Blitz Identity Provider

Сервер аутентификации и управления доступом

ООО «РЕАК СОФТ»

identityblitz.ru

Типичные проблемы

Собственные механизмы входа приложений не всегда безопасны

Разрозненная регистрация событий безопасности усложняет аудит доступа

Пользователям сложно запомнить множество логинов и паролей

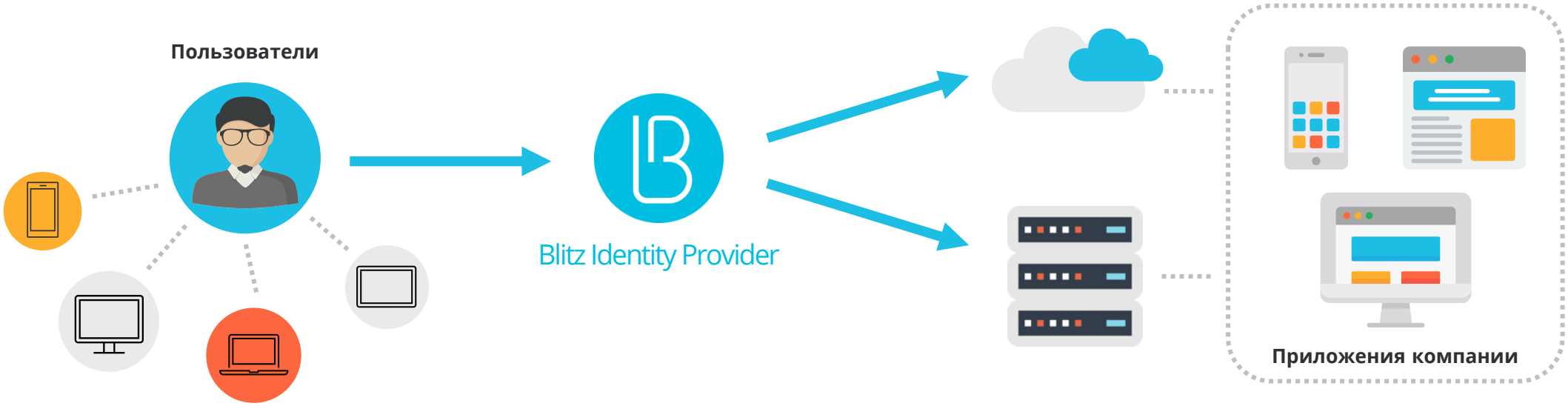
Парольной аутентификации недостаточно для эффективной защиты многих приложений

При удаленной работе сотрудников повышается риск взлома учетных записей

Доступ сотрудников к облачным сервисам неудобен или небезопасен

Решение

Создать единый сервис доступа пользователей к приложениям компании



Blitz Identity Provider

Это программный продукт, развертываемый на серверах компании
Решает задачи идентификации, аутентификации, авторизации и аудита

единый вход и однократная аутентификация (SSO)

поддержка различных методов аутентификации

подходит для разных пользователей: сотрудников, клиентов, контрагентов

подходит для веб-сайтов, мобильных приложений и IoT

защита веб-приложений и сервисов компании (Access Management, API Security)

протоколирование событий безопасности и подотчетность действий пользователей

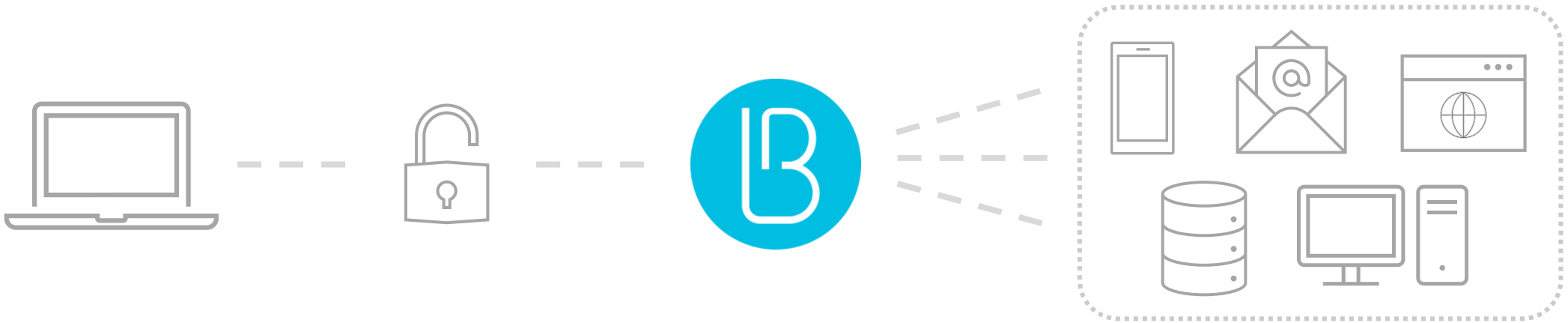
Единый вход (Single Sign-On)

