и, ес: иров: v	tr_name} пример, п пи учетна о заданны ана	. пре attr_name - это има атрибута, получаемог правило CH-\$(name) \$(surname) означает, что а я запись не была идектифицирована м правилам соответствия \$(default_email)	о от поставшика этрибут СN будет	идентификации • формироватьс:
записью поставщика идентикувия. Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и sumame v 2 Предлагать пользователно ввести ло 2 Предлагать пользователно ввести ло 2 Пребовать ввод пароля, если учетная mail	е строки подстановки пе несколько атрибутов через пробел. пи и паропь для привязки только одна учетная запи я запись была идентифиц	\${at: н. Наг и, ес: иров: ~	tr_name} пи учетна о заданны ана =	, где altr_name - это имя атрибута, получаемог правило Cu-\$(name) \$(surname) означает, что а я запись не была идентифицирована м правилам соответствия \$(default_email)	о от поставшика этрибут СN будет	идентификации • формироватьс: • *
записью поставщика идентикувия. Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и sumarre ч д Придлагать пользователно ввести лог д Пля привязки должна быть найдена д Трибовать ввод пароля, если учетная mail	е строня подстановня пе несколько атрибутов через пробел. гин и пароль для привязю только одна учетная запи я запись была идентифиц	\${at: и, ес: и, ес: иров: ~	tr_name} пример, п о заданны ана =	, где altr_name - это имя атрибута, получаемог правило Cit-S(name) S{surname} означает, что а я запись не была идентифицирована м правилам соответствия S{default_email}	о от поставшина зтрибут СN будет	идентификации с формироватьс: • формироватьс: • формироватьс: • формироватьс: • формироватьс: • формироватьс:
записьон поставиция и дентикувия. Пля создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname и а Предлагать пользователю ввести лог для приеязки должка быть найдена требовать ввод пароля, если учетная mail	е строня подстановки пе несколько атрибутов через пробел. гин и пароль для привязки только одна учетная запи я запись была идентифиц	\${at: н. Наг и, ес: иров: ~	tr_name} пример, п о заданны ана =	, де attname - это имл атрибута, получаемог правило CH-\$(name) \${surname} означает, что а я запись не была идентифицирована м правилам соответствия \${default_email}	о от поставшика атрибут СN будет + добавить а	идентификации формироватьс: + добавить услои пытернативное пр
записью поставиция идентифия Для создания правиля используйт окжете указывать в одном правил двух атрибутов - пате и sumame ч [Придлагать пользователю ввести по] Для привлзи должа быть найдена] Требовать ввод пароля, если учетназ mail	те строня подстановки пе несколько атрибутов через пробел. гин и пароль для привязки только одна учетная запи я зались была идентифиц	\${at: h. Har и, ес: иров: ~	tr_name} пи учетна о заданны ана =	. qqe altr_name - это има атрибута, получаемог правило Си-\$(name) \$(surname) означает, что а я запись не была идентифицирована м правилам соответствия \$(default_email)	о от поставшика птрибут СN будет + добавить а	идентифинации формироватьс: + добавить успол пътернативное пр
записью поставщика идентифика Для создания правиля используйт можете указывать в одном правил двух атрибутов - пате и sumarre и д Предлагать пользователно ввести лог Для привязки должна быть найдена д Требовать ввод пароля, если учетная mail	те строня подстановня пе несколько атрибутов через пробел. 	\${at: наг и, ес: иров: У	tr_name} пример, п о заданны ана =	, пре altr_name - это има атрибута, получаемог правило Си-\$(name) \$(surname) означает, что а я запясь не была идентифицирована м правилам соответствия S(default_email)	о от поставшика прибут СN будет + добавить г	идентификации формироватьс: + добавить усло пытернативное пр
записью поставщика идентициях Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и sumare ч] Придлагать попьзователю ввести ло] Для привизки должа быть найдена] Требовать ввод пароля, если учетка mail рибуты Укажите, каким образом должны ф идентификации. Для формирован	е строня подстановня пе несколько атрибутов через пробел. гин и паропь для привязи только одна учетная запи я запись была идентифиц я запись была идентифиц и каждого атрибута до	\${at: и, ес: ись по иров: ГЫ, И	tr_name} ример, о и учетна ана = спользук о быть с	, пде attr_name - это има атрибута, получаемог правило Cti-\$(name) \${surname} означает, что а я запись не была идентифицирована м правилам соответствия \$(default_email) \$(default_email)	о от поставшика прибут СН будет + добавить а получаемых от п	идентифинации формироватьс: * добавить усло вытернативное пр оставщика
записью поставщика идентициях Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и sumarre ч 2 Прадлагать попьзователно ввести по) Для привлаю должа быть найдена 2 Требовать ввод пароля, если учетна таа! рибутъи Указите, каким образом должона ф для создания правила используйт	е строня подстановня не несколько атрибутов через пробел. 	\${at: и, ес: иров: Гы, и рлжн	tr_name} тример, о о заданны ана = спользус о быть с	, де altr_name - это има атрибута, получаемог правило Cik-S(name) S(surname) означает, что а я запись не была идентифицирована м правилам соответствия S(default_email) S(default_email) имые в Biltz Identify Provider, на основе данных, г оздано свое правило. Ir_name - это имя атрибута, получаемого от по	о от поставшика итрибут СN будет + добавить а получаемых от п ставщика идентъ	идентифинации формироваться * добавить усло пытернативное пр оставщика фикации. Вы
записью поставщика идентикрика Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и зиглате ч а Придлагать попьзователю ввести ло для привлахи должна быть найдена а Требовать ввод пароля, если учетка таа! рибуты Указите, каким образом должны и для создания правила используйт можете указывать в одном правил используйт в сами и правила используйт можете указывать в одном правил использовать правила используйт правном ожном использовать для правило можно использовать для правило можно использовать для	е строня подстановня не несколько атрибутов через пробел. 	\${at: Наг и, ес: наг 	tr_name}; пи учетна о заданны ана = = спользуе о быть с о быть с пользуе о быть с спользуе о быть с спользуе	. пре вttr_name - это имя атрибута, получаемог правило Cit-\$(name) \$(surname) означает, что а я запясь не была идентифицирована м правилам соответствия \$(default_email) \$(default_email) имые в Bitz Identity Provider, на основе данных, г оздано свое правило. (г. рале - это имя атрибута, получаемого от по правило cit-\$(name) \$(surname) означает, что а смого значения. Например, правило ut_ostp-sp	о от поставшика итрибут СN будет + добавить и ставщика идент прибут CN будет (\$eanded(\$) пол са адемита)	идентифинации формироватьс: * добавить усло пытернативное пр оставщика нфикации. Вы формироватьс:
записью поставиция диентирика. Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и виглате ч а Предлагать попьзователю ввести по для привязки должна быть найдена а Требовать ввод пароля, если учетная таа! рибуты Укажите, каким образом должна ф идентификации. Для формирован для создания правила используйт можете указывать в одном правил можете указывать в одном правил можете указивать в одном правил можете указивать в одном правил можете указивать в одном правил правило можно использовать для трибуту ий значение двэ-хоссос Пример атрибуков для малтинга	е строня подстановки не несколько атрибутов через пробел. ини и пароль для привязи только одна учетная запи я запись была идентифиц и ались была и ались была идентифиц и ались была и ались был	\${att и, ес: иров: урор	ст_пане}; пример, п и учетна о заданны ана = спользуе о быть с о быть с о быть с пример, п, qe at пример, п, qe at стенерир	, де altr_name - это има атрибута, получаемог правило Cit-\$(name) \$(surname) означает, что а я запись не была идентифицирована м правилам соответствия \$(default_email) \$(default_email) tr_name - это имя атрибута, получаемого от по правило значения, Например, правило utd=bir-\$ ованная величина (набор цифр и букв латинск	о от поставшика прибут СN будет + добавить а получаемых от п ставщика N дент прибут CN будет (girandom(4)) поз гого алфавита).	идентифинации формироватьс: • х • добавить услог пытернативное пр пытернативное пр ставщика ификации. Вы формироватьс:
записью поставиция идентифика Для создания правиля используйт можете указывать в одном правил двух атрибутов - пате и зиглате ч 2 Предлагать попьзователю ввести по 2 Лля привязки должна быть найдена 3 Требовать ввод пароля, если учетная тай рибуты указите, каким образом должны и идентификации. Для формирован Для создания правила используйт можете указывать в одном правил для создания правило можно использовать для атрибуту ий значение виз-госсос Пример атрибутов для маллинга	те строня подстановки пе несколько атрибутов через пробел. син и пароль для привязи только одна учетная запи я запись была идентифиц я запись была идентифиц и собозначение % cotors че обозначение % catter и е несколько атрибута о чарадния константного х, где хохососс — случая	\${att и, есс иров у Гы, и лате или йно	ст_пане}; пи учетна о заданны ана = спользуу о быть с о быть с о быть с с тенерир	. пре attr_name - это има атрибута, получаемог правило CH-\$(name) \$(surname) означает, что а я запись не была идентифицирована м правилам соответствия \$(default_email) мыме в Biltz Identify Provider, на основе данных, г оздано свое правило. tr_name - это има атрибута, получаемого от по равило CH-\$(name) \$(surname) означает, что а емого значения. Например, правило vide-tito-si ованная величина (набор цифр и букв латинско	о от поставшика прибут СN будет + добавить и получаемых от п ставщика идент птрибут CN будет (keandow(4)) пох ого алфавита).	идентификации формироваться + добавить усло пытернативное пр ставщика формироваться волит присвоит Маскол
залисью поставщика идентициях Для создания правила «спользуйт можете указывать в одном правил двух атрибутов - пате и в читате ч 2 Прадлагать попьзователю ввести по 2 Для привлаю должа быть найдена 3 Трябовать веод пароля, если учетна таіl рибуты Указите, каким образом должны ф идентификации. Для формирован для создания правила используйт можете указывать в одном правит ираку атрибуто наяе и воглаве Прамер атрибутов для малянига Пример атрибутов для малянига	е строня подстановня не несколько атрибутов через пробел. 	\${at: . Наг и, ес: . на иров: . на . на . на . на . на . на . на . на	tr_name} пи учетка о заданны ана = спользук о быть с о быть с о быть с о быть с примел, примел, примел, правии stdefr	, де altr_name - это има атрибута, получаемог правило Cit-\$(name) \$(surname) означает, что а я запись не была идентифицирована м правилам соответствия \$(default_email) мыне в Bitz identity Provider, на основе данных, г оздано свое правило. tr_name - это имя атрибута, получаемого от по правило cit-\$(name) \$(surname) означает, что а емого значения, Например, правило utd-etzr-\$; ованная величина (набор цифр и букв латинсс во	о от поставшика прибут СN будет + добавить а получаемых от п ставщика и дент прибут CN будет (grandow(4)) поз гого алфавита).	идентифинации формироватьс: • добавить услог полернативное пр сставщика ификации. Вы формироватьс: • формироватьс: • формироватьс:
залисью поставиция идентифика Для создания правила «спользуйт можете указывать в одном правия двух атрибутов - пате и зиглате ч ались и создания образом должны ф идентификации. Для формирован для создания правила еспользуйт можете указывать в одном должны ф идентификации. Для формирован для создания правила еспользуйт можете указывать в одном можете и идентификации. Для формирован для создания правила еспользуйт можете указывать в одном изовать и дири атрибутов - пасе изовать изовать а трибуту и/ значение вде-хоссос Пример атрибутов для малямика итрибут mail	е строня подстановка пе несколько атрибутов через пробел. гон и пароль для привизи только одка учеткая запи я запись была идентифиц рормироваться атрибут иля каждого атрибута до не обозначения \${ottr и в каждого атрибута до не осознако в уботс. х. где хохохос. – случай	\${at: н, ес: к, ес: к, наг к, наг к, наг или йно но н наг н н н н н н н н н н н н н	tr_name) пи учетна о заданны ана = спользуе о быть с о быть с о быть с о быть с пример, п ример, п ример, п ример, п стенерир	. де аltr_пате - это има атрибута, получаемог правило Cit-\$(name) \$(surname) означает, что а я запись не была идентифицирована м правилам соответствия \$(default_email) мыме в Biltz identity Provider, на основе данных, г оданно свое правило. tr_name - это имя атрибута, получаемого от по правило Cit-\$(name) \$(surname) означает, что равило сit-\$(name) \$(surname) означает, что емого значения. Например, правило uid=tite; ованная величина (набор цифр и букв латинско во мис_email)	 о от поставшика прибут СN будет + добавить а + добавить а - ставщика иденть ставщика иденть ставщика идента - ставщика идента - ставщика идента - ставщика идента 	идентификации формироватьс: + добавить усло пъдернативное пр оставщика формироватьс: Мастер
залисью поставщика идентификоновуй Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и зиглале ч Предлагать попьзователю ввести по Для привязки должка быть найдена 2 Требовать ввод пароля, если учетка таа! рибуты Указитте, казим образом должны и для создания правила используйт можете указывать в одном правил для создания правила используйт правило можно использовать для атрибути и значение в ла-хоссос Пример атрибутов для малямиса травило можно использовать для атрибути и значение в ла-хоссосос Пример атрибутов для малямиса Кази с создания с создания правило использовать для атрибути с создания правила используйт макете указывать в одном правил Стрибут	е строня подстановки не несколько атрибутов через пробел. гин и пароль для привязи только одна учетная запи я запись была идентифиц рормироваться атрибут изи каждого атрибута од не обозначения §асти- те несколько атрибутов чарадния боел. та да обоел. Та итрибутов чарадния боел. та и обоест са итрибутов чарадния обоел. та и обоест са итрибутов чарадния обоел. та и обоест са итрибутов чарадния обоест. та и обоест са итрибутов на обоест са итрибутов на обоест са итрибутов на обоест са итрибутов на обоест. та и обоест са итрибутов на обоест. на и обоест. на и обоест. на и обоест. на обоест. на обоест. на обоест. на обоест. на обоест. на и обоест. на обоест.	\${at: . Наг и, ес: иров: . наг иров: . наг или йно о . наг или или . наг . на . на . на . на . на . на . на . на	tr_name); пи учетна о заданны ана = спользук о быть с о быть с со быть с со быть с со быть с у), где аt вычисляя сленерир Гравии \${defa}	. que altr_name - это има атрибута, получаемог правило Cit-\$(name) \$(surname) означает, что а я запись не была идектифицирована м правилам соответствия (s(default_email) (default_email) миме в Biltz Identity Provider, на основе данењи, г одано сове правило. сисе правило одано сове правило. сисе правило одано сисе (name) \$(surname) означает, что а вмого значения. Например, правило изd-B2P-5 ованная величина (набор цифр и букв латинесо иut_email) 	о от поставшика прибут СN будет + добавить а получаемых от п ставщика идент прибут CN будет (&random(4)) по: го алфаента).	идентификации формироваться * добавить усло тытерыаливное пр ставщика формироваться волит присвоит волит присвоит мастор
записьо поставиция дентикувия Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и виглате ч 2 Предлагать пользователно ввести по 2 Для привлаю должа быть найдена 3 Требовать ввод пароля, если учетна таll	е строня подстановня не несколько атрибутов через пробел. ини и паропь для привязи только одна учетная запи я запись была идентифиц рормироваться атрибута из каждого атрибута до те обозначение \${ettr. че несколько атрибута че несколько атрибута и несколько атрибута и до со случая задания константного х. где хохохос – случая с с случая	\${at: Har и, есс коров: к	спользууства о заданны о заданны ана = спользууства обыть с обыть с обыть с обыть с обыть с обыть с обыть с обыть с у, де аt пример, п у, де аt п у, де ат и у, де ат и у, де ат п у, де ат и у, де ат и у, де ат и у, де ат и у, де ат и у, де ат и у, де ат у, де ат и у, де ат и у, де ат у, де ат и у, де ат и у у, де ат и у, де ат и и и и и и и и и и и и и и и и и и и	, пре attr_name - это имя атрибута, получаемог правило Cit-\$(name) \$(surname) означает, что а я запась не была идентифицирована м правилам соответствия ((default_email) ((default_email)) (tr_name - это имя атрибута, получаемого от по правило сite(\$(name) \$(surname) означает, что а емого значения. Например, правило utd=115-5 нованная величина (набор цифр и буке латинско и du_email) пате)	о от поставшика ктрибут СN будет + добавить а попучаемых от п ставщика идент тирибут CN будет (брановс(4)) пол ого алфавита).	идентифинации формироватьс: + добавить услог пълернативное пр ставщика ификации. Вы формироватьс: Мастер С. С. С

Рисунок 74 – Дополнительные настройки поставщика идентификации Яндекс

8.3. Вход через Facebook

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

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

Базовые настройки Facebook	
Идентификатор поставщика	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

Рисунок 75 – Базовые настройки поставщика идентификации Facebook

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

³⁰ Cm.: https://developers.facebook.com/apps/

🛞 Тестовый сайт 🔻 II	р приложения: 158755007864887 × View Analytics	基 Инструм	енты и поддержка Документы
Панель			
Настройки	Идентификатор приложения	Секрет приложения	
Основное Дополнитепьно	158755007864887	•••••	Показать
Роли	Отображаемое название	Пространство имен	
Предупреждения	Тестовый сайт		
Проверка приложения	Домены приложений	Эл. адрес для связи	
	bip-demo2.reaxoft.ru × idp.reaxoft.ru ×	gavrilov@socio.msk.ru	
продукты	URI -адрес политики конфиленциальности	URI -алрес Пользовательского со	глашения
Вход через Гасебоок	Политика конфиденциальности для диалога «Вход»	Пользовательское соглашение	для диалога «Вход»
+ Добавить продукт	Значок приложения 1024 x 1024	Категория Бизнес +	
	Веб-сайт	Быс	трое начало работы 🛛 🗙
	URL-адрес сайта		
	http://bip-demo2.reaxoft.ru/		

Рисунок 76 – Настройки в панели Facebook для разработчиков

- 5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 77), которые включают в себя:
 - идентификатор приложения (App ID), полученный в панели Facebook для разработчиков;
 - секрет приложения (App Secret), полученный в панели Facebook для разработчиков;
 - запрашиваемые разрешения (scope), предусмотренные в Facebook³¹;
 - запрашиваемые атрибуты, предусмотренные в Facebook; допустимо указывать только те атрибуты, которые предусмотрены выбранными разрешениями;
 - правила, которые будут использоваться для идентификации учетной записи в Facebook и Blitz Identity Provider. Для создания правила следует использовать строки подстановки \${attr_name}, где attr_name – это имя атрибута, получаемого от Facebook. Можно указывать в одном правиле несколько атрибутов. Например, правило CN=\${name} \${surname} oзначает, что атрибут CN будет сопоставляться с сочетанием двух атрибутов – name и surname через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило.

³¹ Cm.: https://developers.facebook.com/docs/facebook-login/permissions/

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

езопасность						
Для заполнения используйте пане приложения.	пь Facebook для разработ	тчиков. Не	забудьте сохранить в настройках приложени:	я Facebook указані	ный домен	
Домен приложения	sudir.reaxoft.ru					
URL-адреса для перенаправления OAuth	http(s)://sudir.reaxoft.ru/sps http(s)://sudir.reaxoft.ru/sps /facebook_1	s/login/exte s/profile/so	ernalldps/callback/facebook/facebook_1/false cial/externalldps/callbackPopup/facebook			
	Эти ссылки должны быты корректной обработки рез https, если вы использует	прописаны ультатов ау ге защищен	в настройках поставщика идентификации для тентификации пользователя. Используйте схему иное соединение.			
Ідентификатор приложения (Арр ID)	158755007864887					
Секрет приложения (App Secret)	Изменить значение					
зрешения и атрибуты						
Запрашиваемые разрешения	public_profile x ет	nail x ния введит	е его имя и нажмите Enter			
	Укажите перечень разреш обращении к поставщику	јений (scop идентифик	е), которые должны быть получены при ации. Перечень досту <mark>пных разрешений Facebook</mark>			
Запрашиваемые атрибуты	id x name x е	етай х введите ег	о имя и нажмите Enter. Укажите перечень			
	идентификации. Перечень запрашиваются.	доступных	к атрибутов зависит от того, какие разрешения			
центификация учетных записей Укажите правила соответствия уче	идентификации. Перечень запрашиваются. тных записей Biliz identify i хавил билет осуществоть	Рrovider и	атрибутов зависит от того, какие разрешения поставщика идентификации. При первом вход	де пользователя ч	ерез поставщи	1ка
дентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих п записью поставщика идентификац Для создания правила используйт можете указывать в одном правил врух атрибутов - пате и surname ч	идентификации. Перечень запрашиваются. тных записей Biltz Identity I завил будет осуществлять ии. s строия подстановки \${at s несколько атрибутов. На врез пробел.	 доступных Provider и Scя поиск у ttr_name} апример, п 	атрибутов зависит от того, какие разрешения поставщика идентификации. При первом вхо, четной записи в Biltz identity Provider для ее г где attr_name - это имя атрибута, получаемо равило Ct+\${name} \${surname} означает, что	де пользователя ч последующего связ ого от поставщика атрибут СN будет	ерез поставци ывания с учет идентификаци формировать	ика тной ии. В ся и
центификация учетных записей Укажите правила соответствия уче идентификации с помощью этих п записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - name и surname ч 2 Предлагать пользователю ввести пог	идентификации. Перечень запрашиваются.	Provider и ъся поиск у ttr_name}, апример, п	атрибутов зависит от того, какие разрешения поставщика идентификации. При первом вхо, четной записи в Blitz Identity Provider для ее г где attr_name - это нмя атрибута, получаемо равило CN+\$(name) \${surname} означает, что запись не была идентифицирована	де пользователя ч последующего связ ого от поставшика атрибут СN будет	ерез поставщи ыывания с учет идентификаци формировать	ика тной ии. Е ся и
центификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пу записью поставщика идентификац Для создания правила используйт можете указывать в одном правил окжете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести лог] Для привязки должна быть найдена т	идентификации. Перечень запрашиваются. тных записей Biliz identify завил будет осуществлять ии. е строки подстановки \${at е несколько атрибутов. На ерез пробел. ин и пароль для привязки, ес олько одна учетная запись п	- доступных Provider и ься поиск у ttr_name} апример, п сли учетная то заданныя	атрибутов зависит от того, какие разрешения поставщика идентификации. При первом вхо, гчетной записи в Bitz Identity Provider для ее г где attr_name - это ния атрибута, получаемо равило CN+\$(name) \${surname} означает, что и запись не была идентифицирована и правилам соответствия	де пользователя ч последующего связ хго от поставшика атрибут СN будет	ерез поставщи ывания с учет идентификаци формировать	ика гной ии. Е ся и
центификация учетных записей Укажите правила соответствия уче идентификации с помощью этих п записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести лоп] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная	идентификации. Перечень запрашиваются. тных записей Biltz Identify I завил будет осуществлять ии. в строки подстановки \${at в несколько атрибутов. На ерез пробел. ян и пароль для привязки, ес олько одна учетная запись п запись была идентифицирот	 доступных Provider и Бося поиск у ttr_name} апример, п сли учетная то заданныя вана 	атрибутов зависит от того, какие разрешения поставщика идентификации. При первом вхо, метной записи в Biltz Identilly Provider для ее п где attr_name - это имя атрибута, получаемо равило CN+\$(name) \$(surname) означает, что и запись не была идентифицирована и правилам соответствия	де пользователя ч последующего свя: хго от поставщика атрибут СN будет	ерез поставщи ывания с учет идентификаци формировать	ика тной ии. Е
дентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пу записью поставщика идентификац Для создания правила исопьзуйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Трябовать ввод пароля, если учетная mail	идентификации. Перечень запрашиваются.	- доступны) Provider и сля поиск у ttr_name); апример, п апример, п сли учетная но заданныя вана	атрибутов зависит от того, какие разрешения поставщика идентификации. При первом вхо, четной записи в Biltz Identity Provider для ее г где attr_name - это имя атрибута, получаемо равило CN=\$(name) \$(surname) означает, что и запись не была идентифицирована и правилам соответствия \$(email)	де пользователя ч последующего связ хго от поставшика атрибут СN будет	ерез поставщи ывания с учет идентификаци формировать Х	ика тной ии. Е ся и
центификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пу записью поставщика идентификац Для созданта правила исопьзуйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail	идентификации. Перечень запрашиваются.	- доступныр Provider и scя поиск у ttr_name) пример, п по заданныя вана =	атрибутов зависит от того, какже разрешения поставщика идентификации. При первом вко, гчетной записи в Biltz Identity Provider для ее г где attr_name - это нимя атрибута, получаемо равило Ct+\$(name) \$(surname) означает, что и запись не была идентифицирована и правилам соответствия \$(email)	де пользователя ч тоследующего связ эго от поставшика атрибут СN будет	ерез поставщи ывания с учет идентификаци формировать х + добавить усл	ика тной ил. Е ся и
дентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйт можете указывать в одном правила можете указывать в одном правила двух атрибутов - пате и surname ч] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail	идентификации. Перечень запрашиваются. тных записей Biltz Identify I завил будет осуществлять ии. в строки подстановки \$(at в несколько атрибутов. На ерез пробел. ин и пароль для привязки, ес олько одна учеткая запись п запись была идентифицирос	- доступных Provider и ься поиск у ttr_name) апример, п сли учетная то заданныя вана =	атрибутов зависит от того, какже разрешения поставщика идентификации. При первом вхо, четной записи в Biltz Identilly Provider для ее п где attr_name - это имя атрибута, получаемо равило CM+\$(name) \$(surname) означает, что и запись не была идентифицирована и правилам соответствия \$(email)	де пользователя ч последующего связ эго от поставшика атрибут СN будет + добавить аз	ерез поставщи ывания с учет идентификаци формировать + добавить усл пьтернативное п	ика тной ил. Е ся и
дентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пу записью поящика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail	идентификации. Перечень запрашиваются. тных записей Biltz Identity I завил будет осуществлять ии. е строии подстановки \${at е несколько атрибутов. На ерез пробел. ин и паропь для привязки, ес олько одна учетная запись п запись была идентифицирос	- доступныр Provider и scя поиск у ttr_name) апример, п сли учетная вана =	атрибутов зависит от того, какже разрешения поставщика идентификации. При первом вко учетной записи в Biltz Identity Provider для ее г где attr_name - это нимя атрибута, получаемо равило Ct+\$(name) \$(surname) означает, что и запись не была идентифицирована и правилам соответствия \$(email)	де пользователя ч тоследующего связ эго от поставшика атрибут СN будет + добавить а	ерез поставщи ывания с учет идентификаци формировать + добавить усл пытерналивное п	ика тной ил. Е ся и
центификация учетных записей Укаянте правила соответствия уче идентификации с помощью этих пу записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пале и surname ч [Предлагать попьзователю ввести пог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны ф идентификации. Для формировани Для создания правила используйт можете указывать в одном правил двух атрибутов - палес и зиголее ч атрибуту uid значение втр-хоссоог	идентификации. Перечень запрашиваются.	 доступных ргоvider и ься поиск у тример, п спи учетная заданныя заданныя заданныя а заданныя спи учетная тример, п спи учетная спи учетная тример, п 	атрибутов зависит от того, какже разрешения поставщика идентификации. При первом вхо, четной записи в Biltz Identity Provider для ее г где attr_name - это имя атрибута, получаемо равило СN-\$(name) \$(surname) означает, что и запись не была идентифицирована и правилам соответствия \$(email) \$(email) мые в Biltz Identity Provider, на основе данных, здано свое правило. r_name - это имя атрибута, получаемого от п равило CN-\$(name) \$(surname) означает, что мого значения. Например, правило uid=вте- ранная величина (набор цифр и букв латинс	де пользователя ч последующего связ иго от поставшика и атрибут СМ будет + добавить в получаемых от по юставщика иденти атрибут СМ будет \${&random(4)} пози кого алфавита).	ерез поставщи ывания с учет идентификаци формировать + добавить усл пытернативное п пставщика фикации. Вы формировать волит присвои	ика тной ил. В ся и равж
дентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пу записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч Предлагать пользователю ввести лог Пля привязки должна быть найдена т Пребовать ввод пароля, если учетная таш рибуты Укажите, каким образом должны ф идентификации. Для формирован Для создания правила используйт правило можно использовать для атрибут и изначение вля-хососососососососососососососососососос	идентификации. Перечень запрашиваются.	 - доступных - доступных - реоvider и ъся поиск у - спи учетная <li< td=""><td>сатрибутов зависит от того, какже разрешения поставщика идентификации. При первом вко, гчетной записи в Biltz Identity Provider для ее г где attr_name - это имя атрибута, получаемо равило Ct+\$(name) \$(surname) означает, что и запись не была идентифицирована и правилам соответствия \$(email) \$(email) мые в Biltz Identity Provider, на основе данных, здано свое правило r_name - это имя атрибута, получаемого от п равило Ct+\$(name) \$(surname) означает, что мого значения. Например, правило uid=втр раанная величина (набор цифр и букв латинс</td><td>де пользователя ч тоследующего связ эго от поставшика атрибут СN будет + добавить а получаемых от по юставщика иденти атрибут CN будет \$(&random(4)) позі кого алфавита).</td><td>ерез поставщи ывания с учет идентификаци формировать + добавить усл натернативное п кставщика фикации. Вы формировать волит присвои Мастер</td><td>ика тной ил. В ся и рави</td></li<>	сатрибутов зависит от того, какже разрешения поставщика идентификации. При первом вко, гчетной записи в Biltz Identity Provider для ее г где attr_name - это имя атрибута, получаемо равило Ct+\$(name) \$(surname) означает, что и запись не была идентифицирована и правилам соответствия \$(email) \$(email) мые в Biltz Identity Provider, на основе данных, здано свое правило r_name - это имя атрибута, получаемого от п равило Ct+\$(name) \$(surname) означает, что мого значения. Например, правило uid=втр раанная величина (набор цифр и букв латинс	де пользователя ч тоследующего связ эго от поставшика атрибут СN будет + добавить а получаемых от по юставщика иденти атрибут CN будет \$(&random(4)) позі кого алфавита).	ерез поставщи ывания с учет идентификаци формировать + добавить усл натернативное п кставщика фикации. Вы формировать волит присвои Мастер	ика тной ил. В ся и рави
дентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пуче даписью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч Предлагать пользователю ввести лог для привязки должна быть найдена т Требовать ввод пароля, если учетная таil Укажите, каким образом должны ф идентификации Для формировани Для создания правила используйт можете указывать в одном правил каките, каким образом должны ф идентификации. Для формировани Для создания правила использовать для атрибуть и зигалее ч Создания правила использовать для атрибуту и из значение вру атрибуто - паве и и зигалее Правило можно использовать для атрибуту из	идентификации. Перечень запрашиваются.	Ргочіdег и ься поиск у спи учетная по заданный вана = используе! но быть ссе е), где аtt апример, п вычисляе о сгенерири Стенери Стенери Стенерири Стенери Стенерири Стенерири Стенерири С	сатрибутов зависит от того, какже разрешения поставщика идентификации. При первом вхо, четной записи в Bitz Identity Provider для ее г где attr_name - это имя атрибута, получаемо равило Ck-\$(name) \${surname} означает, что и запись не была идентифицирована и правилам соответствия \${email} \${email} мые в Bitz Identity Provider, на основе данных, издано свое правило г_name - это имя атрибута, получаемого от п равило Ch-\${name} \${surname} означает, что мого значения. Например, правило uid=вте- ро	де пользователя ч последующего связ атрибут СN будет + добавить аг получаемых от по оставщика иденти атрибут CN будет \$(&random(4)) поз кого алфавита).	ерез поставщи ывания с учет формировать + добавить усл пьтернативное п ставщика фикации. Вы волит присвои Мастер	ика тной ии. В. ся и: раси ся и: тъ

Рисунок 77 – Дополнительные настройки поставщика идентификации Facebook

8.4. Вход через ВКонтакте

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

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

Базовые настройки VK	
Идентификатор поставщика	vk_1
	Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider
Название поставщика	VK
	Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider
Версия	5.52

Рисунок 78 – Базовые настройки поставщика идентификации ВКонтакте

- 4. Перейти в «Панель VK для разработчиков» (Рисунок 79)³², в которой выполнить следующие операции:
 - войдите с помощью своей учетной записи ВКонтакте;
 - перейти в раздел «Мои приложения»;
 - выбрать пункт «Создать приложение»;
 - выбрать тип создаваемого приложения «Веб-сайт», указать его название, адрес, и домен;
 - в появившемся окне настоек приложения прописать базовый домен приложения (должен совпадать с доменом, на котором установлен Blitz Identity Provider).

