Как обеспечить безопасность: ключевые принципы выбора системы аутентификации

Михаил Ванин

Генеральный директор
Identity Blitz

identityblitz.ru

ЗАЧЕМ ВЫБИРАТЬ СИСТЕМУ АУТЕНТИФИКАЦИИ

- модернизация IT-инфраструктуры, повышение уровня безопасности, улучшение пользовательского опыта и оптимизация процессов

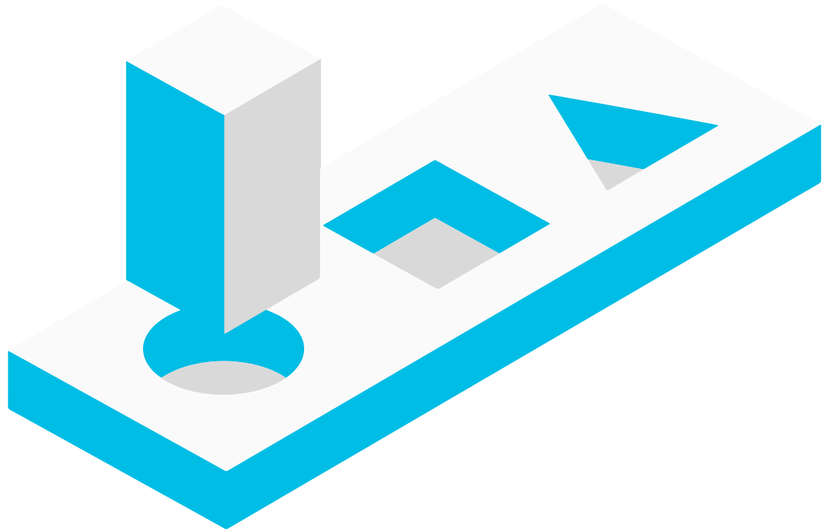
- необходимость импортозамещения, замена зарубежных решений на отечественные продукты

ИМПОРТОЗАМЕЩЕНИЕ

УНИВЕРСАЛЬНОЕ РЕШЕНИЕ?

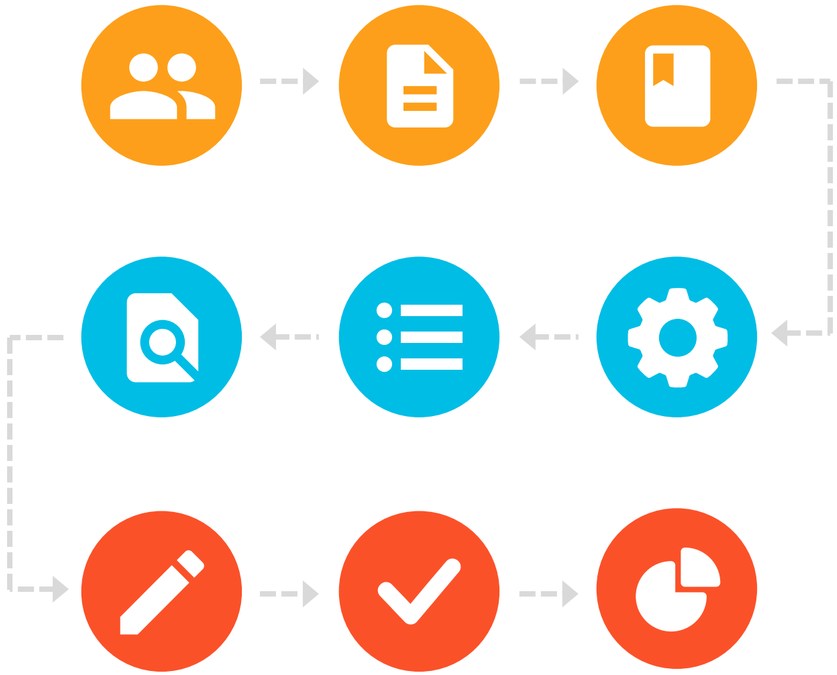
Для выбора решения нужно учитывать:

- структуру организации
- уровень рисков
- используемые приложения
- задачи
- бюджет



ШАГИ НА ПУТИ ВЫБОРА

1. Создание проектной группы
2. Разработка плана проекта
3. Поиск информации
4. Определение требований
5. Выбор решения
6. Проведение пилотного проекта
7. Оценка результатов
8. Внедрение
9. Отслеживание тенденций



СОЗДАНИЕ ПРОЕКТНОЙ ГРУППЫ

Выбор системы аутентификации лучше не осуществлять в одиночку, даже если вы, главный ответственный, являетесь самым опытным специалистом по информационной безопасности в вашей компании.

Желательно включить в проектную группу:

- представителя руководства компании
- ИТ специалиста
- ИБ специалиста
- специалиста технической поддержки
- представителя пользователей

РАЗРАБОТКА ПЛАНА ПРОЕКТА

Временные оценки реализации проекта внедрения системы аутентификации уникальны для каждой организации.

По нашему опыту примерные сроки:

- в малых и средних организациях – от 3 до 6 месяцев
- в крупных компаниях – от 6 месяцев до года

ПОИСК ИНФОРМАЦИИ

Участникам проектной группы желательно разобраться в предметной области.

SSO

IDP

IAM

CIAM

ESSO

MFA

IDM

PAM

ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ

Каких пользователей должно охватывать решение?

- всех сотрудников, определенные группы сотрудников, только администраторов
- сотрудников контрагентов (подрядчики, заказчики, партнеры)
- внешних пользователей (клиенты, абоненты, покупатели)

ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ

Какие задачи требуется решить?

- обеспечить безопасный доступ приложениям (изнутри компании, извне компании)
- унифицировать доступ к приложениям, устранить парольный хаос, упростить вход в приложения
- обеспечить управление учетными записями (регистрация, настройки безопасности, автоматизация восстановление пароля)
- обеспечить управление доступами (назначение/отзыв прав доступа)

ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ

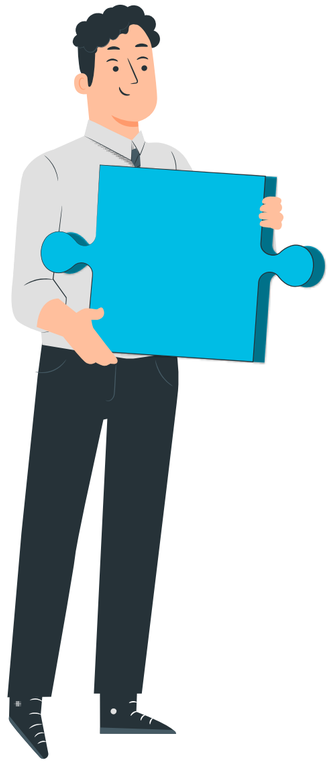
Какие приложения нужно защитить?

- бизнес-приложения (веб-приложения, мобильные приложения, десктопные)
- инфраструктурные сервисы (VPN, VDI, RDP, SSH, почта)

ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ

Какая специфика корпоративной среды?

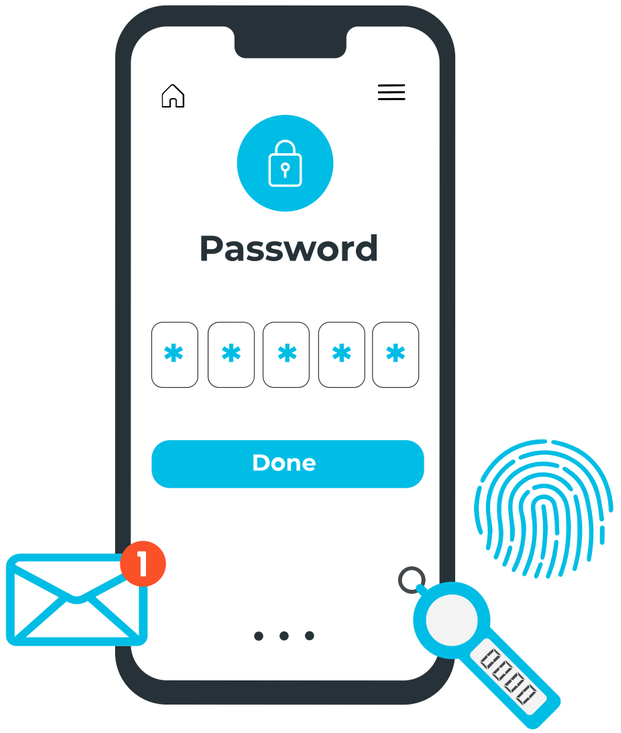
- поддерживаемые ОС, браузеры
- потребность в поддержке дополнительных языков, необходимость доступа из-за границы
- On-Premise или облако
- соответствие compliance (например, нужна ли сертификация ФСТЭК)
- требования к совместимости с существующей инфраструктурой



ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ

Какие методы аутентификации использовать?