Позволяет пользователю однократно войти в свою учетную запись и получить доступ ко всем приложениям компании

повышает удобство пользователей

усиливает безопасность

экономит время и инвестиции

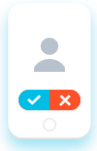


Выбор методов аутентификации

Встроенная поддержка множества методов аутентификации и подтверждения входа
Возможность подключить собственные методы входа, используемые внутри компании

Логин / пароль, встроенная защита от подбора

Смарт-карта / USB-ключ с электронной подписью / Ключи безопасности FIDO2 / U2F



Push-аутентификация

Внешние поставщики идентификации / Вход по QR-коду

Программные TOTP-генераторы

Аппаратные брелоки (HOTP / TOTP / OCRA)

SMS-коды подтверждения

Собственные методы входа

Универсальность

Продукт учитывает потребности всех категорий пользователей: сотрудников, клиентов, контрагентов

Примерные сценарии использования

Сотрудник

При доступе из внутренней сети – автоматически входит через доменную учетную запись, из внешней сети – входит с помощью двухфакторной аутентификации

Клиент

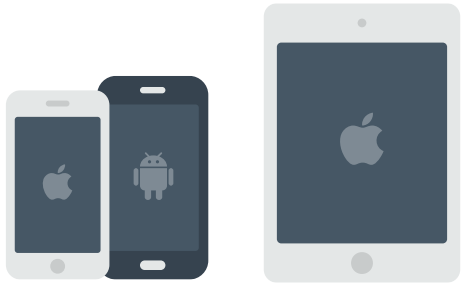
Входит через аккаунт социальной сети / ЕСИА или регистрируется через экранную форму на сайте

Контрагент

Ответственный представитель компании администрирует учетные записи своих коллег

Поддержка любых устройств доступа

Система аутентификации учитывает особенности сценариев доступа и безопасности при использовании различных устройств



Смартфоны и планшеты

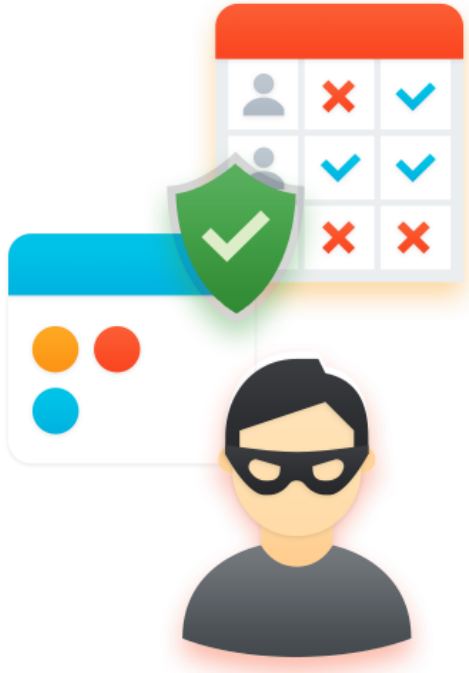
Персональные компьютеры

IoT устройства

Защита веб-приложений и сервисов

Реализована возможность централизованно настраивать логику авторизации доступа пользователей в веб-приложения и сервисы компании

- Использование технологии OAuth 2.0 в составе сервера аутентификации для защиты веб-сервисов
- Правила доступа могут учитывать, например, атрибуты пользователей и параметры окружения
- Политики доступа могут отличаться для различных приложений, организаций и групп пользователей



Аудит и подотчетность

Регистрируются входы пользователей и доступы к приложениям и сервисам компании

Осуществление постоянного мониторинга позволяет своевременно выявить и отреагировать на атаки

Возможность выгрузки событий безопасности во внешнюю систему анализа защищенности (SIEM)

Пользователям доступно управление настройками безопасности учетной записи в Личном кабинете

Наличие системы информирования пользователя о важных событиях безопасности с учетной записью

Преимущества продукта

Российская разработка:

- ✓ включен в Единый реестр российских программ для ЭВМ
- ✓ сертифицирован по требованиям безопасности ФСТЭК
- ✓ стоимость не привязана к курсу доллара

Простота и гибкость настройки:

- ✓ встраивается в ИТ-инфраструктуру
- ✓ есть веб-консоль администрирования

Выбор методов аутентификации:

- ✓ поддерживает современные средства аутентификации
- ✓ вход по квалифицированной электронной подписи

Поддержка внешних систем идентификации:

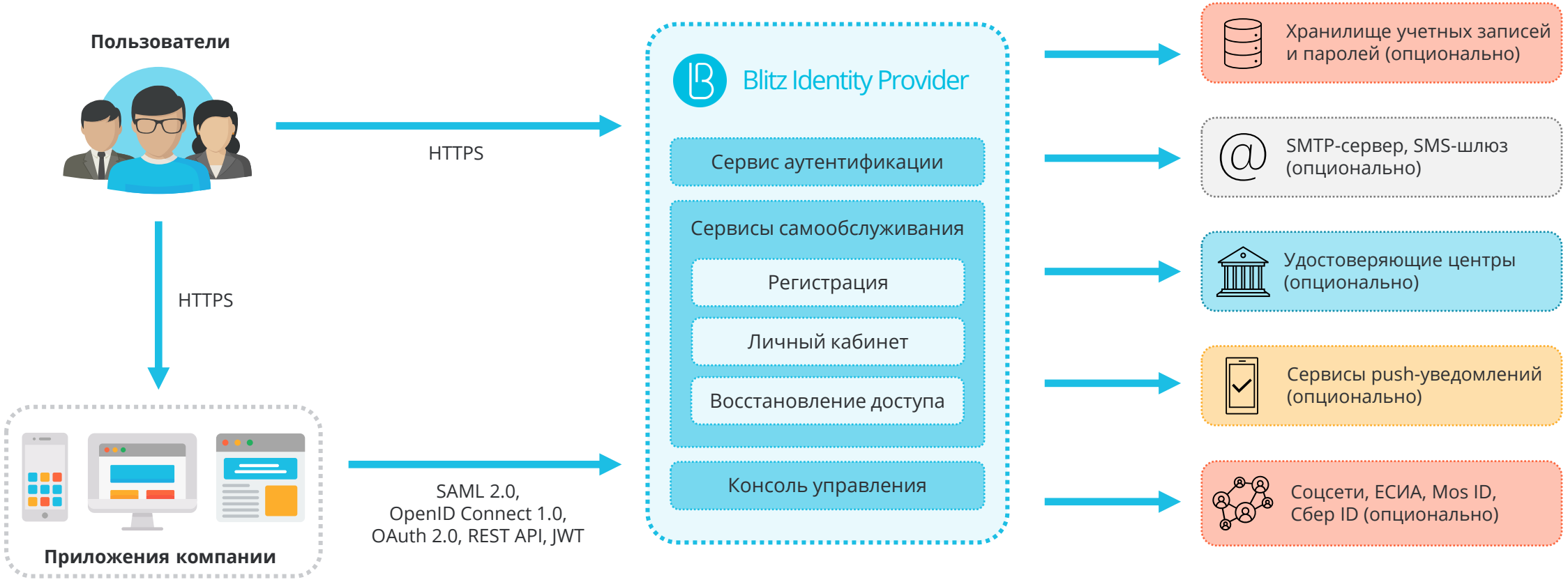
- ✓ популярные в России социальные сети
- ✓ возможность входа с помощью ЕСИА, Mos ID, Сбер ID

Лицензии и сертификаты

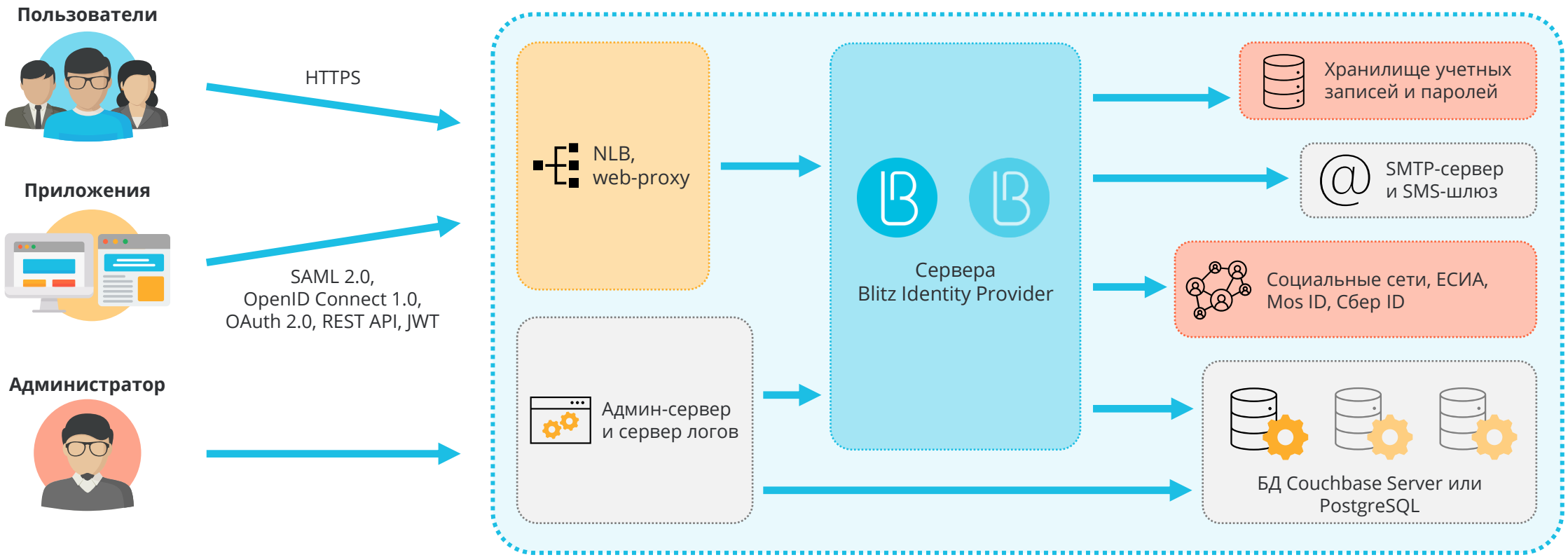
Blitz Identity Provider зарегистрирован в Едином реестре российского ПО (№842) и сертифицирован ФСТЭК России (№4525 от 10.03.2022), что подтверждает соответствие требованиям информационной безопасности и допускает применение продукта в государственных информационных системах