³² См.: https://new.vk.com/dev

	Документация Мои приле	жения Поддержка	Правила	Q. Поиск
Blitz-integration	Настройки			
Информация				
Настройки	ір приложения:	5566286		
Хранимые процедуры	Защищенный ключ:	ologi (MCTSS), pp.		
Статистика	Состояние:	Приложение включено	и видно всем 🔍 🗸	
Руководство	Первый запрос к АРІ:			
Помощь				
	Установка приложения:	Не требуется		
	Open API:	Включён		
		Open API:		
	Адрес сайта:	https://bip-demo2.reaxof	ft.ru	
	Тематика сайта:	Выберите тематику	~	
	Базовый домен:	bip-demo2.reaxoft.ru ×	idp.reaxoft.ru 🚿	
	Доверенный redirect URI: Добавить ещё	http://yoursite.com/verif	у	
		Сохранить изменения		

Рисунок 79 – Настройки в панели VK для разработчиков

- 5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 80), которые включают в себя:
 - ID приложения, полученный в панели VK для разработчиков;
 - защищенный ключ, полученный в панели VK для разработчиков;
 - запрашиваемые разрешения, предусмотренные в ВКонтакте³³;
 - правила, которые будут использоваться для идентификации учетной записи в ВКонтакте и Blitz Identity Provider. Для создания правила следует использовать строки подстановки \${attr_name}, где attr_name – это имя атрибута, получаемого от ВКонтакте. Можно указывать в одном правиле несколько атрибутов. Например, правило CN=\${name} \${surname} означает, что атрибут CN будет сопоставляться с сочетанием двух атрибутов – name и surname через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;

³³ Cm.: https://new.vk.com/dev/permissions

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

езопасность						
Используйте раздел "Мон понложе	ния" панели VK пля оз	110.20	THINKO	а по заполнения указанных ниже параметт	ов Не забульте	
ВКонтакте указанные URI перенапр	равления	ispac	101 HIRDE	рани заполнения указанных ниже параметр	лы. не забудыте	coxpaning a nanoni
Bencus	5.52					
Depensi	0.02					
Доверенные redirect URI	http(s)://sudir.reaxoft.ru	i/sps/	login/ex profile/s	ternalldps/callback/vk/vk_1/false social/externalldps/callbackPopup/vk/vk_1		
	корректной обработки	резу	рописані льтатов а	ы в настроиках поставщика идентификации для зутентификации пользователя. Используйте схег	му	
	nttps, если вы исполь	syere	защищ	енное соединение.		
ID приложения	5566286					
Защищенный ключ	Изменить значение					
зрешения						
Запрашиваемые разрешения	email x					
	Для добавления разр	зшені	ия введи	те его имя и нажмите Enter		
	Укажите перечень раз обращении к поставш	реше ику и	ний (sco дентифи	ipe), которые должны быть получены при ікации. Перечень доступных разрешений		
	ВКонтакте					
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правили двух атрибутов – пате и surname ч	тных записей Blitz Iden завил будет осуществл ии. е строки подстановки е несколько атрибутов ерез пробел.	tity Р іятьс \${att . Han	rovider i ся поиск tr_name] iример,	и поставщика идентификации. При первом ; учетной записи в Blitz Identity Provider для и , где attr_name - это имя атрибута, получа правило сN=\${name} \${surname} означает, ч	входе пользоват ее последующег емого от постав что атрибут СN (геля через поставщи го связывания с учет шика идентификаци будет формироваты
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и surname ч Предлагать пользователю ввести лоп ј Для привязки должна быть найдена п) Требовать ввод пароля, если учетная	тных записей Blitz Iden завил будет осуществл ии. е строки подстановки е несколько атрибутов ерез пробел. ин и пароль для привязк олько одна учетная запи запись была идентифиц	tity P іятьс \${att . Нап и, есг сь по ирова	rrovider i ся поиск tr_name] іример, пи учетна задання ана	и поставщика идентификации. При первом ; учетной записи в Blitz Identity Provider для и , где attr_name - это имя атрибута, получа правило cN=\${name} \${surname} означает, ая запись не была идентифицирована ым правилам соответствия	входе пользоват ее последующег емого от постав что атрибут СN I	геля через поставщи го связывания с учет шика идентификаци будет формировать
(ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и surname чи предлагать пользователю ввести лого] Для привязки должна быть найдена т] Требовать ввод пароля, если учеткая mail	тных записей Blitz Iden равил будет осуществл ии. е строки подстановки е несколько атрибутов ерез пробел. ин и пароль для привязк ин и пароль для привязк запись была идентифиц	tity P Iятьс \${att и, ecr ирова	rovider (:я поиск tr_name) пи учетна о заданны ана =	и поставщика идентификации. При первом учетной записи в Blitz identity Provider для « 4. где attr_name - это имя атрибута, получа, правило Сн+\${name} \${surname} означает, « ая запись не была идентифицирована ым правилам соответствия \${email}	входе пользоват ее последующег емого от постав что атрибут СN (геля через поставщи го связывания с учет шика идентификаци будет формировать
(ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и зиглате ч Предлагать попьзователю ввести лого Пряд привязки должна быть найдена т Пребовать ввод пароля, если учетная mail	тных записей Blitz Iden завил будет осуществл ии. е строки подстановки е несколько атрибутов ерез пробел. ин и пароль для привязк ин и пароль для привязк олько одна учетная запи запись была идентифиц	tity Р іятьс \${att и, есг ирова	rovider : ся поиск tr_name) пи учетна задання ана =	и поставщика идентификации. При первом ; учетной записи в Blitz Identity Provider для и , где attr_name - это имя атрибута, получа правило cN=\${name} \${surname} означает, ч ая запись не была идентифицирована ым правилам соответствия \${email}	входе пользоват ее последующег емого от постав что атрибут СN (геля через поставщи го связывания с учет шика идентификаци будет формировать х
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правиля используйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести лоп] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail	тных записей Biliz Iden завил будет осуществл ии. е строки подстановки е строки подстановки е неколько атрибутов ерез пробел. ин и паропь для привязк опько одна учетная запи запись была идентифиц	tity Р іятьс \$ {att . Нап и, есг ирова	rovider (ся поиск tr_name) пример, пи учетна задання ана =	и поставщика идентификации. При первом учетной записи в Blitz Identity Provider для « , где attr_name - это имя атрибута, получа правило cN=\${name} \${surname} означает, « ая запись не была идентифицирована ым правилам соответствия \${email}	входе пользоват ее последующег емого от постав что атрибут СN (геля через поставщи го связывания с учет шика идентификаци будет формироваты будет формироваты
(ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и surname ч] Предлагать пользователю ввести лоп] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail	тных записей Biltz iden завил будет осуществя ии. 2 строки подстановки несколько атрибутов ерез пробел. ин и паропь для привязк опько одна учетная запи запись была идентифиц	tity Р іятьс \${att и, есг ирова	rovider і я поиск т <u>г</u> па те] пи учетна з задання ана =	и поставщика идентификации. При первом учетной записи в Biliz identity Provider для (, где attr_name - это имя атрибута, получа правило CI+-\${name} \${surname} означает, ч ая запись не была идентифицирована ым правилам соответствия \${email}	входе пользоват ее последующег емого от постав что атрибут СN и + доба	геля через поставщи го связывания с учет шика идентификаци будет формировать будет формировать
(ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и зигпате ч] Предлагать пользователю ввести лог] Пля привязки должна быть найдена т] Требовать ввод пароля, если учетная mail	тных записей Blitz Iden завил будет осуществл ии. е строки подстановки е несколько атрибутов ерез пробел. ин и пароль для привязк ин и пароль для привязк олько одна учетная запи запись была идентифиц	tity Р іятьс \${att и, есг ирова	rovider і :я поиск tr_name] и учетна а заданни ана =	и поставщика идентификации. При первом учетной записи в Blitz Identity Provider для (, где attr_name - это имя атрибута, получа, правило Сн+\${name} \${surname} означает, и ая запись не была идентифицирована ым правилам соответствия \${email}	входе пользоват ее последующег емого от постав что атрибут СN и + доба	геля через поставщи го связывания с учет шика идентификаци будет формировать будет формировать
(ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов – пате и зиглате ч Предлагать пользователю ввести лоп] Пря привязки должна быть найдена т] Требовать ввод пароля, если учетная mail Мбиты	тных записей Blitz Iden завил будет осущестал ии. е строки подстановки е строки подстановки е неколько атрибутов ерез пробел. ин и пароль для привязк олько одна учетная запи запись была идентифиц	tity Р іятьс \${att . Нап ирова	rovider н ;я поиск tr_name) ример, и учетня ана ана =	и поставщика идентификации. При первом с учетной записи в Blitz Identity Provider для « , где attr_name - это имя атрибута, получа правило cN=§{name} {{surname} означает, ч ая запись не была идентифицирована ым правилам соответствия \${email}	входе пользоват ее последующег емого от постав что атрибут СN и + доба	геля через поставщи го связывания с учет шика идентификаци будет формироваты будет формироваты + добавить усл вить альтернативное п
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правил двух атрибутов - пате и surname чи] Предлагать пользователю ввести лоп] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail	тных записей Biliz Iden завил будет осуществя ии. е строки подстановки ерез пробел. ин и пароль для привязк опько одна учетная запи запись была идентифиц	tity P іятьс \${att . Нап и, есг сь по ирова	rovider н ;r_name] ;tr_name] рример, ни учетна з задання ана =	и поставщика идентификации. При первом ; учетной записи в Biliz identity Provider для « , где attr_name - это имя атрибута, получа правило CN={name} {(surname) означает, ч ая запись не была идентифицирована ым правилам соответствия {{rmail}	входе пользоват ее последующег емого от постав что атрибут СN н + доба	геля через поставщи го связывания с учет шика идентификаци будет формироваты будет формироваты
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и surname ч Предлагать пользователю ввести лого 1 Пля привязки должна быть найдена т 1 Требовать ввод пароля, если учетная mail мбуты Укажите, каким образом должны ф	тных записей Biltz iden завил будет осуществя ии. е строки подстановки не и паропь для привязк ерез пробел. ин и паропь для привязк олько одна учетная запи запись была идентифиц	tity P Iятьс \${att и, есг ирова	rovider и л поиск tr_name] и учетна ана ана =	и поставщика идентификации. При первом учетной записи в Biliz identity Provider для « , где attr_name - это имя атрибута, получа правило CIv-\${name} \${surname} означает, « ая запись не была идентифицирована ым правилам соответствия \${email} \${email}	входе пользоват ее последующег емого от постав что атрибут СN и + доба	геля через поставщи го связывания с учет шика идентификаци будет формировать будет формировать (ст поставщика
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и surname чи Предлагать пользователю ввести лог] Пля привязки должна быть найдена т] Требовать ввод пароля, если учеткая mail рибуты Укажите, каким образом должны фи идентификации. Для формировани Для создания правила используйте	тных записей Biltz iden завил будет осуществи ии. е строки подстановки не и пароль для привязк олько одна учетная запи запись была идентифиц запись была идентифиц ормироваться атрибут и каждого атрибута до 2 обозначения Sotter	tity P Iятьс \${att . Нап ирова ты, ис лате	rovider и я поиск грамер, заданни ана = спользу о быть с	и поставщика идентификации. При первом учетной записи в Biliz identity Provider для (, где attr_name - это имя атрибута, получа; правило Ct+\${name} \${surname} означает, и ая запись не была идентифицирована ам правилам соответствия \${email} \${email} емые в Bilitz identity Provider, на основе данн- создано свое правило.	входе пользоват ее последующег емого от постав что атрибут СN и + доба њих, получаемых от поставщика и	геля через поставщи го связывания с учет шика идентификаци будет формировать будет формировать
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и зиглагте ч Предлагать пользователю ввести лог 1 Пря привязки должна быть найдена т 1 Требовать ввод пароля, если учетная mail Укажите, каким образом должны фи идентификации. Для формировани Для создания правила используйте можете указывать в одном правила	тных записей Biltz Iden завил будет осуществи ии. в строки подстановки несколько атрибутов ерез пробел. ин и пароль для привязк олько одна учетная запи запись была идентифиц запись одентифиц запись одентифиц запись одентифиц запись одентифиц запись одентифиц запись одентифиц запись и идентифиц запись одентифиц запись оден	tity P ятъс \${att и, есг ирова ч ты, ии лате . Нап	rovider и я поиск гпате) ример, о заданн ана = спользу о быть с), где а	и поставщика идентификации. При первом учетной записи в Biliz Identity Provider для « , где attr_name - это имя атрибута, получа правило CN+\${name} \${surname} означает, ч ая запись не была идентифицирована ым правилам соответствия \${email} \${email} emake в Biliz Identity Provider, на основе данн- содано свое правило. ttr_name - это имя атрибута, получаемого с правило CN+\${name} \${surname} означает, ч	входе пользоват ее последующег емого от постав что атрибут СN и + доба њих, получаемых от поставцика и что атрибут CN и	геля через поставщи го связывания с учет шика идентификаци будет формировать будет формировать + добавить усл вить альтернативное п с от поставщика дентификации. Вы будет формировать
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правили двух атрибутов - пате и зиглате ч] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны ф идентификации. Для формировани Для создания правила используйте можете указывать в одном правили в одном правило можно использовать для :	тных записей Bilz Iden завил будет осуществл ии. е строки подстановки е строки подстановки е строки подстановки е ресколько атрибуто е одна учетная запи запись была идентифиц запись была идентифиц в каждого атрибута до е обозначение \$(attr несколько атрибута до е обозначение \$(attr несколько атрибута до	tity P Iятьс (, есг ирова ч ч ч ч ч ч ч ч ч ч ч ч ч ч ч ч ч ч ч	rovider : я поиск сг_пате) ример, и учетн ана = = спользу о быть с о быть с), где а вычисля	и поставщика идентификации. При первом сучетной записи в Blitz Identity Provider для « правило CN={name} stoumame} означает, « ая запись не была идентифицирована ым правилам соответствия S{email) Stemail) создано свое правило. ttr_name - это имя атрибута, получаемого с правило CN={name} s{surname} означает, и сонове данн-	входе пользоват ее последующег емого от постав что атрибут СN и + доба њи, получаемых от поставцика и что атрибут СN и IP-5{&random(4)	геля через поставщи о связывания с учет шика идентификаци будет формировать будет формировать + добавить усл вить альгернативное п с от поставщика дентификации. Вы будет формировать) позволит присвои
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правил двух атрибутов - пате и зигпате чи] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны фи идентификации. Для формировани Для создания правила используйте можете указывать в одном правиля атрибуту и/d значение вте-хоососо	тных записей Biliz iden завил будет осуществи ии. е строки подстановки не и пароль для привязк опько одна учетная запи запись была идентифиц запись была идентифиц и и акропь атрибута д е обозначение \${ettr; е несколько атрибута дс е ресколько атрибута дс е ресколько атрибута дс е ресколько атрибута дс е обозначение атрибута и важдото атрибута дс е обозначение атрибута дс е обозначение атрибута дс е обозначение атрибута дс	tity P лятьс \${att . Нап ирова . Нап . Нап или в йно с	rovider и я поиск г_патер задання азадання = = спользу о быть с о быть с у , пде а вычисля генери	и поставщика идентификации. При первом учетной записи в Biliz identity Provider для « , где attr_name - это имя атрибута, получая правило CN={(name) {(surname) означает, « ая запись не была идентифицирована ым правилам соответствия {{mail}} {{mail}} емые в Biliz Identity Provider, на основе дани- содано свое правило. ttr_name - это имя атрибута, получаемого с правило CN={(name) {(surname) означает, « темого значения. Например, правило избев рованная величина (набор цифр и букв лат	входе пользоват ее последующег емого от постав что атрибут СN / + доба њих, получаемых от поставцика и, что атрибут CN / IP-5(&random(4)) инского алфавит	геля через поставщи го связывания с учет шика идентификаци будет формироваты
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и зиглате чи] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail Укажите, каким образом должны фи идентификации. Для формировани Для создания правила используйте можете указывать в одном правиля двух атрибутов - пале и зиглаве ч атрибуту uld значение вте-хосссох	тных записей Biltz Iden завил будет осуществи ии. е строки подстановки несколько атрибутов ерез пробел. ин и пароль для привязк олько одна учетная запи запись была идентифиц запись была идентифиц и каждого атрибута дс е обозначение status е несколько атрибута дс е несколько атрибута дс е несколько атрибута да	tity P Iятьс \${att . Нап ирова у . Нап или I или I йно с	rovider и я поиск гранер заданни ана = спользу о быть с у пде а цример, г пде а цример, г пде а	и поставщика идентификации. При первом (учетной записи в Biliz identity Provider для «), де attr_name - это имя атрибута, получа правило CN-\${name} \${surname} означает, ч ая запись не была идентифицирована ым правилам соответствия \${email} \${email} emake в Biliz identity Provider, на основе данн содано свое правило. ttr_name - это имя атрибута, получаемого с правило CN-\${name} \${surname} означает, ч немого значения. Например, правило uid=в рованная величина (набор цифр и букв лат	входе пользоват ее последующег емого от постав что атрибут СN и + доба вых, получаемых от поставцика и, что атрибут CN и 12-5{&random(4) инского алфавит	геля через поставщи о связывания с учет шика идентификаци будет формировать + добавить усл вить альтернативное п с от поставщика дентификации. Вы будет формировать) позволит присвои та).
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правил двух атрибутов - пате и surname чи] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны фи идентификации. Для формировани Для создания правила используйте идентификации. Для формировани двух атрибутов - пале и surname ч Правило можно использовать для : атрибуту uld значение втр-хососох трибут	тных записей Biliz iden завил будет осуществя ии. е строки подстановки не и пароль для привязк олько одна учеткая запи запись была идентифиц запись была идентифиц и накодото атрибута ди е обозначение \${etrc не неколько атрибута ди е зарания константного и да хохохох — случа	tity P іятьс \${att и, есг сь по ирова "ы, ис лино илин нат или I ийно с	гочіdег н я поиск г. патер з задання а задання а задання = = = спользу о быть с о быть с), где а вычисля генери Прави	и поставщика идентификации. При первом сучетной записи в Biliz identity Provider для « правило CIN-S(name) S(surname) означает, « ая запись не была идентифицирована ым правилам соответствия S(email) S(email) емые в Biliz identity Provider, на основе данн создано свое правило. ttr_name - это имя атрибута, получаемого с правило CIN-S(name) S(surname) означает, « немого значения. Например, правило uid-во рованная величина (набор цифр и букв лат по	входе пользоват ее последующег емого от постав что атрибут СN и + доба ных, получаемых эт поставщика и, что атрибут CN и IP-5(&random(4)) инского алфавит	геля через поставщи го связывания с учет шика идентификаци будет формировать + добавить усл вить альтернативное п с от поставщика дентификации. Вы будет формировать) позволит присвои та).
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правили двух атрибутов - пате и зиглате чи] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны фи идентификации. Для формировани Для создания правила используйте можете указывать в одном правили для создания правила используйте иожно использовать для : атрибуту uid значение втр-хососох трибут mail БітяtName	тных записей Bilz Iden завил будет осуществи ии. е строки подстановки е строки подстановки е рековлько атрибутов ерез пробел. ин и пароль для привязк олько одна учетная запи запись была идентифиц запись была идентифиц и каждого атрибута до е обозначение statr е несколько атрибута до с обозначение statr е несколько атрибута до с обозначение statr и с хохосос – случа	tity P ятьс \${att . Нап и, есг ирова ты, им ты, им или в йно с = =	rovider и я поиск tr_name) ример, и учетн ана = = спользу о быть с о быть с о быть с), где а вычисля сгенери] Правии \$(em	и поставщика идентификации. При первом учетной записи в Blitz Identity Provider для « 4, где attr_name - это имя атрибута, получа, правило (н+\$(name) \$(surname) означает, ч ая запись не была идентифицирована ым правилам соответствия (S(email) (S(email)) (S(email)) емые в Blitz Identity Provider, на основе данн- содано свое правило. ttr_name - это имя атрибута, получаемого с правило (n+\$(name) \$(surname) означает, ч немого значения. Например, правило uid=в рованная величина (набор цифр и букв лат ло all)	входе пользоват ее последующег емого от постав что атрибут СN и + доба њи, получаемых эт поставщика и что атрибут СN и IP-5(&random(4)) инского алфавит	геля через поставщи о связывания с учет шика идентификаци будет формировать + добавить усл вить альтернативное п с от поставщика дентификации. Вы будет формировать) позволит присвои та). Мастер
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правил двух атрибутов - пате и зиглате чи [] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны фи идентификации. Для формировани Для создания правила используйте идентификации. Для формировани двух атрибутов - паке и зиглате ч Правило можно использовать для : атрибуту uid значение втр-хососох трибут mail FirstName	тных записей Biliz iden завил будет осуществя ии. е строки подстановки не и пароль для привязк олько одна учеткая запи запись была идентифиц запись была идентифиц е обозначение \${etc; в собозначение \${etc; в собозначение \${etc; в собозначение \${etc; в собозначение \${etc; в собозначение *{etc; в собозначени	tity P ятьс \${att . Нап ирова ирова 	гочіdег н я поиск г., пате) іример, и учетна и заданни а заба с с с с с с с с с с с с с с с с с с	и поставщика идентификации. При первом сучетной записи в Biliz identity Provider для « правило CI+S{name} это имя атрибута, получая правило CI+S{name} S{surname} означает, « ая запись не была идентифицирована ым правилам соответствия S{email} S{email} S{email} создано свое правило. ttr_name - это имя атрибута, получаемого с правило CI+S{name} S{surname} означает, « немого значения. Например, правило uid=в рованная величина (набор цифр и букв лат по ail)	входе пользоват ее последующег емого от постав что атрибут СN / + доба њих, получаемых эт поставцика и, что атрибут CN / IP-5(&random(4)) инского алфавит	геля через поставщи го связывания с учет шика идентификаци будет формироваты + добавить усл вить альтернативное п с от поставщика дентификации. Вы будет формировать) позволит присвои та). Мастер
ентификация учетных записей Укажите правила соответствия уче идентификация с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиля двух атрибутов - пате и зиглате чи] Предлагать пользователю ввести лог] Для привязки должка быть найдена т] Требовать ввод пароля, если учеткая mail Укажите, каким образом должны фи идентификация. Для формировани Для создания правила используйте можете указывать в одном правиля двух атрибутов - пале и зиглаве трибут трибут mail FirstName LastName	тных записей Biltz Iden завил будет осуществя ии. е строки подстановки не исколько атрибутов ерез пробел. ин и паропь для привязк олько одна учетная запи запись была идентифиц в икаждого атрибута до е обозначение \$(attr неколькон стантного с дания константного с обозначение \$(attr неколькон стантного с обозначение \$(attr неколькон стантного с с обозначение (с с с с с с с с с с с с с с с с с с с	tity P ятъс \${att . Нап ирова ч ты, ис ламе . Нап или I йно с	rovider н я поиск сг_пате) іример, и учетні ана = = спользу о быть с о быть с о быть с о быть с о быть с о быть с сгенери Прави	и поставщика идентификации. При первом (учетной записи в Biliz Identity Provider для «), де attr_name - это имя атрибута, получа правило CH-\$(name) \$(surname) означает, ч ая запись не была идентифицирована ам правилам соответствия \${email} \${email} stemail} email Biliz Identity Provider, на основе данн- создано свое правило. ttr_name - это имя атрибута, получаемого о правило CH-\$(name) \$(surname) означает, ч немого значения. Например, правило uid=в рованная величина (набор цифр и букв лат ло ail) t_name) t_name)	входе пользоват ее последующег емого от постав что атрибут СN и + доба вых, получаемых эт поставцика и, что атрибут CN и 12P-\${&random(4) инского алфавит	геля через поставщи го связывания с учет шика идентификаци будет формировать + добавить усл вить альтернативное п с от поставщика дентификации. Вы будет формировать) позволит присвои та). Мастер

Рисунок 80 – Дополнительные настройки поставщика идентификации ВКонтакте

8.5. Вход через Одноклассники

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

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

Базовые настройки Одноклассники	lастройки поставщика идентификации Одноклассники	
Идентификатор поставщика	ok_716 Уникальный идентификатор поставщика. Используется только внутри Bitz Identity Provider	
Название поставщика	Одноклассники Отображаемое в консоли ния поставщика. Используется только внутри Bitz Identity Provider	
		Далее

Рисунок 81 – Базовые настройки поставщика идентификации сети «Одноклассники»

- 4. Перейти на страницу «OAuth авторизация»³⁴, где выполнить следующие операции:
 - зарегистрироваться в сети Одноклассники и привязать к своему аккаунту email
 на этот email будут приходить письма, содержащие регистрационные данные приложений;
 - получить права разработчика по ссылке https://ok.ru/devaccess;
 - зарегистрировать свое приложение и получить Application ID, публичный ключ приложения и секретный ключ приложения;
 - запросить следующие права для приложения: VALUABLE_ACCESS, LONG_ACCESS_TOKEN, GET_EMAIL;
 - прописать перечень разрешённых redirect_uri.
- 5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 82), которые включают в себя:
 - ввод регистрационных данных приложения, полученных ранее:
 - название приложения (Application ID);
 - секретный ключ приложения;
 - публичный ключ приложения;

³⁴ См.: https://apiok.ru/ext/oauth/

- правила, которые будут использоваться для идентификации учетной записи в сети Одноклассники и Blitz Identity Provider. Для создания правила следует использовать строки подстановки \${attr_name}, где attr_name – это имя атрибута, получаемого из Одноклассники. Можно указывать в одном правиле несколько атрибутов. Например, правило CN=\${first_name} \${last_name} означает, что атрибут CN будет сопоставляться с сочетанием двух атрибутов – first_name и last_surname через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт сети Одноклассники, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из Одноклассники, в Blitz Identity Provider. Например, правило mail=\${email} означает, что атрибут с именем mail в Blitz Identity Provider будет заполняться значением из атрибута email учетной записи сети Одноклассники (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно 131

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.

зопасность				
Soliachocia				
Используйте раздел "Как начать и сохранить в настройках приложени	спользовать OAuth" стр ия Одноклассники указ	рани анны	цы OAuth авторизация для заполнения указанных ни не ниже разрешенные redirect_uri	кке параметров. Не забудьте
Paзpeшённые redirect_uri	http(s)://sudir.reaxoft.ru http(s)://sudir.reaxoft.ru	ı/sps/ ı/sps/	'login/externalldps/callback/ok/ok_1/false /profile/social/externalldps/callbackPopup/ok/ok_1	
	Эти ссылки должны бі приложения Одноклас пользователя. Исполь соединение.	ыть п сник зуйте	рописаны в Список разрешённых redirect_uri и для корректной обработки результатов аутентификации в схему https, если вы используете защищенное	
Название приложения (Application ID)	1272458752			
Секретный ключ приложения	Изменить значение			
Публичный ключ приложения	Изменить значение			
зрешения				
Запрашиваемые разрешения	VALUABLE_ACCESS	x	GET_EMAIL x	
	Для добавления разри Укажите перечень раз обращении к поставщ Одноклассники	ешені реше іику и	ия введите его имя и нажмите Enter ний (всоре), которые должны быть получены при адентификации. Перечень доступных разрешений	
ентификация учетных записей				
Укажите правила соответствия уче идентификации с помощью этих п записью поставщика идентификац	тных записей Blitz Iden равил будет осуществл ии.	tity P іятьс	rovider и поставщика идентификации. При первом вя ся поиск учетной записи в Biltz Identity Provider для ее	юде пользователя через поставщика последующего связывания с учетной
Укажите правила соответствия уче идентификации с помощью этих п записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч предлагать пользователю ввести пог Для привязии должиа быть найдена т	тных записей Biltz iden равил будет осуществи ии. е строки подстановки (е несколько атрибутов ерез пробел. им и пароль для привязко опыхо одна учетная запи	tity P іятьс \${att . Нап и, есл	точіder и поставщика идентификации. При первом во ся поиск учетной записи в Billz identity Provider для ес сп. name), иде attr_name - это имкя атрибута, получаен ример, правило CN-§(name) \${surname} означает, чт пи учетная запись не была идентифицирована о заданным правилам соответствия	юде пользователя через поставщика : последующего связывания с учетной мого от поставшика идентификации. ю атрибут СN будет формироваться и
Укажите правила соответствия уче идентификации с помоцью этих пу записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная	тных записей Biltz iden равил будет осуществл ии. е строки подстановки (е несколько атрибутов ерез пробел. ин и пароль для привязю олько одна учетная запи запись была идентифиц	tity P Iятьс \${att . Нап и, есг сь по ирова	точіder и поставщика идентификации. При первом во ся поиск учетной записи в Billz Identily Provider для ес ст. паве). ца attr_ name - это имкя атрибута, получае пример, правило CN-§(name) \${surname} означает, чт пи учетная запись не была идентифицирована о заданным правилам соответствия ана	оде пользователя через поставщика : последующего связывания с учетной мого от поставшика идентификации. о атрибут СN будет формироваться н
Укажите правила соответствия учи идентификации с помощью этих пр записью поставцика идентификац Для содания правила кспользуйт можете указывать в одном правил двух атрибутов - пате и surname ч предпагать пользователю ввести лог] Для привязи должка быть найдена т] Требовать ввод пароля, если учетная mail	тных записей Biltz iden равил будет осуществл ии. е строки подстановки е строка отрибутов ерез пробел. ин и пароль для привязко олько одна учетная запи запись была идентифиц	tity P Iятьс \${att и, есг сь по ирова	rovider и поставцика идентификации. При первом во ся поиск учетной записи в Biltz Identity Provider для ее tr_name), где attr_name - это имя атрибута, получае пример, правило (di={fmae} {funnae}) соначает чт пи учеткая запись не была идентифицирована о заданным правилам соответствия ана = {(email)	оде пользователя через поставщика последующего связывания с учетной мого от поставшика идентификации. Е о атрибут СN будет формироваться и х
Укажите правила соответствия уче идентификации с помощью эткся и записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать попьзователю ввести лог] Для привязки должка быть найдена т] Требовать ввод пароля, если учетная mail	тных записей Biltz iden завил будет осуществл ии. е строки подстановки е строки подстановки е несколько атрибутов ерез пробел. ин и пароль для привязю олько одна учетная запи з запись была идентифиц	tity Р іятьс \${att . Нап сь по ирова	точіder и поставщика идентификации. При первом во ся поиск учетной записи в Biltz Identity Provider для ею ст. паве). (де attr_name - это имя атрибута, получае пример, правило (N+\${name} \${surname}) означает, чт пи учеткая запись не была идентифицирована заданным правилам соответствия ана = \${email}	оде пользователя через поставщика последующего связывания с учетной мого от поставшика идентификации. то атрибут СN будет формироваться и со атрибут CN будет формироваться и на собавить условии
Указите правила соответствия учи идентификации с помощью этих п записью поставцика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч 3 Предлагать пользователю ввести лог 1 Для привязки должа быть найдена т 3 Требовать ввод пароля, если учетная mail	тных записей Biltz Iden равил будет осуществл ин. е строки подстановки е строка подстановки ерез пробел. ин и пароль для привязко опько одна учетная запи запись была идентифиц	tity Р іятьс \${att и, есг сь по ирова	rovider и поставщика идентификации. При первом во ся поиск учетной записи в Billz identity Provider для ес ст. паве), иде attr_name - это имкя атрибута, получаен иример, правило CN-§(name) \$(surname) означает, чт пи учетная запись не была идентифицирована заданным правилам соответствия ана = \$(email)	оде пользователя через поставщика е последующего связывания с учетной мого от поставшика идентификации. го атрибут СN будет формироваться н к добавить услови + добавить альтеркативное прав
Укажите правила соответствия учи идентнфикации с помощью этих пр записью поставцика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч 3 Предлагать пользователно ввести лог 1 Для привязки должа быть найдена т 3 Требовать ввод пароля, если учетная mail	тных записей Biltz iden равил будет осуществл ии. е строки подстановки е строки подстановки ерез пробел. ин и паропь для привязко опыхо одна учетная запи запись была идентифиц	tity Р ятъс \${att и, есг ирова	rovider и поставцика идентификации. При первом во ся поиск учетной записи в Biltz Identity Provider для ее tr_name), (де attr_name - это имя атрибута, получае пример, правило (di=§{name} § (surname)) означает, чт пи учеткая запись не была идентифицирована о заданным правилам соответствия ана = \$(email)	оде пользователя через поставщика последующего связывания с учетной мого от поставшика идентификации. Е о атрибут СN будет формироваться и + добавить услови + добавить альтериативное прав
Укажите правила соответствия уче идентификации с помощью этися п записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести пог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail	тных записей Biltz Iden завил будет осуществл ии. е строки подстановки е есколько атрибутов ерез пробел. ин и пароль для привязю олько одна учетная запи запись была идентифиц	tity Р ятъс \${att и, есг ирова	rovider и поставщика идентификации. При первом во ся поиск учетной записи в Biltz identity Provider для ес ст. даве) , сде attr_ name - это имя атрибута, получае пример, правило CI+5{name} \${surname} означает, чт и учетная запись не была идентифицирована о заданным правилам соответствия ана = \${email}	оде пользователя через поставщика последующего связывания с учетной мого от поставшика идентификации. то атрибут СN будет формироваться и коло атрибут СN будет формироваться и кол атрибут СN будет формироват
Укажите правила соответствия учи идентификации с помощью этих п записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести пос] Для привязки должа быть найдена т] Требевать ввод пароля, если учетная mail использователя с поставля и соложите и идентификации. Для формирован для создания правила используйт можете указывать в одном правил и укатамето - паке и в испальзуйт правило можно использовать для атрибуту ий значение втр-ососо	тных записей Biltz Iden равил будет осуществ/ ии. е строки подстановки е есколько атрибутов ерез пробел. ин и пароль для привязко олько одна учетная запи и пароль для привязко олько одна учетная запи запись была идентифиц с абозначение \${atpu6yra и каждого атрибута дс е обозначение \${atpu6yra и каждого атрибута дс е обозначение \${atpu6yra и каждого атрибута дс е несколько атрибута задания константного к, де хохосос – случа	tity Р іятъс \${att и, есг сь по ирова ты, ис лаке , Нап или в йно с	точіder и поставщика идентификации. При первом во ся поиск учетной записи в Biltz Identity Provider для ес ст. даве), сде attr_ name - это имя атрибута, получаен ример, правило CI+5(name) \$(surname) означает, чт и учеткая запись не была идентифицирована о заданным правилам соответствия ана = \$(email) cnonьзуемые в Biltz Identity Provider, на основе данны о быть создано свое правило.), где attr_ name - это имя атрибута, получаемого от ример, правило CI+5(name) \$(surname) означает, чт вычисляемого значения. Например, правило uidempr генерированная величина (набор цифр и бука пати	оде пользователя через поставщика последующего связывания с учетной мого от поставщика идентификации. Е о атрибут СN будет формироваться і + добавить апьтернативное прав «, получаемых от поставщика поставщика идентификации. Вы о атрибут CN будет формироваться і +\${&radiabacture -\${krandom(4)} позволит присвоить ксюго алфавита).
Укажите правила соответствия учи идентификации с помощью этих пу записыо поставщика идентификац Для создания правила еклопьзуйт можете указывать в одном правил даух атрибутов - пате и surname ч 3 Предлагать пользователю ввести лог] Для привязки должка быть найдена т 3 Требовать ввод пароля, если учетная mail рибуты Указите, каким образом должны ф идентификации. Для формирован ля создания правила используйт для создания правила используйт для создания и указивать в одном правил даух атрибуто - пасе и surname с указывать в одном правил атрибуту ий значение в19-хоссоо	тных записей Biltz iden равил будет осуществл ии. с строки подстановки е строки подстановки е строки подстановки е рез пробел. ин и пароль для привязо олько одна учетная запи и ались была идентифиц з запись была идентифиц и каждого атрибута дс с обозначение s(attr. е несколько атрибута исе собозначение s(attr. е несколько атрибута исе константного с, где хохохох – случа	tity Р кятъс \${att . Нап ирова мрова	точіder и поставщика идентніфикации. При первом во ся поиск учетной записи в Billz Identity Provider для ес ст. даве), ще аttr_ name - это имя атрибута, получаен пример, правило CI+\${name} \${urname} означает, чт и учетная запись не была идентніфицирована о заданным правилом соответствия ана = \${email} спользуемые в Billz Identity Provider, на основе данны о быть создано свое правило. }, де attr_ name - это имя атрибута, получаемого от пример, правило cI+\${name} \${urname} означает, чт вычисляемого значения. Например, правило uid=Bir генерированная величина (набор цифр и букв патия	оде пользователя через поставщика последующего связывания с учетной мого от поставшика идентификации. Е о атрибут СN будет формироваться и + добавить апьтернативное прав и, получаемых от поставщика поставщика идентификации. Вы то атрибут CN будет формироваться и
Учажите правила соответствия уче идентификации с помощью этих п записью поставщика идентификац Для создания правила используйт можете указывать в одном правил двух атрибутов - пате и surname ч] Предлагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если ученкая mail рибуты Учажите, каким образом должны ф идентификации. Для формигрован для создания правила используйт можете указывать в одном правил для создания правила используйт можете указывать в одном правил для создания правила используйт можете указывать в одном правил для создания правила использовать для атрибути и значение в ре-хососо	тных записей Biltz Iden завил будет осуществ/ ии. е строки подстановки е есколько атрибутов ерез пробел. ин и пароль для привязо олько одна учетная запи запись была идентифиц солько одна учетная запи и каждого атрибута дс е обозначение \${attr. несколько атрибута да е обозначение \${attr. и каждого атрибута да е обозначение \${attr. и суста с с с с с с с с с с с с с с с с с с	tity Р ятъс (аст к. Нап и, есл съ по ирова у ты, ис ламе или в йно с	точіder и поставщика идентніфикации. При первом во ся поиск учетной записи в Billz Identity Provider для ес ся паясу, це attr_name - это имя атрибута, получаен ример, правило CI+5(name) \$(surname) означает, чт пи учетная запись не была идентифицирована о заданным правилом соответствия ана = \$(email) спользуемые в Billz Identity Provider, на основе данны о быть создано свое правило.), где attr_name - это имя атрибута, получаемого от ример, правило CI+5(name) \$(surname) означает, чт вычисляемого значения. Например, правило utd-етт генерированная величина (набор цифр и букв патти Правило	оде пользователя через поставщика последующего связывания с учетной мого от поставщика идентификации. Е о атрибут СN будет формироваться I + добавить альгернативное прав и, получаемых от поставщика поставщика идентификации. Вы о атрибут CN будет формироваться I - \${&random(e)} позволит присвоить кского алфавита).
Укажите правила соответствия учи идентификации с помоцью этих пу записью поставщика идентификац Для создания правила используйт можете указывать в одном правил даух атрибутов - пате и surname ч 3 Продлагать пользователю ввести лог) Для привлян должа быть найдена т 3 Требовать ввод пароля, если учетная mail эибутьи Указите, каким образом должны ф идентификации. Для формирован идентификации. Для формирован идентификации. Для формирован идентификации. Для формирован изает указывать в одном правиля для создания используйт можете указывать в одном правиля агрибуту ий значение втр-хоссоо Пример атрибутое для малныка трибут	тных записей Biltz Iden равил будет осуществл ии. е строки подстановки е есколько атрибутов ерез пробел. ии и пароль для привязо олько одна учетная запи и ались была идентифиц и каждого атрибута дс е обозначение startи и каждого атрибута дс е обозначение startиото с, где зоосоос – случа	tity Р кятьс \${att . Нап и, есг сь по ирова У Сы, ИС лаже . Нап или Е йно с	точіder и поставщика идентніфикации. При первом во ся поиск учетной записи в Billz Identity Provider для ес агодаве), ще аttr_name - это имя атрибута, получаен ример, правило Cl+\$(name) \$(surname) означает, чт и учеткая зались не была идентніфицирована о заданным правилам соответствия ана = \$(email) cnonьзуемые в Biltz Identity Provider, на основе данны о быть содано свое правило.), де attr_name - это имя атрибута, получаемого от ример, правило Cl+\$(name) \$(surname) означает, чт вычисляемого значения. Например, правило uld-817 генерированная величина (набор цифр и бука пати [равило	оде пользователя через поставщика последующего связывания с учетной мого от поставщика идентификации. Е о атрибут СN будет формироваться и + добавить апьтернативное прав и, получаемых от поставщика поставщика идентификации. Вы о атрибут CN будет формироваться и *-\${&rados(4)} позволит присвоить какого алфавита).
Укажите правила соответствия учи идентификации с помощью этки пу запкско поставидика идентификац Для создания правила еспользуйт можете указывать в одном правил аух атрибутов - пате и surname ч предпагать пользователю ввести лог] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны ф идентификации. Для формирован Для создания правила используйт можете указывать в одном правил дву создания правила используйт правило можо использовать для атрибуту иі значение вдр-хоссоо Пример атрибутов для малликга грибут mail	тных записей Biltz iden равил будет осуществл ии. с строки подстановки е строки подстановки е строки подстановки е исколько атрибутов ерез пробел. ин и пароль для привязо олько одна учетная запи з запись была идентифиц з запись была идентифиц з запись была идентифиц с обозначение \${ctrr е несколько атрибута дс о собозначение \${ctrr е несколько атрибута исе пробел. задания константното с, где хоохоох – случа	tity P. ятъс \${att и, есг ирова ч то ирова ч то ирова ч то ирова ч то ирова ч то ирова ч то ирова ч то ирова ч то и и и и и и и и и и и и и	точіder и поставщика идентніфикации. При первом во ся поиск учетной записи в Biliz identity Provider для ес ст. паве), це аttr_ name - это имя атрибута, получаен ример, правило Cl+\${name} \${urname} означает, чт и учеткая запись не была идентніфицирована о заданным правилам соответствия ана = \${email} спользуемые в Biliz identity Provider, на основе данные о быть создано сосо еправило. }, де attr_ name - это имя атрибута, получаемого от ример, правило cl+\${name} \${urname} означает, чт вычисляемого значения. Например, правило uid=Bir renepupoванная величина (набор цифр и букя латия Правило \${email}	оде пользователя через поставщика последующего связывания с учетной мого от поставщика идентификации. Е о атрибут СN будет формироваться и + добавить апьтернативное прав ак, получаемых от поставщика поставщика идентификации. Вы то атрибут CN будет формироваться и ->5(&rended(4)) позволит присвоить кского алфавита).
Укажите правила соответствия учи дентификации с помощью этки пу запкью поставщика идентификац Для создания правила еклопьзуйт можете указывать в одном правил даух атрибутов - пате и surname ч 3 Предлагать пользователю ввести лог] Для привлан должка быть найдена т 3 Требовать ввод пароля, если учетная mail жибуты Указите, каким образом должны ф идентификации. Для формирован ла создания правила используйт можете указывать в одном правил для создания правила используйт можете указывать в одном правил для создания и сисли созвать для атрибуту иі значение в17-хоссоо Пример атрибутов для маллинга трибут mail БігstName	тных записей Biltz Iden равил будет осуществл ии. е строки подстановки е есколько атрибутов ерез пробел. ин и пароль для привязо олько одна учетная запи и ались была идентифиц и каждого атрибута дс е обозначение \${atrr, е несколько атрибута и каждого атрибута дс е обозначение \${atrr, е несколько атрибута и с носолько атрибута и с трибел. задания константного с, где зоосоос – случа	tity P вятьс \${att . Нап ирова ирова . Нап или е йно с = = =	точіder и поставщика идентніфикации. При первом во ся поиск учетной записи в Billz identity Provider для ес агодаве), ще attr_name - это имя атрибута, получаен ример, правило CI+5(паке) \$(surname) означает, чт и учеткая зались не была идентніфицирована о заданным правилам соответствия ана = \$(email) cnon.syveмые в Biltz identity Provider, на основе данны о быть создано свое правило.), где attr_name - это имя атрибута, получаемого от ример, правило CI+5(nake) \$(surname) означает, чт вычисляемого значения. Например, правило uide-Bir renepuposанная величина (набор цифр и букя пати \$(first_name) \$(first_name)	оде пользователя через поставщика последующего связывания с учетной мого от поставщика идентификации. Е о атрибут СN будет формироваться и + добавить апьтернативное прав и, получаемых от поставщика поставщика идентификации. Вы о атрибут CN будет формироваться и ->5(&random(4)) позволит присвоить кого алфавита).