- средства аутентификации аппаратные или только программные
- факторы аутентификации (фактор знания, фактор владения, фактор признака – биометрия)
- должен ли один из факторов проверяться по независимому каналу (Out-of-band)
- если аппаратные средства аутентификации, то какой тип – смарт-карты / токены (УКЭП или RSA), OTP брелоки, FIDO2, смартфон
- если аутентификация на основе телефона, то какая – SMS, приложение OTP, приложение push, Passkey (Face ID / Touch ID)



ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ

Какие риски допустимы?

Все методы аутентификации уязвимы — разными способами.

Желательно знать методы обхода для выбранных методов аутентификации.

ВЫБОР РЕШЕНИЯ

Требования проекта определяют, какие функции наиболее важны, а какие просто упрощают процессы, но не являются критичными для выбора системы аутентификации.

Обязательные

Желательные

Потенциально полезные

ПИЛОТНЫЙ ПРОЕКТ

ПЛАНИРОВАНИЕ

- определение границ пилота
- выделение ресурсов

РЕАЛИЗАЦИЯ

- установка и настройка

ПИЛОТИРОВАНИЕ

- испытание
- опытная эксплуатация

ОЦЕНКА

- подведение итогов
- выбор лучшего решения

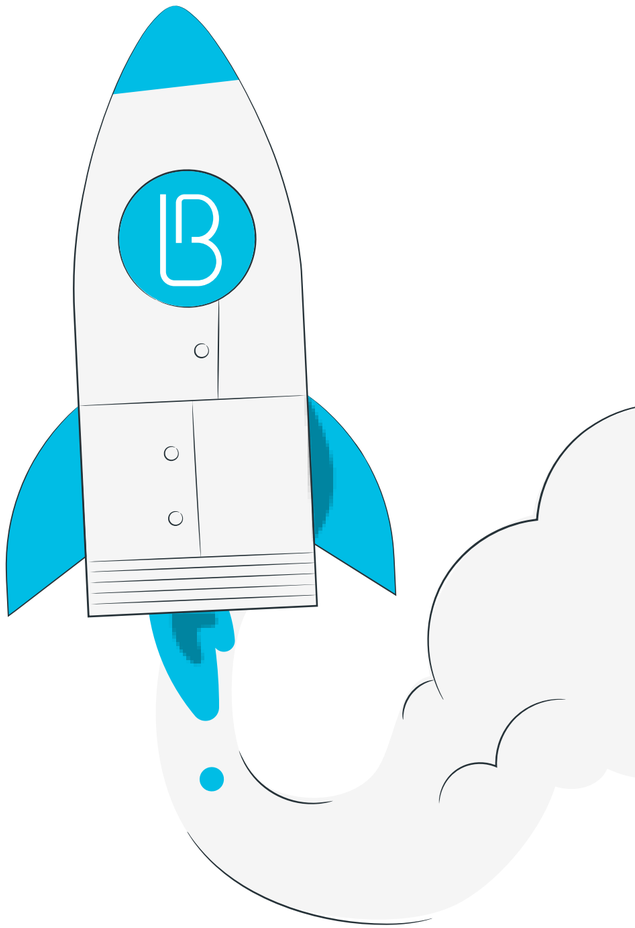
ОТЗЫВ

- предоставление обратной связи вендорам

ЧТО ДАЛЬШЕ?

Проведите внедрение выбранного решения.

Продолжайте следить за новыми тенденциями в области решений по аутентификации. Продукты постоянно совершенствуются, улучшается существующий функционал и добавляется новый.



BLITZ IDENTITY PROVIDER

01

УНИВЕРСАЛЬНОСТЬ

Объединяет функционал IAM, CIAM, SSO, MFA решений

02

ГИБКОСТЬ

Широкий функционал «из коробки», настройка не требует программирования

03

БЕЗОПАСНОСТЬ

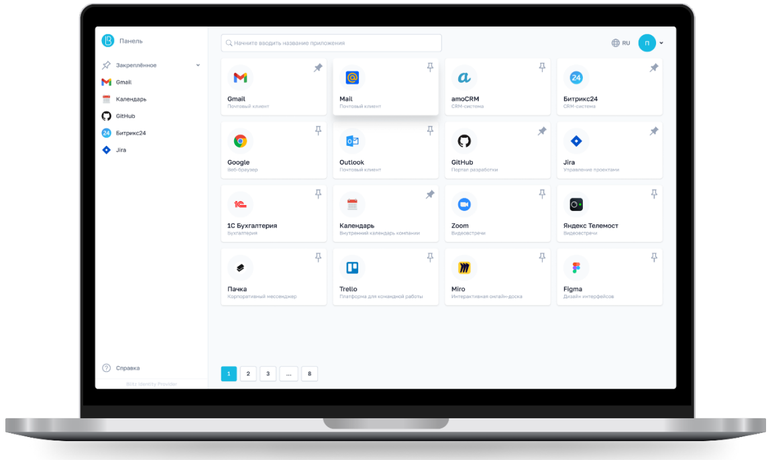
Встроенная защита от брутфорс-атак, фишинга, кражи учетных записей