Минцифры России

Схема работы



Типовая схема развертывания



Как устроен Blitz Identity Provider

Веб-приложения

- Сервис аутентификации
- Сервисы самообслуживания
  - Регистрация
  - Личный кабинет
  - Восстановление доступа
- Консоль управления

Слой «Веб» — Фреймворк Bootstrap

Плагин браузера

Blitz Smart Card Plugin

Слой «Сервисы»

SAML 2.0 и WS-Federation

Поставщик идентификации

OpenID Connect 1.0 и OAuth 2.0

Поставщик идентификации

Blitz Keeper

Шлюз безопасности API

REST API

Сервисы управления учетными записями

Внешние поставщики входа

Сбер ID, Apple ID, госуслуги, Войти через mos.ru, OpenID Connect

Слой «Бизнес-логика»

Java, Scala, play, JS, Blitz Development Kit

Слой «Хранение»

- Хранение событий безопасности и иных данных — Couchbase или PostgreSQL
- Хранение учетных записей — LDAP или Внешняя БД
- Серверный кэш — Memcached
- Очередь событий — RabbitMQ

Слой «Объекты»

- Приложения
- Аутентификаторы
- Пользователи
- Устройства
- Группы пользователей
- События безопасности
- Атрибуты
- Разрешения

Функциональные возможности

Предоставляемые способы идентификации и аутентификации	1. Логин / пароль, встроенная защита от подбора 2. Смарт-карта / USB-ключ с электронной подписью / Ключи безопасности FIDO2 / U2F 3. Аппаратные брелоки (HOTP / TOTP / OCRA) 4. Программные TOTP-брелоки (Google Authenticator, Яндекс.Ключ и другие) 5. SMS-коды подтверждения и push-аутентификация на мобильное приложение	Подключение к внешним хранилищам учетных записей и паролей	1. MS Active Directory / FreeIPA 2. LDAP-совместимый сервер 3. Произвольное хранилище (через коннектор-обертку)
Поддержка внешних систем идентификации	1. Вход через социальные сети (Google / Facebook / VK / Яндекс / Одноклассники / Mail ID / Apple ID) 2. Вход через госуслуги (ЕСИА), Mos ID, Сбер ID 3. Вход через установку Blitz Identity Provider другой организации (федерация) 4. Вход с использованием Kerberos-сервера 5. Вход с использованием совместимого TLS / SSL-шлюза или VPN-шлюза	Сервисы самообслуживания пользователей	1. Регистрация пользователя 2. Восстановление пароля 3. Личный кабинет (обновление данных учетной записи) 4. Настройка двухфакторной аутентификации 5. Просмотр событий безопасности и списка используемых устройств доступа
Способы подключения приложений	1. SAML 1.0/1.1/2.0, WS-Federation 2. OpenID Connect 1.0 / OAuth 2.0 3. Веб-прокси с пробросом логина / пароля в форму входа веб-приложения	Прочее	1. Высокая производительность при развертывании на скромных аппаратных ресурсах 2. Высокая надежность при развертывании в кластере

Преимущества внедрения SSO

Для работников

- ✓ Упрощение доступа к информационным ресурсам
- ✓ Снижение временных затрат на получение доступов
- ✓ Исключение «парольного хаоса»