Рисунок 82 – Дополнительные настройки поставщика идентификации сети Одноклассники

8.6. Вход через Mail ID

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

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

Базовые настройки Mail ID Настройки	поставщика идентификации Mail ID	
Базовые настройки Mail ID		
Идентификатор поставщика	mail_1 Уинкальный идлентефикатор поставщика. Используется телько внутре Bitz Identity Provider	
Название поставщика	Mail D Orošpakastvoe is koncone inter nocrastiцiera. Mcnonubyerce romano selympi Bláz klentity Provider	
		Далее

Рисунок 83 – Базовые настройки поставщика идентификации Mail ID

- 4. Перейти на странице «Создание приложения» Mail.ru³⁵, в котором выполнить следующие операции:
 - нажать на кнопку «Создать приложение»;
 - аутентифицировать под учетной записью Mail.ru;
 - ввести данные приложения, в том числе:
 - название приложения;
 - в поле «Bce redirect_uri» указать перечень URI перенаправления, предложенные в консоли Blitz Identity Provider;
 - в блоке «Платформы» поставить галочку на Web;
 - по результатам регистрации будет сгенерирован ID Приложения и его секрет, они потребуются для последующего ввода в Blitz Identity Provider.
- 5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 72), которые включают в себя:
 - идентификатор клиента (ID приложения), полученный ранее;
 - секрет приложения, полученный ранее;
 - запрашиваемые разрешения (scope), например, userinfo;

³⁵ CM.: https://help.mail.ru/developers/oauth/app

- правила, которые будут использоваться для идентификации учетной записи в Mail ID и Blitz Identity Provider. Для создания правила следует использовать строки подстановки \${attr_name}, где attr_name – это имя атрибута, получаемого от Mail ID. Можно указывать в одном правиле несколько атрибутов. Например, правило CN=\${first_name} \${last_name} означает, что атрибут CN будет сопоставляться с сочетанием двух атрибутов - first_name и last_name через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило.
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт Mail ID, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из Mail ID, в Blitz Identity Provider. Например, правило mail=\${email} означает, что атрибут с именем mail в Blitz Identity Provider будет заполняться значением из атрибута email учетной записи Mail ID (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через Mail ID данный 134

атрибут будет обновлен в хранилище Blitz Identity Provider.

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

астройки поставщика идентифик	ации Mail ID					
взопасность						
Для заполнения используйте данны перенаправления и в качестве испо	ые из приложения oauth@ ользуемой платформы вы	<mark>mail.ru</mark> . Не брать We	е забудьте сохранить в настройках прилож b.	ения OAUTH@!	ИAIL RU указанные	URI
URI перенаправления (redirect_uri)	http{s}://sudir.reaxoft.ru/sps http(s)://sudir.reaxoft.ru/sps	/login/ext /profile/so	ernalldps/callback/mail/mail_1/false ccial/externalldps/callbackPopup/mail/mail_1			
	Эти ссылки должны быть г oauth@mail.ru для коррект Используйте схему https,	трописаны ной обраб если вы ис	і в параметре redirect_uri приложения отки результатов аутентификации пользователя спользуете защищенное соединение.			
ID приложения	4fd2f86426ef418bbec44701	5ffdbd6a				
Секрет приложения	Изменить значение					
зрешения						
Запрашиваемые разрешения	изегілго х Для добавления разрешен	ия введит	re его имя и нажмите Enter			
	Manufacture fundamente					
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле	тных записей Blitz Identity R навил будет осуществлять ии. с строки подстановки \${ot е несколько атрибутов. На	Provider и ся поиску tr_name) пример, г	поставщика идентификации. При первом учетной записи в Biltz Identity Provider для « , где attr_name - это имя атрибута, получа правило CH+\${name} \${surname} означает, ч	аходе пользова не последующе емого от постан то атрибут CN	теля через поставі го связывания с уч зшика идентификаї будет формирова ⁻	щика етной ции. Е ться и
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете укзавать в одном правиле двух атрибутов - пате и surname че] Предлагать пользователю ввести лого] Для привязки должна быть найдена т] Требовать ввод пароля, если учетная	тных записей Biltz identity F навил будет осуществлять и. • строки подстановки \$(at несколько атрибутов. На врез пробел. вн и пароль для привязки, ес алько одна учетная запись п запись была идентифициров	Provider и ся поиску tr_name} пример, г ли учетная о заданны ана	поставщика идентификации. При первом учетной записи в Biltz Identity Provider для (, где attr_name - это имя атрибута, получа правило си-\${name} \${surname} означает, и я запись не была идентифицирована м правилам соответствия	иходе пользова е последующе мого от постан то атрибут СN	теля через поставі го связывания с уч зшика идентификаї будет формирова	щика етной ции. Е гъся и
дентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пате и surname че д Предлагать пользователю ввести лого] Для привяжи должна быть найдена то] Для привяжи должна быть найдена то] Требовать ввод пароля, если учетная mail	тных записей Biltz Identity F иавил будет осуществлять и. - строки подстановки \$(at несколько атрибутов. На ерез пробел. - и пароль для привязки, ес олько одна учетная запись п запись была идентифициров	Provider и ся поиску tr_name) пример, г ли учетназ о заданны ана =	поставщика идентификации. При первом учетной записи в Biltz Identity Provider для (, где attr_name - это имя атрибута, получа правило CN-\$(name) \$(surname) означает, ч я запись не была идентифицирована м правилам соответствия \$(email)	иходе пользова е последующе мого от постан то атрибут СN	теля через постав го связывания с уч зшика идентифика будет формирова	щика етной ции. В
центификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пате и surname че] Предлагать пользователю ввести лого] Для привязки дотича быть найдена то] Для привязки дотича быть найдена то] Требовать ввод пароля, если учетная mail	тных записей Biltz identity F навил будет осуществлять и. • строки подстановки \${at несколько атрибутов. На врез пробел. • и пароль для привязки, ес олько одна учетная запись п запись была идентифициров	Provider и ся поиск ; tr_name) пи учетнаж о заданны ана =	поставщика идентификации. При первом учетной записи в Biltz Identity Provider для и , где attr_name - это имя атрибута, получа правило си-\$(name) \$(surname) означает, и я запись не была идентифицирована м правилам соответствия \$(email)	иходе пользова е последующе мого от постан то атрибут СN + доба	теля через поставл го связывания с уч зшика идентификан будет формирова будет формирова (удет формирова) как и собавить у на обавить уч нвить альгернативнос	щика етной ции. Е ться и сповие
ентификация учетных записей Укажите правила соответствия уче идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пате и surname че] Предлагать пользователю ввести лого-] Для привязки должна быть найдена то] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны фо идентификации. Для формировани Для создания правила используйте можете указывать в одном правиле двух атрибутов - пале ч surname ч Правило можно использовать для з атрибуту ий значение втр-хохоох	тных записей Biltz identity f навил будет осуществлять и с строки подстановки \${at несколько атрибутов. На эрез пробел. вн и пароль для привязки, ес алько одна учетная запись п запись была идентифициров ались была идентифициров у у элись была идентифициров и а какдого атрибута, и я какдого атрибута долж- е несколько атрибута. На е несколько атрибута. На е несколько атрибута. На е несколько атрибута. На е рез пробел.	Provider и ся поиск ; пример, г ли учетная ана = = = спользуе о быть сс со о заданны ана = =	поставщика идентификации. При первом учетной записи в Biltz Identity Provider для « , где attr_name - это имя атрибута, получае правило CI+\$(name) \$(surname) означает, ч я запись не была идентифицирована м правилам соответствия \$(email) \$(email) мые в Biltz Identity Provider, на основе данн- одано свое правило. Ir_name - это имя атрибута, получаемого с правило CI+\$(name) \$(surname) означает, ч емого значения. Например, правило ude-во ованная величина (набор цифр и букв лат	коде пользова е последующе мого от постан то атрибут СN + доба ых, получаемы т поставщика и то атрибут CN (P-S(&random(4) инского алфави	теля через постав го связывания с уч будет формирова будет формирова + добавить у нить альтернативнос к от поставщика центификации. Вь будет формирова)) позволит присво гта).	щика етной ться к слови е прав ться к
кентификация учетных записей Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификац Для создания правила используйте можете указывать в одном правиле двух атрибутов - пате и surname че] Предлагать пользователю ввести лого] Для привязки должна быть найдена то] Для привязки должна быть найдена то] Для привязки должна быть найдена то] Требовать ввод пароля, если учетная mail рибуты Укажите, каким образом должны фр идентификации. Для формировани Для создания правила используйте можете указывать в одном правиле ирух атрибутов - паве и в изглаве ч Пример атрибутов для маллинга трибут	тных записей Biltz identity F навил будет осуществлять и. с троки подстановки \${at несколько атрибутов. На эрез пробел. ы и пароль для привязки, ес элько одна учетная запись п запись была идентифициров ались была идентифициров одоначение будется пасе обозначение \${atte пасе несколько атрибута, на несколько атрибута. На рез пробел. надания константного или , где хоосоос – случайно	Provider и ся поиск; тл. паяе); пи учетная ана = = = спользуе о быть сс е), где аtt вычисляе вычисляе сгенерир	поставщика идентификации. При первом учетной записи в Biltz Identity Provider для (, где attr_name - это имя атрибута, получая правило CI+\$(name) \$(surname) означает, ч я запись не была идентифицирована м правилам соответствия \$(email) \$(email) мые в Biltz Identity Provider, на основе данн- оздано свое правило. tr_name - это имя атрибута, получаемого с правило CI+\$(name) \$(surname) означает, ч вмого значения. Например, правило uideв ованная величина (набор цифр и букв лат	коде пользова е последующе мого от постан то атрибут СN + доба ых, получаемы т поставщика и то атрибут CN P-5[&random(4) ниского алфави	теля через постав го связывания с уч зшика идентификан будет формирова * добавить у + добавить у нвить альгернативное х от поставщика центификации. Вь будет формирова)) позволит присво та).	щика етной тъся и словие о прави тъся и о ла
кентификация учетных записей Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пате и sumame че 3 Предлагать пользователю ввести лого 3 Для привязки должна быть найдена то 3 Пребовать ввод пароля, если учетная mail эибуты Укажите, каким образом должны фи идентификации. Для формировани для создания правила используйте можете указывать в одном правила двух атрибутов - пале и sumame ч правило можно использовать для з атрибуту uid значение втр-хососох Пример агрибутов для маллинга таil	тных записей Biltz Identity F навил будет осуществлять и. строки подстановки \$(аt не и пароль для привязки, ес алько одна учетная запись п запись была идентифициров урмироваться атрибуты, и я каждого атрибута должн- е обозначение \$(attr_name несколько атрибута, на ерез пробел. адания константного или , где хохохох – случайно	Ргочіdег и ся поиск у пример, г ли учетназ ана = = спользуе о быть сс о объть сс со е), где аll вычисляя вычисляя Сгенерир	поставщика идентификации. При первом учетной записи в Biltz Identity Provider для « , где attr_name - это имя атрибута, получая правило Си+\$(name) \$(surname) означает, ч а запись не была идентифицирована м правилам соответствия [\$(email)] мыве в Biltz Identity Provider, на основе данн оздано свое правило. иг_пате - это имя атрибута, получаемого с изравило Си+\$(name) \$(surname) означает, ч емого значения. Например, правило иdене юванная величина (набор цифр и бухв лат во	коде пользова е последующе мого от постан то атрибут СN + добл ых, получаемы т поставщика и по атрибут CN :P-\$(&random(4) ноского алфави	теля через поставл го связывания с уч зшика идентификац будет формироват + добавить уг нала альгернативнос х от поставщика цдентификации. Вы будет формироват (); позволит присво га).	щика етной гъся и словне е правн тъся и эмтъ

Рисунок 84 – Дополнительные настройки поставщика идентификации Mail ID

8.7. Вход через Единую систему идентификации и аутентификации (ЕСИА)

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

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

Базовые настройки ESIA	
Идентификатор поставщика	esia_1
Название поставщика	Эникальный идентификатор поставщика, используется только внутри благ identity Provider Госуслуги
	L Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider

Рисунок 85 – Базовые настройки поставщика идентификации ЕСИА

- Получить в удостоверяющем центре ключ электронной подписи для взаимодействия с ЕСИА и выгрузить сертификат открытого ключа. Произвести конвертацию ключа в формат, совместимый с Blitz Identity Provider.
- 5. Сертификат ключа необходимо зарегистрировать на Технологическом портале ЕСИА (см. следующий пункт).
- 6. Осуществить регистрацию информационной системы организации через Технологический портал ЕСИА³⁶, в котором выполнить следующие операции:
 - нажать на кнопку «Добавить систему»;
 - указать название системы, отображаемое название, мнемонику системы, список URL системы (задать домен развернутой системы Blitz Identity Provider, с указанием протокола https), алгоритм формирования электронной подписи и выбрать ответственного сотрудника (Рисунок 86);
 - сохранить данные и перейти к настройке сертификатов информационной системы;
 - загрузить сертификат для зарегистрированной информационной системы на Технологическом портал (Рисунок 87);

³⁶ См.: https://esia.gosuslugi.ru/console/tech/ До регистрации ИС в ЕСИА необходимо зарегистрировать учетную запись организации в ЕСИА и дать одному из сотрудников доступ к Технологическому порталу.

Название системы	Проверочная система
Отображаемое	Проверочная система
пазвалие	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, регистрирована в ЕСИА с целью получения доступа к сервису ЕСИА в СМЭВ, должна быть предварительно зарегистрирована в СМЭВ
нформация 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	RS256 -
формирования электронной подписи	Выберите криптографический алгоритм формирования электронной подписи, который будет использоваться при выпуске маркеров доступа, маркеров идентификации, маркеров обновления, кода авторизации
JRL для отправки push	
сооощении	Введите адрес (с префиксом "https://"), который будет использоваться ЕСИА для отправки в ИС сообщений - уведомлений (push-сообщений)
АТЕГОРИЯ ИНФОРМАІ	ционной системы
Категория	По умолчанию 👻
информационной системы	
Время жизни access	60
токен, мин	min: 10; max: 180
Время жизни refresh	1051200
	min: 60; max: 1051200
ТВЕТСТВЕННЫЙ ЗА Э	КСПЛУАТАЦИЮ СИСТЕМЫ
ΦΝΟ	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	

Рисунок 86 – Добавление системы в Технологическом портале ЕСИА

Элек прав есиа Технологическия	ТРОННОЕ ИТЕЛЬСТВО й портал	Технологиче ООО "РЕАКСОФ" Сменить организаци	ский портал г" ⊵	🔗 Ванин М.В.	9
Информацио	нные системы	Сервисы	История операций		
Тестон	Зая систе е сертификатам	ма разра(и	ботчиков		
і Для Для	загрузка обновл	сертификата		۲	Ю Обновить
N₂	Для обесп взаимодей Кому Вы можете	ечения идентификации в ствии необходимо испол использовать сертифик	ашей информационной системы прызовать сертификат системы. аты формата X.509 в кодировке DE	ои электронном R или PEM (файлы	ия
1430900149	CN=I с сертифи O=RI Чтобы загр ST=N просто пер	катом обычно имеют рас рузить новый сертификат етащите файл в область	ширения .CER или .CRT). r, нажмите кнопку «Загрузить» и ука s загрузки.	жите путь к файлу, либо	
1202933600	CN=1	рузить			1 D
557224121	CN=E	550115			
инконсказьь России	Сохранит	• сертификат	<u>x</u>	Отмена	

Рисунок 87 – Добавление сертификата системы в Технологическом портале ЕСИА

- 7. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 88), которые включают в себя:
 - URI внешнего поставщика домен среды ЕСИА, к которой производится подключение, например, https://esia.gosuslugi.ru;
 - мнемоника системы, указанная ранее в Технологическом портале ЕСИА;
 - идентификатор ключа электронной подписи (alias) идентификатор ключа электронной подписи, загруженный в хранилище Blitz Identity Provider³⁷. Именно сертификат ключа этой электронной подписи должен быть загружен в Технологический портал ЕСИА;
 - запрашиваемые разрешения перечень запрашиваемых разрешений из ЕСИА;
 - запрашиваемые данные пользователя необходимо отметить те данные,

³⁷ Хранилище, указанное в разделе keystore конфигурационного файла Blitz Identity Provider.

которые следует получать из ЕСИА; эти данные должны быть доступны по запрашиваемым разрешениям;

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

идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через ЕСИА данный атрибут будет обновлен в хранилище Blitz Identity Provider.

8. Сохранить данные в Blitz Identity Provider.

Чтобы вход через ЕСИА заработал, необходимо получить официальное разрешение на проведение идентификации и аутентификации пользователей с помощью зарегистрированной системы и получить доступ к тестовой/промышленной среде ЕСИА³⁸.