04

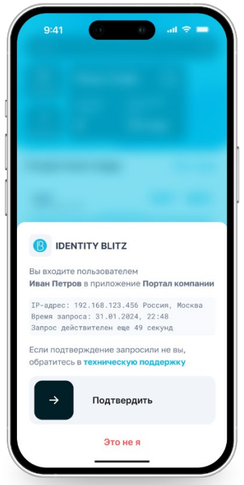
СООТВЕТСТВИЕ СТАНДАРТАМ

OIDC, OAuth 2, SAML, WS-Fed, RADIUS, LDAP, REST API, JWT, WebAuthn

ОБЛАСТИ ПРИМЕНЕНИЯ

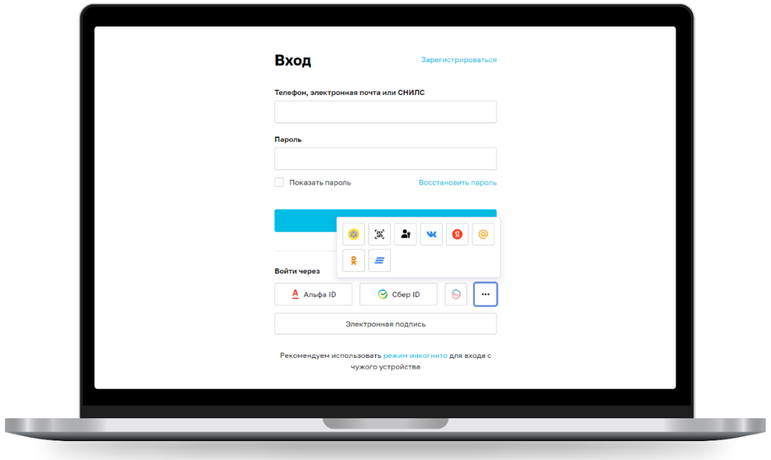


Единый вход
в приложения



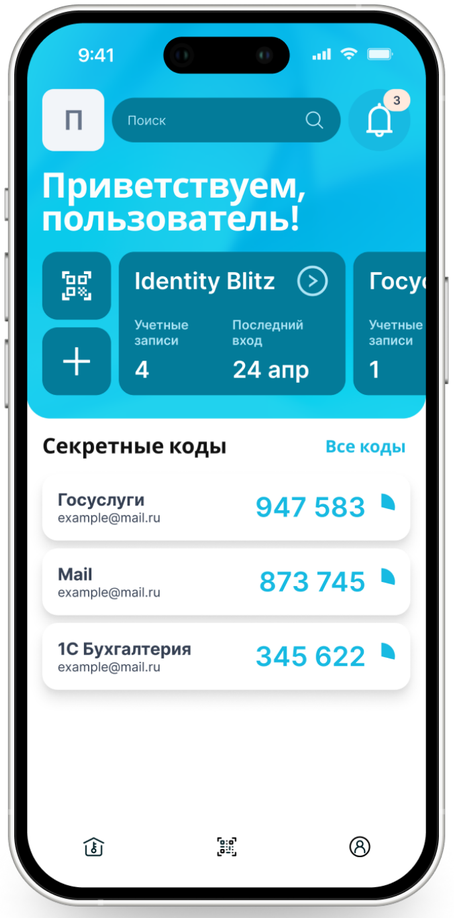
Многофакторная
аутентификация

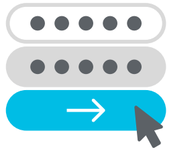
Беспарольная
аутентификация



Подключение к внешним
провайдерам идентификации

МЕТОДЫ АУТЕНТИФИКАЦИИ