Для ИТ-подразделения

- ✓ Сокращение затрат на администрирование
- ✓ Многократное снижение кол-ва заявок от пользователей
- ✓ Упрощение процедуры предоставления внешнего доступа

Для отдела ИБ

- ✓ Снижение рисков несанкционированного доступа
- ✓ Повышение безопасности за счет дополнительных факторов
- ✓ Унифицированные политики аутентификации

Крупнейшие проекты

mos.ru	Департамент информационных технологий города Москвы	Blitz Identity Provider Blitz Smart Card Plugin	8 млн жителей 100 тыс. сотрудников
ИНГОССТРАХ	СПАО «Ингосстрах»	Blitz Identity Provider ESIA-Bridge	2 млн клиентов 4 тыс. сотрудников 20 тыс. агентов
НЛМК	Группа НЛМК	Blitz Identity Provider	20 тыс. сотрудников 50 тыс. рабочих 60 компаний холдинга
Банк России	Центральный Банк России	Blitz Identity Provider	10 тыс. сотрудников

Система управления доступом к информационным ресурсам (СУДИР)

mos.ru

Задача:

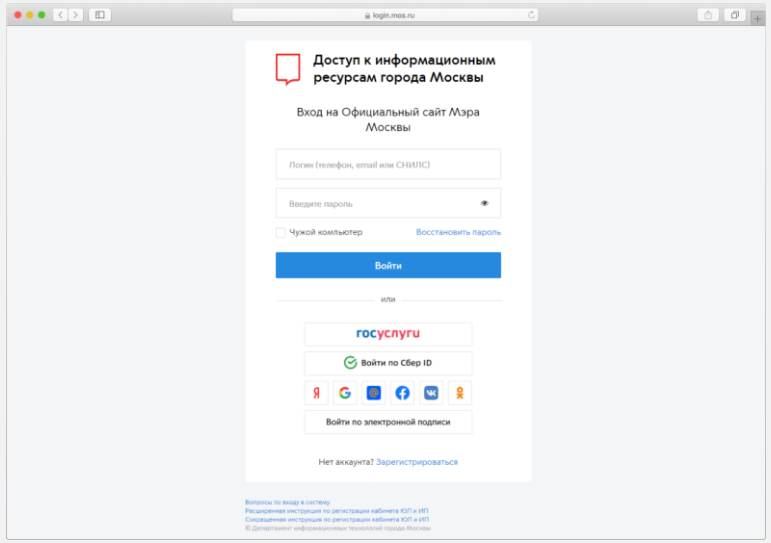
- Унифицировать программную платформу, повысить производительность работы и эффективность эксплуатации СУДИР

Результаты:

- ✓ Унифицирована программная платформа – множество программных продуктов, решающих задачу идентификации/аутентификации пользователей, замещены единым решением
- ✓ Повышена производительность и надежность работы СУДИР, увеличен запас производительности при сокращении аппаратных ресурсов
- ✓ Упрощено подключение к СУДИР новых приложений за счет соответствия платформы стандартным протоколам и спецификациям
- ✓ Расширены функциональные возможности СУДИР, усилена безопасность учетных записей пользователей
- ✓ Повышено удобство работы администраторов и пользователей
- ✓ Осуществлено импортозамещение

8 месяцев

более 8 млн жителей Москвы
100 тыс. сотрудников органов власти



Система аутентификации СПАО «Ингосстрах»

ИНГОССТРАХ

Задачи:

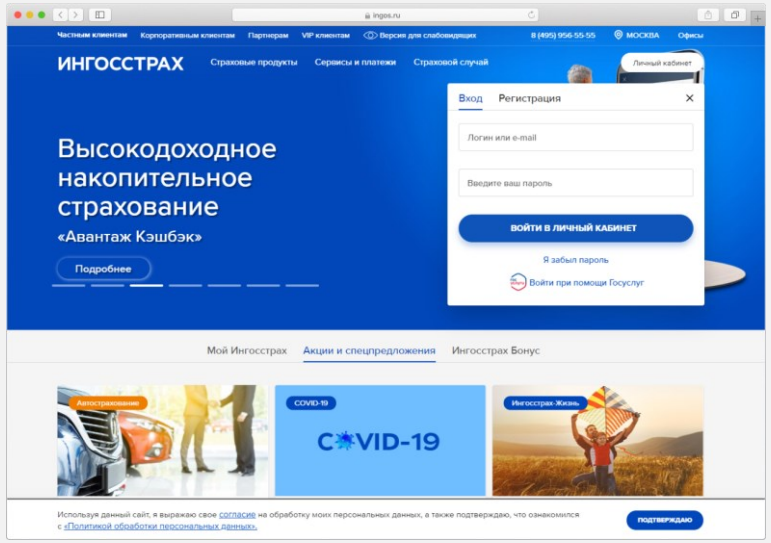
- Обеспечить унифицированное решение по идентификации пользователей, агентов, клиентов
- Обеспечить функционирование разных режимов аутентификации