³⁸ Подробнее см.: https://identityblitz.ru/services/esia-integration

SUNACHOURS								
Заполните данные для корректного	взаимодействия Blitz	Ident	tity Provider c ECI/A.					
URL для авторизации	https://esia-portal1.t	est.go	suslugi ru/aas/oauth2/ac					
URL для получения и обновления маркера	https://esia-portal1.t	est.go	isuslugi ru/aas/oauth2/te					
URL для получения данных	https://esia-portal1.t	est go	isuslugi.ru/rs/pms/\${pm_oid}					
Мнемоника системы (client_id)	ESIA_BRIDGE_RXT							
Адентификатор ключа электронной	gost2012							
подписи (alias)	Предварительно ключ указанное в разделе	i anek keyste	тронной подписи должен б аге конфигурационного фай	іыть загружен в хранилищ Ina Blitz Identity Provider.	6,			
После заполнения этих данных не з указанной мнемоникой и сертифика	абудьте перейти в Те втом ключа электронн	хнола юй па	огический портал ЕСИА, одписи.	где должна быть зареги	стрирована	информаци	онная систея	иа
зрешения и данные пользовател	19							
Выберите разрешения из доступно	о списка							
Доступные разрешения								
запрашиваемые разрешения	для добавления разр	me »	ка введите его имя и нажм	ure Enter				
	Укажите перечень раз обращении к постави	іреше цику и	ний (scope), которые долж дентификации.	ны быть получены при				
Запрашиваемые данные	🕑 Основные дан	ные	🛃 Документы	Адреса				
пользователя	Стмеченные ранее ра	зреш	ения (scope) должны позво	олять получать указанные				
	данные							
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пале и surname че] Предлагать пользователю ввести логи	ных записей Bitz Ider авил будет осуществ и. строки подстановки несколько атрибутог рез пробел. н и пароль для привязи	tity Р яятьс \${att . Han и, есл	rovider и поставщика иде я поиск учетной записи и сг_пате}, где attr_name - пример, правило CN-\${na и учетная запись не была	ентификации. При перес в Bilz Identity Provider дл это имя атрибута, полу me) \${surname} означае идентифицирована	м входе пол кя ее послел чаемого от чт, что атриб	пьзователя ч дующего свя поставшика бут СN будет	ерез постави зывания с учн идентификал формироват	цик етн ции гьсэ
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пате и зиглате че] Предлагать пользователо ввести логи] Для привязки должна быть найдена то] Требовать ввод пароля, если учетная	ных записей Bitz Ider авил будет осуществ ик. строки подстановки несколько атрибутои рез пробел. н и паропь для привязи пько одна учетная запи авпись была идентифис	tity Р 1ятьс \${att 1. Нап и, есг ись по	rovider и поставицика иде я поиск учетной записи и сг. name), тде atlr_name - ример, правило Си-§(na и учетная запись не была заданным правилам соота на	ентификации. При перве в Billz Identity Provider дл это имя атрибута, попу аве) \$(surnae) означає идентифицирована зетствия	м входе пог ка ее послед чаемого от гт, что атриб	ньзователя ч цующего свя поставшика бут СN будет	ерез постав. зывания с уч идентифика. формироват	цик етн ции гьс:
Укажите правила соответствия учет идентификации с помощью этих пр залисью поставцика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пате и зиглате че] Предлагать пользователю ввести логи] Для привязки должна быть найдена то] Требовать ввод пароля, если учелкая еsia_old	ных записей Bitz Ider авил будет осуществ и. строи подстановки несколько атрибутог рез пробел. н и пароль для привязя лько одна учетная запи запись была идентифи.	tity Р лятьс \${att и, есг ись по ирова =	rovider и поставцика иде я поиск учетной записи и сг_name), где attr_name - ример, правило Си-\$(na и учетная запись не была заданным правилам соотв на \$(oid)	ентификации. При перво в Biltz Identity Provider дл это имя атрибута, попу име) \$(surname) соначаю идентифицирована идентифицирована	ми входе пог на ее послер чаемого от т, что атриб	њаователя ч циощего свя поставшика јут СN будет	ерез постави зывания с учи идентификац формироват *	цик етн ции гьсз
Укажите правила соответствия учет идентификации с помощью этих пр залисью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - палее и зиглалее че Предлагать пользователю ввести логи Для привязки должна быть найдена то Для привязки должна быть найдена то д Требовать ввод пароля, если учетная esia_old	ных записей Bitz Ider авил будет осуществ ик строиз подстановия несколько атрибутог рез пробел. н и пароль для привязя пько одна учетная зап запись была идентифик	tity Р іятьс \${att и, есг ись по ирова =	rovider и поставцика иде я поиск учетной записи и гг _name), где attr_name - ример, правило CH-\$(na и учетная запись не была заданным правилам соотв на \$(oid)	ентификации, При перво в ВШZ Identity Provider дл это имя атрибута, полу име) \${sunname} означае в(sunname) означае встаня	ми вкоде послед ня ее послед чаемого от нт, что атриб	њаователя ч дующего свя поставшика јут СN будет	ерез постави зывания с учи идентификац формироват + добавить уг	цик съсз
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пале и зиглалее че] Прадлагать пользователю ввести пол] Для привязки должна быть найдена то] Трябовать ввод пароля, если учелкая еsia_old	ных записей Bitz Ider авил будет осуществ и строим подстановия строим подстановия пессолько атрибутог рез пробел. и и пароль для привяза лько одна учетная запи запись была идентифик у	tity P Iятьс \${att и, есг ись по ирова	rovider и поставцика иде я поиск учетной записи и г ^о _паве), где att_пате- ример, правило Си-\$(na и учетная запись не была заданным правилам сооте на \$(oid)	ентификации. При перве в Biliz identity Provider gr это имя атрибута, полу me) \$(surname) означае идентифицирована идентифицирована	м входе поглед	њаователя ч тучощего свя поставшинка поставшинка ул СN будет + добавить а	нерез постави зывания с учи идентификац формироват + добавить ус пътернативное	ция спо пр
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пате и surname че] Предлагать пользователю веести логи] Для привлзеи дотина быть найдена то] Требовать ввод пароля, если учетная esia_oid	ных записей Bilz Ider авил будет осуществ и. строиз подстановия несколько атрибуто рез пробел. н и пароль для привязи лько одна учеткая зап запись. была идентифик	titty P Iятьс \${att I. Han и, есг ирова =	rovider и поставщика иде л поиск учетной записи и (г_name), где айг_пате – ример, правило СИ-\$(na и учетная запись не была заданным правилам соотв вна \$(oid)	ентификации. При перве в Biltz Identity Provider gr это имя атрибута, попу нее) \${surnaee} Означае идентифицирована истепия	м входе поглед	њзователя ч дующего свя поставшина јут СN будет + добавить а	нерез постави зывания с учи идентификац формироват + добавить ус пытернативное	ция етн гьс: спое
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле друх атрибутов - палее и зиглалее че] Продлагать пользователю ввести логи] Для привлян должа быть найдена то] Для привлян должа быть найдена то] Трабовать ввод пароля, если ученкая esia_oid рибуты	ных записей Bitz Ider авил будет осуществ строиз подстановия несколько атрибутог рез пробел. и и парољ для привяза пљко одна учетная зап запись была идентифик	titty P 1ятьс \${att и, есг ись по ирова =	rovider и поставицика иде я поиск учетной записи и гг_паме), где аttr_паme - ример, правило Си-\$(na и учетная запись не была заданным правилам сооте вна \$(oid) спользуемые в Bittz Identi	ентификации. При перес в Війz Identity Provider дл это имя атрибута, полу име) \$(surnawe) означає идентифицирована нестация	м входе поглед ня ее послед чаемого от гт, что атриб	њаователя ч дующего свя поставшика јут СN будет + добавињ а	нерез постави зывания с учи идентификац формироват + добавить ус пытерналивное	цик етн ции гыс:
Укажите правила соответствия учет идентификации с помощью этих пр записью поставшика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - пале и зиглалее че] Прадлагать пользователю ввести пол] Лля привахи должна быть найдена то] Для привахи должна быть найдена то] Трябоваль ввод пароля, если учетная еsia_oid рибуты Улаконте, клазим образом должны ф идентификации. Для формикрования Для создания правила используйте	ных записей Bitz Ider ванл будет осуществ ин строим подстановия не споим подстановия не пароль для привля ни и пароль для привля пько одна учеткая зап пько одна учеткая зап акось была идентифис у ракироваться атрибута д обозначение \${attr;	tity P 1ятъс \${att 1. Нап и, есг ирова = Гъ., ис ллжно ллжно ллжно	точіder и поставцика иде ля поиск учетной записи и гг_паме), где аttr_пате - ример, правило Си-\$(na и учетная запись не была заданным правилам соотв на \$(oid) Солть создано свое прав), где attr_name - это им	ентификации. При перес в Війz identity Provider дл это имя атрибута, полу- ие) \$(surnave) означає идентифицирована расствия вистиция ву Provider, на основе дл випо.	м входе пог ня ее послед чаемого от г, что атриб инных, получ о от постав	њаователя ч дующего свя поставшика уг СN будет + добавить а чаемых от по щика иденти	ерез постави зывания с уч идентификац + добавить ус пытернативное оставщика финсации. Вы	цик спон про
Укажите правила соответствия учет идентификации с помощью этих пр залисью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле друх атрибутов - палее и зиглалее че] Предлагать пользователю ввести логи] Лля привязеи должа быть кайдена то] Для привязеи должа быть кайдена то] Для привязеи должа быть кайдена то] Требовать ввод пароля, если учеткая еsia_oid	ных записей Bitz Ider авил будет осуществ и к строки подстановки несколько атрибутог ре пробел. ми о одна учетная запи лько одна учетная запи лько одна учетная запи авинсь. была идентифик и римироваться атрибута обозначение Statty реакторобол.	tity P 1ятьс \${att и, есг и, есг ирова = Гы, ис олжно , Нап	точіder и поставщика иде ля поиск учетной записи и (*_name), где аft_name ример, правило Си-\$(na и учетная запись не была заданным правилом Сооте на бонть создано сооте правилом), где aft_name - это им ример, правило Си-5 (ма	ентификации. При перес в Biliz Identity Provider дл это имя атрибута, полу нее) \$(surnaee) означае идентифицирована эетствия III) Provider, на основе ди випо. ия атрибута, получаемо иев) \$(surnaee) означае	мя входе поло ия ее послед чаемого от т, что атрий и от постава	ньзователя « кующего свя поставшика угт СN будет + добавить а чаемых от по щика иденти угт СN будет	ерез постави зывания с уч идентификац формироват + добавить ус 	цик спос про про про про про про про про про про
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле двух атрибутов - палее и зиглавече] Предлагать пользователю веести логи] Для привлян должа быть найдена то] Для привлян и должа быть найдена то] Для привлян и должа быть найдена то] Для привлян и должа быть найдена то] Для привлян можете указывать в одном должны фо идентгификации. Для формировании Для создания правила используйте дожате указывать в одном правиле для у трибутов - пасе и зиглавеч и загрибути ий значение втр-хоссосо	ных записей Bitz Ider авил будет осуществ и строиз подстановия несколько атрибутог рез пробел. и и парољ для привязи ни парољ для чиетная зап лько одна учетная зап авинсь была идентифик и акадоо атрибута д обозначение \${atts: рего атрибута д обозначение \${atts: даника константного иде хоссоск – случа	tity P 1ятьс \${att 1. Нап ирова = Гы, ИС рлжнс или в йно с	точібег и поставцика ида я поиск учетной записи и гг_паме), где аttr_паme - ример, правило CH-S(na и учетная запись не была заданным правилам сооти вна \$(oid) (conusyemble в Blitz Identi в S(oid)), где attr_name - это им пример, правило CH-S(na вычисляемого значения, генерированная величния	ентификации, При перес в Виг Identity Provider дл это имя атрибута, полу ие) \$(surnaee) означае идентифицирована летствия латрибута, получаемог из атрибута, получаемог из атрибута, получаемог на (набор цифр и бука л	או входе пол ия ее послед чаемого от т, что атриб т, что атриб т, что атриб т, что атриб т, что атриб	ньзователя ч учощего свя поставшяна ут СN будет + добавить а чаемых от по щика ндентт ут CN будет со будет со будет чаемых от по щика ндентта ут CN будет	ерез постави зывания с уч идентификац формироват + добавить ус пытерналивное хставщика формироват волит присво	цик етн пься про про про про про про про про про про
Укажите правила соответствия учет идентификации с помощью этих пу записью поставидия идентификаци Для создания правила используйте можете указывать в одном правиле даух атрибутов - пале и зиглале че] Прадлагать пользователю ввести пол] Для привязки должна бить кайдена то] Прабовать ввод пароля, если учелюя евіа_oid рибуты Указите, каким образом должны фи идентификации. Для формикровати можете указывать в одном правино идентификации. Для формикровати можете указывать в одном правино фи правило можно использовать для а атрибуту ий значение вър-хохохос	ных записей Bitz Ider авил будет осуществ и: строиз подстановия несколько атрибутог рез пробел. и и парољ для привлаз пько одна учетная зап пько одна учетная зап пько одна учетная зап пъко одна учетная зап пъко одна учетная зап и и парољ. была идентифик и сакодото атрибута д обозначение §(attr несколько атрибута дания константного дания константного . (де хохохох – случа	ніцу Р. 1ятьс 5 (att и, есг ирова = Гы, ис лале), . Нап или в или в	точіder и поставцика иде я поиск учетной записи и г. повск учетной записи и г. повск учетной записи и г. повску така запись не была и учетная запись не была заданным правилом Сонбу на болть создано свое прав) тде attr_name – это им ример, правило Си-5 (на вычислиемого значенняя генерированная величан	ентификации. При перес в Вій Иепійу Provider дл это имя атрибута, полу ие) §(surnave) означає идентифицирована автопия и атрибута, получаемог има) §(surnave) означає има). из атрибута, получаемог има) §(surnave) означає Например, правило ціє на (набор цифр и буха л	м входе пол я ее послед чаемого от т, что атрий о от постава о от постава нево- steve steve steve нево- steve steve steve steve нево- steve steve steve steve steve нево- steve steve steve steve steve steve steve нево- steve steve steve steve steve steve steve steve steve натинского а	ньзователя ч проставшина поставшина кут СN будет чаемых от по цика иденти уг CN будет сN будет сN будет сN будет обок(4)) поз правита).	ерез постави зывания с уч идентификац • формироват • добавить ус пытернативное оставщика формироват волит присво	ция етн гъсзо про про про про про про про про про пр
Укажите правила соответствия учет идентификации с помощью этих пу записью поставцика идентификаци Для создания правила используйте можете указывать в одном правиле друх атрибутов – палее и зиглалее че] Предлагать пользователю ввести логи] Предлагать пользователю ввести логи] Для привязон должна быть найдена то] Требовать ввод пароля, если учетная евів_oid рибуты Укахите, какам образом должны фо центификации. Для формирования Для создання правила используйте можете указывать в одном правины и працититири можно используйте можете указывать в одном правины Пра создання правила используйте можете указывать в одном правина праним можно использовать для графути заничение втр-хоссо Доступные атрибуты для маляниета изрибут ці	ных записей Bitz Ider авил будет осуществ и и строиз подстановки несколько атрибуто рез пробел. и и паровь для привяза авись была идентифик и ракироваться атрибут в каждого атрибута д обозначение \${atter несколько атрибута адания константного адания константного да хоссоск – случа	tity P 1ятьс \${att h Han и, есг ирова = Гы, ис лаке i, Han или I йно с	точібег и поставцика иде я поиск учетной записи и гпаме), где аffпаme - ример, правило Си-\$(na и учетная запись не была и учетная запись не была и учетная запись не была и учетная запись не была заданным правило Си-\$(na на \$(oid)), где affпавило Си-\$(na ример, правило Си-\$(na ример, правило Си-\$(na па-числиемого значения, генерированная величан Правило	ентификации. При перес в Вій Иелійу Provider дл это имя атрибута, полу- ме) \$(surname) означає идентифицирована зетствия Ву Provider, на основе да випо. вя атрибута, получаемог ме) \$(surname) означає Например, правило ціє на (набор цифр и бука л	м входе пол ка ее послед чаемого от т. что атриб о от постав о от постав	ньзователя ч тутощего свя поставшика нут СN будет + добавить а чаемых от по щика нденты ут CN будет dom(4)) поз правита).	ерез постави зывания с уч идентификац • формироват • добавить ус пытернативное оставщика формироват волит присво Мастер	ция етни цип съссо спон пр съссо и пр
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле даух атрибутов – палее и зиглавече] Предлагать пользовителю ввести логи] Для привлаки должив быть кайдена то] Для привлаки должив быть кайдена то] Для привлаки должив быть кайдена то] Пребовать ввод пароля, если учетная евіа_oid рибуты Укажите, каками образом должны фо идентификации. Для формирования Для создания правила используйте идентификации. Для формирования для создания правила используйте и зиглавет в с одном правиле диух атрибуто – паке и зиглавеч и зиглаветь в одном правиле диух атрибуто – паке и зиглавеч диух атрибуто и спользовать для а атрибуту ий значение втр-хососос	ных записей Bitz Ider авил будет осуществ и и. строки подстановки несколько атрибутог ре пробел. лыко одна учеткая зап пыко одна учеткая зап лакос. была идентифис и римироваться атрибут и каходого атрибута д обосование Stater реак у обосо и стрибута д обосование Stater реак у обосо и стрибута д и обосование Stater и струга и саходого стрибута д и обосование Stater реак у обосо стрибута д и обосование Stater и струга и саходого стрибута д и обосование стрибуто реак пробел дании константного	ntity P Introc S (att ice no ice no i ice no ice no ice no ice no ice no ice no i i i i ice no i i i i i i i i i i i i i i i i i i i	точібег и поставщика иде почібег и поставщика иде (г_паве), где аff_пате – ример, правило Си-\$(па ти учетная запись не была заданным правилом Соотв аданным правилом Соотв виа \$(oid) \$(oid) (гользуемые в Biltz identi о быть создано соос прав), где аff_пате – это им пример, правило Си-\$(па вненспекоюто си-\$) генерированная величия Правило	нтификации. При перес в Вій Иепійу Provider дл это имя атрибута, полу- ме) \$(surnaxe) означає идентифицирована вегствия Ву Provider, на основе др авило. ця атрибута, получаємог на пример, правило ціє на (набор цифр и бука л	м входе пол и не послед чаемого от т, что атриб о от, от оатриб что атриб что атриб атинского а	ньзователя ч кующего свя поставшика ноставшика нут СN будет нут СN будет чаемых от по щика иденты ут CN будет чаемых от по щика иденты за CN будет чаемых от по свя свя свя свя свя свя свя свя свя свя на свя	ерез постави вывания с учи идентифика: формироват + добавить ус ставщика формироват волит присво Мастер	цикана ции простоя
Укажите правила соответствия учет идентификации с помощью этих пу записью поставидия идентификаци Для создания правила используйте можете указывать в одном правиле даух атрибутов - пале и зиглалее че] Предлагать пользователю вести логи] Для привязки должна быть найдена то] Для привязки должна быть найдена то] Трабовать ввод пароля, если учиться ваіа_oid рибуты Указите, казами образом должны фо идентификация. Для формирования Пля создания ил. Для формирования Пля создания правила используйте можете указывать в одном правиля идентификация. Для формирования Правило можно использувать можете указывать в одном правиля и создания агрибуты для маляние в грабуть доступные агрибуты для маляние в грабут	ных записей Bitz Ider вани будет осущества и строим подстановки несколько атрибутот рел пробел. и и парољ. для привлаз пъко одна учетная зап ванись была идечитифик а какдого атрибута д а какдого атрибута а данини будет несколько атрибута адания константного дания константного и де хоссост – случа	titty P 1ятьс \${att и, есг пось по ирова = гы, ис рожно уляне , Нап или t йно с	точіder и поставцика иде я поиск учетной записи и гг паве), где аttr_name - ример, правило Си-S(na и учетная запись не была заданным правилам соота на S(oid) 5 быть создано саое прав), где attr_name - это им ример, правило Си-S(na вънисляемого значения генерированная величи S(oid) S(oid) S(oid)	ентификации. При перес в Війz Identity Provider дл это имя атрибута, полу ве) \$(surnae) означає идентифицирована цастиция випо. и атрибута, получаемог ви атрибута, получаемог ви атрибута, получаемог ве) \$(surnaee) означає Например, правило і́с́с	мя входе пол ия ее послед чаемого от т, что атриб о от постава о от постава невот с т, что атриб	њзователя ч цующего свя поставшика југ СN будет + добавить а наемых от по цика идентти уг СN будет сN будет сN будет абак(а)} поз пфавита).	ерез постави зывания с уч идентифика, формироват + добавить ус пытернативное хставщика формироват волит присво Мастер	ция траниции простоя протостоя по по по по по по по по по по по по по
Укажите правила соответствия учет идентификации с помощью этих пу для соодания правила используйте можете указывать в одном правиле длях атрибутов - пале и зиглале че] Прадлагать пользователю ввести логи] Прадлагать пользователю ввести логи] Прадлагать пользователю ввести логи] Требовать ввод пароля, если ученаят евів_oid рибуты Ликоите, каким образом дотяны фо ицентификации. Для формирования Для создания правила используйте можете указывать в одном правиле иди создания правила используйте можете указывать в одном правиле для создания правила используйте можете указывать в одном правиле пате	ных записей Bitz Ider ванл будет осуществ и и строиз подстановки несколько атрибуто ре пробел. и и паровь для привязя лько одна учетная зап лько одна учетная зап дались была идентифи и обозначение \${attr несколько атрибута д обозначение \${attr несколько атрибута дадная константного адания константного дадняя константного и и и	titly P 1ятьс 5 (att и, есг ись по ирова = - - - - - - - -	точібег и поставцика иде я поиск учетной записи и гпаме), где аffпаme - ример, правило Си-S(na и учетная запись не была и учетная запись не была заданным правилам соото на быть создано соото правилам о быть создано соото пра у, где affпаme - это им ример, правило Си-S(ni ример, правило Си-S	нтификации. При перес в Вій Иелійу Provider дл это имя атрибута, полу- ве) \$(surname) означає идентифицирована затолина растаня (у Provider, на основе да вило. на атрибута, получаемог ва атрибута, получаемог на (набор цифр и бука л	м входе пол я ее послед чаемого от т, что атриб о от постав о от постав атинского а	ньзователя ч учощего свя поставшика нут СN будет чаемых от по щика нденти ут CN будет dom(4)) поз правита).	ерез постави зывания с уч идентификац • формироват • добавить уг • добавить уг • ставщика формироват • ставщика формироват • ставщика • формироват • ставщика • формироват • ставщика • ст	Linere Contraction of the second seco
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификации Для создания правила используйте можете указывать в одном правиле даух атрибутов - палее и зиглалее че] Предлагать пользователю веести логи] Для привязии должив быть найдена то] Для привязии мользователи работ и работати во должив проможение для создания правила используйте длях создания правила использование длях создания правила использование длях создания правила использование длях атрибуть и из качаение длях создания правила использование длях создания правили использования прав	ных записей Bitz Ider авил будет осуществ и и строиз подстановия несколько атрибутог несколько атрибуто на кларова. Для привязя лыко одна учеткая запі ланись, была идентифик и рамироваться атрибут а каходого атрибута д обосольки будет правина констатичного ура тробел адания констатичного у де хоосос – струга	titly P 1ятьс \$ (att и, есг ись по ись по ирова = Гы, но лале ь Нап или I йно с	точібег и поставщика иде почібег и поставщика иде почіск учетной записи и (г	нтификации. При перес в Вій Иелійу Provider дл это имя атрибута, полу ие) \$(surnae) означає идентифицирована нетствия пу Provider, на основе да вило. и атрибута, получаемог и атрибута, получаемог на (набор цифр и бука л	мя входе пол ия не послед чаемого от т, что атриб о от поста чаемого от о от поста на что атриб на триба соот о атриб на на на на на на на на на на на на на	њзователя ч цующего свя поставшика нут СN будет чаемых от по щика иденти ут CN будет чаемых от по цика идента тут CN будет	ерез постави вывания с уч идентифика: формироват + добавить ус ставщика формироват волит присво Мастер	ция
Укажите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле даух атрибутов - пале и зиглалее че] Прядлагать пользователю ввести логи] Для привязии допена быть найдена то] Трябовать ввод пароля, если ученаяя езіа_oid рибуты Указите, казым образом должны фо идентификации. Для формирования Пла создания Л. Для формирования Пла создания правила используйте можете указывать в одном правите идентификации. Для формирования Правило можно использовать для з атрибути ий значение втр- ососос Проступные атрибуты для малинига валае палее палее	ных записей Bitz Ider ваки будет осущества и строим подстановки пессолько атрибутот рел пробел. и и парољ. для привяза лако одна учетная зап вако одна учетная зап запись была идентифик и а каждого атрибута д а каждого атрибута а каждого атрибута ракороваться а атрибута и каже одна и учетная зап соргание была идентифик и с с с с с с с с с с с с с с с с с с с	tity P 1ятьс 5 (att и, есг ись по ирова = Гы, ис упане , нап или t яйно с	точіder и поставцика иде почіder и поставцика иде почіск учетной записи и г. повск учетной записи и г. повск), тде аttr_name - ример, правило Си-S(na заданным правилам соота ніа S(oid) Солть создано свое правила б создано свое правило Си-S(na ример, правило Си-S(na вънчеслиемого значения переноранная величии S(oid) S(firstName) S(firstName) S(firstName)	нтификации. При перес в Війz Identity Provider дл это имя атрибута, полу ие) \$(surnave) означає идентифицирована настаня інстаня випо. и атрибута, получаемог има атрибута, получаемог има) \$(surnave) означає Например, правило и ба на (набор цифр и бука л	м входе пол ия ее послед чаемого от т, что атриб о от постава о от постава невот у (кто атриб	њзователя ч цующего свя поставшика југ СN будет чаемых от по цика иденти уг СN будет сN будет сN будет сN будет	ерез постави зывания с учи идентификации + добавить ус потернативное оставщика формироват волит присво Мастер 2 2 2	ция странати страна
Указите правила соответствия учет идентификация с помощью этих пу для создания правила используйте можете указывать в одном правиле длях атрибутов - палее и зиглалее че] Прадлагать пользователю ввести пол] Для привязки должна бить кайдена то] Для привязки должна бить кайдена то] Трабовать ввод пароля, если учетная евіа_oid рибуты Указите, клани образом должны фи идентификация. Для формикровати идентификация. Для формикровати идентификация. Для формикровати идентификация. Для формикровати идентификация. Для формикровати идентификация. Для формикровати палее пале палее пизибелале	ных записей Bitz Ider ванл будет осуществ и и строиз подстановия несколько атрибуто ре пробел. и и парољ. для привлаз пико одна учетная зап пико одна учетная пико одна учетная зап пико одна учетная пико одна учетная зап пико одна учетная зап	tity P 1ятьс \$(att и, есл ись по ирова = - - - - - - - - - - - - -	точіder и поставцика иде почіder и поставцика иде почіск учетной записи и г. повіск учетной записи и г. повіск учетной записи и г. повіск, так са ставання соота на заданным правилом соота на S(oid) Спользуемые в Війс Іdenti о быть создано свое прав уста садствить со та ми ример, правило Сіт-S (na ример, правило Сіт-S (na ример, правило Сіт-S (na въчислятемого значения, пенерированная величая Бравило S(Inid) S(InidleName) S(InideName) S(InideName)	нтификации. При перес в Вій Иепіtly Provider дл это имя атрибута, полу- ме) \$(surname) означає идентифицирована расствия ву Provider, на основе дл ви атрибута, получаемог има атрибута, получаемог на атрибута, получаемог на (набор цифр и буха л	м входе пол я ее послед чаемого от т, что атрий о от постава о от постава невот, получа невот, сто атрий	ньзователя ч тутощего свя поставшика ут СN будет + добавить а чаемых от по щика иденти ут CN будет dom(4)) поз правита).	ерез постави зывания с учи идентификац • формироват • добавить ус • доб	
Указите правила соответствия учет идентификации с помощью этих пр эписью поставщика идентификаци Для создания правила используйте можете указывать в одном правиле для привази должна быть найдена то] Прадлагать пользователю ввести логи] Прадлагать пользователю ввести логи] Прадлагать пользователю авести логи] Трабовать ввод пароля, если учетная езів_eid рибуты Указите, какам образом должны фо центификации. Для формирования Для создания правила используйте можете указывать в одном правиле для создания правила используйте можете указывать в одном правина для создания правила используйте пате езів_oid пате пате tusted разврот	ных записей Bitz Ider авил будет осуществ и и строиз подстановия несколько атрибуто рез пробел. • и паровь для привязя авинсь была идентифик • • • • • • • • • • • • • • • • • • •	tity P татьс \${att L Han и, есг пось по ирова = Гы, ис Сллжне Сллжне или t йно с	точіder и поставщика иде я поиск учетной записи и гпаме), где аffпаme - ример, правило Си-S(na и учетная запись не была заданным правилам соото на в S(oid) 5 (oid) 5 (oid) 5 (oid) 5 (lasthame) 5 (lasthame) 5 (lasthame) 5 (passport) 5 (passport)	нтификации. При перес в Вій Иелійу Provider дл это имя атрибута, полу- ве) \$(surname) означає идентифицирована затотания ви ртоvider, на основе да випо. вя атрибута, получаемог ва дрибута, получаемог ва дрибута, получаемог ва дрибута, получаемог ва дрибута, получаемог ва (набор цифр и бука л	м входе пол и е послед чаемого от т, что атриб	ньзователя ч кующего свя поставшика нут СN будет чаемых от по щика ниренти нут СN будет dom(4)) поз правита).	ерез постави зывания с учи идентификац • формироват • добавить ус • доб	Line control of the c
Указите правила соответствия учет идентификации с помощью этих пр записью поставщика идентификации Для создания правила используйте можете указывать в одном правиле для привлан должна быть найдена го] Продлагать пользователю веести логи] Продлагать пользователю веести логи] Пробовать ввод пароля, если учетная евів_oid Указите, каким образом должны фо центификации. Для формирования Для создания правила используйте можете указывать в одном правиле идентификации. Для формирования Для создания правила используйте можете указывать в одном правиле идентификации. Для формирования Для создания правила используйте можете указывать в одном правиле израбуты и изичение вЪтоковать для с прибути вигалее пате пате пате пате разврой_вя	ных записей Bitz Ider ваки будет осуществ и и строиз подстановия несколько атрибуто не пароль Для привязя вых одна учетная зап лько одна учетная зап запись была идентифик и рамироваться атрибут в каждого атрибута д обозначение \$fatt обозначение \$fatt обозначение \$fatt обозначение \$fatt обозначение \$fatt обозначение \$fatt обозначение \$fatt обозначение \$fatt обозначение \$fatt и и и и и и и и и и и и и и и и и и	ыны на оказана и на кака и на оказана и кака и на оказана и кака и на оказана и кака и на оказана и на оказ и на оказана и на оказ и на оказана и на оказ и на оказана и на оказ и на оказана и на оказана	точіder и поставщика иде почск учетной записи и (*	ентификации. При перес в Вій і іdentity Provider дл это имя атрибута, полу- ме) \$(surname) означає идентифицирована эетствия ву Provider, на основе да вило. на атрибута, получаемос ме) \$(urname) означає Например, правило ціб на (набор цифр и бука л	м входе пол и е послед часмого от т, что атриб о от постал о от постал назв-б(сам	ньзователя ч кующего свя поставшика нут СN будет чаемых от по щика иденти уг CN будет чаемых от по щика иденти уг CN будет	ерез постави вывания с учи идентифика: • формироват • добавить ус • ставщика ерикарият. Вы ерикарият. Вы формироват волит присво Мастер • • • •	

Рисунок 88 – Дополнительные настройки поставщика идентификации ЕСИА

8.8. Вход через систему идентификации Сбербанка (Сбер ID)

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

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

азовые настройки Сбер	ID	
Адентификатор поставщика	sbrf_1	
	Уникальный идентификатор поставщика. Используется только внутри Blitz Identity Provider	
Название поставщика	Cõep ID	
	Отображаемое в консоли имя поставщика. Используется только внутри Blitz Identity Provider	

Рисунок 89 – Базовые настройки поставщика идентификации Сбер ID

- Зарегистрировать приложение в системе Сбер ID. Для этого воспользоваться инструкцией, размещенной на официальном сайте этого поставщика идентификации³⁹. По результатам регистрации вы должны иметь:
 - идентификатор клиента (Client ID);
 - секрет клиента (Client Secret);
 - сертификат своей системы, подключенной к Сбер ID;
 - сертификат Сбер ID.
- 5. Настройте защищенный канал связи между организацией и банком с использованием сертификата, полученного от ПАО «Сбербанк».
- 6. Перейти в Blitz Identity Provider и заполнить настройки поставщика идентификации (Рисунок 90), которые включают в себя:
 - URL для авторизации адрес, по которому должна инициироваться аутентификация, например: https://online.sberbank.ru/CSAFront/oidc/authorize.do;
 - URL для получения и обновления маркера адрес, по которому происходит получение и обновление маркера доступа. Должен быть указан внутренний адрес сети, обращение через который обеспечит работу по защищенному каналу связи между организацией и банком;

³⁹ Cm.: https://developer.sberbank.ru/doc/v1/sberbank-id/enrollsteps

- URL для получения данных адрес, по которому происходит получение данных пользователя. Должен быть указан внутренний адрес сети, обращение через который обеспечит работу по защищенному каналу связи между организацией и банком;
- идентификатор клиента (Client ID);
- секрет клиента (Client Secret);
- запрашиваемые группы данных перечень запрашиваемых групп данных из Сбер ID;
- правила, которые будут использоваться для идентификации учетной записи в Сбер ID и Blitz Identity Provider. Для создания правила следует использовать строки подстановки \${attr_name}, где attr_name – это имя атрибута, получаемого от Сбер ID. Можно указывать в одном правиле несколько атрибутов. Например, правило CN=\${first_name} \${last_name} означает, что атрибут CN будет сопоставляться с сочетанием двух атрибутов – first_name и last_name через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт Сбер ID, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;

- опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из Сбер ID, в Blitz Identity Provider. Например, правило mail=\${email} означает, что атрибут с именем mail в Blitz Identity Provider будет заполняться значением из атрибута email учетной записи Сбер ID (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через Сбер ID данный атрибут будет обновлен в хранилище Blitz Identity Provider.
- 7. Сохранить данные в Blitz Identity Provider.
- В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п. 4.3).
| езопасность | | | | | | | |
|--|---|--|---|--|--|---|--|
| Для заполнения используйте данны | е, полученные при р | егистр | рации своей системы в Банке. | | | | |
| URI перенаправления (Redirect URI) | http(s)://sudir.reaxoft.n
http(s)://sudir.reaxoft.n | ı/sps/l
ı/sps/j | ogin/externalldps/callback/sbrf/sbrf_1/false
profile/social/externalldps/callbackPopup/sbrf/sbrf_1 | | | | |
| | Адрес страницы, на к
аутентификации в сис | оторун
теме В | о будет перенаправлен ответ после успешной
Банка. | | | | |
| URL для авторизации | https://sudireaxoft.ru/auth/authentication/WS/abd/proxyAe | | | | | | |
| URL для получения и обновления
маркера | http://localhost:9010/a | uth/au | thenticationWS/sbrt/proxyTe | | | | |
| URL для получения данных | http://localhost:9010/a | uth/au | thenticationWS/sbrl/proxyGetUserData | | | | |
| Client ID | 76ee4aa5-5745-42d2-a | i5ce-d | a158dd0e0d7 | | | | |
| Client Secret | Изменить значение | | | | | | |
| уппы данных | | | | | | | |
| Запрашиваемые группы данных | name x email
international_passp
driving_license x
Для добавления груп | х
ort x
sni | address_reg X openid x
bitbidate X maindoc X Iss X mobile x
6 x gender X address_of_actuat_residence x
muck beguns ee Han II Haskanre Enter | | | | |
| | | | | | | | |
| дентификация учетных записей | | | | | | | |
| doys arphoyrob - name in sumame is | | | | | | | |
| доул ат уму тоо – полнос и долналис ча
Продлагать пользователю ввести логл
Для привязки должка быть найдека то
Д Требовать ввод пароля, если учеткая | н и пароль для привязк
ілько одна учетная запі
запись была идентифиц | и, есл
сь по
ирова | и учетная запись не была идентифицирована
заданным правилам соответствия
на | | | | |
| другот улиу тоор - полес и изликанс и изликанс и
Предлагать пользователю ввести логи
] Для привлаки допона быть найдена т
] Требовать ввод пароля, если учетная
mail | н и паропь для привязк
ілько одна учетная запи
запись была идентифиц | и, есл
ись по
ирова | и учетная запись не была идентифицирована
адданным правилам соответствия
на
=S(email.) | | × | | |
| доун анулку кое - нален и чолнале и
] Продлагать пользователю ввести пол-
] Для привязки должи быть найдена то
] Требовать ввод пароля, если учеткая
mail | н и паропь для привязи
лько одна учетная запи
запись была идентифиц | и, есл
ісь по
ирова | и учетная запись не была идентифицирована
заданным правилам соответствия
на
=S(email.) | | х
+ добавить ус | слов | |
| друк округу той – налися и должно и и
Прадлагать пользователю ввести логи
Для привлаки должка быть найдена то
2 Требовать ввод пароля, если учетная
mail
8 | н и пароль для привлэн
пько одна учетная запи
запись была идентифиц | и, есл | и учетная запись не была идентифицирована
адданным правилам соответствия
на
= | | х
+ добавить ус | слов | |
| друс отрисутос – налися и должлис и должлис и
Прадлагать пользователю ввести лога
Для привлаки должна быть найдена т
2 Требовать ввод пароля, если учетная
mail
R
mobile | н и паропь для привязи
пьихо одна учетная запи | и, есл
ирова | и учетная запись не была идентифицирована
адданным правилам соответствия
на
= \${email}
= \${phone_number} | | ×
+ добавить ук | слов | |
| друк опулну тою - палес и излитале и излитале и
Предлагать пользователно ввести логи
Для привязки должна быть найдена т
у Требовать ввод пароля, если учетная
mail
R
mobile | н и паропь для привязн | и, есл
ись по
ирова | и учетная запись но была идентифицирована
адданным правилам соответствия
на
= | | х + добавить ус х + добавить ус | слое | |
| дуу са улуу тоо - наласа и долалас и долалас и
Прадлагать пользователю ввести логи
Для привязки долока быть найдена то
Для привязки долока быть найдена то
Требовать ввод пароля, если учеткая
mail
t
mobile | н и паропь для приняза
пько одна учетная запи | и, есл | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить | + добавить ус
+ добавить ус
+ добавить ус
альгернативное | слов
слов | |
| друс от рису той - типис и излипис и от
Прадлагать пользователю ввести логи
Для приялаки долока быть найдена то
2 Требовать ввод пароля, если учетная
mail
8
mobile | н и паропь для привязя
пько одна учетная зап
запись была идентифиц | и, есл | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить | + добавить ус
+ добавить ус
+ добавить ус
альгернативное | слов
слов | |
| друг от улу тое - нален и изливне и
Прадлагать пользователю ввести лога
Для привлаки допона быть найдена т
2 Требовать ввод пароля, если ученкая
mail
3
тоbile | н и пароль для привязи | и, есл
ирова | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить | + добавить ус
+ добавить ус
+ добавить ус
альтернятивное | слов
слов | |
| друк опринутов - налися и авлиалися на
Прадлагать пользователно ввести логи
Для привлаю долока быть найдена та
∑ Требовать веод пароля, если учетная
mail
R
mobile
трибуты
Указите, каким образом доляны фе | н и паропь для привязи
пько одна учетная зап
запись была идентифиц
принроваться атрибу
в каждого атрибута да | и, есл
ирова | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
ных, получаемых от | + добавить ус
+ добавить ус
+ добавить ус
апьтернативное | слов
слов | |
| друк окринутов - налене и колиале и к
Прадлагать пользователю ввести логи
Для привязки должка быть найдена то
2 Требовать ввод пароля, если учетная
mail
R
mobile
Украите, клаим образом должны ф
идентификации. Для формировани
Для соддания правила используйт | н и паропь для привла
выко одна учетная зап
запись была идентифи
ракироваться атрибута
я каждого атрибута д
обозначение §дабуто
несколько атрибуто | и, есл
ирова
У | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= S{ernal}
= S[phone_number-}
S[phone_number-}
пользуемые в Bitz Identity Provider, на основе дан
обыть создано свое правило.
. це аtt_name - это имя атрибута, получаемого | + добавить
+ добавить
ных, получаемых от
от поставщика иден
от поставщика иден | + добавить ус
+ добавить ус
+ добавить ус
альтернятивное
поставщика
пефикации. Вы | слов
: пра | |
| друг от улку тое - налек и излекане то
Прадлагать пользователю веести лого
Для привлаки допона быть найдена то
2 Требовать веод пароля, если учетная
mail
mobile
рибуты
Указите, какама образом должны фо
идентификации. Для сорданов
для сордания и колонаето учить
для сордания и колонаето учить
окожете указывать в одном правнов
двух атрибутов - лаке и загласе
Правило можно колользовать для з
Правило можно колользовать для з | н и пароль для привязи
выко одна учетная зап
запись была идентифис
авлись была идентифис
в важдона нетир от работ
в важдона нетир батку
несколько атрибуто
грез пробел.
адания константного | и, есл
ирова
У
Гы, ИС
олжно
Нап
или в | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
+ добавить
ных, получаемых от
от поставицика иден
что атрибут СИ буд
110-5{&random(4)) п | + добавить ус
+ добавить ус
- х
+ добавить ус
альгернативное
поставщика
пофикации. Выа
теформироват
эзволит присве | слов
пра
пра
и пра | |
| друг от улку току току току току току току учетная Прадлагать пользователю ввести лога Для привлани допона быть найдена та Tpeбовать ввод пароля, если учетная mail рибуты Указите, ккаим образом долхоны финдентификации. Для формирования идентификации. Для формирования для создания правила используйте можете указывать в одном правило вух атрибуту и из начение вде-хоссооза пример агрибутов для магимете и | н и паропь для привязи
выко одна учетная запі
запись была идентифик
а каждого атрибута д
обозначение \${etc;
несколько атрибута
адания константного
адания константного
. де 2000000 – случа | и, есл
ирова
У
Гы, ис
элжно
паве)
или в
йно с | и учетная запись но была идентифицирована
заданным правилам соответствия
на
= <u>S(ernal-)</u>
= <u>S(phone_number-)</u>
пользуемые в Bitz Identity Provider, на основе дан
быть создано свое правило.
, где attr_пате - это има атрибута, получаемого
ример, правило CieS(ame) S(surrame) означает.
акчисляемого значения. Например, правило side-
reнерированная величана (набор цифр и бука па | + добавить
ных, получаемых от
от поставщика иден
что атрибут СN буд
217-5[&random(4)] п
пинского алфавита). | + добавить ус
+ добавить ус
+ добавить ус
апьтернативное
поставщика
пификации. Вы
ст формироват
эзволит присво | слов
слов
н пра | |
| друк от рису тое - полсе и коллансе на оплансе на
□ Предлагать пользоватевно ввести лога
□ Для привязки должа быть найдена та
□ Тробовать ввод пароля, если учетная
mail
пoble
рибуты
Указите, какам образом должны фо
центитьрикации. Для сормировани
для содания правила непользуйтя
можете указывать в одном правило
идентитерикации. Для сормировани
для содания правила непользуйтя
можете указывать в одном правило
примете агрибутов - паке и вислик чита
Правило можно использовать для за
агрибут у из минение в 27-хоссоссос
Пример агрибутов для маляния | н и паропь для привязи
выко одна учетная запи
запись была идентифик
а каждого атрибута д
обозначение Statter
исколько атрибуто
врез пробел.
адания константного
адания константного
с с луча | и, есл
ирова
У
Гы, ис
олжно
или в
йно с | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
ных, получаемых от
от поставцика иден
что атрибут СИ буди
згр-\${&randow(4)} пл
писского алфавита). | + добавить ук
+ добавить ук
* добавить ук
альтернативное
поставщика
поставщика
порикорал
эт формироват | слое
слое
пра | |
| друг стулку тое - налес и колналес и
Прадлагать пользователю веести лого
Для привлаки должна быть найдена та
Требовать веод пароля, если учетная
mail
в
mobile
рибуты
Указите, какам образом должны фо
идентификации. Для соодания правила используйтя
для соодания правила используйтя
для соодания правила используйтя
для соодания правила используйтя
а трибуть и зигнаес
правило можете указывать в одном правила
имогте указывать в одном правила
имогте указывать в одном правила
имогте указывать в одном правила
имогте указывать в одном правила
для соодания правила использовать для з
а трибуту ий значение вдр-хоссоска
Правира можете указывать в одном правила
итрибут и из начение вдр-хоссоска
Правира можете указывать в одном правила использовать для з
а трибуту ий значение вдр-хоссоска
Правира можете указывать в одном правила
итрибута и и и и и и и и и и и и и и и и и и и | н и паропь для привлзи
пько одна учетная запи
запись была идентифиц
а каждого атрибута д
обозначение \${ (атс.
нессолько атрибута
реа пробел.
адания консталитного
и, где хохохох – случа | и, есл
ирова
У
Гы, исс
папе]
. Нап
или в
йно с | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= S[email]
= S[phone_number.]
пользуемые в Bitz Identity Provider, на основе дан
быть создано свое правило.
, де аtt_пате - это има атрибута, получаемого
имер, правило Сибе(пале) § сигнате), созначаемо
акто создано свое правило.
, де аtt_пате - это има атрибута, получаемого
имер, правило Сибе(пале) § сигнате), созначаемо
вите создано свое правило. | + добавить
ных, получаемых от
от поставщика иден
что атрибут СМ буд
178-5{&random(4)} п
пинского алфавита). | + добавить ус
+ добавить ус
+ добавить ус
альтернативное
поставщика
пификации. Вы
ти формирования
заволият присве
Мастер | слое
слое
пра | |
| друг от рису тое - налее и волналее не Прадлагать пользователю ввести лога Для приелзах должна быть найдена т Требовать ввод пароля, если учетная тааl тоbile рибуты Указите, каким образом должны фе идентификации. Для формировани для создания правила используйте можете указывать в одном правиле идентификации. Для формировани для создания правила используйте можете указывать в одном правите Транипо можно использовать для са транипо можно использовать для атрибутую для маллания Траниро транирования Пример агрибутов для маллания | н и паропь для привязи
пько одна учетная зап
запись была идентифиц
а каждого атрибута д
обозначение \${attr
несколько атрибута
даваня константного
адавая константного
. де хохохох – случа | и, есл
ирова
У
Гы, ис
олжно
нап
или в
йно с | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
ных, получаемых от
от поставщика иден
что атрибут СN буд
зтр-s{&random(4)} п
пинского алфавита). | + добавить ус
+ добавить ус
+ добавить ус
альтернативное
поставщика
пификация. Вы
ет формироват
заволит присво | спое
при
гъся | |
| Друк от рису тое - налек и и илиппе, че
Предлагать пользователю ввести лога
Для приеязии должа быть найдена та
Тробовать ввод пароля, если учетная
тай
тобые
тобые
тобые
Пример агрибутов для малликга
Пример агрибутов для малликга
Пример агрибутов для малликга
Пример агрибутов для малликга
Пример агрибутов для малликга
тай | н и паропь для привлан
выко одна учетная зали
зались была идентифиц
в саждого атрибута д
носозначение State;
носозначение State;
адания константного
адания константного
дария константного
и де хоососс – спуча | и, есл
ирова
У , и
Калика
или в
или в
или в
или в | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
ных, получаемых от
от поставцика иден
что атрибут СИ буди
что атрибут СИ буди
эзр-\${&randow(4)} пт
писского алфавита). | + добавить ус
+ добавить ус
+ добавить ус
+ добавить ус
альтернативное
поставщика
поставщика
порикороват
эте формироват
эзволит присво
Мастер | аларана и при стана и при с | |
| друг от рису тое - полсе и волнале, че
друг от рису тое - полсе и волнале, че
для привлаки должна быть найдена т
для привлаки должна быть найдена т
для привлаки должна быть найдена т
товые
товые
товые
указите, каким образом должны фо
центификации. Для формирования
для создания солакии в должно формирования
для создания и зиглаяся ч
для создания и зиглаяся и
правило можно использовать для з
агрибуту из значение в гр. хососос
Пример агрибутов для малликга
товые
вольки и спользовать для з
агрибуте для малликга | н и паропь для привлан
пько одна учетная запи
запись была идентифиц
я каждого атрибута д
обозначение §{аста;
реа пробел.
адания константного
реа пробел.
адания константного
и де хохохох – случа | и, есл
ирова
у Солоно
тън, ис
олоно
или в
йно с | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= S[ernal.]
= S[phone_number.]
пользуемые в Bitz (dentity Provider, на основе дан
бить создано свое правило.
, де аttname - это има атрибута, получаемого
имер, правило Сне{st_ename}] сизначает
очитаеции основе дани
бить создано свое правило.
, де аttname - это има атрибута, получаемого
имер, правило Сне{st_ename}] сизначает
очитаеции основе дани
бить создано свое правило.
, де аttname - это има атрибута, получаемого
имер, правило Сне{st_ename}] сизначает
очитаеции основного значения. Например, правило иdde
тенерированная величина (набор цифр и бука лат
б(enail)
§(enail)
§(phone_number)
§(eub) | + добавить
ных, получаемых от
что поставщика иден
что атрибут СМ буд
178-5{&random(4)} п
пинского алфавита). | × + добавить ус × + добавить ус + до | спов
пра
и пра | |
| Друк от р. му току току току току току току току ток | н и паропь для привлан
выко одна учетная зали
заянсь была идентифии
в саждого агрибута д
обозначение \${etc;
несколько агрибута
дазняя константного
аданяя константного
дазняя константного
и де хохохох – случа
у
у | и, есл
ирова
урова
гы, исс
ллане
лане
или в
йно с | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
ных, получаемых от
от поставщика иден
что атрибут СК буд
137-5{&rendom(4)} пл
пиского алфавита). | х + добавить ух х добавить ух + добавить ух + добавить ух + добавить ух - слованить ух | спов
пра
и пра | |
| друг от рису тое - полне и коллание, че
друг от рису тое - полне и коллание, че
для приязки должа быть найдена та
для приязки должа быть найдена та
для приязки должа быть найдена та
для от учетная
для от учетная
для от учетная на
для на
для от учетная на
для
для от учетная на
для от учетная на
для от учетная на
для на | н и паропь для привлан
пько одна учетная зап
запись была идеятнфик
а каждого атрибута д
обозначение Statter
обозначение Statter
обобобобобобобобобобобобобобобобобобоб | и, есл
ирова
урова
ирова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
у
урова
урова
у
у
урова
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у | н учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
ных, получаемых от
от поставцика иден
что атрибут CN будь
137-5{(&randoc())) п
ниского алфавита). | × + добавить ус × + добавить ус × + добавить ус + добавить ус - -<td>і
правілістов</td> | і
правілістов | |
| Друк са рису ток - палас и колланс и колланс и
☐ Прадлагать попьзователю ввести лога
☐ Для привлази долока быть найдена т
☐ Для привлази долока быть найдена т
mail
поbile
грибуты
Уидияте, каким образом долоке и
идентификация. Для формирования
Для создания правила используйте
можете указывать в одном правите
идентификация. Для формирования
Для создания правила используйте
можете указывать в одном правите
идентификация. Для формирования
Пример агрибутов для маллоига
Пример агрибутов для маллоига
поbile
выя́с
Бизбид
Бизбид
Карибут
МізсіеName
LastName | н и паропь для привлан
пько одна учетная зали
зались была идентифиц
я какдого атрибута д
обозначение §(41ст,
иссолько атрибута д
обозначение §(41ст,
иссолько атрибута д
адания констатичого
и де хососос – случа
и и
и и
и и
и и
и и
и и
и и
и и
и и
и | и, есл
ирова
у при | и учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
ных, получаемых от
от поставщика иден
что атрибут СМ буд
137-5{&random(4)} п
пинского алфавита). | Х добавить ус + добавить ус + добавить ус + добавить ус + добавить ус | і пра | |
| Approx or provide of instruct in Administration Approximation of the administration of the administration American and approximation of the administration of the administre administrat | н и паропь для привлан
пько одна учетная зали
зались была идеятнфик
азались была идеятнфик
и саходого атрибута д
обозначение Sfatter
обозначение Sfatter
и саходого атрибута д
обозначение Sfatter
и саходого атрибута д
обозначение Sfatter
и саходого атрибута д
обозначение Sfatter
и саходого атрибута д
обозначение Sfatter
и саходого атрибута д
и саходого и саходого атрибута д
и саходого и саходого и саходого атрибута д
и саходого и саходого и саходого и саходого и
и саходого атрибута д
и саходого и саходого и саходого и
и саходого и саходого и саходого и
и саходого и саходого и
и саходого и саходого и
и саходого и саходого и
и саходого и | и, есл
ирова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
урова
у
урова
урова
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у
у | н учетная запись не была идентифицирована
заданным правилам соответствия
на
= | + добавить
ных, получаемых от
от поставцика иден
что атрибут CN будь
137-5{(&randod()) п
ниского алфавита). | × + добавить ус - + добавить ус - + добавить ус - + | анарана и правола и п | |

Рисунок 90 – Дополнительные настройки поставщика идентификации Сбер ID

8.9. Вход через систему идентификации Mos ID (СУДИР)

Для конфигурирования входа через учетную запись Mos ID (СУДИР) следует выполнить следующие шаги в разделе «Поставщики идентификации»:

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

Базовые настройки СУДИР Настройки поставщика идентификации СУДИР			
Базовые настройки СУДИР			
Идентификатор поставщика	mos_1 Уникальный идентификатор поставщика. Используется только внутри Bitz Identity Provider		
Название поставщика	СУДИР Отображаемое в консоли имя поставщика. Используется только внутри Bitz Identity Provider		
		Далее	

Рисунок 91 – Базовые настройки поставщика идентификации СУДИР

- Зарегистрировать приложение в системе СУДИР. Для этого подать заявку согласно инструкции, размещенной на официальном сайте этого поставщика идентификации⁴⁰. По результатам регистрации вы должны иметь:
 - идентификатор (client_id);
 - секрет (client_secret).
- 5. Перейти в Blitz Identity Provider и заполнить настройки поставщика идентификации (Рисунок 92), которые включают в себя:
 - URL для авторизации адрес, по которому должна инициироваться аутентификация, например: https://login.mos.ru/sps/oauth/ae;
 - URL для получения и обновления маркера адрес, по которому происходит получение и обновление маркера доступа, например: https://login.mos.ru/sps/oauth/te;
 - URL для получения данных адрес, по которому происходит получение данных пользователя, например: https://login.mos.ru/sps/oauth/me;
 - идентификатор (client_id);
 - секрет (client_secret);
 - запрашиваемые разрешения перечень запрашиваемых разрешений, например, openid и profile;

⁴⁰ См.: https://login.mos.ru/support (внешний СУДИР) и https://sudir.mos.ru/support (внутренний СУДИР)

- идентификатор укажите имя атрибута в СУДИР, который должен использоваться в качестве уникального идентификатора учетной записи. Для внешнего СУДИР это guid, для внутреннего СУДИР это uid.
- правила, которые будут использоваться для идентификации учетной записи в СУДИР и Blitz Identity Provider. Для создания правила следует использовать строки подстановки \${attr_name}, где attr_name – это имя атрибута, получаемого от СУДИР. Можно указывать в одном правиле несколько атрибутов. Например, правило CN=\${FirstName} \${LastName} означает, что атрибут CN будет сопоставляться с сочетанием двух атрибутов – FirstName и LastName через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт СУДИР, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если учетная запись была идентифицирована»:
 - опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту СУДИР;
 - опция не выбрана: учетная запись будет автоматически привязана к аккаунту СУДИР.
- правила сохранения атрибутов, полученных из СУДИР, в Blitz Identity Provider.
 Например, правило mail=\${mail} означает, что атрибут с именем mail в Blitz
 Identity Provider будет заполняться значением из атрибута mail учетной записи

СУДИР (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через СУДИР данный атрибут будет обновлен в хранилище Blitz Identity Provider.

