



# BLITZ IDENTITY PROVIDER

Сервер аутентификации и управления доступом

ООО «PEAK СОФТ»

 [identityblitz.ru](https://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



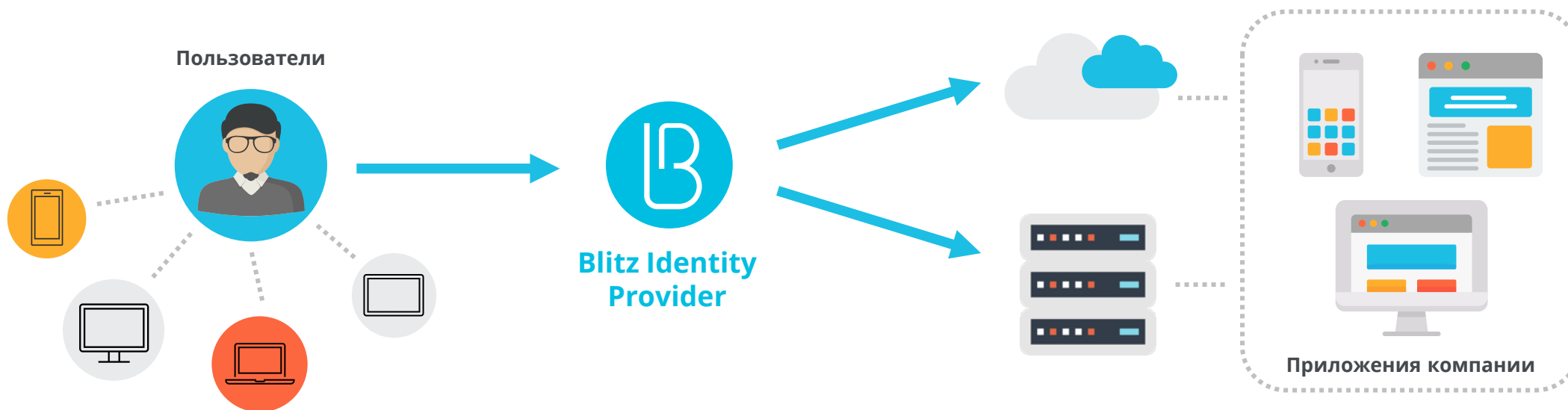
При удаленной работе сотрудников повышается риск взлома учетных записей



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)



подходит для веб-сайтов, мобильных приложений и смарт-устройств



мультифакторная аутентификация (MFA)



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



поддержка входа через социальные сети, банки и госуслуги (ЕСИА)



доступ к инфраструктурным сервисам (SSH, RDP, VPN)



подходит для разных пользователей: сотрудников, клиентов, контрагентов



протоколирование событий безопасности и подотчетность действий пользователей

# ЕДИННЫЙ ВХОД (SINGLE SIGN-ON)

Позволяет пользователю однократно войти в собственную 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 и пароль, встроенная защита от подбора



Генераторы разовых кодов HOTP и TOTP



Смарт-карта, USB-ключ с электронной подписью, ключи безопасности FIDO2 и U2F



Passkey и WebAuthn, биометрическая аутентификация по Face ID и Touch ID



Push-аутентификация, вход по QR-коду



SMS и email коды подтверждения, Flash Call



Внешние поставщики идентификации (социальные сети, банки, ЕСИА)



Собственные методы входа

# УНИВЕРСАЛЬНОСТЬ

Возможность учитывать потребности разных групп пользователей для безопасного и эффективного управления идентификацией, аутентификацией и доступом

Сотрудник



безопасный и удобный доступ к корпоративным ресурсам с помощью Single Sign-On (SSO), многофакторной аутентификации (MFA) и политик контроля доступа

Клиент



вход через аккаунт социальной сети, банков, ЕСИА или регистрация через экранную форму на сайте могут быть использованы для улучшения клиентского опыта