Логин
и пароль

SMS,
email

Flash Call

Passkey,
FIDO2

Push,
QR-код

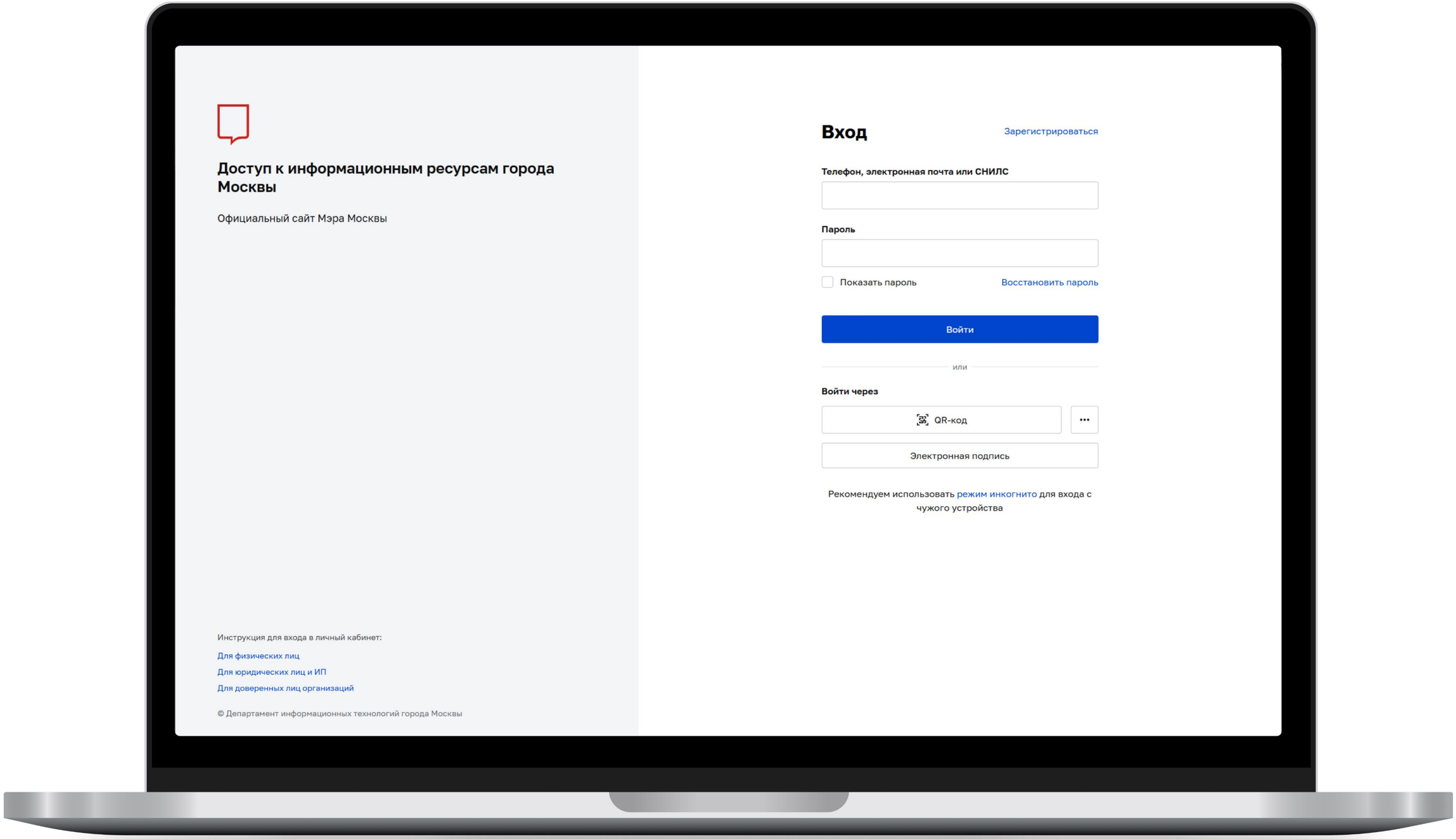
Смарт-карта,
USB-токен

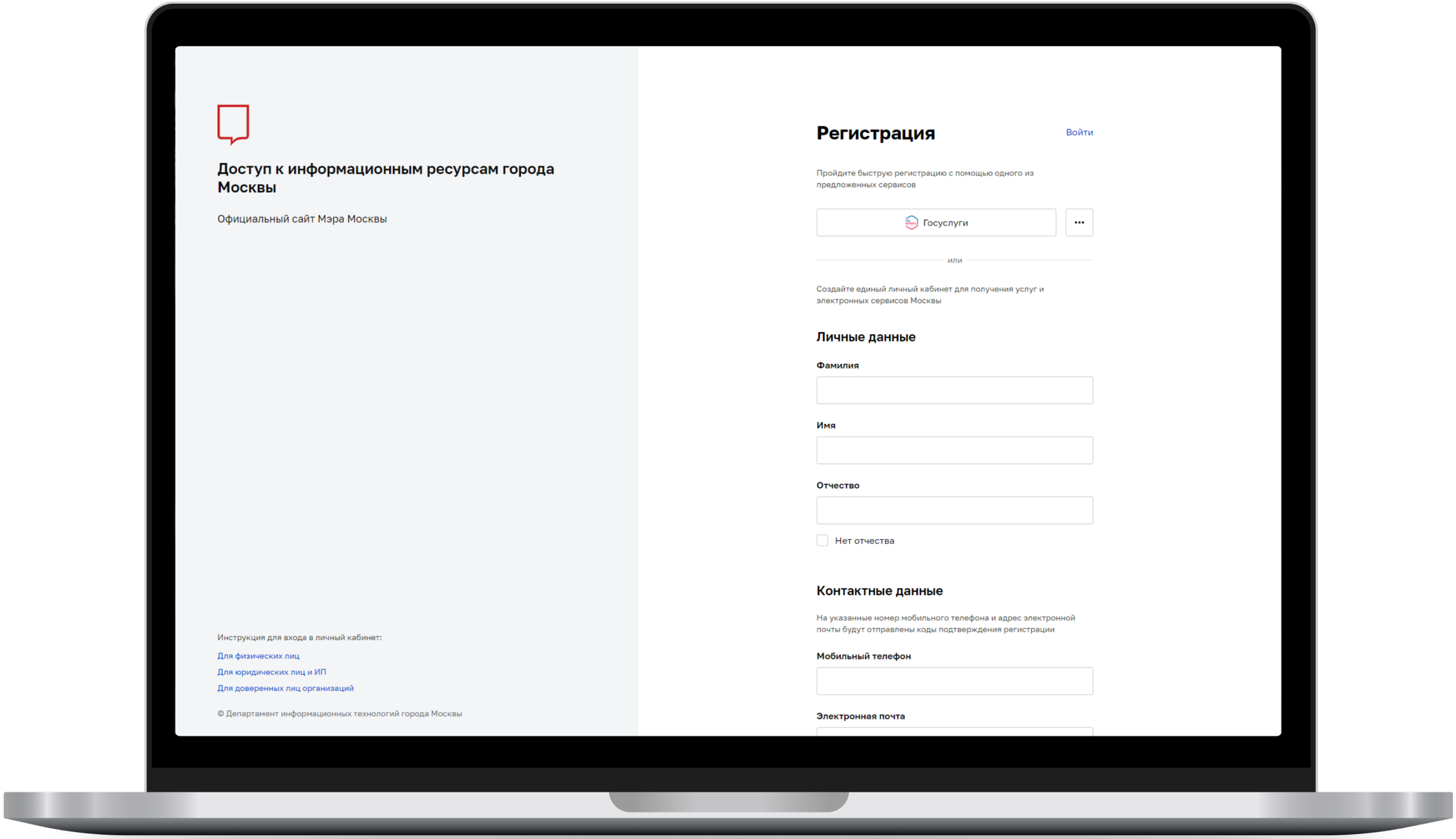
Генераторы
кодов

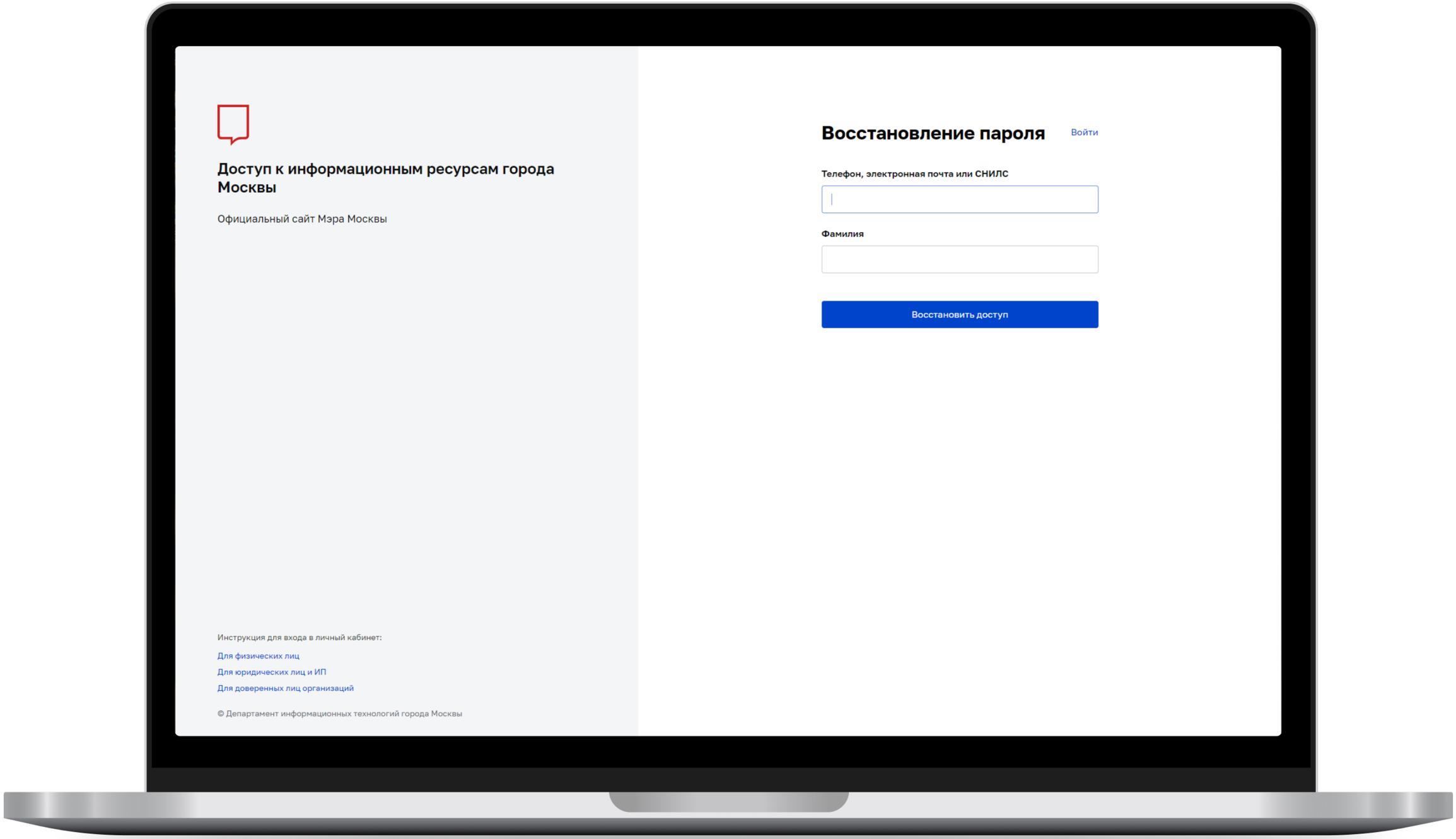
Внешние
поставщики

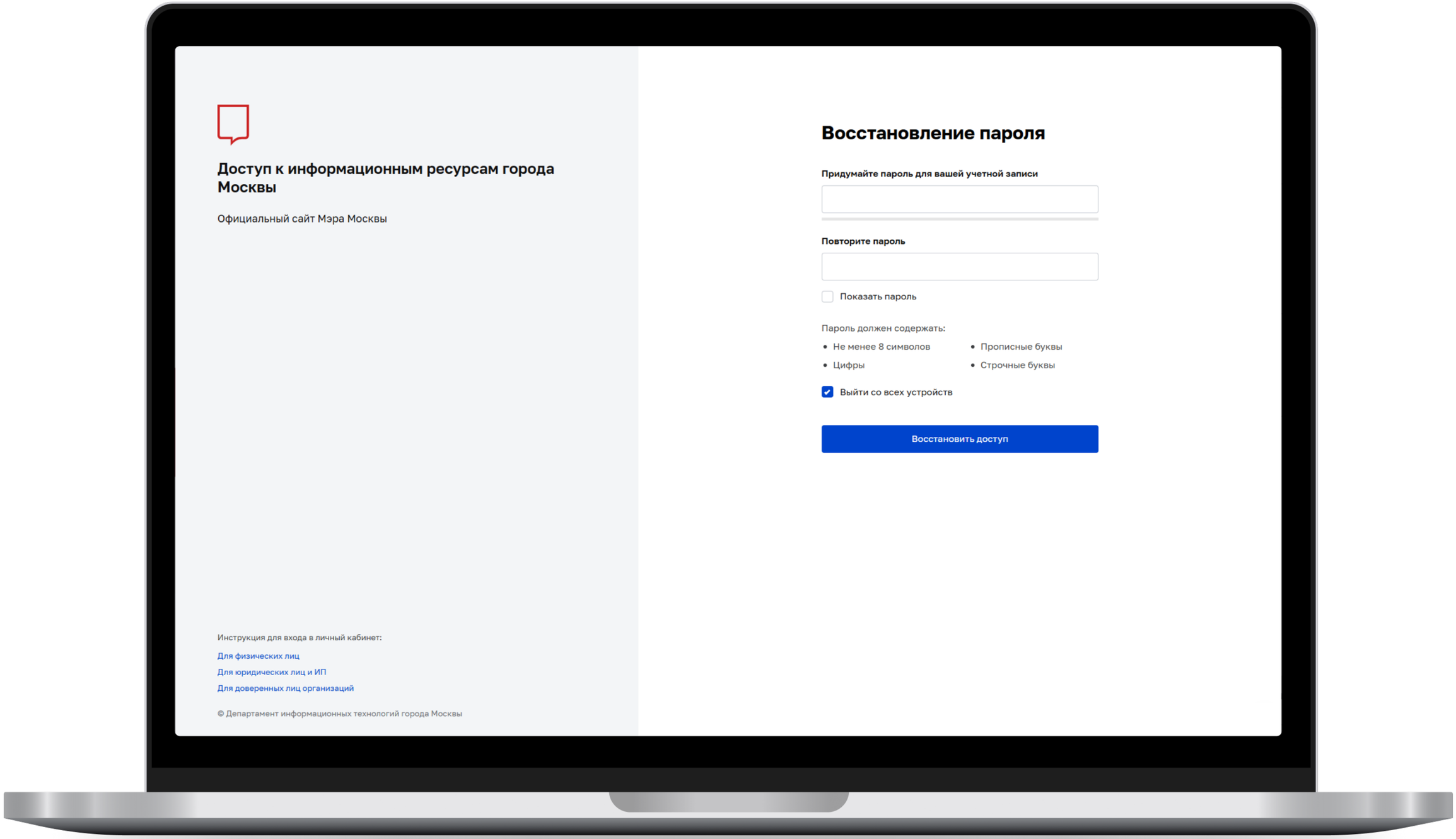
Интеграции
со сторонними MFA

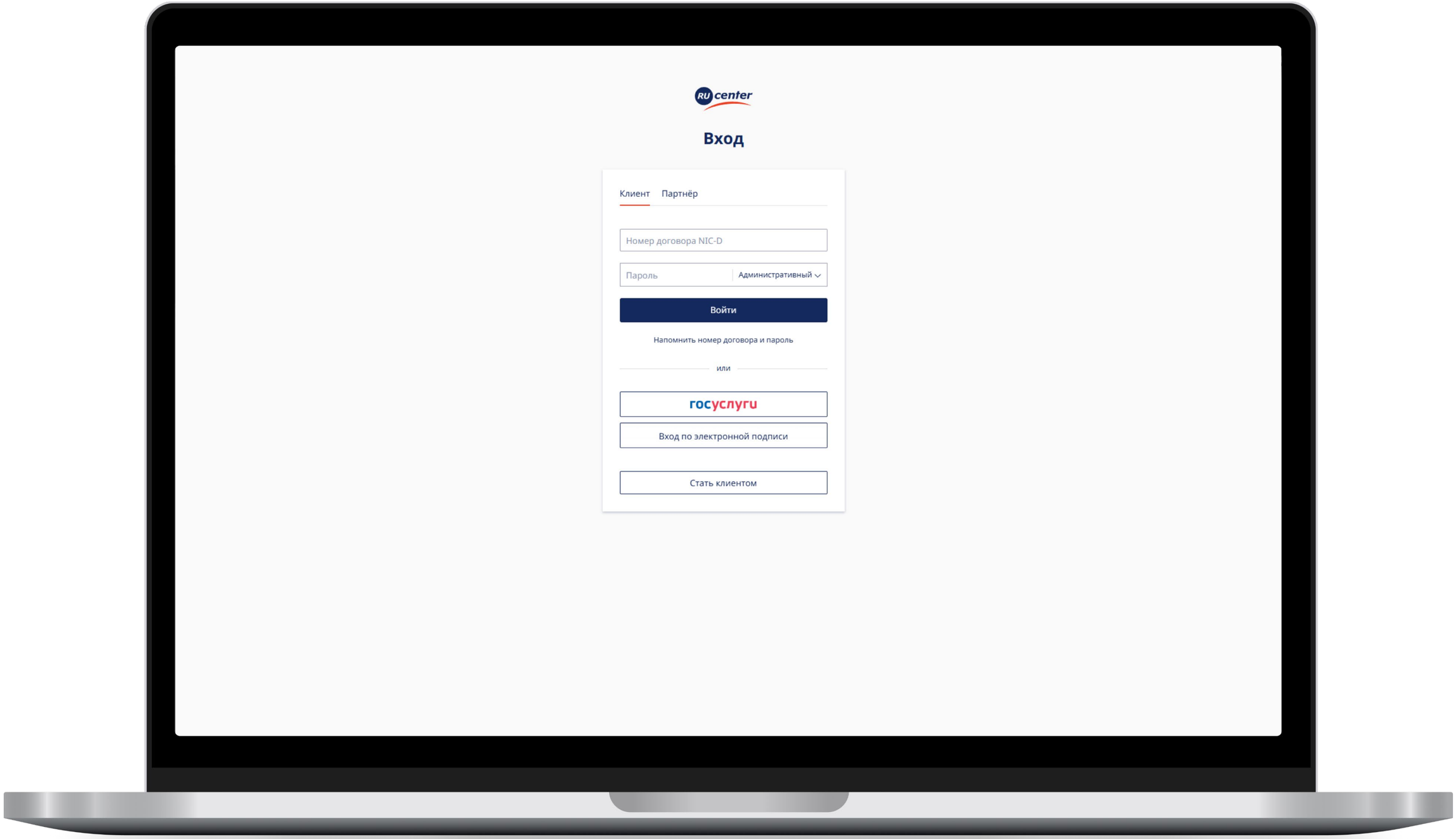
ДЕМОНСТРАЦИЯ ПРОДУКТА

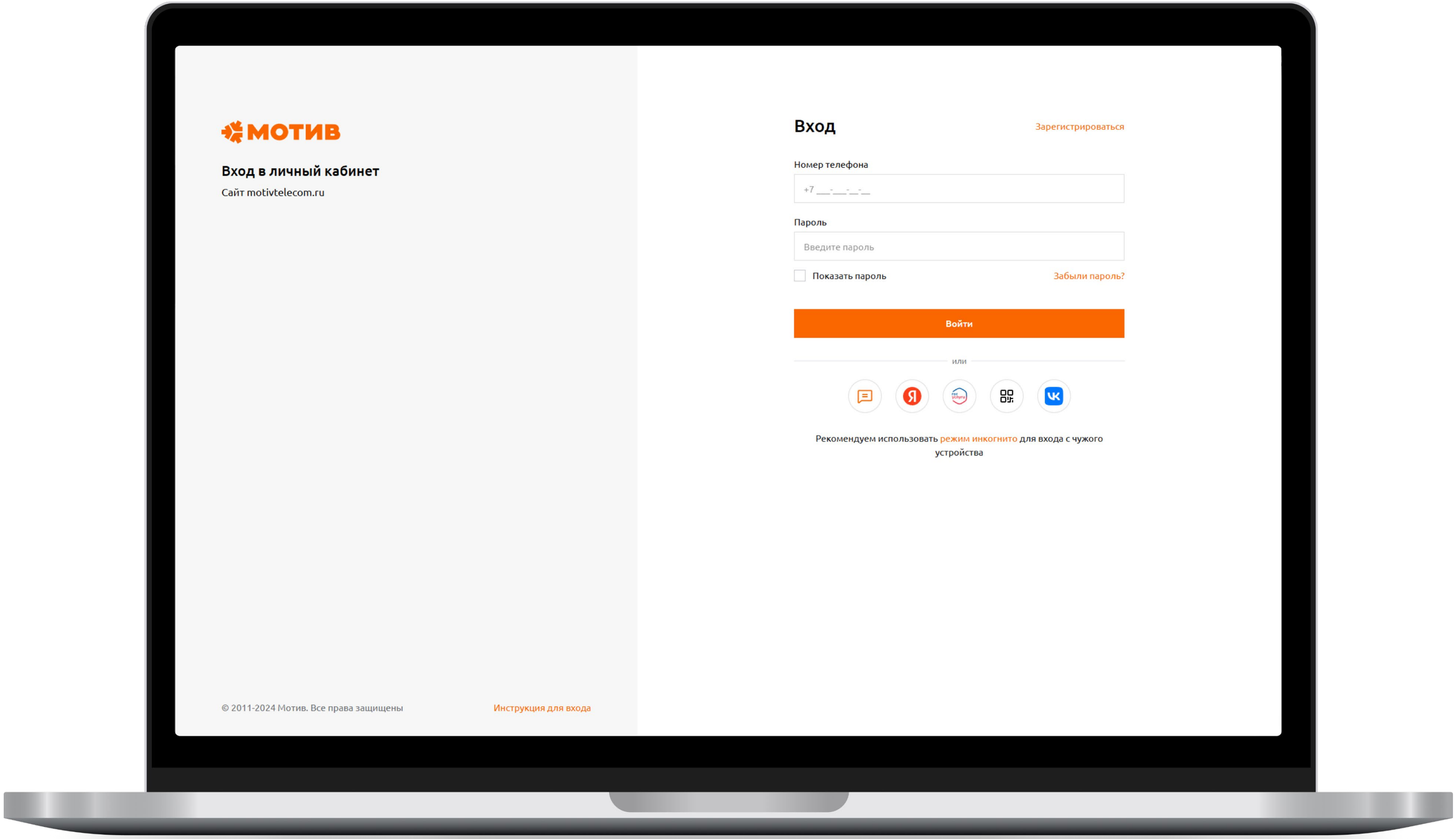

Доступ к информационным ресурсам города Москвы
Официальный сайт Мэра Москвы
Инструкция для входа в личный кабинет:
Для физических лиц
Для юридических лиц и ИП
Для доверенных лиц организаций
© Департамент информационных технологий города Москвы
Вход
Зарегистрироваться
Телефон, электронная почта или СНИЛС
Пароль
Показать пароль
Восстановить пароль
Войти
или
Войти через
QR-код
Электронная подпись
Рекомендуем использовать режим инкогнито для входа с чужого устройства