Результаты:

- ✓ Создано унифицированное техническое решение по идентификации пользователей к приложениям компании
- ✓ Реализована интеграция с AD/Kerberos для сотрудников компании
- ✓ Обеспечена возможность использования двухфакторной аутентификации для агентов
- ✓ Подготовлена единая точка контроля доступа: разным категориям сотрудников предоставляется доступ к различным приложениям

6 месяцев

более 2 млн клиентов
4 тыс. сотрудников
20 тыс. агентов



Система аутентификации для интранет-портала Группы НЛМК

Задачи:

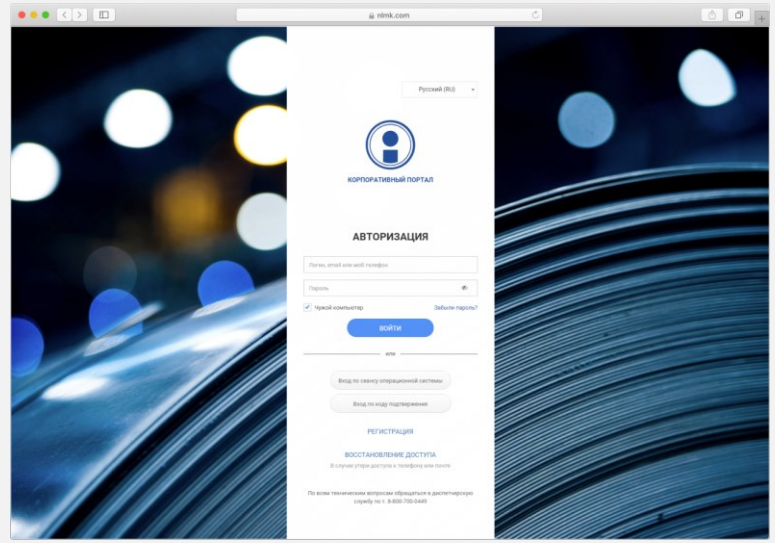
- Обеспечить регистрацию и достоверную идентификацию учетных записей работников Группы НЛМК
- Обеспечить единый вход в кадровые и обучающие приложения НЛМК для офисных сотрудников

Результаты:

- ✓ Обеспечены самостоятельная регистрация учетных записей, а также регистрация через отделы кадров. В процессе регистрации данные сверяются с кадровой системой
- ✓ Обеспечена одновременная работа с двумя каталогами – каталог учетных записей офисных сотрудников и каталог внешних работников, которым не требуется доступ ко внутренним ИТ-ресурсам
- ✓ Реализована поддержка интерфейса на английском, французском, датском и итальянском языках
- ✓ Обеспечен единый вход пользователей в корпоративный портал, мобильное приложение, веб-приложения и облачных сервисов компании

3 месяца

более 20 тыс. сотрудников
50 тыс. рабочих
60 компаний холдинга



Доменная аутентификация в приложения Банка России

Банк России

Задача:

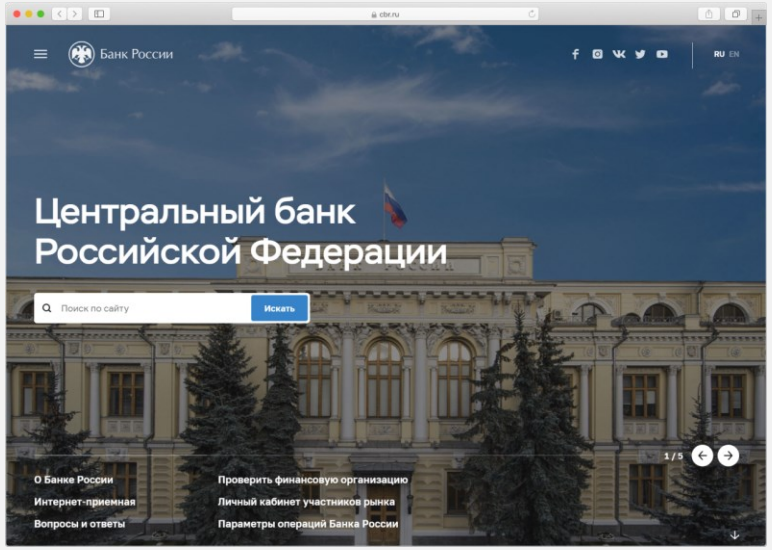
- Обеспечить сквозную доменную аутентификацию пользователей в приложения организации

3 месяца

более 10 тыс. сотрудников

Результаты:

- ✓ Обеспечена сквозная доменная аутентификация сотрудников при доступе в приложения (AD/Kerberos)
- ✓ Реализована технология Web Single Sign-On
- ✓ Обеспечена простая интеграция – используются стандартные возможности подключения приложений (SAML 2.0 / OpenID Connect 1.0 / web-proxy)
- ✓ Реализована аутентификация по смарт-карте / USB-ключу электронной подписи
- ✓ Подключена веб-консоль администрирования пользователей



О компании

РЕАК СОФТ – один из ведущих российских разработчиков программного обеспечения для идентификации, аутентификации и управления доступом пользователей к информационным ресурсам предприятий

Компания является активным участником на рынке информационной безопасности с 2014 года

Более **7 лет** на рынке

Более **50 проектов** успешно реализовано

Более **10 млн** пользователей

Наши преимущества

Опыт проектирования	Используемый технологический стек, продуманные архитектурные решения и накопленный опыт успешных внедрений обеспечивают любую требуемую производительность, быстродействие и отказоустойчивость
Сертифицированные продукты	Все продукты и решения компании сертифицированы по требованиям безопасности информации ФСТЭК России и внесены в Единый реестр российского ПО
Кастомизация и интеграция решений	Продукты компании поддерживают многочисленные стандарты, что позволяет интегрировать их в существующую ИТ-инфраструктуру организации. Есть возможность масштабировать и адаптировать решения с учетом требований и конкретных бизнес-задач заказчика
Качественная техническая поддержка	Команда высококвалифицированных разработчиков постоянно совершенствует программное обеспечение, что позволяет выработать оптимальное решение для каждой компании