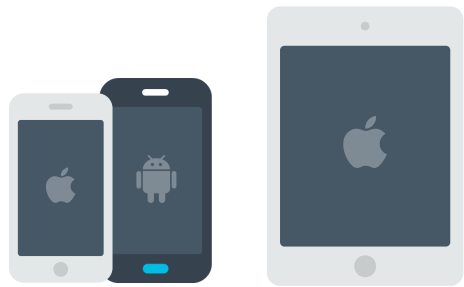
Контрагент



делегирование управления доступом для внешних партнеров и контрагентов без нарушения внутренних политик безопасности компании

# ПОДДЕРЖКА УСТРОЙСТВ ДОСТУПА

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



Смартфоны и планшеты



Персональные компьютеры



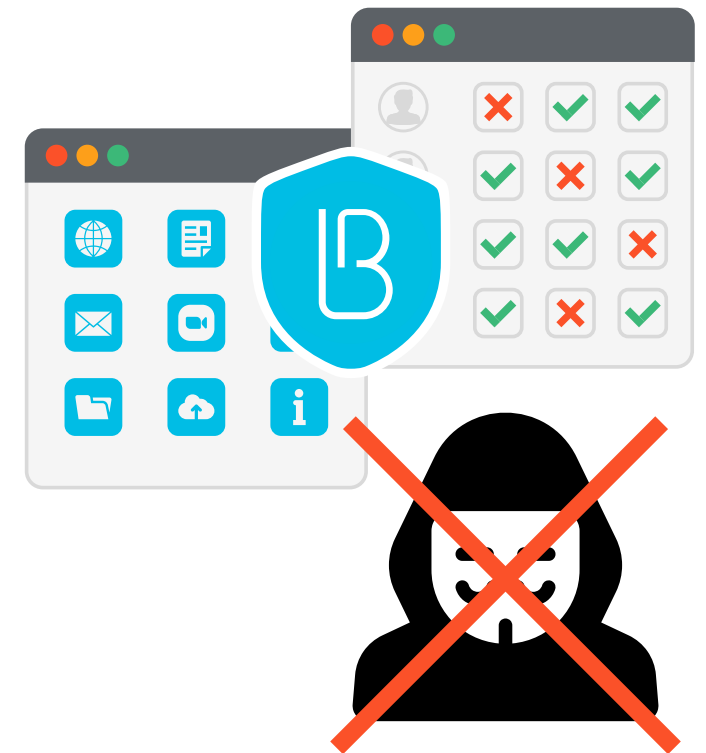
Смарт-устройства



# ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ И СЕРВИСОВ

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

- ✓ Использование API Security Gateway 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
- ✓ поддерживает большинство популярных отечественных ОС и СУБД



## Простота и гибкость настройки

- ✓ встраивается в ИТ-инфраструктуру
- ✓ администрируется через веб-интерфейс



## Множество методов аутентификации

- ✓ более 20 современных способов аутентификации
- ✓ вход по квалифицированной электронной подписи (УКЭП)
- ✓ возможность беспарольной аутентификации