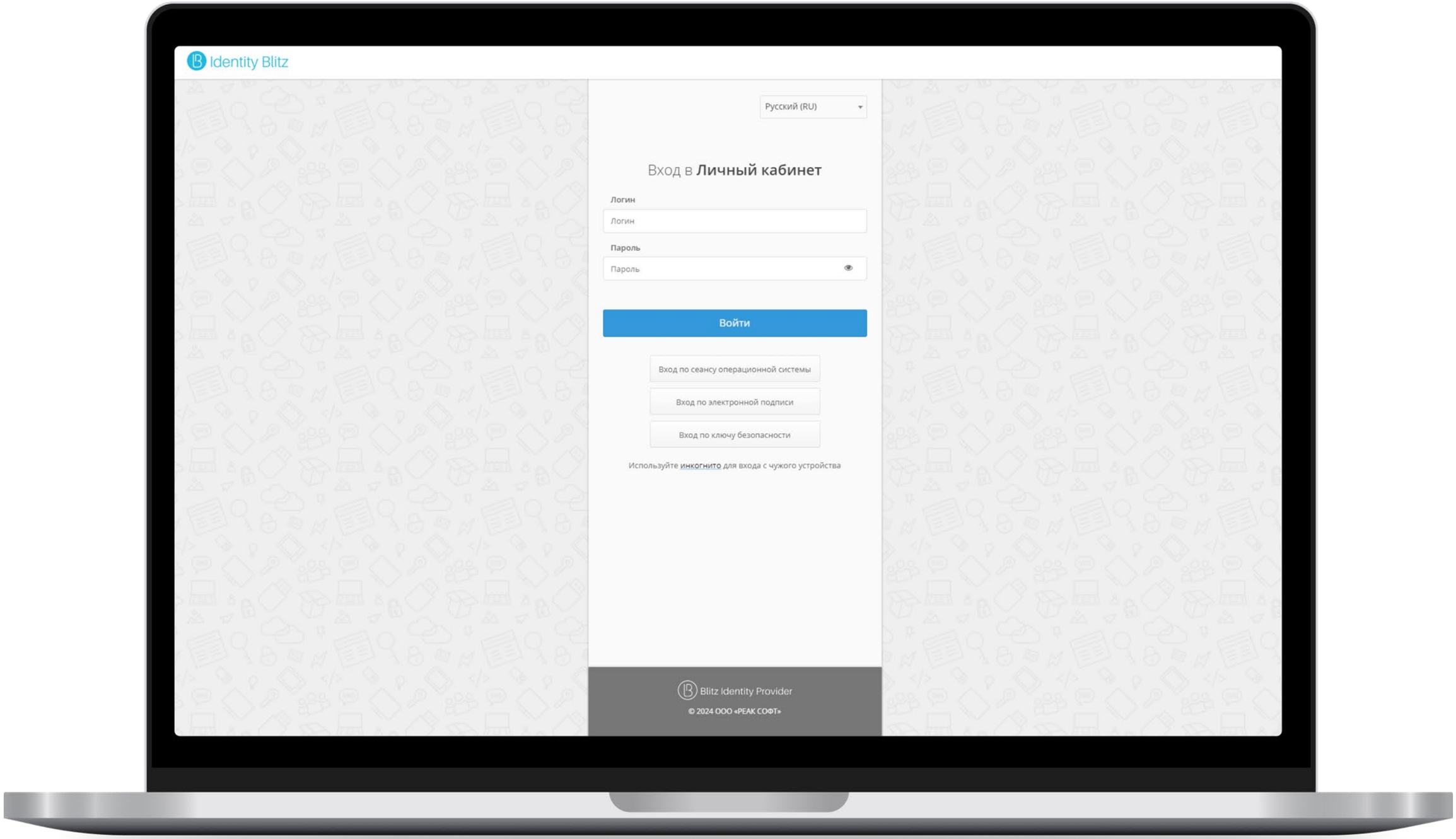

Доступ к информационным ресурсам города Москвы
Официальный сайт Мэра Москвы
Инструкция для входа в личный кабинет:
Для физических лиц
Для юридических лиц и ИП
Для доверенных лиц организаций
© Департамент информационных технологий города Москвы
Регистрация
Войти
Пройдите быструю регистрацию с помощью одного из предложенных сервисов
Госуслуги
или
Создайте единый личный кабинет для получения услуг и электронных сервисов Москвы
Личные данные
Фамилия
Имя
Отчество
Нет отчества
Контактные данные
На указанные номер мобильного телефона и адрес электронной почты будут отправлены коды подтверждения регистрации
Мобильный телефон
Электронная почта

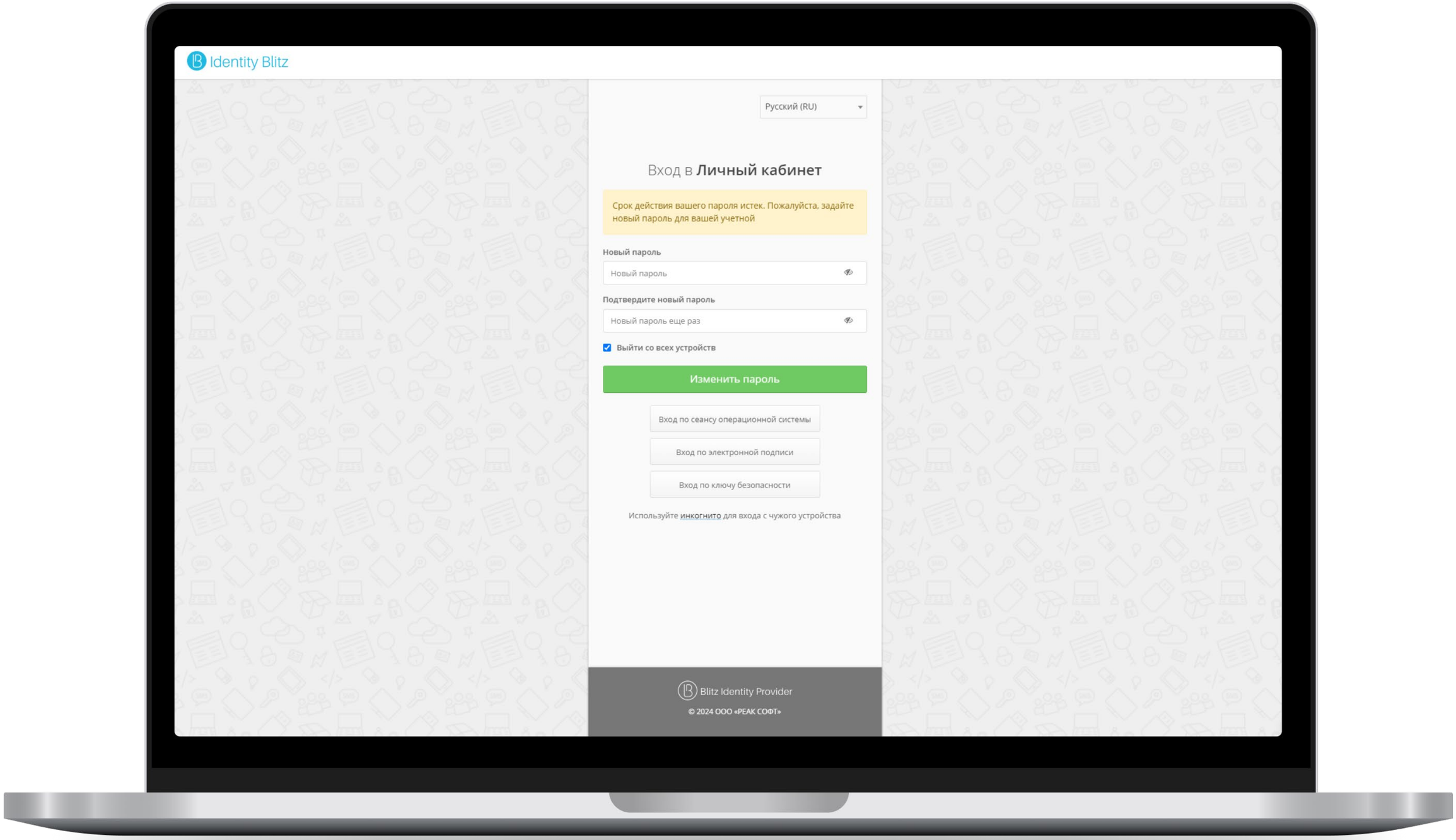

Доступ к информационным ресурсам города Москвы
Официальный сайт Мэра Москвы
Инструкция для входа в личный кабинет:
Для физических лиц
Для юридических лиц и ИП
Для доверенных лиц организаций
© Департамент информационных технологий города Москвы
Восстановление пароля
Войти
Телефон, электронная почта или СНИЛС
Фамилия
Восстановить доступ