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

настройки поставщика идентификации СУДИР					
езопасность					
Заполните данные для корректного взаимс подключения к порталу Москвы (mos.ru) мс	адействия Blitz Identity Provi жно посмотреть здесь. Инф	der с системой управ формация о работе с	ления доступом города Москвы. Подробнее о внутреннем контуром СУДИР размещена зде	получении доступа и съ.	и настройках
Предопределенные ссылки возврата (redirect_uri)	http(s)://agumerov.identityblit http(s)://agumerov.identityblit	z.ru/biitz/login/externs z.ru/biitz/profile/social	lldps/callback/mos/mos_1/false /externalldps/callbackPopup/mos/mos_1		
	Эти ссылки должны быть пр обработки результатов ауте используете защищенное со	оописаны в настройка энтификации пользов задинение.	х поставщика идентификации для корректной ателя. Используйте схему https, если вы		
URL для авторизации	https://login.mos.ru/sps/oauth	/ae			
URL для получения и обновления маркера	https://login.mos.ru/sps/oauth	Λe			
URL для получения данных	https://login.mos.ru/sps/oauth	Ime			
Идентификатор (client_id)	testapp				
Секрет (client_secret)	Изменить значение				
зрешения Запрашиваемые разрешения	ореліd х profile х Для добавления разрешения	я введите его имя и н	aximitro Enter		
	Укажите перечень разреше поставщику идентификация Biltz Identity Provider, чтобы п	ний (scope), которые ; 4. Обратитесь к админ золучить перечень до	олжны быть получены при обращения к истратору инешнего поставщика идентификации ступных разрешений		
іентификация учетных записей					
Укажите уникальный атрибут внешнего пос	ставщика идентификации, н	который будет испол	ьзоваться для связи учетной записи в Blitz Ide	entity Provider.	
guid					
дентификация учетных записей					
Укажите правила соответствия учетных за этих правил будет осуществляться поиск у	писей Blitz Identity Provider и четной записи в Blitz Identity	и поставщика иденти / Provider для ее пос	кфикации. При первом входе пользователя че педующего связывания с учетной записью пос	рез поставщика иде тавщика идентифик	тификации с помощью ации.
Для создания правила используйте строки правиле несколько атрибутов. Например, п	подстановки \${attr_name) равило CN=\${name} \${surr	, где attr_name - это ame} означает, что	имя атрибута, получаемого от поставшика и атрибут CN будет формироваться из двух атр	центификации. Вы м ибутов - name и sum	ожете указывать в одно ате через пробел.
Предлагать пользователю ввести логин и пар	оль для привязки, если учетн	ая запись не была ид	ентифицирована		
Для привязки должна быть найдена только о	дна учетная зались по заданн	ым правилам соответ	ствия		
2 Требовать ввод пароля, если учетная запись	была идентифицирована				
mail •			\$(mail-)	×	
					+ добавить услови
				+ добав	ить альтернативное прав
риоуты					
Укажите, каким образом должны формиро каждого атрибута должно быть создано св	ваться атрибуты, использує ое правило.	мые в Blitz Identity P	rovider, на основе данных, получаемых от пост	авщика идентифика	ции. Для формирования
Для создания правила используйте обозна правиле несколько атрибутов. Например, п Правило можно использовать для задания XXXXXXX, где XXXXXXIII – случайно сгенерир	чение \${attr_name}, где а равило ON=\${name} \${surr константного или вычисляе хованная величина (набор и	ttr_name - это имя ат ame} означает, что амого значения. Нал ифр и букв латинск	рибута, получаемого от поставщика идентиф атрибут CN будет формироваться из двух атр ример, правило uid=BIP-\${&random(4)} позв гго алфавита).	икации. Вы можете у ибутов - name и sur юлит присвоить атри	казывать в одном name через пробел. буту uid значение BIP-
Атрибут		Правило			Мастер
mail	·	= \$(mail-)			•
					+ Добавить атри
				Отмена	Удалить Сохран

Рисунок 92 – Дополнительные настройки поставщика идентификации СУДИР

8.10. Вход через другую установку Blitz Identity Provider

Для конфигурирования входа через учетную запись другого Blitz Identity Provider (например, установленного в другой организации, далее – «доверенный Blitz Identity Provider») следует выполнить следующие шаги в разделе Поставщики идентификации:

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

базовые настройки Blitz Identity Provide	звые настройки Blitz identity Provider		
Идентификатор поставщика	bitz_1 Уникальный идентификатор поставщика. Используется только внутри Bitz Identity Provider		
Название поставщика	Филиал в Санкт-Петербурге Отображаемое в консоли имя поставщика. Используется только внутри Bitz identity Provider		

Рисунок 93 – Базовые настройки поставщика идентификации Blitz Identity Provider при настройке федеративного доступа

- 4. Открыть консоль управления доверенного Blitz Identity Provider (или попросить администратора другого Blitz Identity Provider это сделать) и выполнить следующие операции:
 - перейти в раздел «Приложения»;
 - нажать на кнопку «Добавить приложение»;
 - указать идентификатор приложения, название и домен приложения;
 - сохранить приложение и перейти к его настройке;
 - выбрать протокол подключения OAuth 2.0;
 - указать секрет (client_secret), либо оставить предзаполненный вариант;
 - указать префикс ссылки возврата, в качестве которой указать URL основной Blitz Identity Provider, в который будет осуществляться вход;
 - произвести настройку необходимых разрешений в разделе «OAuth 2.0».
- 5. Перейти в Blitz Identity Provider и заполнить дополнительные настройки поставщика идентификации (Рисунок 94), которые включают в себя:
 - URL для авторизации адрес доверенного Blitz Identity Provider, по которому можно получить код авторизации;
 - URL для получения и обновления маркера адрес доверенного Blitz Identity Provider, по которому можно получать маркеры доступа;
 - URL для получения данных адрес доверенного Blitz Identity Provider, по которому можно получать данные пользователя;

- идентификатор (client_id), указанный в настройках доверенного Blitz Identity Provider;
- секрет (client_secret), указанный в настройках доверенного Blitz Identity Provider;
- запрашиваемые разрешения, данные разрешения должны быть определены в разделе «OAuth 2.0» доверенного Blitz Identity Provider;
- идентификатор атрибут доверенного Blitz Identity Provider, который будет использоваться в качестве идентификатора пользователя (обеспечивает уникальность учетной записи даже при изменении атрибута, отвечающего за имя пользователя);
- правила, которые будут использоваться для идентификации учетной записи в доверенном Blitz Identity Provider и Blitz Identity Provider. Для создания правила следует использовать строки подстановки \${attr_name}, где attr_name – это имя атрибута, получаемого от доверенного Blitz Identity Provider. Можно указывать в одном правиле несколько атрибутов. Например, правило CN=\${name} \${surname} означает, что атрибут CN будет сопоставляться с сочетанием двух атрибутов – name и surname через пробел. Можно указать несколько условий, которые должны выполняться одновременно, а также добавлять альтернативное правило;
- при необходимости следует отметить опцию «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована»:
 - опция выбрана: пользователю, будет предложено ввести логин и пароль учетной записи Blitz Identity Provider, чтобы привязать аккаунт доверенного Blitz Identity Provider, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider;
 - опция не выбрана: пользователь будет автоматически направлен на страницу регистрации, если по настроенным правилам не удалось найти учетную запись Blitz Identity Provider.
- при необходимости следует отметить опцию «Для привязки должна быть найдена только одна учетная запись по заданным правилам соответствия»:
 - опция выбрана: если по правилам соответствия найдено более одной учетной записи, то пользователю будет выведено сообщение об ошибке;
 - опция не выбрана: если по правилам соответствия найдено более одной учетной записи, то будет возможность продолжить процесс привязки;
- при необходимости следует отметить опцию «Требовать ввод пароля, если

учетная запись была идентифицирована»:

- опция выбрана: пользователю нужно вводить пароль для привязки его учетной записи к аккаунту социальной сети;
- опция не выбрана: учетная запись будет автоматически привязана к аккаунту социальной сети.
- правила сохранения атрибутов, полученных из доверенного Blitz Identity Provider, в Blitz Identity Provider. Например, правило mail=\${email} означает, что атрибут с именем mail в Blitz Identity Provider будет заполняться значением из атрибута email учетной записи доверенного Blitz Identity Provider (для пользователей, воспользовавшихся этим поставщиком идентификации). Кроме того, у каждого атрибута можно поставить опцию «Мастер». Если она отмечена, то при каждом входе через доверенного Blitz Identity Provider данный атрибут будет обновлен в хранилище Blitz Identity Provider.
- 6. Сохранить данные в Blitz Identity Provider.
- В разделе «Аутентификация» консоли управления включить использование метода аутентификации с использованием соответствующего внешнего сервиса идентификации (см. п 4.3).

фентификатор поставщика	bitz_1		
	Уникальный иденти внутри Blitz Identity	ификатор поставщика. Используется только Provider	
Название поставляния	Biltz		
	Отображаемое в ко	нсоли имя поставщика. Используется только	
	BHYTPH Bilt2 Identity	Provider	
Частройки поставщика и	дентификации Bli	itz Identity Provider	
Безопасность			
Для заполнения указання Identity Provider. Необход OAuth 2.0). Также переда	ых параметров обрат имая информация ра ийте администратору	итесь к администратору внешнего поставщи взмещена в свойствах подключаемого прил приведенные нике URI перенаправления.	яка идентификации Biltz ожения (по протоколу
Предопределенные ссылки возврата (redirect_uri)	http(s)://demo.reaxol /blitz_1/false http(s)://demo.reaxol /callbackPopup/blitz/	ft.ru/blitz/login/externalldps/callback/blitz ft.ru/blitz/profile/social/externalldps /blitz_1	
	Эти ссылки должны идентификации для аутентификации по вы используете заи	а быть прописаны в настройках поставщика и корристной обработак разультатов изызвателя. Используйте скому https, если изшимение соотичение	
URL для авторизации	https://login-tech.ex	ample.ru/sps/oauth/ae	
IIDI ana aomenina a	https://lipio.tech.ev	envola suizon (an statu	
обновления маркера	ings: nogimetries	anger to spir outliste	
URL для получения данных	https://login-tech.ex	ample.ru/sps/oauth/me	
Идентификатор (client_id)	test		
Cesper (client_secret)	Изменить значен	ие	
Раарешения			
Запрашиваемые	openid x pro	ofile x	
разрешения	Для добавления ра	арешения введите его имя и нажмите Enter	
	Укажите перечень ј получены при обра	разрешений (scope), которые должны быть щении к поставщику идентификации.	
	Обратитесь к адми идентификации Blit	нистратору внешнего поставщика tz Identity Provider, чтобы получить перечень	
Адентификация учетных	Обратитесь к адым идентификации Вій доступных разреши записей	нястратор внецието поставцика с Láenthy Provider, чтобы попучать перечень звай	
Адентификация учетных Укахоте уникальный атр учетной записи в Biltz ide Идентификатор gold	Обратитесь к кадин В идентификации В доступных разреши залисей ибут внешнего постая ntty Provider.	ынстратору инкличето поставирка Lidentry Provider, чтобы получить перечень вий	ьзоваться для связи
Адентификация учетных Укажите уникальный атр учетной заявко в Bill2 ide Идентификация учетных Адентификация учетных	Ократитесь к кадио ВВ деступных разреши азликсей ибут внешнего постан пфу Римидег.	ынстратору инкличето поставирка Lidentry Provider, чтобы получить перечень вий	ьзоваться для связи
Адентификация учетных Указотте уникальный атр учетной заявког в Битг ide Идентификалор gold Адентификация учетных Указотте правило соответ	Ократитесь к кадио ВВ здеступных разрешя доступных разрешя взлиссей ибут викцинего постан лялу Provider.	непратору инкличето поставирка (dentry frontide, чтобы получить перечень вий вцика идентификации, который будет испол	ьзоваться для саязи названиция При переом
Адентификация учетных Укажите унякальный агр учетной заявко в Війг іde Адентификатор guid Адентификация учетных Укажите правила соответ входя попьовален черн	Ократитсь к кадио ВВ диступнак разреши доступнак разреши азликсей ибут внешнего постан плу Ргочидет. заликсей сстана учетных залико в юстанцика центи	инстратору инкличето поставцика (инстр) Provider, чтобы получить перечень вий парика идентификации, который будет испол сёй Bltz Identity Provider и поставщика идент фикации с помощью этик правил будато поста идито свликации с учетной алики, рановало будато поста парито свликации с учетной алики, рановало будато поста	ьзоваться для связи нефикации. При пераои арстиалы локас учен
Адентнфикация учетных Укахите учикальный атр учетной заянки в Війг іос Флентификация учетных вода Адентификация учетных коходе пользовання чор заянка в Війг Іо́елій у учетных Пат создання в Війг Іо́елій у Пат создання водання обща пате и зипале через пр	Ократитсь к кадио ВВ деступные разреши деступные разреши азликсей ибут таньшиего постан ибут таньшиего постан ибу Ргондег. азликсей таника учетных запио станик учетных запио которы и срока по как идентификации. I (симат) \$ (симаная) от обоп.	нетратору инкличето поставцика с Центру Проибе, чтобы получить перенонь вый пцика идентификации, который будет испол в ВЕД Мол?Ву Розибет и поставщика идент фикации с покоцию этих правлит будет одо сциго сплонации с учетной залижае поста в алижнате учезнийть в адгонт правлете нест внамат, что априбут СМ будет формировать	ьзоваться для саязи ификации. При пераом царствиться пакся учет пира атрибута. опыз атрибута.
Адентификация учетных Указонте унякальный агр учетной заянки в Elitz ide Идентификация учетных gald Адентификация учетных Ликахите правила соотве ланкие в Bitz Identify Pro Дипс создания правила и получаемого от поставши пале и яшпале через пр	Обратитсь к кран органиция 201 доступные разреши азписей ибут внешнего постан ибут	ынстратору инкликето поставцика Liednity Provider, чтобы получить перечень вой видика идентификации, который будет испол водика идентификации, который будет испол фикацие, помощью этих правит будат ору- правит будат ору- сарит спикации, учитей завись, и подали не несе вижнаст, что атрибут СМ будет формировать и для приятихи, всях учитвая завись, но была и	њоваться для связи ификации. При первои церствита, поискучети ицика изрегија, опико агрибута, опико агрибута, опи агрибута, опи агрибута,
Адентификация учетных Учалите учикальный атр учетной заявке в Вілг і de Ицентификация учетных дві Адентификация учетных Учалите правила соответ входя пользователи чро лалка в Вілг (dontify Fro лалка в вілга от поставши Например, правило осно пале и виглаль пользователя о Предлигать пользователя быт	Обратитсь к кран органитесь к кран диступных разреши азликсей «бут внешнего постан плу Ргочиес. азликсей сстана учетных записо в постанцика цент истора с учетных записо в постанцика цент стана учетных записо в состанцика цент стана учетных записо в постанцика цент стана учетных записо в постанцика цент (чент) 5 (четных записо в центания учетных записо в постанцика цент стана учетных записо в состанцика цент стана учетных записо в состанцика цент стана учетных записо в состанция и состану стана учетных записо в состану с состан с состания и постану в состану с состания с состану в состану с состания с состану в состану с состания с состану с состания с состану с состания с состану в состану с состану с состану с состания с состану с состану с состания с состану с состану с состания с состания с состану с состания с состану с состания с с состания с сос	непратори инсцието поставцика Lidentry Provider, чтобы получить перечень вой парика идентификации, который будет испол сей BILZ (dentity Provider и поставцика идент фикацие с помощью этих правит будет орс- центо с помощью этих правито будет испол парите с помощью этих правито будет испол парите с помощью этих правито будет испол парите с помощью этих правито будет испол на помоще у использования организации и на применяние сону учитала запись не была и и учитная запись по заденным правитим соответ	ьзоваться для связи нфикация. При пераом адестатиться поискучен има агрифука. окако агрифуга. ся из двух агрифуга. ся из двух агрифуга.
Адентнфикация учетных Указотте унясальный атр учетной заянки в Биіг іос Идентяфикация учетных оди Адентнфикация учетных жара гопьзанетия чор заянка в Вйг іосяцаятеля чор для содания правела в например, правело см- нален и зилагателя чаравела в Гарадията пользователя Предолжать пользователя Пребевать вед гароле, е	Ократитска к кадон ВВ деступнак разреши деступнак разреши азликсей ибут внешнего постат явлу Provider. азликсей става угномание и воставщия кадонт истава учетнак запис воставщия цент истава учетнак запис воставщия цент (семе) с (селена) от селена записа бы	непратори инскието поставирка Lidentry Provider, чтобы получить перечень вой вържа идентификации, который будет испол воднка идентификации, который будет испол финацие с помощио этих правил будет оду- ири сознажаное с помощио этих правил будет оду- ири сознажаное с номощио этих правил будет оду- ири сознажаное с номощио этих правил будет оду- ири сознажаное с учетска запаса поста водна с учетска и поставицика и оди- на идентификации, который будет испол- в и исполнение с на исполнатири оди- в и исполнение с на исполнатири оди- в и правили, кото учетская запась но была и и учетная запась по заденным правилам созтае на идентифирована	ьзоваться для связи нафикации. При первои арститита плака учент арститита плака учент арститита и при при при при има агрифуга. Сн на двух агрифуга. Сн на двух агрифуга.
Идентнификация учетных Укахотте уникальный атр учетной заянки в Elitz loc идентификация учетных вода Идентификация учетных Козор ополозитети чор заянко в Bitz locatify for дана и в Bitz locatify for аанное и виталие через пр опорациятия пользователи () Требовать кема пароно, е mobile	Обратитсь к идиа одеступные разреши доступные разреши валисей ибут вичшието постан ибут ремивет. валисей стинку Ромбет. валисей стинку четных залися ибот постанциях идиато постанциях идиато исторон по ван идетитфикация. I собет. навести логии и паропо и навдена только одна стин учетная зались бы	нетратори инклието поставирия сибитор Инойски, чтобы получить перенень видика идентлификации, который будет испол видика идентлификации, который будет испол водина идентлификации, который будет испол фикации с помоцию этих правити будет осу оциго сознавания сучетной заликае поста поликание учетной заликае поста ранкими с учетной заликае поста визначити учетной заликае поста визначити учетной заликае поста и учетная залика, по заденны правития соэтем по изрептификации (genoble)	ьозовлъся для связи наченкации. При первои при первои первои первои при первои при
Адентнфикация учетных Указонте унякальный агр учетной заянки в Elitz ide Идентнфикация учетных диа Идентнфикация учетных Указите правила соответ заянки в Bitz Identify Fro Для создане правила и Пля создане правила и получаемого от постави пале и зиглале через пр аление и вит Аление и Солтвет аление и Вitz Identify Fro Для оржения целяма быт пале и зиглале через пр Прадпигать пеньзователя получения должа быт требовать евод паропо, е meble	Обратитсь к крани денстринание разроши доступные разроши азписей ибут внешнего постан ибут внешнего постан ибут внешнего постан азписей спине учетных загино обстанцика царито и опостанцика и опостан и опостанцика и опостан и опостанцика и опостан и опостанцика и опостан и опостание опостание и опостание и опостание опостание и опостан	siezpatopy mexicien o occasional (clearity Provider in occasional supera spectradynacijes, koropuli dyger econo el ditiz klenitij Provider in occasionale a speci glana spectradynacijes, koropuli dyger econo el ditiz klenitij Provider in occasionale a speci glana spectradynacijes o special dyger econo special constantino o special dyger special dyger econo special dyger ec	ьооваться для связи афякация. При пераон цестатиска поискусти или атрибука ся на даух атрибутов - или атрибука ся на даух атрибутов - арагнефскрована тетвия • дабавать условая
Адентнфикация учетных Укаюте уняслъчна атр учетной заянся в Битг Ide Идентяфикация учетных оди Адентнфикация учетных кооде пользователя чоре заянов в Вйг Identify Pro Для соддания правяла и например, правяло сен- нален в Иштание через п с Прадлигать пользователя Для преклая должа быт для преклая должа быт пробовать вед пароле, е тобе	Обратитесь к какуо ВВ деступных разреши деступных разреши азликсей ибут внешнего постат или // внешнего постат ил	неправори никането поставирна (сибнот) Ройоне (чтоби попучить перечина варнаа идентификации, который будет испол соб ВВС Мол10у Ройоне и поставицика идент фикацие с помациа и эки правил будет оден оди сознавание учетной а замася на била и использование о поставицика и оден правило сознавание о одено правило будет оден использование о одено правило будет оден использование о одено правило будет оден использование одено одено правила использование одено и учетная замась по заденным правилам созтае и учетная замась по заденовым правилам созтае и учетная замась по заденным правилам созтае (genoble)	ьооваться для связи ификация. При первои арстигата плася учен арстигариа, при первои арстигариа, си на двух агрибута. си на двух агрибута.
Адентнификация учетных Укахотте уникальный агр учетной заянки в Elitz loc идентификация учетных балите правила солтен входе пользователя чор заянка в Bitz locatify то дана в Bitz locatify то дана в Bitz locatify то дана в Bitz locatify то дана в Bitz locatify то данаемого от постави пате и виталее через пр от полученого от постави пате и виталее через пр от полученого и постави пате и виталее через пр от поредонаталь пельзователия поредонаталь пельзователия поредонатели со поредонателия поредонатели поредонателия поредонатели со поредонателия поредонателия поредонателия со поредонателия поредонатели со поредонателия поредонатели со поредонателия поредонателия поредонатели со поредонателия поредонатели со поредонателия поредонателия поредонатели со поредонателия поредонатели со поредонателия поредонателия поредонатели со поредонателия поредонатели со поредонателия поредонателия поредонатели со поредонателия поредонатели со поредонателия поредонатели со поредонателия поредонатели со поредонателия поредонатели со поредонателия поредонатели со поредонатели со поредонателия поредонатели со поредонателия поредонатели со поредонатели со поредонатели со поредонатели со поредонатели со поредонатели со поредонатели со поредонатели поредонатели со поредонатели с	Обратитсь к крани одеступные разреши доступные разреши валисей ибут вичшието постан ибут ричивет. валисей стоине учетные записе постанциясы центр ибот дительной и паропо в найдена только одна и назреня запись бы стои учетныя запись бы	непратору никането поставирна (dentry Provider, чтобы получить перечинь вид паряка идентификации, который будет испол — об BBZ Monthy Provider и поставицика иденти об BBZ Monthy Provider и поставицика иденти на испете указания заникале поста пранеции с поставицика иденти и принации с поставицика и принати и принати заника, по заденема правитике соответ и принати заника, по заденема правитике соответ и принати и принати с поставицика и принати и принати и принати и поставицика и принати и	ьооваться для связи мфикации. При пераом ицика храстивност полоскучет ицика храстивност полоскучет ицика храстивност полоскучет ицика храстивности ицика храстивности и храстивно и храстивности и храстивн
Адентнификация учетных Укахогте унякальный агр учетной заянки в Elitz Ide Ицентификация учетных диа Карентификация учетных Ицентификация учетных Идентификация учетных Идентификация учетных Диа содания правня и получаемого от постави алиска в Bitz Identify Fro Дито содания правня и получаемого от постави Дито содания правня и получаемого от постави Преблеать пользователя Преблеать пользователя получаемого от поставия Преблеать пользователя получаемого от поставия Преблеать пользователя получаемого от поставия Преблеать пользователя получаемого от поставия получаемого от поставия Преблеать пользователя получаемого от поставия получаемого от поставия Преблеать пользователя Преблеать пользо	Обратитска и дана денетофикации ВВ доступные разреши записей ибут тичешнего постан иву Ргоилог. записей спиня учетных записе постанцика записея а постанцика записе постанцика записе обосп. в некладичения запись бы спи и учетных записе обосп.	непратору никането постащина (Leidenty Provider, чтобы получить перечинь видика идентификации, который будет испол видика идентификации, который будет испол финации с помощью этих правит будет осу оцито спомощью этих правити иссле вижают, что атрибут СN будет формировать с ули принятих, если учитива залисью пости и учитивах запись, по заденным правитив соответ па идентификрирована [блеобе-] 4 диба	ьзовать са для саязи нарнящия. При первои царствить сл лаксу чен прия прибута, паксу чен прия прибута, са на друх атрибута - са на друх атрибута - цантафосьрована техния * добавить устани * добавить устани произвет, на основа далана
Адентнификация учетных Указонте уникальный агр учетной заянки в Elitz Ide идентификация учетных диа Идентификация учетных Указонте правина соответ колде пользователя чир заянка в Bitz Identify Fro Для ордания правила и получаемого от поставши пале и зиглале черо пр Преблана вови должав быт пале и зиглале черо пр получаемого и постави получаемого и постави получаемого и постави получаемого ст постави	Обратитсь к крани оденстринание разреши доступные разреши азликсей ибут танкцинего постан ибут танкцинего постан ибут танкцинего постан аликсей станик учетных залико постанциках залико постанцика	непратору никането постащина (Lidentry Provider, чтобы получить перечинь вид падека идентификации, который будет испол ей BBL Identity Provider и поставщика идент фикации с понощью этих правити будет осу оцито сильжание сучетной заликае поста паликае поставицика идент будет произодно и поставщика идент одино произодно и поставщика идент одино произодно и поставщика идент фикации с понощью этих правити о поста висти произодно и поставицика идент одино произодно и поставщика идент фикации с понощью и поставини будет осу оцито сильжание учетной заликае поста и и понте участная заликае поста и учетная заликае поста и учетная заликае поставити соответ па идентифицирована (Денове] с доба со атрибуты, используемые в IBIZ Identity F	ьзоелься для связи ифеклации. При первои церствитися поискучен щика трифута отно атрифуто са на друх атрифуто са на друх атрифуто са на друх атрифуто и и и и и и и и и и и и и
Адентнификация учетных Укахогте унякальный агр учетной заянки в Elitz Ide Ицентификация учетных диа Карнтификация учетных Ицентификация учетных Идентификация учетных Идентификация учетных Для оравния развеля и Пробланать обрато пате и зиглате пользователя Пробланть пользователя обрато полученных от поставира полученных от поставира Пробланть пользователя Турибуты Изанте пользователя обратом Прогозация и дианно и дианно обратом Прогозация и дианно обратом	Обратитсь к кран денстринание разреши доступные разреши азписей ибут вичешнего постан ибут вичешнего постан ибут вичешнего постан алинсей асписае аписей стивия учетных записо постанциках записо	непратори никането постащина L dentry Provider, чтобы получить перечинь видика идентификации, который будет испол видика идентификации, который будет испол видика идентификации, который будет испол финации с помощью этих правит будет осу оцито сознавания сучетной записью поста виканири с помощью этих правит будет осу оцито сознавания сучетной записью поста виканири с помощью этих правите исслание правити учетной записью поста виканири с помощью этих правите исслание виканири с помощью запись по была и иссла прибута, используевана записью то техно викание участная записью то была и учетная записью то заденным правитем соэтее па идентификрована брезове] са атрибуты, используевано в Bitz Identity F па форморожания кладото прибута должно ие § бусловене носталько заприбута должно	ьзоель-ся для секон ифекации. При первои цествити-са лаксу чен щика трибута. са на двух атрибутов - са на двух атрибутов - са на двух атрибутов - са на двух атрибутов - са на двух атрибутов - чатрибана, чело на ракон * добавить услеви * добавить услеви * добавить услеви рабони, на основе данны обать содно свее грабута, получаенихо он
Адентнфикация учетных Узахогте унякальный агр учетной закнога в Білг Ido Дентгификация учетных Карантификация учетных Узахогте правила соответ водо гользования четных Узахогте правила и получаемых от поставши алися в Віл (dentify Fro Для создания правила и получаемых от поставши алися в Вілг (dentify Fro Для создания правила и получаемых со то поставши алися в Вілг (dentify Fro Для создания развила и получаемых со то ставила и во со то со то со то со то со то алися в Вілг (dentify Fro Для создания со то со то со то и во со то со то со то со то со то со то для создания со то со то со то со то со то получаемых со то с	Обратитесь к крани одностофикации ВВ доступных разреши азликсей ибут внешнего поста пату Ргондег. аликсей аликсей аликсей истива учетнак запис постанция постания и пароп в найдена топько одна и достябрикации. Г сово учетная запись бы сти учетная запись бы	неправори никането поставирна Leidentry Provider, чтобы получить перечинь водна и денти фикации, который будет испол водна и дентификации, который будет испол водна и дентификации, который будет испол фикации с помацио этих правил будет оду- дито сознавание у чентка запись на идент прикации с помацио этих правил будет оду- иров сознавание у чентка запись на была и и рината запись по заданным правитых созтае вижает что агрибут СМ будет формировать соз агрибуты, используемые в Bitz Identity F и формарование на кандого агрибута должи- не \${ottom represented in a status и и и и и и и и и и и и и и и и и и и	вобоваться для связи нафикации. При первои арстиванся ложе учен- паратификарована си на друх агрибута. си на друх агрибута. си на друх агрибута. си на друх агрибута. С на друх агрибута. С на друх агрибута. С на друх агрибута. С на соцано свето точбог, на основе данны о бить содано свет грабута, получаемого от наще на рискание права.
Адентнификация учетных Укахотте уникальный агр учетной заянки в Elitz loc guid Адентнификация учетных входе пользователя входе пользователя чоре заянка в Bitz location укахоте правила соответ входе пользователя чоре заянка в Bitz location Пля создания правета и получаемого от поставии заянка в Bitz location Пля создания правета и получаемого от постави заянка в Bitz location Пля создания далянае бит палее и зигнале через пр получаемого от постави палее и зигнале через пр получаемого от постави палее и зигнале через пр получаемого сто постави получаемых сто поставира получаемых от поставира по избето поставирая центерная специона (Suprame) с пробел.	Обратитсь к дажа денстрикация ВВ доступные разреши залисей ибут знешнего постан ибут леншнего постан ибут ремиест. записей стини угонные записо постанция и денти ибог дини е по следву стини учетных запись бы стину учетных запись бы стину учетных запись бы сти учетных запись бы	настратори инсцието поставирна () Edentry Provider, чтобы получить перечень вой пцияка идентификации, который будет испол е в BBIz Monthy Provider и поставицика идент ократо спознавлика сучетной записье постав и в вологте узаказато в дорока провито будет ос осцего спознавлика сучетной записье по была и и вологте узаказато в дорока провито ос и вологте узаказато в дорока провито на поставности с учетной записье на была и и учетная запись по заденным правитом соотеке винаети с участной соотеке и учетная запись по заденным правитом соотеке винаети участное дорока родината запись на была и и учетная запись по заденным правитом соотеке и учетная запись по заденным правитом должном и учетная запись по запись на двух прифутор должном и тактисото записамитом должном и патинского аправитом.	ьолелться для связи нернация При первои перекация При первои перекация перекация изма аруктарносток са на даух агрибута - аритефицирована истеня * добавть условен э добавть условен точабот, на основе данны о быть соцано свое грабута, получението с работа, получението с работа, получението с в слажие и распие, черес орано, содавно осно – случавно
Адентнификация учетных Указолге унякальный арт учетной заянки в Elitz Ide Ицентификация учетных дой Адентификация учетных Казолге правила соответ указолге правила соответ указолге правила соответ и указолге правила соответ окоде пользователя чер заянкое в Bitz Identify Fro- лаго садания правила и Пля сорания правила и Пля сорания оказонателя Для привихия должае бит пате и зиглале через пр Преблеать лека соответ потучених должае бит оказонате правила и потучених ст поставира потоставирия систома образом, правило и сорания правила и Соефсием (сорания правила и соефсием) (согдания правила и соефсием) (составирати составирати соефсием) (согдания правила и соефсием) (составирати правила и соефсием) (составирати составирати со	Обратитска и дража денетофикация ВВ денетофикация ВВ денетофикация ВВ денетофикация ВВ денетофикация В азписей записей стиви учетных запися поставщика запися поставщика запися поставщика запися поставщика запися поставщика запися обост. ввести логии и парала в найдена только одна сли учетных запися одна сти учетных запися обост. ввести логии и парала в найдена только одна сли учетных запися одна обост. ввести логии и парала сли учетных запися одна обост. ввести логии и парала сли учетных запися одна обост. ввести логии и парала сли учетных запися одна обост.	непратори никането постащина L dentry Provider, чтобы получить перечинь I dentry Provider и поставщика адоит в BIEz Monthy Provider и поставщика адоит финации с почицью этих правит будет осу- ставляети (дентафикации, который будет испол финации с почицью этих правит будет осу- сциго сильании с учетной заликаю поста пананая и сучетной заликаю поставицика адоит раконски учетной заликаю поставицика и пананая и сучетной заликаю постави- в обла и сучетной адиись учетной заликаю постае пананаяти учетной заликаю постае пананаяти с учетной заликаю постае пананаяти с учетной подавите и согтае пананаяти с учетной подавите и согтае пананаяти с по заденными правитем соответ пананаяти с по заденными правитем соответ пананаяти с по задениеми правитем соответ пананаяти с по заденными правитем соответ пананаяти с по задениеми с полько зарибутов СМ будет форморование в водоко правичения с датоко панатекско аправити). Правило	ызовать са для саязия нарежащие. При первои церствитися поискучен щита трибута отно атрибута са на атрибита са на на на на на на на на
Адентнфикация учетных Ухахогге унякальный арт учетной записи в Elitz ide Ицентификация учетных gold Адентификация учетных боловансти цевила соотвен улахоге правила соотвен улахоге правила соотвен для создажи в Bitz identify Pro- Для создажи дляма быт Порблеать вонд парона, е потученкос поставира Ктрибуты Ухахоге клася образом, полученкос с поставира роденто, Для создажи правила и соъбдения усилива с поставира родения Странорите, какия образом, полученкос с поставира Создажи правила и Соъбдения усиливая с поставира Создажи правила Соъбдения усиливая с поставира Создажи правила Соъбдения Странорите, какия образом, Создажи правила Соъбдения С стенеророванная вселная Соъбдения С стенеророванная вселная Сородения Странорите С стенеророванная вселная Сородения С стенеророванная вселная С составира составира С стенеророванная вселная С стенеророванная вселная С составира составира С стенеророванная вселная С составира составира С стенеророванная вселная С составира составира С стенеророванная вселная С составира С стенеророванная вселная С составира С составированная С составира С составир	Обратитсь к идиа оденстрикации ВВ доступных разреши залисей ибут викцикстр Лостан ибут викцикстр Лостан паку Регинаст аписей спиня учетных залисе постанциках залисе постанцика	непратори никането постащина L dentry Provider, чтобы получить перечинь I dentry Provider и поставщика адеит в BIEz Monthy Provider и поставщика адеит финации с почицью этих правит будет осу- ството и почицью тих правит будет осу- ството и почицью тих правит будет осу- правили с почицью этих правит будет осу- ството и почицью этих правити почисания финации с почицью этих правити почисания правили с учетной записью поставичника адеит разниками с учетной записью поставит в и оконст участнаять записью поставит почисания учетной записью поставити соответ по премятия, если учетной записью поставити соответ по премятия, со заденным правития соответ по премятия, со заденными по по прибуто с Модет форморование валадого прибуто правития, со алифонитования, то со заденния на работ со алития со аливития со то ответ на в по	ызовать-ся для связня нарнязация. При первои царствити-са локсу чент при атрибута. са на атрибита. са на н

Рисунок 94 – Настройки подключения к внешнему поставщику идентификации

Blitz Identity Provider

9. Управление учетными записями пользователей

В разделе «Пользователи» консоли управления доступны следующие операции:

- поиск учетных записей пользователей;
- добавление учетных записей пользователей;
- просмотр и редактирование идентификационных данных пользователей;
- смена пароля учетной записи;
- просмотр и отвязка учетных записей внешних систем;
- задание значений дополнительных атрибутов пользователей;
- привязку устройств для проведения двухфакторной аутентификации;
- просмотр групп, в которые включен пользователь;
- просмотр прав;
- просмотр выданных приложениям разрешений на доступ к данным;
- удаление учетной записи.