Клиенты

Государственное казенное учреждение города Москвы Информационный город

Банк России

ДОМ РФ

ЦЕНТР КОРПОРАТИВНЫХ РЕШЕНИЙ

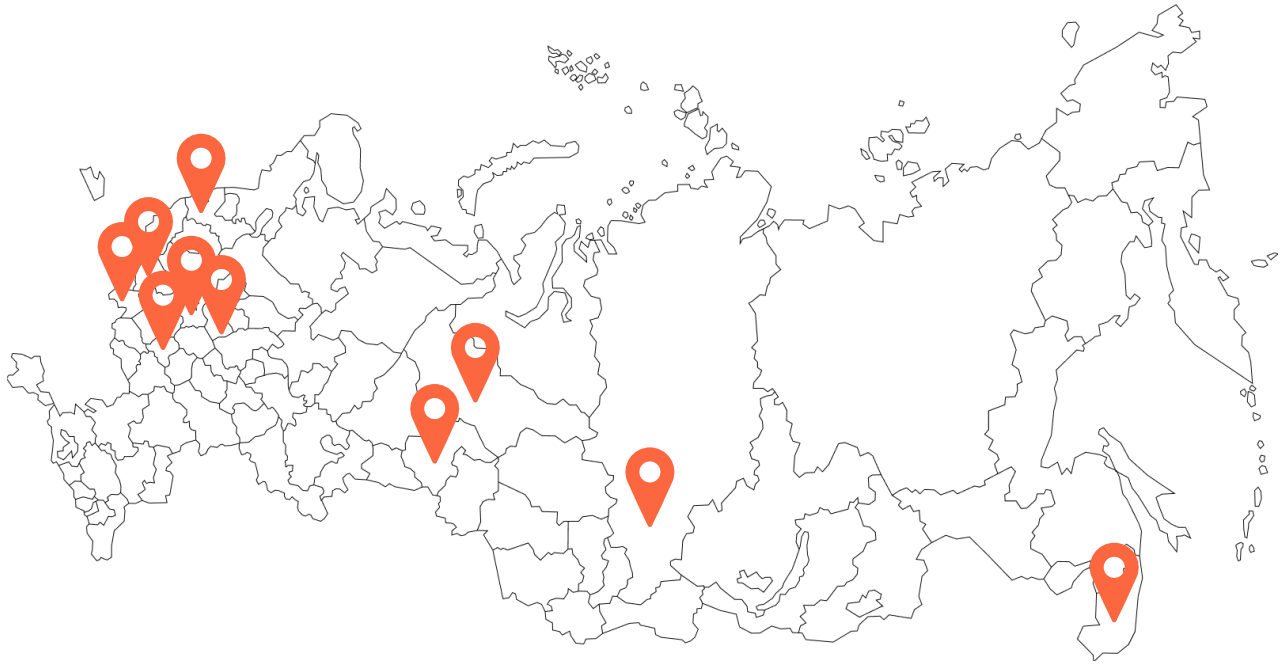
НЛМК

интерфакс

Рыбаков фонд

Альфа Капитал

ИНГОССТРАХ



Ханты-Мансийский Негосударственный Пенсионный Фонд

ИНГОССТРАХ инвестиции

РЕГИОН ГРУППА КОМПАНИЙ

Ренессанс. ЖИЗНЬ

ПримСоцБанк

СБЕР НПФ

БЛАГОСОСТОЯНИЕ НЕГОСУДАРСТВЕННЫЙ ПЕНСИОННЫЙ ФОНД

открытие Пенсионный фонд

АЛЬФА СТРАХОВАНИЕ

Запсибкомбанк

Руководство компании

Михаил Ванин

Генеральный директор

В период с 2011 по 2015 руководил разработкой Единой системы идентификации и аутентификации (ЕСИА)

Преподаватель в МГТУ им. Н.Э. Баумана на кафедре «Информационная безопасность»

mvanin@reaxoft.ru

Кирилл Гаврилов

Директор по развитию

Ответственный за развитие продуктов компании и маркетинговую стратегию

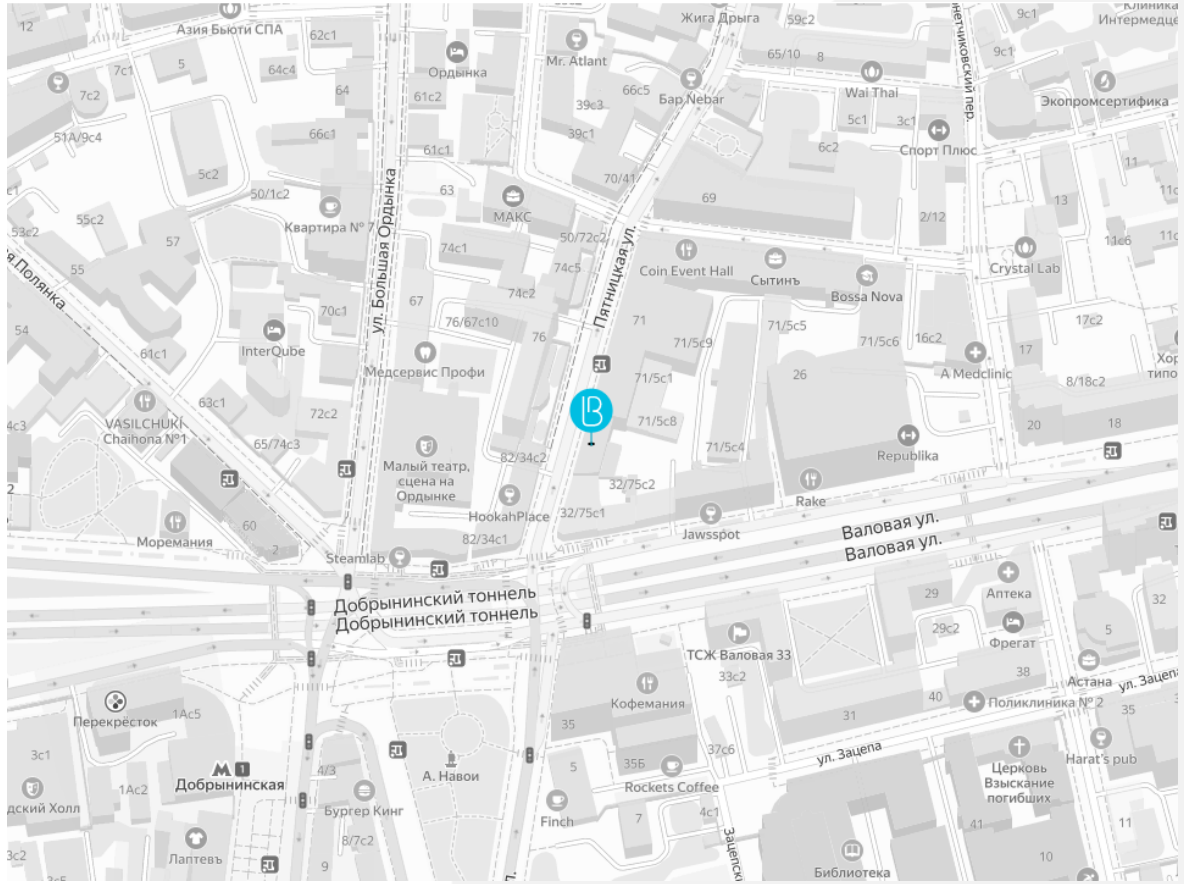
Кандидат социологических наук, доцент НИУ «Высшая школа экономики»

kgavrilov@reaxoft.ru

Контакты

115054, Москва, Пятницкая улица, дом 73

+7 (499) 322-14-04

info@reaxoft.ru

identityblitz.ru