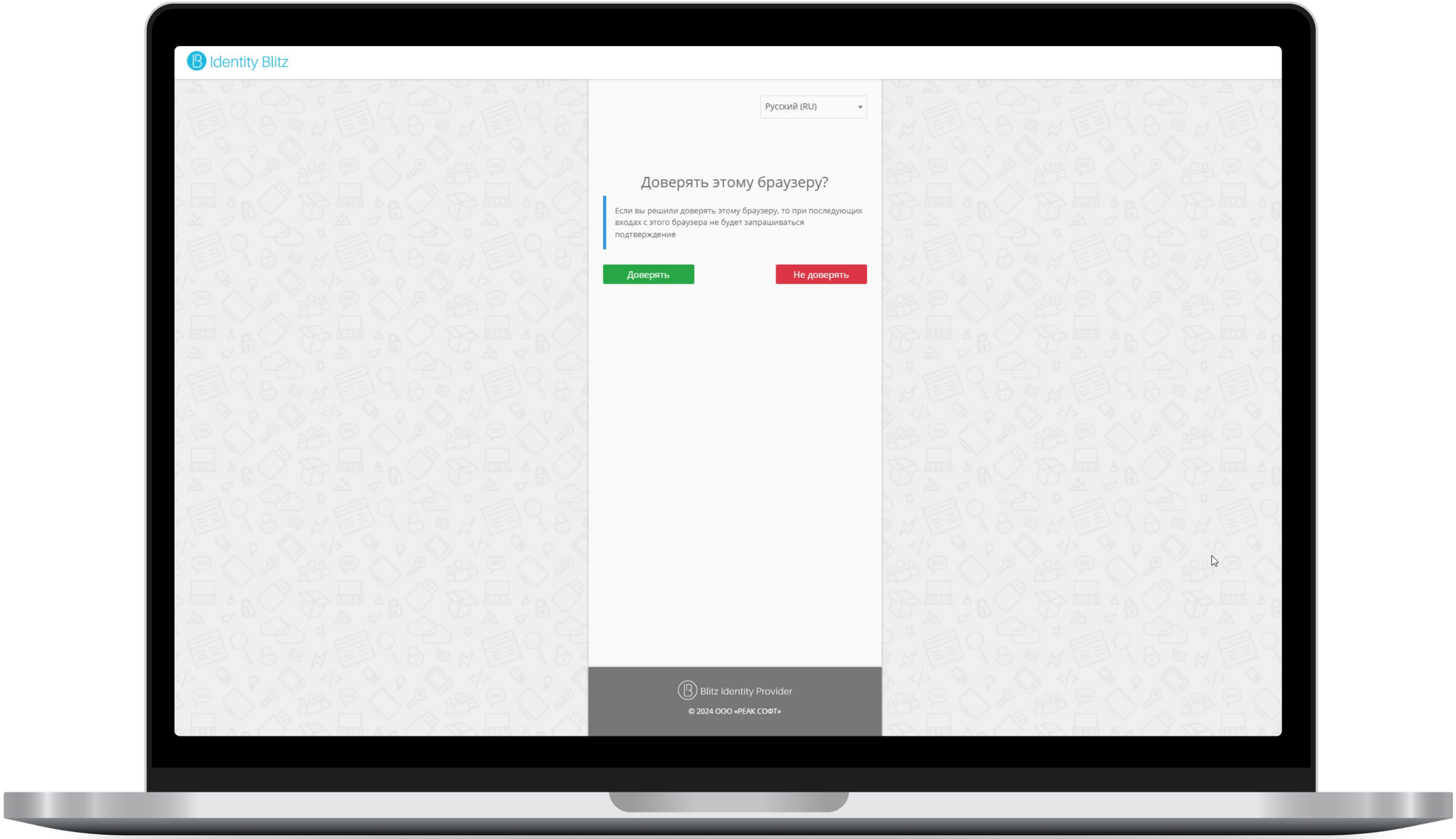

Доступ к информационным ресурсам города Москвы
Официальный сайт Мэра Москвы
Инструкция для входа в личный кабинет:
Для физических лиц
Для юридических лиц и ИП
Для доверенных лиц организаций
© Департамент информационных технологий города Москвы
Восстановление пароля
Придумайте пароль для вашей учетной записи
Повторите пароль
Показать пароль
Пароль должен содержать:
Не менее 8 символов
Прописные буквы
Цифры
Строчные буквы
Выйти со всех устройств
Восстановить доступ

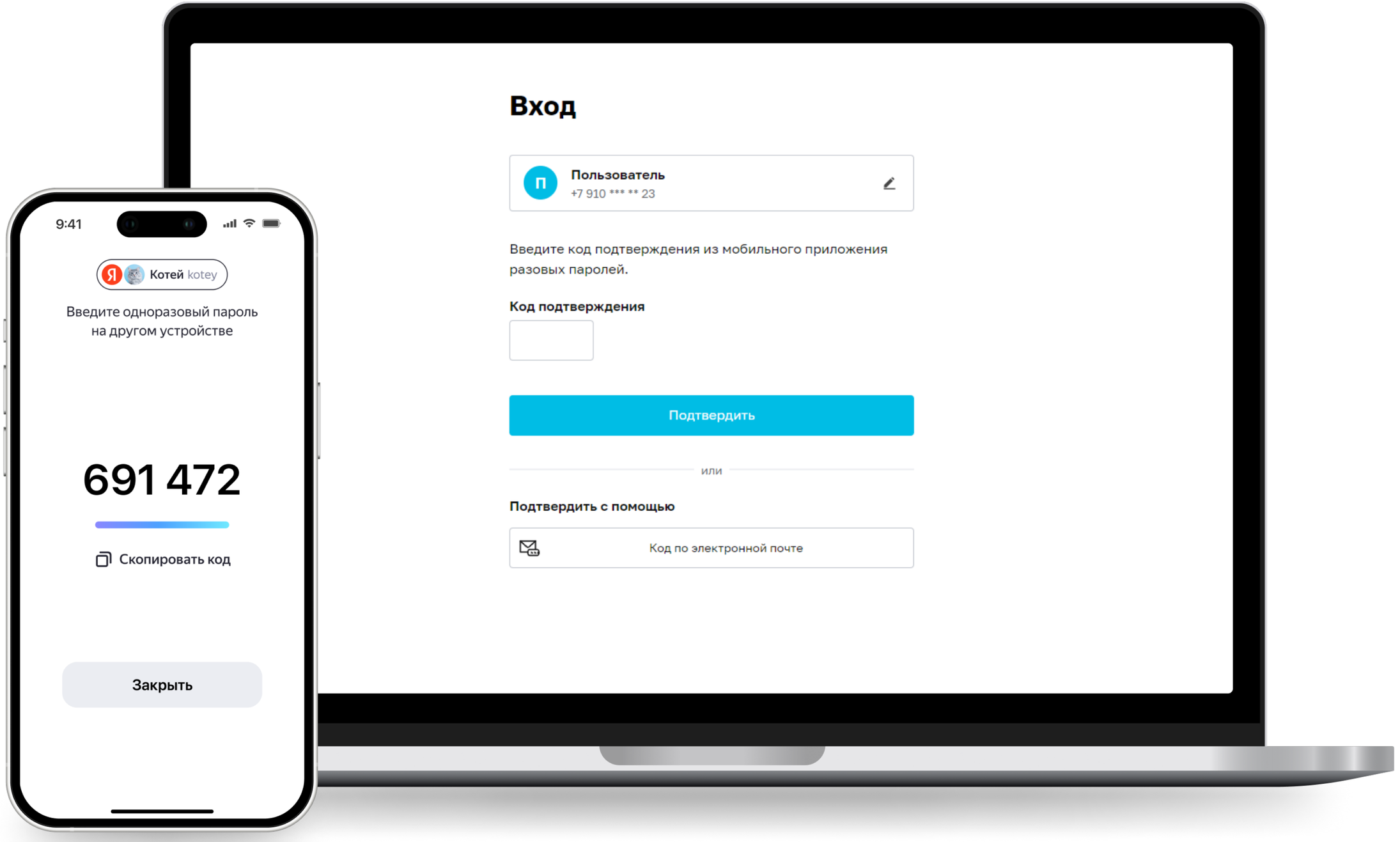

RU center
Вход
Клиент
Партнёр
Номер договора NIC-D
Пароль
Административный
Войти
Напомнить номер договора и пароль
или
госуслуги
Вход по электронной подписи
Стать клиентом