Общий вид страницы управления данными пользователей представлен на рисунке 95.

Пользователи					
test@reaxoft.ru					Q Найти
				Создать учетную запись поль	зователя
Учетные записи пользователей					
built-in: BIP-JHAV7DQ Петров Иван	Данные пользователя	a			
		name	Иван		
	use	rname	petrov		
	su	rname	Петров		
		mail*	test@reaxoft.ru		
		uid	BIP-JHAV7DQ		
	,	mobile	+7(910)4135615		
		email	test@reaxoft.ru		
					Сохранить
	Смена пароля				
	Новый пароль			Сгенерировать пароль	
				1	Изменить

Рисунок 95 – Вид страницы управления пользователями

9.1. Поиск учетных записей пользователей

Для поиска пользователей необходимо ввести идентификатор пользователя и нажать на кнопку «Найти». В качестве отображаемого идентификатора используется атрибут, определенный в разделе «Источники данных» в качестве базового идентификатора, а также атрибуты, отмеченные как поисковые.

Перечень найденных пользователей содержит:

- значение идентификатора найденного пользователя;
- хранилище, в котором найден пользователь;
- имя пользователя, сконфигурированное в разделе «Источники данных».

Нажатие на любую из найденных учетных записей открывает детальную информацию о пользователе.

9.2. Добавление учетных записей пользователей

Для добавления новой учетной записи требуется нажать на ссылку «Создать учетную запись пользователя...». В отрывшемся окне:

- указать хранилище, в которым 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» (*)).

		_
юиск		Q Найт
Укажите атрибуты пользователя.		
Хранилище	internal-only Idap	
givenName	1	
telephoneNumber		
cn		
sn		
mail		
uid*		
Пароль		
	Создать Отменить	

Рисунок 96 - Создание учетной записи пользователя

9.3. Просмотр и изменение атрибутов пользователей

При нажатии на идентификатор любого найденного пользователя отображается информация о нем – карточка пользователя. Она содержит значения атрибутов, которые были определены в разделе «Источники данных», а также привязанные учетные записи внешних поставщиков идентификации, привязанные средства аутентификации и др.

Пользователи				
test@eesuch zu				O Hožev
เราเพิ่มสุรงแก่น				
				создать учетную запись пользователя
Учетные записи пользователей				
built-in: BIP-JHAV7DQ Петров Иван	Данные пользователя	я		
		name	Иван	
	use	ername	petrov	
	su	irname	Петров	
		mail*	test@reavoft.ru	
		uíd	BIP-JHAV/DQ	
		mobile	+7(910)4135615	
		email	test@reaxoft.ru	
				Сохранить
	Смена пароля			
	Новый пароль			Сгенерировать пароль
				Изменить
	Привязанные учетны	е записи в	внешних систем	
	Учетные записи внешних	к систем от	сутствуют	
	Требуемый уровень а	аутентифи	кации	
	Вы можете настроить пользователь должен	ь требуемы н иметь урс	й уровень аутентификации для данного пользовате/ звень, указанный в разделе "Аутентификация".	я. Вариант "по умолчанию" означает, что
	Требуемый уровень	Первый и	второй фактор	×
				Сохранить

Рисунок 97 – Просмотр информации о пользователе (фрагмент)

На карточке пользователя можно совершать следующие операции:

- редактировать атрибуты пользователя;
- изменять пароль;
- просматривать перечень привязанных аккаунтов внешних поставщиков аутентификации;
- изменять требуемый уровень аутентификации для пользователя;
- привязывать устройства для проведения аутентификации: генераторы разовых паролей (см. п. 9.3.3) и мобильные приложения для получения push-уведомлений (см. п. 9.3.5);
- просматривать группы, в которые включен пользователь (см. п. 9.3.6);
- просматривать права пользователя и права, которые имеются в отношении данного пользователя (см. п. 9.3.7);
- просматривать и удалять выданные приложениям разрешения.

9.3.1. Редактирование атрибутов пользователя

При просмотре карточки выбранной учетной записи пользователя администратор может изменить любой атрибут пользователя. При редактировании учетной записи следует учитывать те ограничения, которые настроены для хранилища данных, в которое осуществляется запись.

Следует учитывать, что при изменении данных через интерфейс редактирования атрибутов не учитываются правила, используемые в процессе самостоятельной регистрации пользователя. Например, изменение адреса электронной почты или номера мобильного телефона не требует подтверждения.

9.3.2. Смена пароля пользователя

Для смены пароля используется блок «Смена пароля». Новый пароль можно ввести вручную, либо сгенерировать – для этого необходимо оставить чекбокс «Сгенерировать пароль». Новый пароль будет отображен в информационном блоке успешного выполнения операции.

При задании нового пароля вручную следует учитывать ограничения парольной политики для того хранилища, куда сохраняется пароль.

Смена пароля	
Новый пароль: kJ5pVXmT	×
Новый пароль	🕼 Сгенерировать пароль
	Изменить

Рисунок 98 - Смена пароля

9.3.3. Просмотр и отвязка аккаунтов социальных сетей

В блоке «Привязанные учетные записи внешних систем» можно посмотреть перечень аккаунтов внешних поставщиков идентификации (социальных сетей, ЕСИА, Сбер ID), привязанных к учетной записи найденного пользователя. Каждая привязка характеризуется уникальным идентификатором, где последняя часть – это внутренний идентификатор аккаунта в соответствующем поставщике идентификации. Например, в записи esia:esia_1:1000347601 последняя часть (1000347601) – это идентификатор аккаунта в ЕСИА. При необходимости можно удалить соответствующую привязку.



Рисунок 99 – Просмотр информации о пользователе: привязанные аккаунты внешних поставщиков

9.3.4. Привязка устройств для проведения двухфакторной аутентификации по разовому паролю

Администратор может привязать к учетной записи выбранного пользователя средство для проведения двухфакторной аутентификации. Например, можно привязать аппаратный HOTP/TOTP генератор по серийному номеру (Рисунок 100) либо привязать к учетной записи по QR-коду мобильное приложение, осуществляющее выработку TOTP-кодов (Рисунок 101).

Серийный номе	0	
	Серийный номер устройства генерации разовых паролей	
Пароль	1	
Пароль	2	

Рисунок 100 – Привязка НОТР-устройства по серийному номеру администратором

Название генератора	GoogleAuthenticator	
Алгоритм шифрования	SHA1 Y	
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	NAWGF7K7DXV75DH2SFCMBOSBUPVJ2CQG	

Рисунок 101 – Привязка ТОТР-приложения по QR-коду администратором

9.3.5. Привязка мобильного приложения Duo Mobile

Для проведения аутентификации средствами Duo Mobile необходимо провести привязку мобильного приложения к учетной записи пользователя. Рекомендуемый сценарий – пользователь самостоятельно привязывает свое мобильное приложение в веб-приложении «Личный кабинет».

Альтернативный способ привязки – через консоль управления. Для этого необходимо в разделе «Пользователи» найти необходимую учетную запись и блок настроек «Приложение Duo Mobile (QR-код)». В этом блоке следует нажать на кнопку «Привязать Duo Mobile», далее отсканировать отображенный QR-код мобильным приложением Duo Mobile.



Рисунок 102 – Привязка мобильного приложения Duo Mobile

9.3.6. Просмотр групп, в которые включен пользователь

Если пользователь включен в группы, то эта информация будет отображена в блоке «Членство в группах» (Рисунок 103). По каждой группе будет отображены следующие данные:

- идентификатор группы;
- значения атрибутов группы.

Членство в группах		
Идентификатор	Данные группы	
admins	name: Администраторы	

Рисунок 103 – Просмотр групп пользователя

9.3.7. Просмотр прав

Если в отношении пользователя есть права со стороны приложений или других учетных записей, то это будет отображено в блоке «Права в отношении пользователя» (Рисунок 104). Если пользователь имеет права в отношении объектов, например, других учетных записей, то это будет отображено в блоке «Права пользователя в отношении объектов» (Рисунок 105).

Каждое право характеризуется следующими параметрами:

- идентификатор объекта;
- имя;
- право.

Права в отношении пользователя					
Идентификатор	Имя	Право			
test-system	АИС (Тест)	Назначать права (registrator)			
prod-system	АИС (Прод)	Назначать права (registrator)			

Рисунок 104 – Просмотр прав в отношении пользователя

Права пользователя в отношении объектов						
Идентификатор	Имя	Право				
018180a6	Петров Илья Андреевич	Менять пароль (parent)				
ec43af55	Сергеев Иван Петрович	Менять пароль (parent)				

Рисунок 105 – Просмотр прав пользователя в отношении объектов

9.3.8. Просмотр и удаление выданных приложениям разрешений

Администратор имеет возможность просмотреть перечень выданных пользователем разрешений приложениям на доступ к его данным (Рисунок 106). Каждое разрешение описывается:

- идентификатор приложения;
- перечень разрешений (scope);
- дата выдачи разрешений.



Рисунок 106 – Просмотр выданных разрешений

10. Просмотр групп пользователей

Если в Blitz Identity Provider настроена возможность работы с группами пользователей (см. п. 15.1.14), то в консоли управления появится раздел «Группы». В данном разделе можно осуществлять поиск групп по одному из сконфигурированных атрибутов.

По каждой найденной группе отображаются ее атрибуты (см. Рисунок 107). Кроме того, в блоке «Члены группы» отображаются все пользователи, включенные в данную группу. По каждому пользователю отображается:

- идентификатор;
- имя пользователя согласно шаблону, определенному в разделе «Источники данных» («Имя пользователя в консоли»).

Группы							
Профиль grps	Атрибут id	T	Значени	ve	Q Найти		
Группы пользователей		Ланные гоуппы					
ponerusers		пате Расширенные права					
		Члены группы					
		Идентификатор		Имя пользователя			
		e99495e8-ef2b-4a48- b15b-5840849bdf41		Иванова Ксения Сергеевна			

Рисунок 107 – Просмотр групп пользователей

11. Просмотр событий безопасности

Для ведения аудита безопасности и для просмотра зарегистрированных в журнале Blitz Identity Provider событий безопасности используется раздел «События» консоли управления. Здесь имеется возможность осуществлять фильтрацию событий безопасности по различным критериям:

- по пользователю (указание идентификатора пользователя обязательно);
- по диапазону дат;
- по конкретному приложению;
- по группам событий;
- по IP-адресам;
- по протоколам взаимодействия.

После настройки фильтров и их применения предусмотрен просмотр детальной информации о найденных событиях.

Зн	ачение			Период		Групг	па событий	
0d3f5621-9725-4a48-b0f0-210d9b890dd0			0890dd0	28.05.2021 00:00	28.05.2021 23:59	Вход Авторизация доступа 05.2021 23:59 Историзация доступа		Авторизация доступа
Идентификатор объекта				за сегодня за нед	а неделю за месяц Изменения учетной записи Операции с г		анных данных писи 🔲 Операции с группами	
ſ	Толный IP-ад	дрес или маска				Прото	окол Auth 2.0 🔲 SAML	🗌 Другие
H	Название приложения							
	Трименить ID процесса	Очистить Время	Событие		Субъект	Объект	Приложение	IP-адрес
	Трименить ID процесса e0341c6a	Очистить Время 28.05.2021 14:02:28	Событие Выполнен выход		Субъект 0d3f5621-9725- 4a48-b0f0- 210d9b890dd0	Объект 0d3f5621-9725- 4a48-b010- 210d9b890dd0	Приложение Личный кабинет	IР-адрес 89.255.71.120

Рисунок 108 – Просмотр событий безопасности

12. Настройка уведомлений и отправки сообщений

Для задания настроек уведомлений и подключения к системам отправки сообщений используется раздел «Сообщения» консоли управления Blitz Identity Provider (Рисунок 109). В этом разделе можно настроить уведомления и подключение к:

- сервису отправки SMS-сообщений;
- сервису отправки push-уведомлений;
- SMTP-серверу.

Для настройки уведомлений необходимо на основной странице раздела:

- выбрать канал для восстановления (электронная почта, мобильный телефон) и указать атрибут со значением этого контакта. Атрибут задается с помощью регулярного выражения, например, \${mobile} означает, что информация будет отправлена на телефон mobile;
- выбрать события, по которым требуется отправлять уведомления. Возможно уведомление при следующих событиях:
 - вход с неизвестного устройства;
 - смена пароля;
 - смена пароля в зависимой учетной записи;
 - восстановление доступа;
 - восстановление доступа в зависимой учетной записи;
 - привязка учетной записи социальной сети;
 - настройка метода двухфакторной аутентификации;
 - изменение режима подтверждения входа;
 - получение права менять пароль в зависимой учетной записи;
 - предоставление права менять пароль;
 - отзыв права менять пароль в зависимой учетной записи;
 - отзыв предоставленного права менять пароль;
 - регистрация учетной записи.

Уведомления						
Настройте уведомления и пользователи будут оповещаться о различных событиях безопасности						
Способы уведомления						
Способ уведомления	Атрибут с контактом					
Электронная почта	\${email-}					
	+ Добавить способ уведомления					
Уведомлять пользователя о событиях						
Вход с неизвестного устройства						
Смена пароля						
Смена пароля в зависимой учетной записи						
Восстановление доступа						
 Восстановление доступа в зависимой учетной зап 	иси					
 Привязка учетной записи социальной сети 						
 Настройка метода двухфакторной аутентификаци 	И					
 Изменение режима подтверждения входа 						
Получение права менять пароль в зависимой учет	ной записи					
 Предоставление права менять пароль 						
Отзыв права менять пароль в зависимой учетной :	записи					
 Отзыв предоставленного права менять пароль 						
Регистрация учетной записи						
	Сохранить					

Рисунок 109 – Настройка уведомлений и подключения к системам отправки сообщений

12.1. Настройка подключения к SMS-шлюзу

Blitz Identity Provider необходима возможность отправлять SMS-сообщения, если используются следующие функции:

- аутентификация на основе отправки по SMS кода подтверждения (первый и второй фактор);
- информирование о важных событиях безопасности по SMS;
- изменение номера мобильного телефона через «Профиль пользователя»;
- восстановление забытого пароля с использованием мобильного телефона как канала подтверждения владения учетной записью;
- подтверждение номера мобильного телефона при регистрации пользователя.

Настройки задаются в консоли управления Blitz Identity Provider в разделе «Сообщения». Экран настроек приведен на рисунке 110.

Настройка сервиса отправ	ки SMS
Протокол доставки	НТТР-GET 🖌
При формировании URL и \${login} - логин для дост	заголовков НТТР-запроса используйте строки подстановки: упа к сервису
\${message} - сообщение (обязательный параметр)
\${mobile} - номер мобил	ьного телефона (обязательный параметр)
URL	https://smsc.ru/sys/send.php?psw=S{password}&login=S{login}&phones=S{mobile}&mes=S{message}& charset=utf-8
Логин	геахоft Логин для доступа к сервису отправки сообщений
Пароль	Изменить зиачение
Заголовки	С Использовать Basic HTTP аутентификацию
	заголовка н II II->запроса, каждый заголовок описывается в отдельной строке, пазвание и значение заголовка должны быть разделены символом з
Шаблон ответа успешной отправки	•ОК.* 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 110 – Настройка подключения к SMS-шлюзу

Необходимо задать следующие настройки:

- вид протокола доставки (GET или POST);
- URL SMS-шлюза задается в виде паттерна для формирования запроса к SMS-шлюзу для инициирования отправки им SMS. Пример настройки для SMS-шлюза:

https://smsc.ru/sys/send.php?psw=\${password}&login=\${login}&phones=\${mobile}&mes=\${message}&charset= utf-8

- логин и пароль для доступа к SMS-шлюзу. Логин и пароль могут быть переданы в качестве параметров GET-запроса или в виде HTTP-заголовка запроса (схема авторизации HTTP Basic Authorization);
- HTTP-заголовке запроса на SMS-шлюз;
- шаблон проверки ответа от шлюза, означающего успешную отправку. Задается в виде регулярного выражения;
- шаблон проверки ответа от шлюза, означающего ошибку отправки сообщения.
 Задается в виде регулярного выражения.

12.2. Настройка подключения к сервису отправки push-уведомлений

Настройки push-уведомлений задаются в веб-приложении администрирования в разделе «Сообщения».

Необходимо задать следующие настройки:

- вид протокола доставки (GET или POST);
- URL сервиса отправки push-уведомлений, например:

http://api.system.ru/json/v1.0/communication/mobile/push

- данные – сообщение, передаваемое в теле (body) запроса, например:

{"token":"\${password}","title":"\${title}","body":"\${message}","msisdn":\${subscriberId}}

 - логин и пароль для доступа к сервису. Логин и пароль могут быть переданы в качестве параметров GET-запроса или в виде HTTP-заголовка запроса (схема авторизации HTTP

Basic Authorization);

- НТТР-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).

Протокол	HTTP-POST v
доставки	Протокол доставки сообщений
При формиров	ании URL, тела и заголовков HTTP-запроса используйте строки подстановки:
\${login} - ЛОГ	ин для доступа к сервису
<pre>\${password} -</pre>	пароль для доступа к сервису
\${message} -T	екст сообщения (обязательный параметр)
\${title} - 380	оловок сообщения (обязательный параметр)
\${subscriberI	 - 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	
	Данные передаваемые в теле HTTP-запроса
Логин	test
	Логин для доступа к сервису отправки сообщений
Пароль	Изменить значение
	☑ Использовать Basic HTTP аутентификацию
Заголовки	
	заголовки НТТР-запроса. Каждый заголовок описывается в отдельной строке. Название и значение заголовка должны быть разделены символом : .
Іаблон ответа	.+\"errorCode\":0.+
успешной отправки	Регулярное выражение, определяющее успешную отправку сообщения. Например, ^OK.+
lаблон ответа при ошибке	.+\"errorCode\":[1-9].+
	Регулярное выражение, определяющее наличие ошибки при отправке сообщения. Например, ^ERROR.+

Рисунок 111 – Настройка интеграции с сервисом отправки push-уведомлений

12.3. Настройка подключения к SMTP-шлюзу

В Blitz Identity Provider необходимо настроить возможность отправлять по email сообщения, если используются следующие функции:

- информирование о важных событиях безопасности по email.
- изменение адреса электронной подписи через «Профиль пользователя».
- восстановление забытого пароля с использованием email как канала подтверждения владения учетной записью.
- подтверждение адреса электронной почты при регистрации учетной записи пользователя.

Настройки задаются в консоли управления Blitz Identity Provider в разделе «Сообщения». Экран настроек приведен на рисунке 112.

Настройка SMTP-сервера			
Хост	mail01.reaxoft.loc		
Порт	25		
	🗌 Использовать TLS		
Отправитель	notif@reaxoft.ru		
	email-адрес отправителя		
Логин		Совпадает с адресом отправителя	
	Логин учетной записи для соединения с SMTP-сервером		
Пароль	Изменить значение		
			Отмена Сохранить

Рисунок 112 – Настройка подключения к SMTP-шлюзу

Необходимо задать следующие настройки:

- имя хоста SMTP-шлюза;
- порт хоста SMTP-шлюза;
- необходимо или нет использовать TLS для защищенного подключения к шлюзу;
- email отправителя сообщений;
- логин учетной записи на SMTP-шлюзе, от имени которой Blitz Identity Provider будет производить отправку email (если логин совпадает с email отправителя, то следует отметить соответствующий чекбокс);
- пароль от учетной записи на SMTP-шлюзе, от имени которой Blitz Identity Provider будет производить отправку email.

13. Настройка внешнего вида страницы входа

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

В разделе «Внешний вид» консоли управления администратор может настроить параметры отображения единой страницы входа. Если применяются приложения Blitz Identity Provider по регистрации пользователей и восстановлению пароля, то их внешний вид также будет соответствовать заданным настройкам внешнего вида единой страницы входа.

При входе в раздел «Внешний вид» отображается перечень настроенных шаблонов страницы входа. Каждый шаблон описывается:

- идентификатором;
- названием;
- перечнем приложений;
- описанием.

По умолчанию создан шаблон с идентификатором default – он используется для всех приложений, подключенных к Blitz Identity Provider, а также для страниц единого логаута.

Редактирование шаблона по умолчанию осуществляется с помощью специального конструктора (см. п. 13.1).

Также имеется возможность:

- создавать и изменять новые шаблоны с помощью конструктора и назначать их разным приложениям (п. 13.2);
- создавать и изменять новые шаблоны в ручном режиме (п. 13.3).

13.1. Редактирование шаблона по умолчанию

При открытии страницы редактирования шаблона по умолчанию отображается информация о самом шаблоне (идентификатор шаблона, название шаблона, описание и перечень приложений), а также интерфейс конструктора страницы входа.

Свойства шаблона			
Идентификатор	default		
шаолона Название шаблона	Стандартный шаблон		
Onicaino	Menopi protect do integricular		
Описание	истользуется по умолчанию		
Приложения	http://jira.reaxoft.ru/secure/Dashboard	d.jspa, oauth2_demo_app02, openschool, re	
			Сохранить
Внешний вид страницы	входа		
	Тема Светлая	•	
Расположение основ	вного блока Слева	 По центру Справа 	
	6	6 6	
	_		
Логотип			
		B Identity Blitz	
		Ucertity Bitz	
<u>‡</u> 3ar	рузить логотип		
Рекомендуемая высота лог	отипа 32рх		
Фоновый рисунок			
		Или выбрать из предложенных рисунков	
		Рисунок 1 Рисунок 2	
土 Загрузит	гь фоновый рисунок		
		and the second	
Parattaumiatu là pastrap és	1400 VA 60000 1140		
накоментламен бязмер фе	NUS HE COLLEE TWD	Рисунок 3	
Настройка футера			
Добавьте фрагмент НТ	ML-кода для отображения в футере	страницы входа.	
1 Скопируйте сюда фр	атмент HIML кода		
			Сохранить

Рисунок 113 – Настройка внешнего вида страницы входа

В стандартной поставке конструктор Blitz Identity Provider предоставляет следующие возможности:

- три цветовых темы оформления элементов интерфейса;
- возможность определить местоположения блока ввода сведений (идентификации и аутентификации, регистрации, восстановления пароля);
- возможность загрузки логотипа компании для отображения в заголовке страницы;
- выбор фонового рисунка (можно выбрать из 3 стандартных рисунков в каждой теме оформления, либо загрузить свой собственный фоновый рисунок);
- настройка содержания футера страницы входа.

На рисунках 114, 115, 116 приведены примеры страниц входа в результате стандартной настройки.



Рисунок 114 – Пример страницы входа с social login и дополнительным футером



Рисунок 115 – Пример страницы входа в темном интерфейсе и с режимами входа по электронной подписи, сеансу операционной системы или через ЕСИА



Рисунок 116 – Пример страницы входа в светлом интерфейсе, с логотипом в заголовке страницы и без специальных режимов входа

13.2. Создание и изменение новых шаблонов с помощью конструктора

Blitz Identity Provider позволяет настроить разный вид страниц входа для случая входа пользователя в различные подключенные приложения. Для этого необходимо создавать новые шаблоны входа – проще всего это сделать на базе существующего default-шаблона, нажав на кнопку «Копировать». После этого будет создан новый шаблон, который можно редактировать с помощью конструктора.

аблоны страниц входа						
Для оформления страницы входа используются шаблоны. Вы можете отредактировать основной шаблон или создать дополнительные шаблоны, которые будут применяться для страниц. Вы можете создавать дополнительные шаблоны, сохранив копию основного шаблона, а также редактировать шаблоны вручную.						
Идентификатор Название шаблона Приложения Описание						
Default theme	oauth_test	Generated at 1482151154	8			
default_1482928471 V Default theme Generated at 1482151154						
	а входа используются шабл инительные шаблоны, сохр Название шаблона Default theme Default theme	а входа используются шаблоны. Вы можете отредактировать с лиительные шаблоны, сохранив колию основного шаблона, а Название шаблона Приложения Default theme oauth_test Default theme	а входа используются шаблоны. Вы можете отредактировать основной шаблон или создать дополнительные шаблоны, которые инительные шаблоны, сохранив колию основного шаблона, а также редактировать шаблоны вручную. Название шаблона Приложения Описание Default theme oauth_test Generated at 1482151154 Default theme Generated at 1482151154			

Рисунок 117 – Создание нового шаблона на базе существующего основного шаблона

Чтобы новый шаблон использовался при входе в некоторое приложение, необходимо в разделе «Приложения» перейти к редактированию нужного приложения и выбрать требуемый шаблон страниц.

араметры прило	жения	
Идентификатор (entityID или client_id)	test_app Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).	
Название	Тестовое приложение Отображаемое пользователям имя приложения. Используется	
Домен	только внутри Blitz Identity Provider test.ru Ссылка на стартовую страницу приложения, например, http://testdomain.ru/. При TLS-аутентификации приложения	
Ключ шифрования дентификаторов	проверяется, что в сертификате приложения указан именно этот домен Если ключ задан, то идентификатор пользователя для приложения будет зашифрован с использованием данного	
Шаблон страниц	ключа. Значение ключа можно выорать из списка. Также можно назначить новый ключ, для этого введите его в строке поиска и нажмите Enter	7
	Шаблон страниц определяет внешний вид страниц входа. Если шаблон не указан, то используется шаблон по умолчанию.	
Префиксы сылок 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	
		Удалить приложение

Рисунок 118 – Назначение шаблона страницы входа приложению

13.3. Создание и изменение новых шаблонов в ручном режиме

Можно настроить вид страницы входа под индивидуальные требования организации, т.е. нет необходимости ограничиваться только возможностями конструктора.

Каждый шаблон страницы входа представляет собой zip-архив. Все шаблоны размещены в директории:

 $\state{lassets}$

Самый простой способ перейти к ручному редактированию шаблона – выполнить следующие шаги:

- создать копию существующего шаблона (например, default-шаблона), нажав в консоли

кнопку 💾

- перейти в соответствующую директорию с шаблонами;

- распаковать архив с только что созданным шаблоном;
- отредактировать файл meta.conf, содержащийся в архиве, удалив параметр builder (см. рисунок 119);
- обратно заархивировать файлы шаблона, убедившись, что файл meta.conf находится в корневой директории.

	C:\Program Files (x86)\blitz-io	dp\assets\themes\new_theme\meta.con	f - Notepad++	_ □	×
<u>Ф</u> айл <u>П</u> равка По <u>и</u> ск <u>В</u> ид	<u>К</u> одировки <u>С</u> интаксисы <u>О</u> пции	<u>М</u> акросы <u>З</u> апуск Плаги <u>н</u> ы Окн <u>а</u> ?			Х
	k 🖻 🜔 🤉 C # 🏂 🔍	🔍 🖪 🗟 🎫 🏾 🔚 🖉 💹 🖉 🗀 [• • • • •		
🔚 meta.conf 🔀					
1 {"name":"Default	theme","desc":"Generated	at 1482151154", "builder":{"layou	t":"center","th	eme":"blitz"}	
Normal text file	length : 103 lines : 1	Ln:1 Col:1 Sel:0 0	Dos\Windows U	JTF-8	INS

Рисунок 119 – Удаление параметра builder из файла meta.conf

После выполнения этих шагов появится возможность редактирования темы в ручном режиме. Помимо стандартных полей, описывающих саму тему, доступен блок «Шаблон страниц». Он позволяет создать или изменить шаблон – текстовый файл, который компилируется с помощью шаблонизатора Twirl⁴¹.

Шаблон должен иметь сигнатуру:

@(headers: Html, form: Html, scripts: Html, pathAssets: String)(implicit request: RelyingPartyRequest[_], messages: Messages)

В качестве параметров при создании шаблона следует использовать:

- headers HTML-код заголовка страницы, который надо расположить в теге head;
- form HTML-код основной формы, который необходимо расположить в теге body;
- scripts HTML-код с JavaScript, который необходимо расположить в теге body;
- pathAssets контекстный путь к ресурсам шаблона.

Функция @form добавляет на страницу код основной формы аутентификации (пример основной формы приведен на рисунке 120). Форма аутентификация (перечень и состав полей, расположение кнопок) не настраивается за исключением изменений, реализуемых средствами CSS. Иными словами, через CSS можно изменить цвет отдельных элементов или скрыть их – для этого следует найти соответствующий класс в CSS-файле темы и изменить его свойства.

⁴¹ Cm.: https://www.playframework.com/documentation/2.5.x/ScalaTemplates

Вход в Личный кабинет					
Логин					
Логин					
Пароль					
Пароль			Ø		
 Чужой ко 	омпьютер		Забыли пароль?		
	Войт	и			
	или				
	Я <mark>G</mark> f	ĸ	×		
госуслуги					
ど Войти по Сбербанк ID					
E	Вход по сеансу операционной системы				
	Вход по электронной подписи				
	Нет аккаунта? Заре	гистрировать	ъся		

Рисунок 120 – Блок с основной формой аутентификации

Листинг простейшего шаблона приведен ниже:

```
@(headers: Html, form: Html, scripts: Html, path: String)(implicit request: RelyingPartyRequest[],
messages: Messages)
<!DOCTYPE html>
<html>
<head>
   @headers
</head>
<body>
   <div id="main">
       <section id="content_wrapper">
               @form
       </section>
       <div>
            <div>
               @Html(messages("author.copyright"))
           </div>
       </div>
    </div>
    @scripts
  </body>
```

</html>

При использовании такого шаблона страница входа будет иметь вид, приведенный на

рисунке 121.

	Вход в Личный кабинет	
Логин		
Логин		
Пароль		
Пароль		
	Забыли пароль?	
	Войти	
	Нет аккаунта? Зарегистрироваться	

Рисунок 121 – Внешний вид простейшей страницы входа

При формировании шаблона страницы входа имеется возможность использовать ресурсы – например, таблицы стилей или рисунки.

Для их загрузки следует использовать блок «Ресурсы» внешнего вида страницы, который позволяет загрузить необходимые файлы в zip-архиве. Чтобы соответствующие файлы были доступны, их следует размещать в директории архива с названием assets. Необходимые ресурсы также можно вручную включить в состав исходного zip-архива с шаблоном страницы.

Ресурсы	
► a css ► a img	
	Загрузить новый zip-архив

Рисунок 122 – Внешний вид: доступные ресурсы

14. Настройки шлюза безопасности

С помощью Blitz Identity Provider можно осуществлять контроль доступа при вызове приложениями защищаемых сервисов.

Обеспечение авторизации при вызове приложениями сервисов основано на спецификациях OAuth 2.0. Перед использованием сервисов приложение должно получить у Blitz Identity Provider маркер доступа (access_token). Для получения маркера доступа приложению доступны различные способы взаимодействия (см. «Руководство по интеграции»). При этом маркер доступа может быть получен:

- в контексте входа пользователя маркер будет включать информацию о пользователе и наборе согласий (разрешений), предоставленных пользователем приложению;
- на приложение вне контекста входа пользователя маркер будет включать набор согласий (разрешений) из числа разрешенных приложению.

Далее с использованием полученного маркера доступа приложение может вызывать сервисы. При этом будут следующие сложности:

- внутри каждого сервиса необходимо будет реализовывать собственную логику авторизации – проверять предоставленный маркер доступа, извлекать из него информацию о пользователе и предоставленных согласиях(разрешениях) и анализировать, достаточно ли их для выполнения сервиса или нет. Осуществлять протоколирование принятого решения по доступу.
- приложение будет использовать единый маркер доступа для вызова различных сервисов. Маркер доступа в таком случае может содержать больше информации о пользователе и больший набор согласий (разрешений), чем нужно конкретному вызванному сервису. Это будет нарушать принцип наименьших привилегий – сервис получит больше прав доступа, чем ему необходимо для выполнения своей задачи.

Чтобы решить вышеописанные сложности в Blitz Identity Provider предусмотрено специальное приложение – шлюз безопасности (blitz-keeper). Это приложение представляет собой специализированный прокси-сервер, используемый при вызове защищаемых сервисов – приложение вызывает сервисы не напрямую, а через шлюз безопасности. При этом шлюз безопасности берет на себя выполнение следующих задач:

- Проверяет включенный в вызов сервиса заголовок авторизации, извлекает из заголовка маркер доступа и, во взаимодействии с сервисом авторизации (blitz-idp) выполняет проверку, действителен ли маркер доступа, а также, достаточно ли у пользователя и приложения прав для вызова защищаемого сервиса.
- Во взаимодействии с сервисом авторизации (blitz-idp) заменяет маркер доступа таким

образом, чтобы передаваемый от шлюза безопасности к защищаемому сервису маркер безопасности содержал только тот набор сведений о пользователе и разрешений, который необходим для работы защищаемого сервиса. При этом из маркера безопасности могут быть как изъяты излишние разрешения и сведения о пользователе, так и наоборот, добавлены в маркер доступа дополнительные разрешения и сведения, если такое установлено политикой безопасности.