## Поддержка внешних систем идентификации

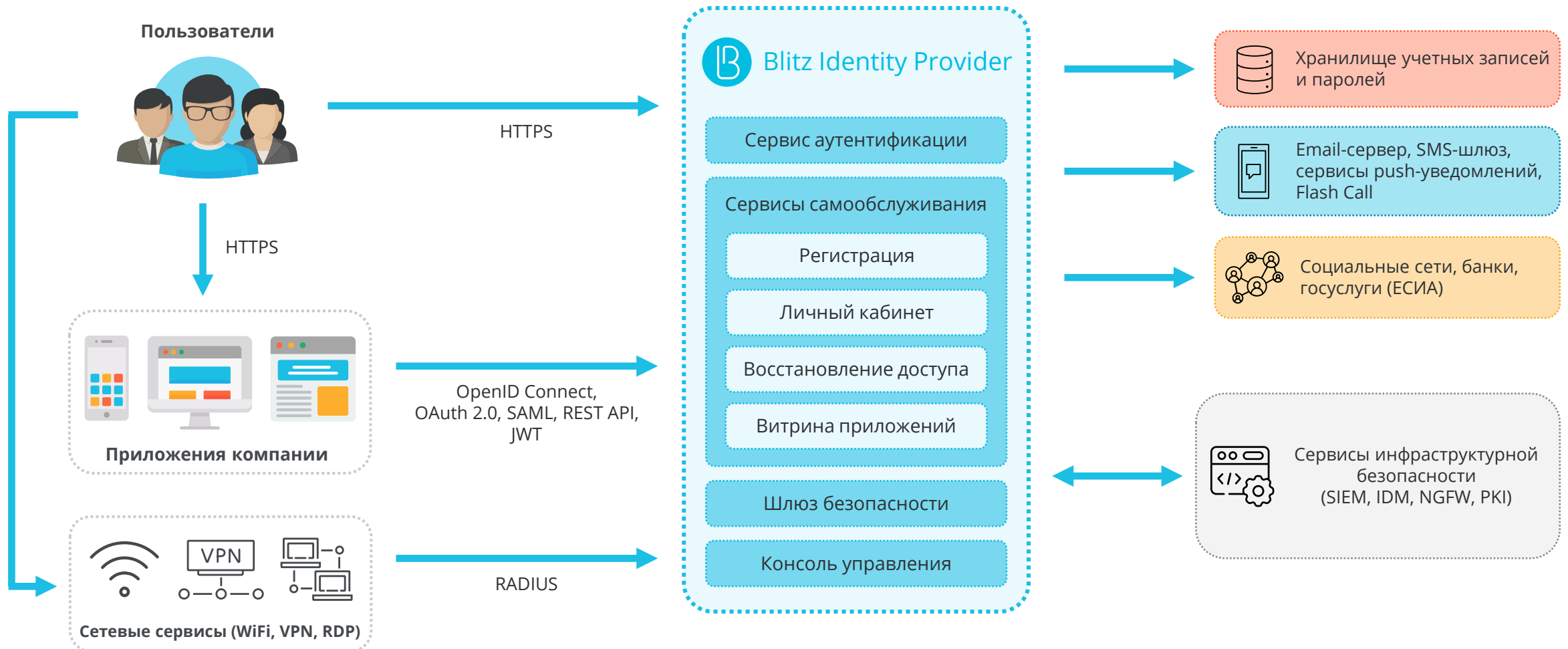
- ✓ популярные в России социальные сети
- ✓ доверенная аутентификация через учетные записи банков и госуслуги (ЕСИА)

# ЛИЦЕНЗИИ И СЕРТИФИКАТЫ

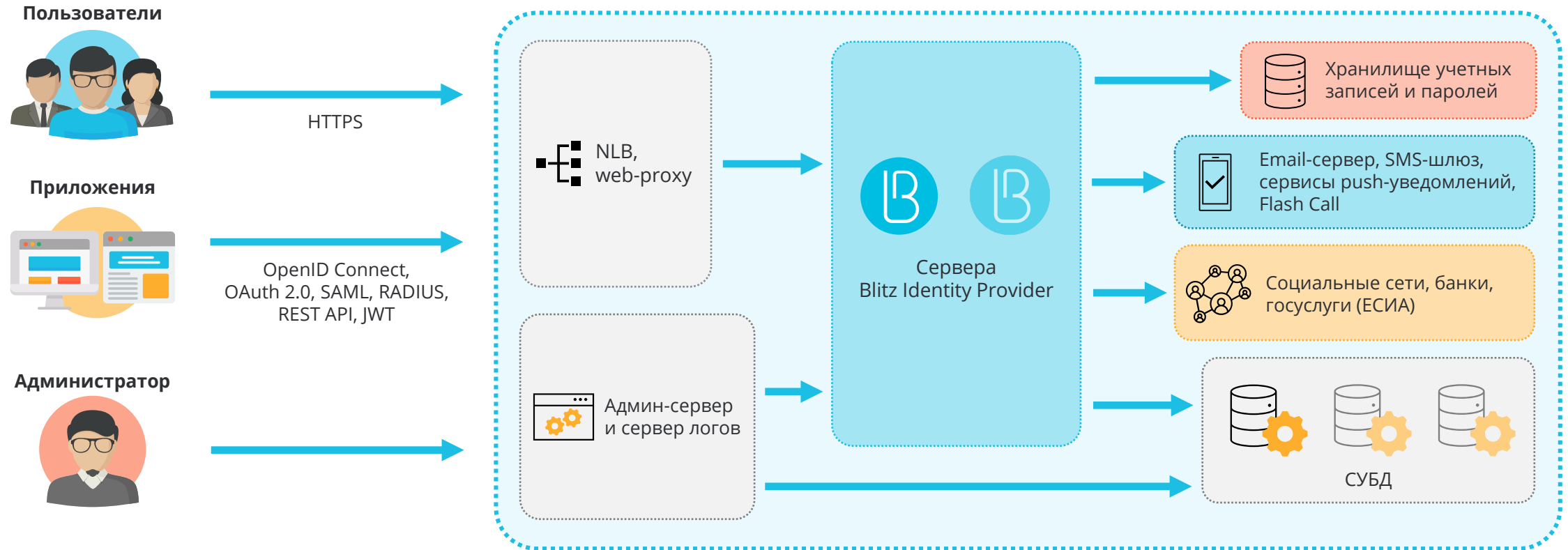
Blitz Identity Provider зарегистрирован в Едином реестре российского ПО (№842) и сертифицирован ФСТЭК России (№4525 от 10.03.2022), что подтверждает соответствие требованиям информационной безопасности и допускает применение продукта в государственных информационных системах



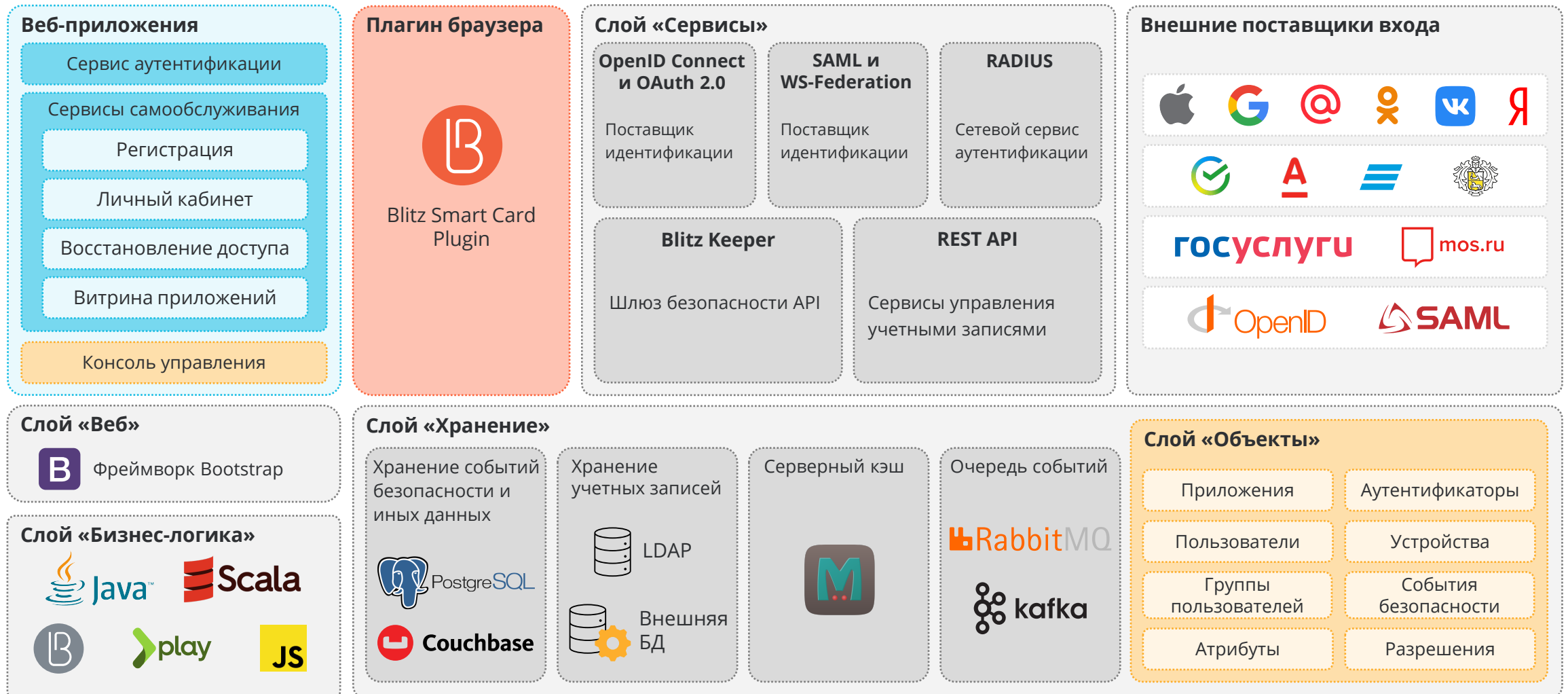
# СХЕМА РАБОТЫ



# ТИПОВАЯ СХЕМА РАЗВЕРТЫВАНИЯ



# КАК УСТРОЕН BLITZ IDENTITY PROVIDER



# ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

## Предоставляемые способы идентификации и аутентификации

1. Логин и пароль, встроенная защита от подбора
2. Смарт-карта, USB-ключ с электронной подписью, FIDO2 и U2F токены, WebAuthn, Passkey
3. Аппаратные брелоки (HOTP, TOTP, OCRA)
4. Программные TOTP-брелоки (Google Authenticator, Яндекс.Ключ и другие)
5. SMS и email коды подтверждения, push-аутентификация, вход по QR-коду, Flash Call

## Поддержка внешних систем идентификации

1. Вход через социальные сети (Яндекс ID, VK ID, Одноклассники, Mail ID, Google ID, Apple ID)
2. Вход через госуслуги (ЕСИА), Mos ID, банки
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

## Способы подключения приложений

1. OpenID Connect, OAuth 2.0, SAML, WS-Federation, RADIUS
2. Веб-прокси с пробросом логина и пароля в форму входа веб-приложения

## Подключение к внешним хранилищам учетных записей и паролей

1. FreeIPA, MS Active Directory
2. LDAP-совместимый сервер
3. Произвольное хранилище (через коннектор)

## Сервисы самообслуживания пользователей

1. Регистрация пользователя
2. Личный кабинет
3. Восстановление доступа
4. Витрина приложений
5. Настройка двухфакторной аутентификации
6. Просмотр событий безопасности и списка используемых устройств доступа

## Прочее

1. Высокая производительность при развертывании на скромных аппаратных ресурсах
2. Высокая надежность при развертывании в кластере
3. Сервис для мониторинга Prometheus



# ПРЕИМУЩЕСТВА ВНЕДРЕНИЯ SSO



## Для сотрудников

- ✓ Упрощение доступа к информационным ресурсам
- ✓ Ускорение процедуры получения доступов
- ✓ Исключение «парольного хаоса»



## Для IT-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 В ПОРТФОЛИО



Департамент информационных технологий города Москвы

Blitz Identity Provider  
Blitz Smart Card Plugin

15 млн пользователей  
100 тыс. сотрудников

**ИНГОССТРАХ**

СПАО «Ингосстрах»