 Протоколирует в журнале событий безопасности Blitz Identity Provider события успешной и неуспешной проверки прав доступа.

Взаимодействие шлюза безопасности с сервисом авторизации осуществляется на основе спецификации OAuth 2.0 Token Exchange⁴². Иллюстрация взаимодействия приведена на схеме (см. рисунок 123).

Пользователь	Приложение	Шлюз безоп (Blitz Identity Provide	асности er — blitz-keeper)	Защищаемы	й сервис Серви (Blitz Identit	с авториза y Provider	іции – blitz-idp)
			•	API	•	B	
1. Запрос дейсте	зия в приложении /api/v1/sen Authorizatio 2. Вызов чер- безопасност заголовке ма	tice1 HTTP/1.1 nr: Bearer ORSqyIGx га прокси-сервер шлюза г сервиса с передачей в ркера доступа	 Запрос авторизации и выпуска доступа для вызова защищаемого от имени пользователя и прилож 	маркера о сервиса ения	Authorization: Basic aS&uQWvz grant_type=urn:[]:token_exchange &clent_id=app&scope=service1 &resource=service1&audience=service1 &subject_token=ORSqvIGx &subject_token_type=urn:[] :access_tok	en	
			4. Передача шлюзу безопасности маркера доступа, предназначенн вызова защищаемого сервиса	і нового юго для	<pre>{ "access_token": "TSEasdX", "token_type": "bearer", "expires_in": 3600, "scope": "service1", "sub": "user1", "aud": "service1", "aud": "service1", "act": {"client_id": "app"} }</pre>		
			5. Вызов сервиса с передачей ему нового маркера доступа		5. (опционально) Проверка маркера доступа самостоятельно сервисом либо нерез сервиса авторизации	Ì	
9. Результат зап	роса 8. Результат	вызова сервиса	7. Результат вызова сервиса			⇒ ■	

Рисунок 123 - Схема взаимодействия при вызове приложением защищаемого сервиса

Настройка использования шлюза безопасности для защиты сервисов заключается в выполнении следующих шагов и описана в последующих подразделах:

- Настройка blitz-keeper.
- Создание правил доступа к сервисам.
- Регистрация правил обмена маркеров доступа в blitz.conf.

14.1. Настройка blitz-keeper

Настройка blitz-keeper осуществляется путем редактирования конфигурационного файла blitz-keeper.conf, расположенного в каталоге /etc/blitz-keeper.

⁴² Спецификация, описывающая способы обмена маркеров в целях делегирования вызовов между сервисами и для задач имперсонификации пользователей. См.: https://tools.ietf.org/html/rfc8693.

Пример конфигурационного файла:

```
"authenticators": {
  "prod-auth": {
    "type": "token-exchange",
    "te": "https://blitz-host/blitz/oauth/te",
  },
"api-1":{
    "display-name" : "secured services",
    "host": "service-host.com",
    "locations": {
      "/api/service1/**": {
        "methods" : ["GET", "POST"],
        "authenticator": "prod-auth",
"required-scopes": ["scope1","scope2"]
      "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 раздельных установок Blitz Identity Provider (например, ПРОД- и ТЕСТ-среда или внутренний контур для сотрудников и внешний контур для клиентов), то можно использовать общий шлюз безопасности, который будет взаимодействовать с несколькими разными сервисами авторизации – тогда нужно в блоке authenticators задать настройки нескольких сервисов авторизации. Для каждого сервиса авторизации задается имя (в примере использован prod-auth, но можно задать любое имя). В блоке настроек сервиса авторизации задается тип взаимодействия (type) в значении token-exchange (пока это единственный поддерживаемый тип взаимодействия) и адрес (te) вызова обработчика Token Endpoint сервиса авторизации. Если blitz-keeper развернут на отдельных серверах, то рекомендуется задать адрес обработчика с https и доменным именем. Если приложение blitz-keeper развернуто на том же сервере что сервис авторизации blitz-idp, то рекомендуется задать в te локальное имя, например, http://localhost:9000/blitz/oauth/te.

В блоке services нужно зарегистрировать защищаемые сервисы. Для всех защищаемых сервисов можно создать общий блок настроек или несколько отдельных блоков. Каждый блок имеет имя (в примере, api-1). Внутри блока задаются настройки:

- display-name текстовое описание сервиса (любой комментарий или описание);
- host адрес сервера защищаемого сервиса;
- locations допустимые пути и операции вызова сервиса.

В блоке locations указываются настройки всех путей сервиса и разрешенных методов. В качестве имени каждого вложенного блока указывается адрес сервиса. Допустимо в адресе использовать звезду (*), чтобы указать на пропуск отдельного компонента в адресе пути сервиса и допустимо использовать двойную звезду (**), чтобы указать, что вся оставшаяся часть пути сервиса может быть любая. Внутри вложенного блока с адресом сервиса можно опционально перечислить разрешенные методы сервиса (настройка methods), указать имя используемого сервиса авторизации (настройка authenticator) и перечень разрешений (настройка required-scopes) для целевого маркера доступа, которые будут включены в маркер доступа, передаваемый в защищаемый сервис.

После изменения настроек в blitz-keeper.conf необходимо перезапустить шлюз безопасности.

14.2. Создание правил доступа к сервисам

Правила доступа к сервисам создаются в директории /usr/share/identityblitz/blitzconfig/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": [],
    "userClaims": {},
    "userClaims": {},
    "userGroups": []
  },
"issue": {
    "ttlInSec": 3600,
    "allowedScopes": ["openid","profile"],
    "addingScopes": [],
    "addingClaims": []
  }
}
```

Нужно заполнить следующие атрибуты правила доступа:

- name имя правила, которое должно совпадать с именем файла с правилом доступа;
- type тип правила. Пока поддерживается один тип правил specialize;
- desc описание правила. Можно ввести любую текстовую информацию;
- subjectTokenCond условия выполнения правила. Если все указанные в правиле условия будут выполняться, то правило считается выполненным. Если хотя бы одно из условий в правиле не будет выполнено, то все правило считается невыполненным. Условия выполнения правил могут быть следующие:
 - clientRights проверка наличия у приложения указанных прав доступа
(см. п. 15.1.10);

Пример правила:

```
"clientRights": [
    {
        "rights": ["right1"],
        "target": {
            "type": "its",
            "name": "app1"
        }
    }
]
```

В указанном примере проверяется наличие у вызывающего приложения права доступа right1 в отношении другого приложения (app1). Параметр its в настройке target указывает тип объекта, в отношении которого проверяется наличие права доступа. Возможные значения: its – право на приложение; grps – право на группу доступа; отсутствие type – право на учетную запись пользователя.

- userRights – проверка наличия у пользователя указанных прав доступа (см. п. 15.1.10).

Пример 1 правила:

```
"userRights": [
    {
        "rights": ["right2"],
        "target": {
            "type": "grps",
            "name": "org1",
            "ext": "orgs"
        }
]
```

1

В указанном примере проверяется наличие у пользователя права доступа right2 в отношении группы пользователей (org1). В случае типа объекта группы доступа указывается дополнительный параметр ext, определяющий профиль группы доступа (см. п. 15.1.14).

Пример 2 правила:

```
"userRights": [
{
    "rights": ["security_administrator"],
    "target": {
        "type": "grps",
        "name": "${org_id}",
        "ext": "orgs"
    }
}
```

В указанном правиле проверяется наличие у пользователя права доступа security_administrator в отношении группы пользователей из профиля orgs, имеющей идентификатор, совпадающий со значением атрибута org_id из состава исходного маркера доступа. В отличии от примера 1 в данном примере иллюстрируется возможность в качестве имени объекта права доступа указывать не конкретное значение объекта, а ссылаться на объект на основе

значений из присланного маркера доступа (\$org_id).

Пример 3 правила:

```
"userRights": [
    {
        "rights": ["right3"],
        "target": {
            "type": "its",
            "name": "app1"
        }
    }
]
```

В данном примере проверяется наличие у пользователя права доступа right3 в отношении приложения app1.

 scopes – проверка присутствия в маркере доступа требуемых разрешений (см. п. 5.3.2);

Пример правила:

```
"scopes": ["scope1"]
```

- В данном примере проверяется наличие в исходном маркере доступа разрешения с именем scope1.
- userClaims проверка, что у учетной записи пользователя атрибуты имеют указанные значения.
 - Пример правила:

"userClaims": {"role":"FIN"}

- В данном примере проверяется наличие у пользователя в учетной записи атрибута role с заполненным значением FIN. Допустимо использовать только атрибуты с типом String.
- userGroups проверка, что учетная запись пользователя входит в указанные группы доступа.

Пример правила:

```
"userGroups": [
    {
        "name": "admin",
        "profile": "roles"
    }
]
```

В данном примере проверяется, что пользователь входит в группу доступа admin с профилем roles.

- issue правила выпуска нового маркера доступа, применяемые в случае, если правило было успешно выполнено. Правила выпуска нового маркера доступа состоят из:
 - ttlInSec время жизни (в секундах) выпускаемого маркера доступа;
 - allowedScopes разрешения, которые можно оставить в выпускаемом маркере доступа;
 - allowedClaims атрибуты пользователя, которые можно оставить в выпускаемом маркере доступа;

- addingScopes добавляемые в маркер доступа разрешения;
- addingClaims добавляемые в маркер доступа атрибуты пользователя.

14.3. Настройка правил обмена маркеров доступа

Чтобы определить, для каких защищаемых сервисов какие должны применяться правила доступа, необходимо в конфигурационном файле blitz.conf добавить блок настроек blitz.prod.local.idp.token-exchange следующего вида:

```
"token-exchange" : {
    "resources" : [
    {
        "rules" : [
        "rule1", "rule2"
    ],
        "audience" : "secured-api",
        "uri" : http://secured service host/api/service1,
        "methods" : ["GET","POST"]
    },
    {
        "rules" : [
        "rule3"
    ],
        "uri" : http://secured_service_host/api/service2
    },
        ...
]
```

В блоке resources нужно для каждого сервиса заполнить настройки:

- rules перечислить имена правил доступа к сервису. Каждому правилу соответствует свой файл настроек (см. п. 14.2). Доступ к сервису разрешается, если хотя бы одно из правил из этого списка будет выполненным. Если все перечисленные правила не будут выполнены, то тогда доступ к сервису будет запрещен;
- uri адрес защищаемого сервиса. В задании адреса сервиса допустимо использовать звезду (*) для пропуска одного компонента пути адреса и двойную звезду (**) для пропуска оставшейся части пути адреса сервиса;
- audience необязательный параметр, может задавать логическое имя вызываемого сервиса. Данное значение будет включено в выпущенный новый маркер доступа в атрибут aud;
- methods необязательный параметр, указывает перечень НТТР-методов вызываемого сервиса.

15. Настройки конфигурационных файлов

Конфигурационные файлы всех приложений Blitz Identity Provider кроме приложения blitz-keeper расположены в каталоге /usr/share/identityblitz/blitz-config.

Используются следующие конфигурационные файлы:

- assets/* настройки пользовательского интерфейса (см. п. 4.2.2, п. 7, п. 13);
- custom_messages/* строки пользовательского интерфейса (см. п. 15.2);
- devices/* вспомогательные каталоги для обработки загрузки НОТР и ТОТР устройств (см. п. 4.10.1);
- flows/* процедуры входа (см. п. 6.1);
- saml/* настройки SAML (см. п. 5.2);
- simple/* настройки подключения приложений по протоколу Simple (см. п. 5.1);
- token_exchange/rules/* настройки правил обмена маркеров доступа (см. п. 14);
- blitz.conf основной файл конфигурации (см. п. 15.1);
- boot.conf настройки путей к конфигурационным файлам;
- console.conf настройки консоли управления (см. п. 15.3);
- credentials учетные записи администраторов консоли управления (см. п. 15.3.3);
- play.conf настройки серверов приложений (см. п. 2.5 и п. 15.1.9);
- logback.xml настройки журналирования событий и ошибок.

Большинство настроек задается с использованием консоли управления. Для ряда настроек необходимо самостоятельное редактирование конфигурационных файлов. Такие настройки описаны далее в подразделах.

Конфигурационный файл приложения blitz-keeper расположен в /etc/blitz-keeper. Используются следующие конфигурационные файлы:

- blitz-keeper.conf настройки шлюза безопасности (см. п. 14);
- blitz-keeper-log4j.xml настройки журналирования событий и ошибок.

15.1. Файл настроек blitz.conf

Основной конфигурационный файл blitz.conf состоит из следующих блоков настроек, имеющих следующее назначение:

- blitz.prod.local.idp.apps настройки подключенных приложений;
- blitz.prod.local.idp.federation настройки внешних поставщиков идентификации;
- blitz.prod.local.idp.flexible-flows настройки процедур входа;
- blitz.prod.local.idp.id-attrs настройки атрибутов;
- blitz.prod.local.idp.id-stores настройки хранения атрибутов в LDAP-каталоге;

- blitz.prod.local.idp.internal-store настройки подключения к СУБД;
- blitz.prod.local.idp.keystore настройки доступа к хранилищу ключей;
- blitz.prod.local.idp.license лицензионный ключ Blitz Identity Provider;
- blitz.prod.local.idp.logger настройки логгеров;
- blitz.prod.local.idp.login настройки методов аутентификации;
- blitz.prod.local.idp.logout настройки процесса логаута;
- 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 САРТСНА;
- blitz.prod.local.idp.events настройки отправки событий в очередь;
- blitz.prod.local.idp.net настройки сети;
- blitz.prod.local.idp.notifier настройки уведомлений о событиях;
- blitz.prod.local.idp.oauth настройки разрешений (scope);
- blitz.prod.local.idp.password-policy настройки парольной политики;
- blitz.prod.local.idp.play настройки сервера приложений Blitz Identity Provider;
- blitz.prod.local.idp.provisioning настройки сервисов регистрации пользователей и восстановления забытого пароля;
- blitz.prod.local.idp.realms настройки шифрования идентификаторов приложений («домены приватности);
- blitz.prod.local.idp.saml настройки SAML;
- blitz.prod.local.idp.tasks настройки механизма обработки задач;
- blitz.prod.local.idp.user-profile настройки личного кабинета;
- home путь к каталогу установки Blitz Identity Provider на сервере приложений.

Далее приведено описание настроек, недоступных из консоли управления, и проводимых посредством редактирования конфигурационного файла blitz.conf.

15.1.1. Настройка парольных политик

Блок настроек blitz.prod.local.idp.password-policy содержит запись с настройками парольной политики Blitz Identity Provider.

Пример настройки приведен ниже:

```
"password-policy" : {
    "groups": [
        {
            "desc": "password.policy.desc.digits",
            "group": "[0-9]",
            "minCount": 1
        },
        {
            "desc": "password.policy.desc.lowercase",
            "group": "[a-z]",
            "minCount": 1
        }
```

```
},
{
    "desc": "password.policy.desc.capital",
    "group": "[A-Z]",
    "minCount": 1
    },
    {
        "desc": "password.policy.desc.special",
        "group": "[!@#$%^&*()+\\-?.,;:'`\"{}\\[\]><=~/\\\\_]",
        "minCount": 1
    }
    ,
    /,
    "minGroups": 3,
    "minIength": 6,
    "dicPath": "/usr/share/identityblitz/blitz-config/password dic.txt",
    "passwordHistoryLen": 5,
    "minPasswordAgeSec": 3600,
    "maxPasswordAgeSec": 2592000,
    "minNewChars": 1</pre>
```

Предусмотрены следующие настройки:

- groups задает описание (desc) группы символов, набор символов (group), минимально достаточное количество символов группы в пароле (minCount).
- minGroups задает минимально необходимое количество групп символов в пароле.
- minLength задает минимальную длину пароля.
- dicPath задает путь к файлу со словарем паролей; это должен быть текстовый файл,
 где каждый пароль размещен на новой строке;
- passwordHistoryLen количество старых паролей, которое требуется хранить и не допускать задания нового пароля при наличии его в перечне использованных паролей;
- minPasswordAgeSec минимальное время жизни пароля, в секундах; пока это время не истекло, пользователю не будет разрешено поставить новый пароль. Если такую проверку не следует выполнять, то нужно удалить данный параметр;
- maxPasswordAgeSec максимальное время жизни пароля, в секундах; как только это время истечет, пользователю потребуется задать новый пароль. Если такую проверку не следует выполнять, то нужно удалить данный параметр;
- minNewChars минимальное количество новых символов при задании нового пароля (для случаев, когда пользователь меняет текущий пароль на новый).

15.1.2. Ограничение количества одновременных проверок пароля пользователя

Можно установить ограничение на количество одновременных парольных аутентификаций с одинаковым логином пользователя за период времени. По умолчанию установлен режим, что Blitz Identity Provider разрешает пройти не более 3 аутентификаций на один и тот же логин в течение 600 мс. Чтобы скорректировать стандартные настройки, blitz.conf необходимо В конфигурационном файле добавить В раздел blitz.prod.local.idp.login.methods.password следующий блок:

"throughput": {

"limit": 3, "window": 600

15.1.3. Настройка времени отображения экрана логаута

По умолчанию при вызове приложением логаута в Blitz Identity Provider пользователю в течение 5 секунд отображается экран, поясняющий, что происходит логаут. После этого экран автоматически закрывается, а пользователь перенаправляется на страницу, указанную при вызове логаута в качестве параметра возврата.

Скорректировать время отображения страницы логаута можно через конфигурационный файл. Для blitz.prod.local.idp.logout этого В разделе нужно скорректировать параметр timeout-sec:

```
"logout" : {
   "timeout-sec" : 2
}
```

15.1.4. Настройка вызова внешнего сервиса проверки электронной подписи

Для интеграции с внешним сервисом проверки электронной подписи должна быть разработана специальная библиотека проверки подписи. Система будет производить проверку электронной подписи через эту систему после прописывания данной библиотеки в конфигурационном файле, в разделе blitz.prod.local.idp.login.methods.x509, следующим образом:

```
"x509-verifier" : {
	"javaClass" : "<Java-класс реализации коннектора>",
	"pathToJar" : "/usr/.../check-signature-1.0.0.jar",
	"signatureValidationServiceUrl" : "<адрес сервиса >"
}
```

15.1.5. Настройка САРТСНА

Для отображения сервиса САРТСНА 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:

```
"name": "check",
                "newState": {
                     "uniqueFormHash": "${rsp.result.uniqueFormHash-}"
            },
                 "call": {
                     "headers": [
                         "accept:application/json",
                         "Authorization:Bearer ${cfg.bearerToken}"
                     1,
                     "method": "get".
                     "url":
"https://captcha.example.com/captcha/1.0.0/create?type=${cfg.type}&options[system]=${cfg.system}&opt
ions[token]=${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.t
ype & 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 САРТСНА (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 САРТСНА на странице входа;
- mode режим отображения САРТСНА, предусмотрены следующие режимы:

- always_on САРТСНА отображается всегда
- on_header САРТСНА отображается, если в запросе есть заголовок, указанный в параметре name, и значением, указанном в параметре value.
- В случае использования в качестве САРТСНА сервиса Google reCAPTCHA v343

необходимо:

задать следующие настройки в blitz.prod.local.idp.captcha:

```
"captcha" : {
  "reCAPTCHAv3" : {
    "operations" : [
        "call" : {
          "headers" : [],
          "method" : "post",
          "url" :
"https://www.google.com/recaptcha/api/siteverify?secret=${cfg.secret}&response=${ocp.response}"
        },
         "check" : {
          "errRegExp" : {},
          "okRegExp" : {
             "score" : "1\\.0|0\\.(5|6|7|8|9)",
             "success" : "true"
          }
        },
        "name" : "verify"
      }
    ],
    "plainParams" : {
  "sitekey" : "SITE_KEY"
    "secureParams" : {
      "secret" : "SITE SECRET"
    }
  }
}
```

Вместо SITE_KEY и SITE_SECRET нужно заполнить значения, полученные при регистрации Google reCAPTCHA v3 на сайте https://g.co/recaptcha/v3. Также нужно скорректировать значение в параметре score – установить требуемый порог успешного прохождения проверки (в примере выставлен порог не ниже 0,5).

- задать следующие настройки в blitz.prod.local.idp.password.captcha:

```
"captcha" : {
    "mode" : {
        "name" : "X-Captcha-Check",
        "type" : "on header",
        "value" : "true"
    },
    "enabled" : true,
    "initJs" : "require(['/blitz/assets/blitz-common/javascripts/recaptcha_v3.js', 'captcha-conf'],
function(captcha, conf) { captcha(conf);});",
    "mode" : {
        "type" : "always_on"
    },
    "name" : "reCAPTCHAv3"
}
```

15.1.6. Настройка отправки событий в сервер очередей

В сервер очередей могут быть отправлены следующие события:

- регистрация пользователя (USER_REGISTERED);

⁴³ CM.: https://developers.google.com/recaptcha/docs/v3

- смена пароля (USER_PASSWORD_SET);
- смена признака аннулирования сессий (USER_CRID_CHANGED);
- изменения атрибутов пользователя (USER_ATTRIBUTE_CHANGED);
- очистка атрибутов пользователя (USER_ATTRIBUTE_REMOVED);
- удаление пользователя (USER_REMOVED);
- привязка внешней учетной записи (FEDERATION_POINT_BOUND);
- отвязка внешней учетной записи (FEDERATION_POINT_UNBOUND);
- отзыв выданного приложению разрешения (scopes) (SCOPES_REVOKED);
- создание группы (GROUP_CREATED);
- изменение атрибутов группы (GROUP_UPDATED);
- удаление группы (GROUP_REMOVED);
- включение пользователя в группу (GROUP_MEMBER_ADDED);
- исключение пользователя из группы (GROUP_MEMBER_REMOVED).

Для отправки событий в очередь следует создать блок blitz.prod.local.idp.events следующего содержания (на примере регистрации пользователя и смены пароля):

```
"events" : {
   "drivers" : {
        "rabbit driver" : {
            "properties" : {},
            "server" : {
                 "host" : "<RMQ HOST>",
                 "port" : 5672
             },
             "type" : "RMQ",
             "user" : {
                 "password" : "<RMQ PASS>",
                 "username" : "<RMQ USERNAME>"
            }
        }
   },
    "routes" : {
        "USER PASSWORD SET" : [
            "password sync"
        ],
        "USER REGISTERED" : [
            "registration"
        1
    },
    "targets" : [
        {
            "discardList" : "PSWD SYNC DISCARD",
            "driver" : {
    "ext" : {
                     "exchange_name" : "users",
                     "routing key" : "pwd sync"
                },
"id" : "rabbit_driver"
             },
            "encCertificate" : "rmqkey",
            "name" : "password sync",
            "redelivery" : 3
        },
        {
            "discardList" : "REG DISCARD",
            "driver" : {
    "ext" : {
                     "exchange name" : "users",
                     "routing key" : "registration"
                },
```

```
"id" : "rabbit_driver"
},
"encCertificate" : "rmqkey",
"name" : "registration",
"redelivery" : 3
}
```

В данных настройках следует задать:

- RMQ_HOST домен сервера очередей RabbitMQ;
- RMQ_USERNAME имя пользователя для работы с сервером очередей;
- RMQ_PASS пароль для работы с сервером очередей.

Кроме того, для шифрования паролей, отправляемых в очередь, в параметре encCertificate следует указать псевдоним ключа электронной подписи (в стандартном хранилище ключей BlitzIdPKeystore.jks), которым следует шифровать пароли в сообщениях.

15.1.7. Запрос проверочного атрибута при восстановлении пароля

Можно настроить веб-приложение «Восстановление доступа», чтобы при восстановлении пароля пользователь вводил значение дополнительного атрибута для подтверждения владения учетной записью. Добавление такой проверки усложняет атаку на сброс пароля через множественный перебор в форме восстановления забытого пароля. На главной странице у пользователя будут запрошены атрибуты для сверки (например, фамилия) и восстановление будет выполнено только в том случае, если найденная учетная запись будет иметь идентичное значение атрибута.

Для настройки атрибутов сверки следует отредактировать параметр security-question в блоке blitz.prod.local.idp.provisioning.recovery. Пример настройки, позволяющей запрашивать фамилию на форме восстановления доступа:

```
"security-question" : {
    "attrs" : [
    "LastName"
]
}
```

15.1.8. Настройка хранения объектов в Couchbase Server

Можно переназначить внутренние хранилища (buckets) Blitz Identity Provider в СУБД Couchbase Server, используемые для хранения данных. Предусмотрена возможность для следующих наборов данных указать необходимость использования иных хранилищ (buckets), чем стандартно используемые.

Для настройки иных хранилищ (buckets) нужно в блоке blitz.prod.local.idp.internal-storeсb 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, a clt и iat – в apps. По умолчанию все три набора данных записывались в хранилище oauth.

```
"internal-store-cb" : {
    ...
    "buckets" : {
      ["users", "oauth", "audit", "builtin_idstore", "ctxs"]
    },
    "bucketsMapping" : {
      "acl" : "users",
      "clt" : "apps",
      "iat" : "apps"
    },
    ...
}
```

Можно настроить для данных аудита ограничение по сроку хранения записей (по умолчанию записи хранятся бессрочно). Для этого в в блоке blitz.prod.local.idp.internal-storecb нужно добавить настройку ttlMapping с указанием doc_type записи (aud) и времени хранения в секундах.

Пример настройки (время хранения аудита ограничено до 90 суток):

```
"internal-store-cb": {
    ...
    "ttlMapping": {
        "aud": 7776000
    },
    ...
}
```

15.1.9. Настройка домена Blitz Identity Provider

Изменение домена Blitz Identity Provider осуществляется путем редактирования в блоке настроек blitz.prod.local.idp.net конфигурационного файла настройки domain.

```
Пример настройки:
```

```
"net" : {
    "domain" : "demo.identityblitz.com"
}
```

При необходимости можно изменить путь до приложений (по умолчанию приложения доступны с использованием пути /blitz). Отредактировать путь можно в конфигурационном файле play.conf. Нужно изменить параметр context в блоке play.http:

```
"http" : {
    "context": "/blitz",
    ...
}
```

15.1.10. Настройка справочника прав доступа

Чтобы использовать REST API в Blitz Identity Provider по назначению и отзыву прав доступа субъектов (пользователи и приложения) на объекты (пользователи, группы пользователей, приложения) необходимо зарегистрировать справочник прав доступа. Для этого в конфигурационный файл добавить блок настроек blitz.prod.local.idp.rights следующего вида, указывая в name и desc имя и описания права доступа:

```
"rights" : {
    "meta" : [
        {
            "desc" : "Текстовое описание права доступа",
            "name" : "right1"
        },
        {
            "desc" : "r,
            "name" : "right2"
        },
        ...
}
```

15.1.11. Расширенные настройки подключения к хранилищам

В консоли управления можно создать настройки подключения к хранилищам атрибутов, работающим по LDAP-протоколу. При этом через консоль управления можно задать настройки пула коннектов к LDAP. Blitz Identity Provider будет использовать общие настройки пула коннектов для установки подключений каждым приложением, использующим подключение к хранилищам. Это может привести к созданию большого числа коннектов к LDAP. Через конфигурационный файл blitz.conf можно настроить параметры начального и максимального числа коннектов в разрезе различных приложений Blitz Identity Provider (например, для консоли управления задать меньшие значения коннектов в пуле, чем для сервиса аутентификации). Для этого в блоке blitz.prod.local.id-stores в настройках соответствующего хранилища наряду с настройками initialConnections и maxConnections можно создать настройки вида initialConnections#BLITZ_APP и maxConnections#BLITZ_APP, где в качестве BLITZ_APP указывается имя соответствующего приложения (blitz-console, blitz-idp, blitz-registration, blitz-recovery). Пример настройки, когда для консоли управления задается меньший размер пула коннектов, чем для остальных приложений:

```
"id-stores" : {
   "list" : [
    {
        "type" : "LDAP",
        ...
        "initialConnections" : 10,
        "initialConnections#blitz-console" : 1,
        "maxConnections" : 20,
        "maxConnections#blitz-console" : 1
    }
]
```

При выполнении запросов в LDAP хранилище атрибутов Blitz Identity Provider берет имеющееся соединение с LDAP-каталогом из пула соединений. После выполнения запроса Blitz Identity Provider не закрывает соединение, а возвращает его обратно в пул соединений для возможности повторного использования. Такой порядок взаимодействия с LDAP обеспечивает высокую производительность, но требует длительное время поддерживать соединения с LDAP-каталогом открытыми. Настройки межсетевых экранов или самих LDAP-каталогов могут препятствовать длительному сохранению открытых соединений приложений Blitz Identity Provider с LDAP-каталогом. TCP-соединения Blitz Identity Provider с LDAP-каталогом могут быть закрыты без согласованного разрыва соединения, так что а 193

LDAP-каталоге соединение будет закрыто, a 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 параметров 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:

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 случае 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 firstSucceded в настройке authStrategy. В этом случае все найденные учетные записи будут проверены, и к какой из них первой подойдет пароль пользователя, с этой учетной записью и будет выполнен вход.

Пример настройки:

```
"login" : {
    "authStrategy" : {
        "mode" : "firstSucceeded"
    },
    ...
}
```

15.1.12. Блокирование неактивных пользователей

Вlitz Identity Provider отслеживает время последней активности пользователя. Предусмотрена возможность выполнять блокирование учетных записей пользователей, которые долгое время неактивны. Для активации этой возможности необходимо запустить в cron выполнение скрипта lockinactive.sh. Скрипт находится в директории /usr/share/identityblitz/blitz-console/bin на сервере с приложением blitz-console. Рекомендуется выполнять скрипт раз в день во время минимальной активности в системе. Перед запуском скрипта необходимо отредактировать его в текстовом редакторе – установить:

- inactive_period требуемый период неактивности (в днях), после которого должна быть произведена блокировка учетной записи;
- range_size диапазон охвата учетных записей (в днях), под блокировку попадут учетные записи, последняя активность по которым была в период с (текущая дата – inactive_period – range size) до (текущая дата – inactive_period).

15.1.13. Запрет повторного использования идентификатора удаленного пользователя

Blitz Identity Provider отслеживает использованные ранее идентификаторы пользователей, чтобы их нельзя было использовать повторно после удаления учетной записи пользователя в течение установленного периода времени. Для этого в блок blitz.prod.local.idp.provisioning нужно добавить раздел remove следующего содержания, указав нужное число дней (days), в течение которых идентификатор пользователя нельзя будет использовать при повторной регистрации:

```
"provisioning" : {
    ...
    "remove": {
        "mode": "keepRemovedId",
        "days": 365
    }
}
```

15.1.14. Настройка групп пользователей

Чтобы включить возможность просмотра групп пользователей, необходимо добавить блок настроек blitz.prod.local.idp.groups следующего вида:

```
"id": "389ds",
       "desc": "Группы",
       "ldapStore": "389ds",
       "baseDN": "ou=external,ou=groups,dc=test",
       "searchScope": "SUB",
       "idAttrName": "cn",
       "membersAttrName": "uniqueMember",
       "memberOfAttrName": "memberOf",
       "newGroupAttrs": [
           "attr": "objectclass",
           "format": "strings",
           "value": "top,groupOfUniqueNames,group"
         },
         {
           "attr": "dn",
           "format": "string",
"value": "cn=${id},ou=external,ou=groups,dc=test"
         }
      ]
    }
  ]
}
```

Особенности указания настроек:

- в profiles.groupStore, stores.list.id, stores.ldapStore должен быть идентификатор
 LDAP-каталога, используемый для хранения пользователей;
- в profiles.attrsMap и в stores.list.idAttrName должны быть указаны атрибуты группы (класс groups), например name. Имена атрибутов при желании можно назвать и подругому, поддерживаются только LDAP-атрибуты типа string;
- в stores.list.baseDN нужно проверить (и исправить если необходимо) путь для хранения организаций в LDAP. Если путь будет исправлен, то скорректировать также настройку "value": "cn=\${id},ou=external,ou=groups,dc=test" соответствующим образом.

15.1.15. Вход через ЕСИА в режиме выбора сотрудника организации

Когда для входа в Blitz Identity Provider сконфигурирован внешний поставщик идентификации ЕСИА, то к обычному режиму входа пользователя (см. п. 8.7) можно сконфигурировать следующие дополнительные возможности:

 Отображение пользователю экрана выбора режима входа и организации, если вошедший через ЕСИА пользователь имеет в ЕСИА роли сотрудника индивидуального предпринимателя, юридического лица или органа государственной власти (см. рисунок 124).



Рисунок 124 – Пример страницы выбора режима входа через ЕСИА

- Получение из ЕСИА сведений о выбранной при входе организации, автоматическое создание на основе этих сведений в LDAP-хранилище группы пользователей с атрибутами, соответствующими организации (если соответствующая организации группа не найдена в момент входа), добавление пользователя в созданную (или найденную) группу пользователей.
- Обновление атрибутов группы пользователя значениями атрибутов организации из ЕСИА в момент входа, если атрибуты в ЕСИА изменились.
- Возможность добавления в маркер доступа и маркер обновления сведений о выбранной в момент входа пользователя роли в ЕСИА (физическое лицо, индивидуальный предприниматель, должностное лицо юридического лица, должностное лицо органа государственной власти).

Для настройки режимов входа необходимо предварительно настроить в Blitz Identity Provider использование групп доступа (см. п. 15.1.14) и вход через ЕСИА (см. п. 8.7). После этого необходимо в конфигурационном файле в секции blitz.prod.local.idp.federation в блоке esia создать дополнительный блок настроек org следующего вида:

```
"federation" : {
  "points" :
    "esia" :
        "org" : {
           "embeds" : [
             "documents.elements-1",
             "addresses.elements-1",
             "contacts.elements-1"
           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" : "${org.agencyType-}"
    },
     {
          "attr" : "org_agencyterrange",
          "master" : true,
          "value" : "${org.agencyTerRange-}"
    },
     {
          "attr" : "org_address_post",
          "master" : true,
          "value" : "${org.postAddress-}"
    },
          "attr" : "org_address_leg",
          "master" : true,
          "value" : "${org.legalAddress-}"
    }
],
"matchingRules" : [
 ſ
    {
       "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"
      1
    },
 ]
}
```

В добавленном блоке нужно скорректировать:

- набор получаемых из ЕСИА сведений об организации и их маппинг на атрибуты группы пользователей (блок group.mapping), признаком master отметить те атрибуты, которые должны перезаписываться в группе пользователей при каждом обновлении из ЕСИА, полученном в момент входа;
- набор запрашиваемых в ЕСИА разрешений (настройка scopes).

Если необходимо передавать в маркер идентификации и маркер доступа сведения о текущей выбранной организации и о роли пользователя в ЕСИА, то необходимо настроить соответствие необходимых атрибутов ЕСИА сессионным утверждениям в Blitz Identity Provider. Это выполняется с помощью настройки claims в блоке настроек ЕСИА:

```
"federation" :
   "points" :
     "esia" : [
       {
          "claims" : [
             {
               "name" : "org_id",
"value" : "org.oid"
             },
             {
               "name" : "global_role",
"value" : "globalRole"
             },
             {
               "name" : "org_shortname",
"value" : "org.shortName"
             },
             {
               "name" : "org_fullname",
               "value" : "org.fullName"
             },
             {
               "name" : "org_type",
"value" : "org.type"
             },
             {
               "name" : "org_ogrn",
               "value" : "org.ogrn"
             },
             {
               "name" : "org inn",
               "value" : "org.inn"
             },
             {
               "name" : "org_oktmo",
```

```
"value" : "org.oktmo"
}
},
...
]
}
```

15.2. Настройки текстов интерфейса

15.2.1. Мультиязычность

Веб-интерфейс Blitz Identity Provider поддерживает мультиязычность. По умолчанию предусмотрено два языка – русский и английский.

По умолчанию пользователю отображается интерфейс на том языке, который соответствует его системному языку в ОС и предпочтительному языку в браузере. В этом случае переключение языка осуществляется посредством изменения основного языка ввода (языка отображения веб-страниц) в используемом браузере. Например, для изменения языка в браузере Chrome нужно выполнить шаги:

- перейти к настройкам браузера (chrome://settings/);
- выбрать пункт «Показать дополнительные настройки»;
- нажать на кнопку «Изменить языковые настройки»;
- переместить нужный язык на первое место в списке (рис. 125).

Языки	×
Выберите основной и дополнительный языки ввода. [Тодробнее
Языки	русский
русский	Google Chrome отображается на этом языке
английский (Соединенные Штаты)	🗷 Использовать этот язык для проверки правописания
английский	Предлагать перевести страницы на этом языке
Добавить	
🖉 Включить проверку правописания. Пользовательс	кий словарь для проверки правописания
	Готово

Рисунок 125 – Настройка языка для браузера Chrome

Для изменения языка в браузере Firefox нужно выполнить шаги:

- перейти к настройкам браузера (about:preferences);
- выбрать раздел «Содержимое» настроек;
- в подразделе «Языки» нажать на кнопку «Выбрать»;
- переместить нужный язык на первое место в списке:

Языки		×
Некоторые веб-страницы могут быть доступны более чем на одном языке. Ука: выбора языка страницы:	жите порядок	c
[ru-ru]	Вверх	
Русский [ru]	В <u>н</u> из	
Английский [en]	Удалить	i l
Английский/США [en-us]	, Ferrie	1
Выберите язык, чтобы его добавить	До <u>б</u> авить	
ОК Отмена	С <u>п</u> равка]

Рисунок 126 – Настройка языка для браузера Firefox

Дополнительно возможно провести настройку языка через конфигурационный файл blitz.conf. Для этого следует отредактировать раздел для настройки языка blitz.prod.local.idp.lang со следующими параметрами:

- languages список доступных языков. Первый язык в списке считается языком по умолчанию;
- portal-lang-cookie имя (name) и домен установки (domain) cookie с текущим языком портала (опциональный). Если портальная cookie задана, то смена языка в Blitz Identity Provider сохраняется в указанной cookie;
- ignore-browser включен или нет режим игнорирования языка браузера.

Пример фрагмента конфигурационного файла:

```
"lang" : {
  "ignore-browser" : true,
  "languages" : [
     "ru",
     "en"
 ],
  "portal-lang-cookie" : {
     "domain" : "domain.com",
     "name" : "blitzlng"
 }
}
```

Таким образом, например, если применение английского языка интерфейса не требуется, то его можно удалить из параметра languages.

15.2.2. Модификация текстовых сообщений веб-интерфейса

Blitz Identity Provider позволяет менять текстовые строки, используемые в интерфейсе системы. Для этого необходимо отредактировать файл messages, размещенный в директории /custom_messages/, добавив строку вида «параметр=значение», где параметр – идентификатор текстовой строки, а значение – необходимый текст.

Все текстовые строки, используемые Blitz Identity Provider по умолчанию, сохранены в архиве messages.zip, входящий в состав ПО.

Например, следующая строка отвечает за текст на форме регистрации, где размещена

ссылка на условия использования:

reg.page.reg.action.agreement=Нажимая на кнопку «Зарегистрироваться» вы соглашаетесь c условиями использования

Для корректного отображения файл должен быть сохранен в кодировке UTF-8.

При необходимости изменить английский язык следует добавить в указанную директорию файл messages.en и изменить в нем необходимые файлы.

При необходимости использовать в текстах символ @ его следует ввести дважды.

15.2.3. Модификация шаблонов писем и SMS-сообщений

Шаблоны писем представляют собой текстовые строки, сохраняемые аналогично обычным строкам в веб-интерфейсе. Их изменение производится аналогичным образом (см п. 15.2.2 документа).

Используется унифицированный формат кодов сообщений, который имеет вид:

message.\$[группа_сообщений].\$[тип_сообщения].\$[вариация].\$[канал].\$[часть]

Используются группы сообщения:

- notif для информационных сообщений;
- auth для взаимодействия с пользователем при аутентификации;
- reg для взаимодействия с пользователем при регистрации;
- recovery для взаимодействия с пользователем при восстановлении доступа;
- profile для взаимодействия с пользователем в Личном кабинете;
- арі для взаимодействия с пользователем при использовании API;

Вариации позволяют помимо базового шаблона сообщения задать его варианты (например, отдельный шаблон в разрезе приложений). Наличие вариации проверяется по основному шаблону с текстом сообщения (часть body). Если вариация основного шаблона описана в системе, то все остальные шаблоны (email.subject, email.from, push.title) будут применяться с этой же вариацией. Если вариаций несколько, то они будут проверяться в некотором заданном порядке (обычно от большей детализации к меньшей). При отсутствии вариаций будет использован базовый шаблон. В большинстве случаев вариации отсутствуют

Возможны следующие каналы:

- «sms» отправка сообщений по SMS. Части для этого канала отсутствуют;
- «email» отправка сообщений по электронной почты. Части для этого канала:
 - «subject» тема;
 - «body» основное содержание;
 - «from» отправитель (необязательно);

- «push» отправка push-уведомлений. Части для этого канала:
 - «title» тема;
 - «body» основное содержание.

Пример ключей для сообщений типа login_unknown_device:

- message.notif.login_unknown_device.email.subject тема сообщения по email;
- message.notif.login_unknown_device.email.body текст сообщения по email;
- message.notif.login_unknown_device.email.from отправитель email сообщения;
- message.notif.login_unknown_device.sms текст сообщения по SMS.

В таблицах ниже представлены описания типов сообщений из различных групп.

Таблица 6

Типы сообщений из группы «информирование» (notif)

Тип сообщения	Описание	Параметры
login_unknown_device	Информирование пользователя о входе с неизвестного устройства	 device – код устройства device.msg – название устройства, вычисленное через строку msg(audit.device.\$[device]) browser – браузер пользователя атрибуты из сессии пользователя
link_social_network	Информирование пользователя о присоединении к социальной сети	 fp.humanReadableName – название внешнего поставщика идентификации атрибуты пользователя
change_pwd	Информирование пользователя о смене пароля	 атрибуты пользователя
changed_pwd_to_object	Информирование о смене пароля в зависимой учетной записи	 атрибуты зависимой учетной записи с префиксом obj.
access_recovery	Информирование пользователя о восстановлении пароля	 атрибуты пользователя
access_recovery_by_obj ect	Информирование о восстановлении пароля в зависимой учетной записи	 атрибуты зависимой учетной записи с префиксом obj.
set_2factor_auth	Информирование пользователя о назначении второго фактора аутентификации	 method – код метода аутентификации method.msg – имя метода аутентификации, полученное через строку

Тип сообщения	Описание	Параметры	
		msg(message.method.name.\$[meth od] - атрибуты пользователя	
granted_access_to	Информирование субъекта о предоставление доступа к объекту	 blitz_right – код права доступа атрибуты субъекта атрибуты объекта с префиксом obj. 	
granted_access_on	Информирование объекта о предоставление доступа к нему	 blitz_right – код права доступа атрибуты объекта атрибуты субъекта с префиксом obj. 	
revoked_access_to	Информирование субъекта об отзыве доступа к объекту	 blitz_right – код права доступа атрибуты субъекта атрибуты объекта с префиксом obj. 	
revoked_access_on	Информирование объекта об отзыве доступа к нему	 blitz_right – код права доступа атрибуты объекта атрибуты субъекта с префиксом obj. 	
on_registration	Информирование пользователя о регистрации его учетной записи	 _entryPoint_ – канал регистрации _appId_ – приложение _requesterId_ _ атрибуты пользователя 	

Таблица 7

Типы сообщений из группы «регистрация» (reg)

Тип сообщения	Описание	Параметры	
vrf_code	Отправка кода подтверждения контакта при регистрации	 соdе – код подтверждения link – ссылка для подтверждения (только для email) req.ip – IP-адрес req.userAgent – userAgent пользователя cfg.domain 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 	

Тип сообщения	Описание	Параметры
		 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 атрибуты пользователя из контекста регистрации с префиксом attrs.

Таблица 8

Типы сообщений из группы «восстановление доступа» (recovery)

Тип сообщения	Описание	Параметры	
vrf_code	Отправка кода подтверждения контакта при восстановлении доступа	 соdе – код подтверждения link – ссылка для подтверждения (только для email) 	

Таблица 9

Типы сообщений из группы «аутентификация» (auth)

Тип сообщения	Описание	Параметры
vrf_code	Отправка кода подтверждения мобильного номера (каналы: SMS/push)	 code – код подтверждения

Таблица 10

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) соde – код подтверждения

Таблица 11

Типы сообщений	из группы	«программный	интерфейс» (арі)

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 АРІ	 соdе – код подтверждения link – ссылка (только для email) attr.value – новый контакт (email или мобильный номер) attr – код атрибута контакта

15.2.4. Модификация сообщений для разных приложений

Возможно изменение всех текстовых сообщений и шаблонов таким образом, чтобы использовались специфические тексты и шаблоны для разных приложений. Таким образом можно, например, брендировать письма, отправляемые при регистрации на разных сайтах, подключенных к одной установке Blitz Identity Provider, или давать ссылку на скачивание различных правил использования ресурса.

Для привязки набора шаблонов к конкретному приложению следует выполнить шаги:

- Создать экземпляр файла с текстами, который будет использоваться исключительно для данного приложения. Для этого в директории custom_messages/ создать текстовый файл messages.ru-123456 (messages.en-123456) для данного приложения, где 123456 – последовательность из 5-8 символов (допускаются как цифры, так и буквы латинского алфавита).
- 2. Отредактировать файл messages.ru-123456 (messages.en-123456), добавив в него специфические строки для данного приложения (подробнее см. п. 15.2.2). Все остальные строки будут взяты из базы строк по умолчанию.
- 3. Отредактировать файл blitz.conf следующим образом:
 - в разделе blitz.prod.local.idp.apps файла найти идентификатор приложения, который должен использовать созданный файл шаблона;
 - добавить параметр вида "lang-variant" : "123456", где 123456 использованная для маркировки шаблона последовательность символов. Пример:

```
"demo-application" : {
    "domain" : "http://testdomain.ru",
    "lang-variant" : "123456",
    "name" : "test",
    "oauth" : {
        "autoConsent" : false,
        "clientSecret" : "1234567890",
        "defaultScopes" : [],
        "enabled" : true,
        "redirectUriPrefixes" : [
        "http://localhost"
```

```
},
"theme" : "default"
```

После этого при входе в данное приложение будет использоваться специально созданный файл сообщений.

15.3. Файлы настроек консоли управления

Консоль управления настраивается с помощью файлов console.conf и credentials. Далее в подразделах описаны возможные настройки.

15.3.1. Настройка входа в консоль управления через SSO

В консоль управления Blitz Identity Provider можно настроить вход через поставщика идентификации OIDC. В качестве такого поставщика может выступить как текущая установка Blitz Identity Provider, так и отдельная его установка или даже стороннее ПО, если оно совместимо с OIDC.

Поддерживаются следующие режимы входа в консоль управления:

- стандартный режим по логину/паролю учетных записей, заведенных в разделе «Администраторы» (см. п. 2.11);
- режим входа через SSO;
- гибридный режим входа, когда администратор может войти как по логину/паролю в стандартном режиме, так и через SSO.

При использовании режима SSO учетные записи администраторов все равно должны быть заведены в разделе «Администраторы», и им должны быть назначены роли. Просто при SSO задание пароля учетной записи администратора становится необязательным, если указанный пользователь будет использовать для входа только SSO.

Для настройки режима входа в консоль управления с помощью SSO необходимо:

- В настройках внешнего поставщика идентификации (SSO) зарегистрировать приложение. В разрешенные префиксы возврата (redirect_uri) нужно, чтобы был прописан домен установки Blitz Identity Provider. По итогам регистрации получить client_id и client_secret приложения для консоли управления;
- в конфигурационном файле console.conf создать блок настроек login следующего содержания:

```
"login" : {
    "fp" : {
        "authUri" : "https://idp-host.com/blitz/oauth/ae",
        "clientId" : "blitz-console",
        "clientSecret" : "client_secret_value",
        "logoutUrl" :
    "https://idp-host.com/blitz/login/logout?post logout redirect uri=https://idp-host.com/blitz/console
    ",
        "scopes" : [
```

```
"openid"
],
"subjectClaim" : "sub",
"tokenUri" : "https://idp-host.com/blitz/oauth/te"
},
"mode" : "sso"
}
```

Необходимо уточнить параметры:

}

- В параметрах authUri и tokenUri нужно указать адреса Authorization Endpoint и Token Endpoint обработчиков внешнего поставщика идентификации.
- В параметрах clientId и clientSecret указать значения client_id и client_secret, присвоенный зарегистрированному во внешнем поставщике идентификации приложению, соответствующему консоли управления.
- В параметре logoutUrl прописать ссылку, на которую должен перенаправляться пользователь при выходе из консоли управления, чтобы был произведен единый выход через внешний поставщик идентификации.
- В параметре scopes прописать список разрешений, который должны быть запрошены (минимально необходимо только разрешение openid).
- B subjectClaim указать имя атрибута из маркера идентификации (id_token), используемого в качестве идентификатора учетной записи. Именно с таким идентификатором должна быть создана учетная запись в разделе «Администраторы» консоли управления, чтобы администратор мог войти в консоль управления.
- В параметре mode нужно указать требуемый режим страницы входа: sso вход только через внешний поставщик идентификации (Рисунок 127); credentials – вход только по логину и паролю из настроек консоли управления (Рисунок 3); если параметр не задан, то доступны оба варианта на выбор пользователя (Рисунок 128).



Рисунок 127 - Окно входа в консоль при включенном режиме SSO

Вход в Консоль управления
Логин
🛔 Введите логин
Пароль
Введите пароль
Войти
или
Войти через SSO

Рисунок 128 – Окно входа в консоль при всех включенных режимах входа

Чтобы не показывался промежуточный экран входа, в котором пользователь нажимает кнопку «Войти через SSO», можно вызывать консоль управления с помощью ссылки следующего вида: https://hostname:port/blitz/console?mode=SSO.

15.3.2. Ограничение сессий

По политике безопасности может требоваться, чтобы пользователь или администратор одновременно не мог быть залогинен с нескольких устройств. Для удовлетворения такой политики безопасности при доступе администратора в консоль управления необходимо в конфигурационном файле console.conf добавить блок session:

```
"session" : {
   "mode" : "exclusive",
   "check-interval" : 10
}
```

При наличии такой настройки в случае, если будет зафиксирован вход администратора с учетной записью, которой уже выполнен вход, то в прежнем входе при любом действии в консоли управления будет отображена страница входа. Настройка check-interval (задается в секундах) указывает в секундах период, как быстро в прежней сессии произойдет выход при появлении новой сессии.

Если по политике безопасности требуется также запретить наличие нескольких сессий для обычных пользователей, то такой режим можно включить избирательно для определенных пользователей при входе в определенные приложения. Это выполняется с помощью настройки процедуры входа (см. п. 6). Также может требоваться ограничить вход временных учетных записей после истечения срока их действия. Пример процедуры входа, реализующей обе политики, приведен ниже:

```
List<String> methods = new ArrayList<String>(Arrays.asList(ctx.availableMethods()));
   methods.remove("cls");
   return StrategyState.MORE(methods.toArray(new String[0]), true);
  } else {
   if(ctx.claims("subjectId") != null)
     return StrategyState.ENOUGH();
   else
     return StrategyState.MORE(new String[]{});
  }
}
@Override public StrategyState next(final Context ctx) {
  /*закомментировать следующий if, если временные учетные записи не используются*/
 if (ctx.claims("valid until") != null && isExpired(ctx.claims("valid until")))
   return StrategyState.DENY("account expired", true);
   String reqFactor = ctx.userProps("requiredFactor");
 if(reqFactor == null || Integer.valueOf(reqFactor) == ctx.justCompletedFactor())
    /* расскомментировать этот блок и закомментировать следующий, если нужна мультисессионность
   return StrategyState.ENOUGH();*/
   return StrategyState.ENOUGH BUILDER().withClaims(ctx.claimsBuilder().addClaim(" touch crid",
true).build()).build();
 else
   return StrategyState.MORE(new String[]{});
public static boolean isExpired(String strData) {
  try {
   Date now = new Date();
           Date date = new SimpleDateFormat("yyyy-M-d").parse(strData);
           return now.after(date);
        } catch (ParseException e) {
            throw new RuntimeException(e);
   }
```

Дополнительно в веб-приложении «Личный кабинет» нужно включить настройку, согласно которой будет происходить досрочный выход из веб-приложения в случае, если учетная запись пользователя заблокирована или была нарушена политика, запрещающая множественный вход пользователя. В конфигурационный файл blitz.conf в блок настроек blitz.prod.local.idp.user-profile нужно добавить настройку check-session-interval, задающую период проверки веб-приложением активности сессии:

```
"user-profile" : {
   "check-session-interval" : 10,
   ...
}
```

15.3.3. Настройка ролей и прав доступа в консоль управления.

Стандартные роли администраторов описаны в п. 2.11. В конфигурационном файле credentials можно создать дополнительные роли администраторов или исправить права доступа в существующих ролях. Для этого в блоке roles нужно скорректировать состав прав доступа (privileges), соответствующих роли (name). Пример настройки:

```
"roles" : [
{
    "name" : "new-role",
    "privileges" : ["w_app","w_system","w_ui","w_user","w_admin","r_audit"]
}
```

В случае создания новых ролей для них также нужно определить текстовые строки с названием ролей (см. п. 15.2). Пример текстовой строки для новой роли new_role:

```
page.admins.role.new-role=имя новой роли
```

Список доступных прав доступа для заполнения настройки privileges приведен в таблице 12:

Таблица 12

Право доступа	Доступные разделы консоли управления
w_app	«Приложения»
w_system	«Источники данных», «Аутентификация», «Процедуры входа»,
	«Поставщики идентификации», «SAML», «OAuth 2.0», «Устройства»,
	«Сообщения»
w_ui	«Сервисы самообслуживания», «Внешний вид»
w_admin	«Администраторы», «События»
w_user	«Пользователи», «Группы»
r_user	«Пользователи» (только просмотр), «Группы» (только просмотр)
r_audit	«События» (только просмотр)

Права доступа консоли управления Blitz Identity Provider

16. Решение проблем

Логи работы Blitz Identity Provider записываются в директорию /var/log/identityblitz на каждом сервере. Журнал событий каждого приложения называется в соответствии с приложением:

- blitz-console.log –журнал событий консоли управления;
- blitz-idp.log журнал событий сервиса аутентификации.
- blitz-registration.log журнал событий сервиса регистрации;
- blitz-recovery.log журнал событий сервиса восстановления доступа;
- blitz-keeper.log журнал событий шлюза безопасности.

При возникновении ошибок, связанных с работой Blitz Identity Provider (записываются в лог как [ERROR]), рекомендуется обратиться в техническую поддержку Blitz Identity Provider по адресу support@reaxoft.ru.

При необходимости повысить уровень логирования необходимо в конфигурационном файле /usr/share/identityblitz/blitz-config/blitz.conf в блоке logger изменить уровни логирования. По умолчанию все уровни логирования выставлены в INFO:

```
"levels" : {
 "ROOT" : "INFO",
"application" : "INFO",
  "com.couchbase.client" : "INFO",
  "com.identityblitz" : "INFO",
  "com.identityblitz.idp" : "INFO",
  "com.identityblitz.idp.events" : "INFO",
  "com.identityblitz.idp.flow.dynamic" : "INFO",
 "com.identityblitz.idp.flow.dynamic.extend" : "INFO",
 "com.identityblitz.idp.rabbitmq" : "INFO",
"com.identityblitz.idp.task.processing" : "INFO",
  "com.identityblitz.login-framework" : "INFO",
  "com.identityblitz.login-framework.ldap-timings" : "INFO",
 "com.identityblitz.login.store" : "INFO",
  "com.identityblitz.play.memcached" : "INFO",
  "com.identityblitz.play.memcached.RefreshableMemcachedConnection" : "INFO",
  "com.unboundid.ldap.sdk" : "INFO",
  "org.asynchttpclient.netty" : "INFO",
  "org.opensaml" : "INFO",
  "org.opensaml.util.resource" : "INFO",
  "play" : "INFO",
 "plugin.memcached" : "INFO"
```

Для повышения уровня логирования необходимо параметрам ROOT и всем com.identityblitz.* присвоить значение TRACE.

В случае если случайно было произведено изменение конфигурации Blitz Identity Provider в консоли управления, то в скрытой директории /usr/share/identityblitz/blitzconfig/.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:

Приложение 1. Функциональная спецификация Blitz Identity Provider

Γ	A	Доступность функции в редакции				
т руппа функции	Функция		Enterprise	Ultimate		
Технологии единог	Технологии единого входа					
OpenID Connect и	RFC 6749 "The OAuth 2.0 Authorization Framework"	да	да	да		
OAuth 2.0	OpenID Connect Core 1.0	да	да	да		
	Передача атрибутов пользователя в составе id_token/access_token в JSON Web Token (JWT)	да	да	да		
	Конфигурируемый REST-сервис UserInfo, настройка возвращаемых атрибутов в зависимости от scope	да	да	да		
	RFC 7636 "Proof Key for Code Exchange by OAuth Public Clients"	да	да	да		
	RFC 7662 "OAuth 2.0 Token Introspection"	да	да	да		
	RFC 7591 "OAuth 2.0 Dynamic Client Registration Protocol"	нет	да	да		
	RFC 7592 "OAuth 2.0 Dynamic Client Registration Management Protocol"	нет	да	да		
	RFC 8252 "OAuth 2.0 for Native Apps"	нет	да	да		
	RFC 8414 "OAuth 2.0 Authorization Server Metadata"	да	да	да		
	RFC 8693 "OAuth 2.0 Token Exchange" с проверкой правил доступа	нет	нет	да		
SAML	SAML Web Browser SSO Profile	да	да	да		
	SAML Single Logout Profile	да	да	да		
WS-Federation	WS-Federation (для подключения Microsoft-приложений)	да	да	да		
Proxy SSO	Подключения веб-приложений, получающих состояние сессии из HTTP-заголовков и cookies	нет	нет	да		
	Поддержка возможности заполнения за пользователя логина/пароля от учетной записи в размещенное за proxy веб-	нет	нет	да		
	приложение, не поддерживающее стандартным образом подключения к SSO					
	Обеспечение контроля доступа к REST-сервисам через Blitz Keeper (API Security Gateway)	нет	нет	да		
Другое	Единый вход работает между приложениями, которые подключены к IDP с использованием любых поддерживаемых	да	да	да		
	технологий (например, SSO между OpenID Connect и SAML-приложениями)					
	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 а	аутентификация пользователей					
Вход по логину и	Проверка логина/пароля при аутентификации	да	да	да		
паролю	Возможность в качестве логина одновременно использовать несколько сущностей (телефон, email, логин) и вводить логин	да	да	да		
	в разных форматах (например, вводить телефон как +7, 8, с разным вариантом ввода скобок, дефисов, пробелов)					
	Запоминание логина, если пользователь ранее уже входил с этого устройства	да	да	да		
	Обработка события «пароль требует смены» при входе. Возможности сменить пароль в момент входа	да	да	да		
	Проверка соответствия пароля действующей парольной политике при входе. Рекомендация сменить пароль	да	да	да		
	Встроенная защита от подбора пароля (перебор паролей на одну учетную запись) и подбора логина (попытка подбора	нет	да	да		
	пароля на набор учетных записей):					
	– проверка САРТСНА;	нет	да	да		
	 временное олокирование входа по паролю учетнои записи при выявленных попытках перебора 	нет	да	да		
	- замедление входа пользователя	нет	да	да		
	предупреждение пользователя о попытке входа с паролем, которыи оыл недавно изменен	да	да	да		

Вход на основе	Идентификация пользователя на основе результата входа в домен (Kerberos)	да	да	да
сеанса ОС	Возможность подключения системы входа одновременно к нескольким доменам и обеспечения сквозного входа	нет	да	да
	пользователей из разных доменов			
	Возможность настройки, чтобы режим входа на основе сеанса ОС применялся только при входе из внутренних сетей и с	нет	да	да
	ПК, но не применялся при входе с мобильных приложений и из вне рабочей сети			
Вход через	Социальные сети и внешние поставщики идентификации, через которые поддерживается возможность входа	Facebook, Google, Mail ID, VK,		ID, VK,
аккаунт	пользователей без необходимости доработок и написания коннекторов	Одноклассники, Яндекс		декс
социальной сети /	1/ Вход через ЕСИА в режиме физического лица		да	да
стороннего	Вход через ЕСИА в режиме представителя организации (с выбором организации при входе)	нет	нет	да
поставщика	Вход через Сбер ID	нет	нет	да
идентификации	Вход через Mos ID (СУДИР)	нет	да	да
	Сопоставление/регистрация учетной записи в процессе первичного входа через социальную сеть	да	да	да
	Возможность привязки к одной учетной записи пользователя одновременно нескольких учетных записей социальных сетей	да	да	да
Вход на основе	Автоматическая идентификация пользователя, если он уже входил с этого устройства и согласился запомнить свой вход	да	да	да
запомненного	Возможность пользователю отследить, на каких устройствах запомнен вход, и выйти с этих устройств	да	да	да
устройства	Автоматический выход с запомненных устройств при смене/восстановлении пароля пользователем	да	да	да
Вход с помощью	Вход с помощью средств квалифицированной электронной подписи	нет	да	да
смарт-карты /	Поддерживаемые средства электронной подписи: КриптоПро CSP 3.9 и выше, VipNet CSP 4.2, Signal-COM CSP 3.0,	нет	да	да
USB-ключа	Рутокен, JaCarta, ISBC ESMART, SafeNet eToken			
	Поддерживаемые пользовательские ОС: Windows 7/8.1/10, macOS 10.13/10.14/10.15/11.3, Linux Debian 9, Mint 19, Ubuntu 18	нет	да	да
	Поддерживаемые браузеры: Internet Explorer 11, Chrome, Firefox, Yandex, Спутник	нет	да	да
	Возможность сопоставления/регистрации учетных записей в процессе первичного входа на основе данных из сертификата	нет	да	да
	квалифицированной электронной подписи			
	Возможность проверки действительности подписи/сертификата встроенными возможностями ПО	нет	да	да
	Возможность проверки действительности подписи/сертификата через вызов внешнего сервиса проверки	нет	да	да
Двухфакторная	Подтверждение входа разовым паролем из SMS (SMS-шлюз предоставляет Заказчик)	да	да	да
аутентификация	Подтверждение входа разовым паролем из email	да	да	да
	Подтверждение входа разовым паролем TOTP-приложения (RFC 6238 "TOTP: Time-Based One-Time Password Algorithm")	да	да	да
	Подтверждение входа разовым паролем из аппаратного брелока. Поддержка брелоков HOTP (RFC 4226 "HOTP: An HMAC- Based One-Time Password Algorithm"). Брелоки предоставляет Заказчик.	нет	да	да
	Подтверждения входа разовым паролем в push-уведомлении в мобильном приложение Заказчика (сервис для отправки push и мобильное приложение предоставляет Заказчик)	нет	нет	да
Другое	Возможность Заказчику самостоятельно добавить собственный метод аутентификации	нет	да	да
	Возможность Заказчику настроить вызов вспомогательного внешнего приложения, вызываемого в процессе входа, и	нет	ла	ла
	выполняющего взаимолействие с пользователем в процессе входа	ner	дu	дu
	Возможность Заказчику самостоятельно настроить внешний вил страницы вхола разлельно лля кажлого приложения. в	да	да	да
	которое осуществляется вход		<u> </u>	
	Предоставление API, позволяющее мобильным приложениям зарегистрировать событие входа и получить маркеры	нет	да	да
	безопасности при входах с использованием ПИН-кода, Touch ID, Face ID			
	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		
Возможности поль	зователя по управлению своей учетной записью					
Регистрация	Настраиваемое веб-приложение самостоятельной регистрации пользователей. Можно настроить набор атрибутов, заполняемых пользователем при регистрации, требования к подтверждению email/телефона, настроить внешний вид страницы регистрации, вызов сервисов проверки Заказчика	да	да	да		
	Можно задать различные настройки веб-приложения самостоятельной регистрации пользователя для различных сценариев вызова регистрации	нет	да	да		
	Возможность вызова внешнего приложения регистрации с передачей ему контекста входа и сведений, полученных из внешнего поставщика (ЕСИА или соц.сети) в процессе входа	нет	да	да		
	По результатам успешной регистрации пользователь автоматически входит в приложение, при попытке входа в которое изначально была инициирована регистрация	да	да	да		
Настройки	Веб-приложение, позволяющее пользователю управлять настройками безопасности его учетной записи:	да	да	да		
безопасности	– возможность самостоятельно сменить пароль	да	да	да		
учетной записи	 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	Веб-приложения, позволяющего восстановить забытый пароль, с подтверждением email или телефона	да	да	да		
забытого пароля	По результатам успешного восстановления пароля пользователь автоматически входит в приложение, при попытке входа в которое изначально была инициирована процедура восстановления	да	да	да		
Парольные политики	Проверка пароля на соответствие парольной политике: минимальная длина, требования к алфавиту, запрет словарных паролей, запрет повтора паролей, проверка срока действия паролей	да	да	да		
Мониторинг и ауд	ЛТ					
Оповещения	Оповещение пользователей о событиях безопасности с их учетными записями: вход с необычного устройства, изменение	да	да	да		
пользователен о	пароля (сам сменил, администратор соросил, смена в результате восстановления пароля), привязка учетной записи					
безопасности	Возможность настроить набор событий оповешения и тексты оповешений для SMS и для email	па	ла	ла		
Регистрация	Регистрация успешных и неуспешных событий безопасности с учетной записью: события входа, регистрации, изменения	ла	ла	ла		
событий	настроек безопасности, восстановления пароля. Должны регистрироваться как действия, инициированные пользователем,	<u> </u>	<u> </u>	<u> </u>		
безопасности	так и действия, инициированные администратором					
	Интерфейс администратора для поиска/просмотра событий безопасности	да	да	да		
Мониторинг	Возможность в момент входа пользователя вызывать системы сбора метрик и статистики, антифрод системы	нет	да	да		
	Возможность осуществлять мониторинг компонент из внешней системы мониторинга (Zabbix и аналоги)	нет	да	да		
Очереди	Возможность передавать в очередь RabbitMQ события, связанные с учетными записями пользователей и групп доступа	нет	да	да		
Администрирование						
-------------------	---	-----	----	----	--	--
	Веб-приложение администрирования:	да	да	да		
	– задание настроек подключенных приложений (параметры приложений, разрешенные режимы взаимодействия)	да	да	да		
	 настройка атрибутов пользователей и сопоставление атрибутов 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	нет	да	да		
	задать разный набор доступных действий					
	– управление настройками веб-приложений регистрации, управления настройками безопасности, восстановления пароля	да	да	да		
	– администрирование учетных записей пользователей (поиск, просмотр, управление атрибутами, настройками	да	да	да		
	двухфакторной аутентификации, привязками запомненных устройств и социальных сетей, сброс пароля,					
	блокирование/разблокирование учетной записи)					
	 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		
	– взможность входа в веб-приложение администрирования через SSO	нет	да	да		
	Интерфейс администратора на русском и английском языках	да	да	да		
	Возможность добавления переводов на дополнительные языки	да	да	да		

Приложение 2. Рекомендации по обеспечению мер защиты информации согласно требованиям ФСТЭК

Условное обозначение и номер меры	Мера защиты информации в информационных системах	Рекомендации по настройке			
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Настроить методы аутентификации пользователей, см. п. 4. Для администраторов консоли управления настроить вход через Blitz (см. п. 15.3.1). Настроить через процедуры входа для администраторов и пользователей требования к прохождению двухфакторной аутентификации (см. п. 6) Задать для подключаемых приложений client_id и client_secret (см. п. 5)			
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Задать атрибут, который будет использоваться в качестве идентификатора учетной записи (см. п. 3.1.5). Настроить запрет на повторное использование идентификатора после удаление учетной записи (см. 15.1.13) и блокирование неактивных учетных записей (см. 15.1.12)			
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Установить парольную политику (см. п. 15.1.1). Управлять учетными записями пользователей (см. п. 9).			
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Специальная настройка не требуется			
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Настроить вход через внешние поставщики идентификации (см. п. 8.7, п. 8.9, п. 8.10)			
Управление дос	тупом 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 истечение срока действия записей (см. п 15.3.2). Для использования функций работы с группами пользователей настроить группы пользователей (см. п. 15.1.14). Управлять учетными записями через консоль управления (см. п. 9)			
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Настроить права доступа (см. п. 15.1.10), разрешения (см. п. 5.3.2), установить разрешения приложений (см. п. 5.3.1), настроить шлюз безопасности (см. п. 14), настроить атрибуты пользователей (см. п. 3) и группы пользователей (см. п. 15.1.14), процедуры входа в приложения (см. п. 6).			

УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Использовать сервисы изменения атрибутов, включения и исключения пользователей в группы, назначения и отзыва прав доступа (см. «Руководство по интеграции»)
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Назначать роли администраторов (см. п. 2.11), управлять атрибутами пользователей (см. п. 9), назначать права доступа с использованием сервисов (см. «Руководство по интеграции»)
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Настроить политику ограничения числа попыток входа с последующим блокированием учетной записи (см. п. 4.1)
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации	Настроить для приложений экран согласия пользователя (см. п. 5.3.1, п. 5.3.2, п. 15.2)
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему	Настроить доступ к аудиту по себе для пользователей (см. п. 7.2.2)
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	Настроить политику ограничения числа параллельных сеансов (см. п. 15.3.2)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Настроить период неактивности (см. п. 4)
Регистрация со	бытий безопасности (РСБ)	
Регистрация со РСБ.1	бытий безопасности (РСБ) Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Специальная настройка не требуется
Регистрация со РСБ.1 РСБ.2	бытий безопасности (РСБ) Определение событий безопасности, подлежащих регистрации, и сроков их хранения Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Специальная настройка не требуется Специальная настройка не требуется
Регистрация со РСБ.1 РСБ.2 РСБ.3	бытий безопасности (РСБ) Определение событий безопасности, подлежащих регистрации, и сроков их хранения Определение состава и содержания информации о событиях безопасности, подлежащих регистрации Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Специальная настройка не требуется Специальная настройка не требуется Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11)
Регистрация со РСБ.1 РСБ.2 РСБ.3 РСБ.4	Бытий безопасности (РСБ) Определение событий безопасности, подлежащих регистрации, и сроков их хранения Определение состава и содержания информации о событиях безопасности, подлежащих регистрации Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения 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	Специальная настройка не требуется Специальная настройка не требуется Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11) Просматривать журналы событий на предмет возникновения ошибок (см. п. 16)
Регистрация со РСБ.1 РСБ.2 РСБ.3 РСБ.4 РСБ.5	Бытий безопасности (РСБ) Определение событий безопасности, подлежащих регистрации, и сроков их хранения Определение состава и содержания информации о событиях безопасности, подлежащих регистрации Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения 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 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Специальная настройка не требуется Специальная настройка не требуется Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11) Просматривать журналы событий на предмет возникновения ошибок (см. п. 16) Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11)
Регистрация со РСБ.1 РСБ.2 РСБ.3 РСБ.4 РСБ.5 РСБ.6	Бытий безопасности (РСБ) Определение событий безопасности, подлежащих регистрации, и сроков их хранения Определение состава и содержания информации о событиях безопасности, подлежащих регистрации Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения 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 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Специальная настройка не требуется Специальная настройка не требуется Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11) Просматривать журналы событий на предмет возникновения ошибок (см. п. 16) Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11) При установке ПО сконфигурировать использование сервиса точного времени (NTP)
Регистрация со РСБ.1 РСБ.2 РСБ.3 РСБ.4 РСБ.5 РСБ.5 РСБ.6 РСБ.7	Бытий безопасности (РСБ) Определение событий безопасности, подлежащих регистрации, и сроков их хранения Определение состава и содержания информации о событиях безопасности, подлежащих регистрации Определение состава и содержания информации о событиях безопасности, подлежащих регистрации Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения 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 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них Генерирование временных меток и (или) синхронизация системного времени в информационной системе Защита информации о событиях безопасности	Специальная настройка не требуется Специальная настройка не требуется Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11) Просматривать журналы событий на предмет возникновения ошибок (см. п. 16) Просмотр событий безопасности периодически осуществлять в консоли управления (см. п. 11) При установке ПО сконфигурировать использование сервиса точного времени (NTP) Настроить резервное копирование СУБД (см. п. 2.3)