Blitz Identity Provider  
ESIA-Bridge

3 млн клиентов  
4 тыс. сотрудников  
20 тыс. агентов



Группа НЛМК

Blitz Identity Provider

30 тыс. сотрудников  
50 тыс. рабочих  
60 компаний холдинга



Банк России

Центральный Банк России

Blitz Identity Provider

50 тыс. сотрудников

# СИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ (СУДИР)



## ЗАДАЧА:

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

## РЕЗУЛЬТАТЫ:

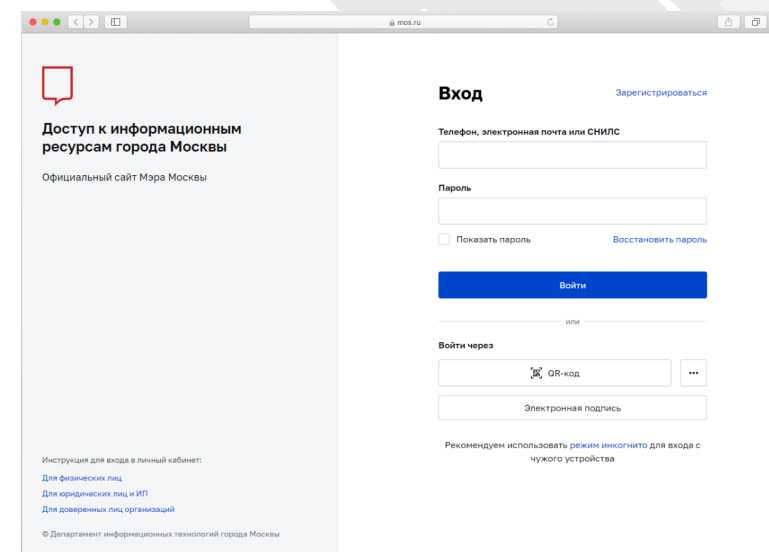
- ✓ Унифицирована программная платформа – множество программных продуктов, решающих задачу идентификации/аутентификации пользователей, замещены единым решением
- ✓ Повышена производительность и надежность работы СУДИР, увеличен запас производительности при сокращении аппаратных ресурсов
- ✓ Упрощено 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



15 млн пользователей  
100 тыс. сотрудников  
органов власти



# СИСТЕМА АУТЕНТИФИКАЦИИ СПАО «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

## ИНГОССТРАХ



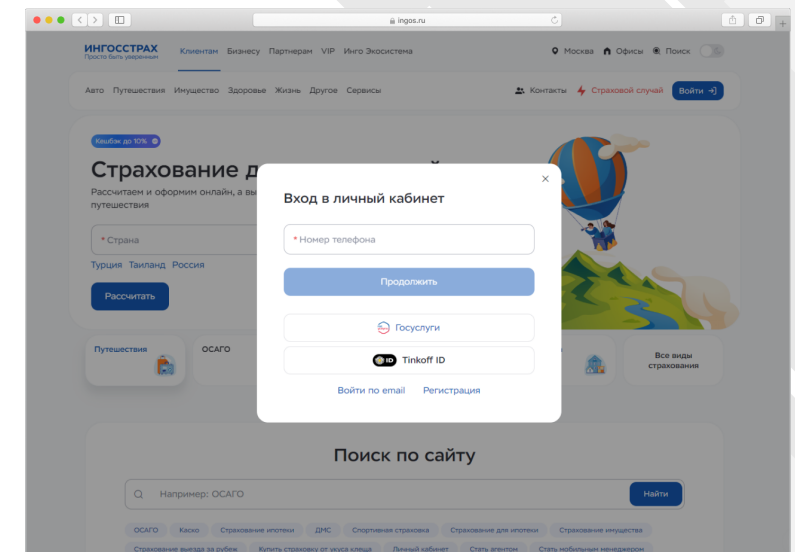
6 месяцев



3 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



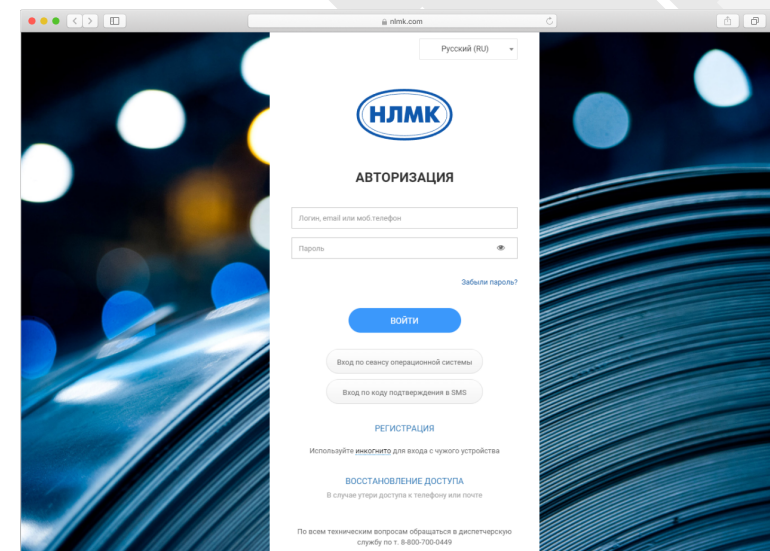
3 месяца



30 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

## РЕЗУЛЬТАТЫ:

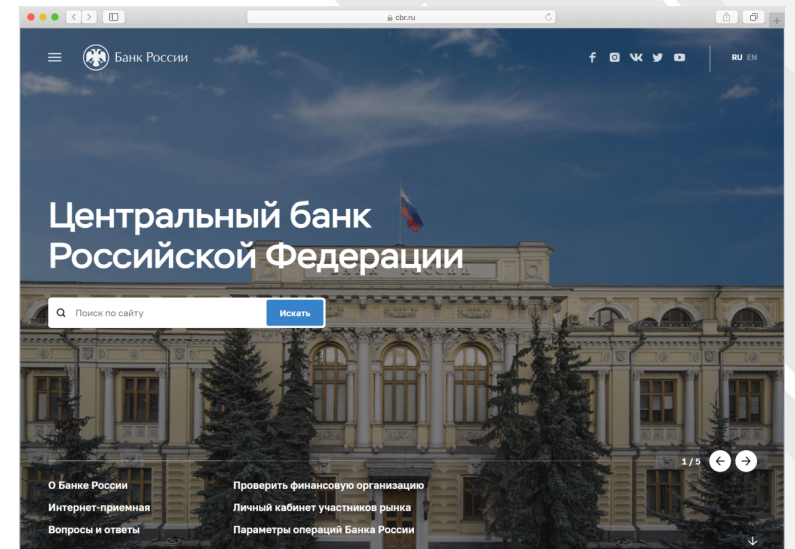
- ✓ Обеспечена сквозная доменная аутентификация сотрудников при доступе в приложения (AD, Kerberos)
- ✓ Реализована технология Web Single Sign-On
- ✓ Обеспечена простая интеграция – используются стандартные возможности подключения приложений (OpenID Connect, SAML, web-proxy)
- ✓ Реализована аутентификация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



3 месяца



50 тыс. сотрудников



# О КОМПАНИИ

**IDENTITY BLITZ** – российский разработчик программного обеспечения. Специализируется в решении задач управления идентификацией, аутентификацией и контролем доступа пользователей к информационным ресурсам



Компания является активным участником на рынке информационной безопасности с 2014 года. Деятельность компании лицензирована ФСТЭК

БОЛЕЕ **10 лет**  
НА РЫНКЕ

БОЛЕЕ **50 проектов**  
УСПЕШНО РЕАЛИЗОВАНО

БОЛЕЕ **100 млн**  
ПОЛЬЗОВАТЕЛЕЙ

# НАШИ ПРЕИМУЩЕСТВА

## ЭКСПЕРТИЗА В IAM

Команда высококвалифицированных специалистов готова оказать помощь партнерам и клиентам на всех этапах: от предпродажной подготовки и проектирования архитектуры до внедрения и техподдержки

## ГИБКОЕ ЦЕНООБРАЗОВАНИЕ

Клиенты платят только за услуги, которые им необходимы. Выберите тип лицензии, который наилучшим образом соответствует потребностям вашего бизнеса

## РАСШИРЕННАЯ КАСТОМИЗАЦИЯ

Все услуги и функции доступны "из коробки". Настройка не требует программирования, нет необходимости нанимать разработчиков для адаптации программного обеспечения к среде клиента

## ОРИЕНТАЦИЯ НА КЛИЕНТА

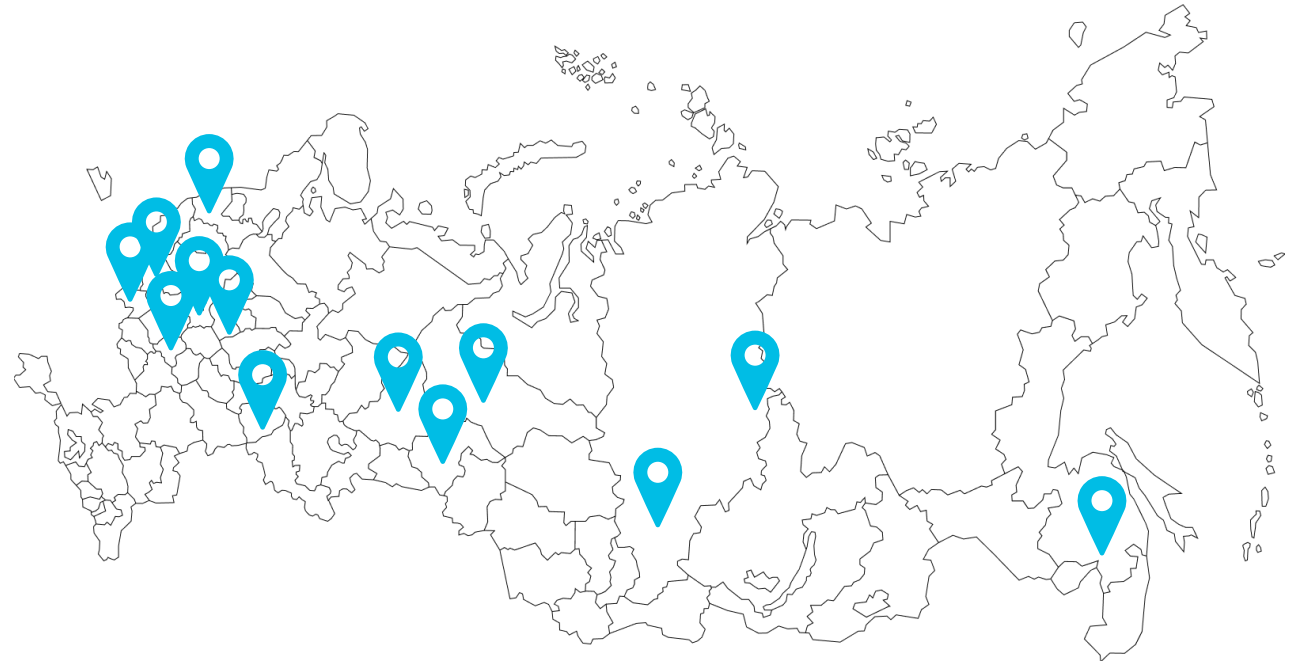
Наше программное обеспечение может быть быстро адаптировано для удовлетворения конкретных запросов и требований клиентов

## ИСКЛЮЧИТЕЛЬНАЯ ЭФФЕКТИВНОСТЬ

Достигните высокой производительности при минимальных системных требованиях. Наше решение легко масштабировать и объединять в кластеры



# КЛИЕНТЫ



# РУКОВОДСТВО КОМПАНИИ

## Михаил Ванин

Генеральный директор

Ответственный за управление компанией и ключевые решения, обеспечивающие успешную работу и развитие

С 2011 по 2015 год руководил разработкой ЕСИА. Преподаватель МГТУ им. Н.Э. Баумана, кафедра «Информационная безопасность»

[mvanin@idblitz.ru](mailto:mvanin@idblitz.ru)



## Кирилл Гаврилов


Исполнительный директор

Ответственный за реализацию стратегии развития компании и развитие продуктов компании

Кандидат социологических наук, доцент НИУ «Высшая школа экономики»

[kgavrilov@idblitz.ru](mailto:kgavrilov@idblitz.ru)

# КОНТАКТЫ

 115054, Москва, Пятницкая  
улица, дом 73

 +7 (499) 322-14-04

 [info@idblitz.ru](mailto:info@idblitz.ru)

 [t.me/identityblitz](https://t.me/identityblitz)

 [identityblitz.ru](http://identityblitz.ru)