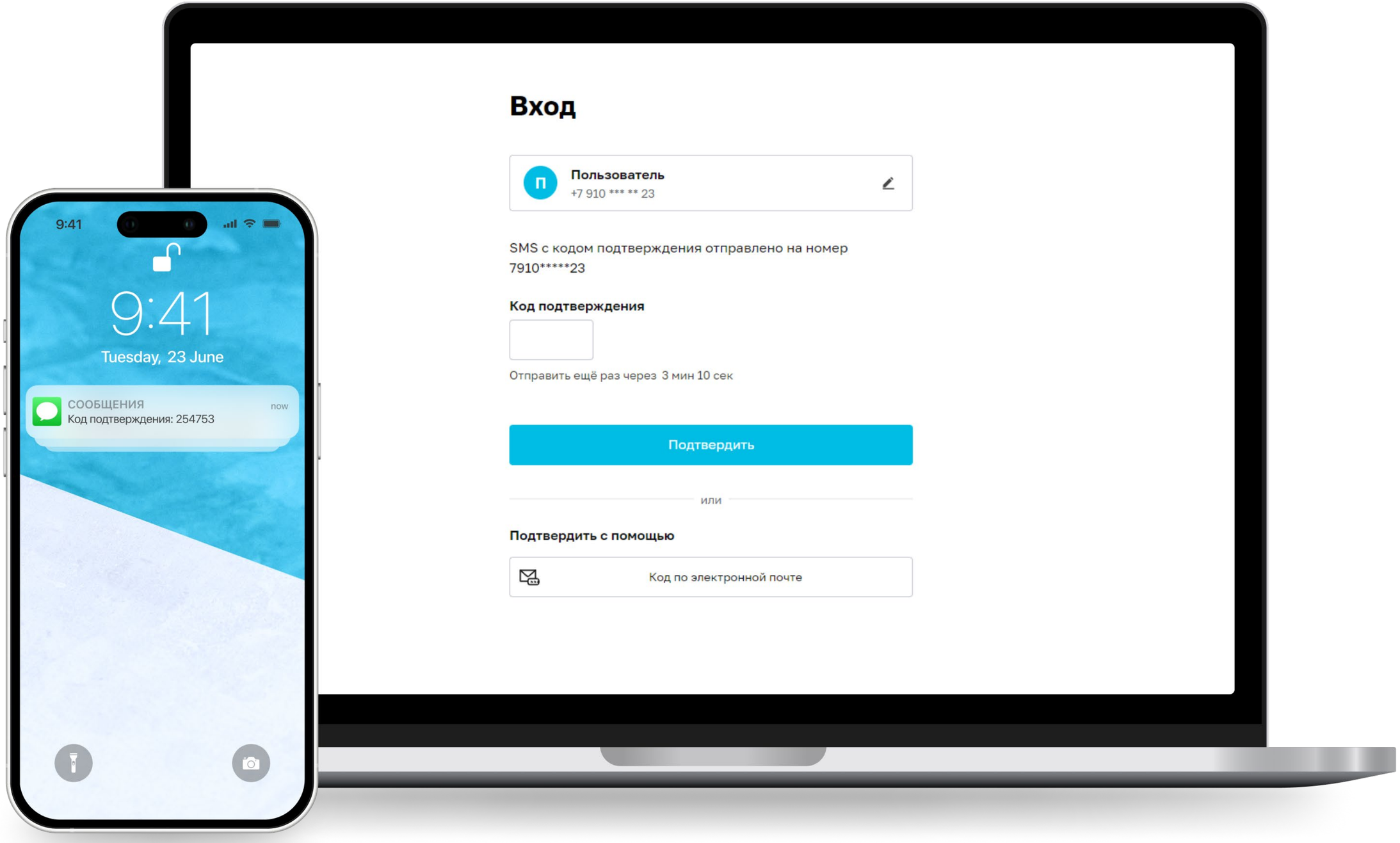

МОТИВ
Вход в личный кабинет
Сайт motivtelecom.ru
© 2011-2024 Мотив. Все права защищены
Инструкция для входа
Вход
Зарегистрироваться
Номер телефона
+7 ___-___-__-__
Пароль
Введите пароль
Показать пароль
Забыли пароль?
Войти
или
Рекомендуем использовать режим инкогнито для входа с чужого устройства

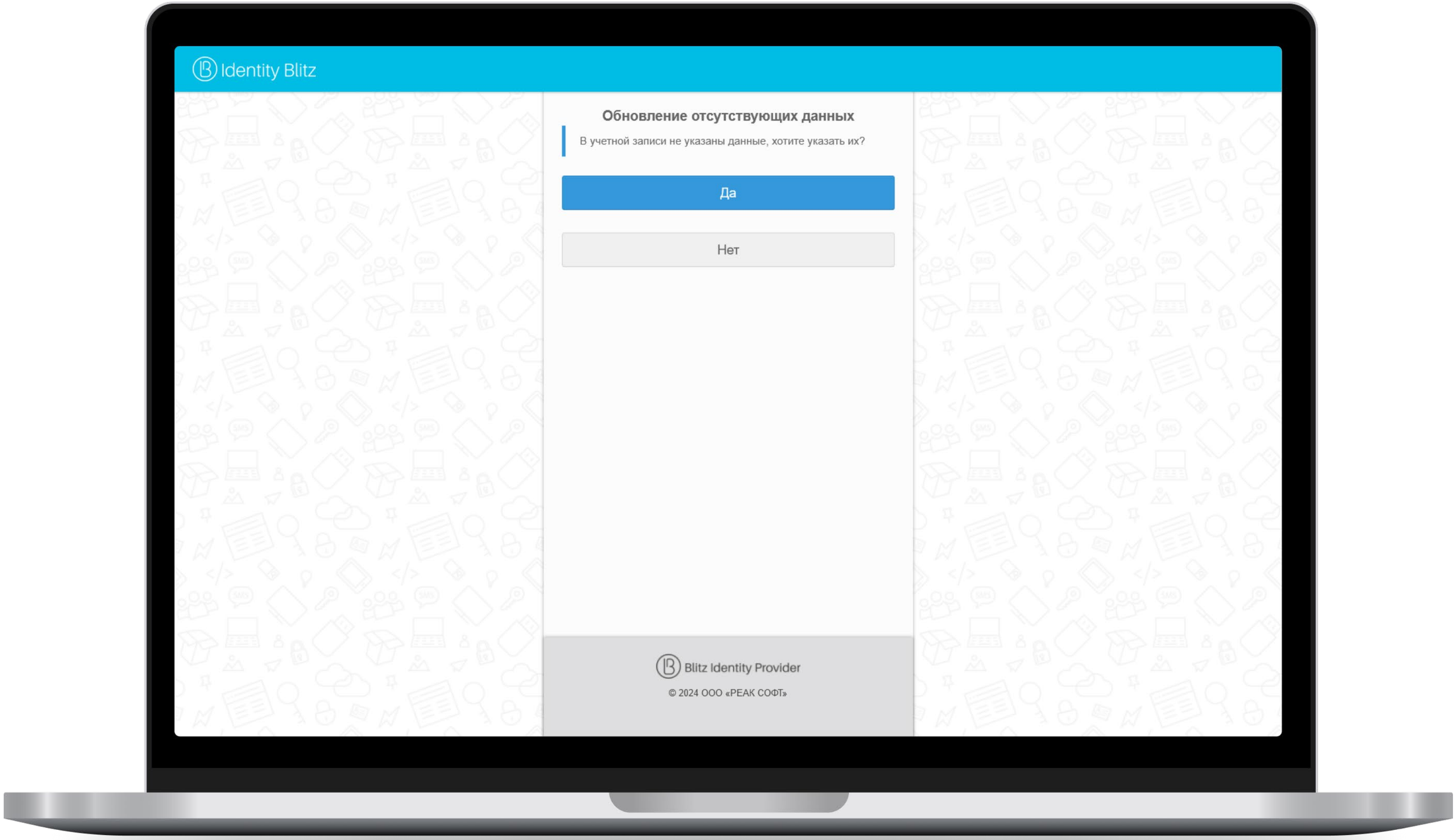

Identity Blitz
Русский (RU)
Вход в Личный кабинет
Логин
Логин
Пароль
Пароль
Войти
Вход по сеансу операционной системы
Вход по электронной подписи
Вход по ключу безопасности
Используйте инкогнито для входа с чужого устройства
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»

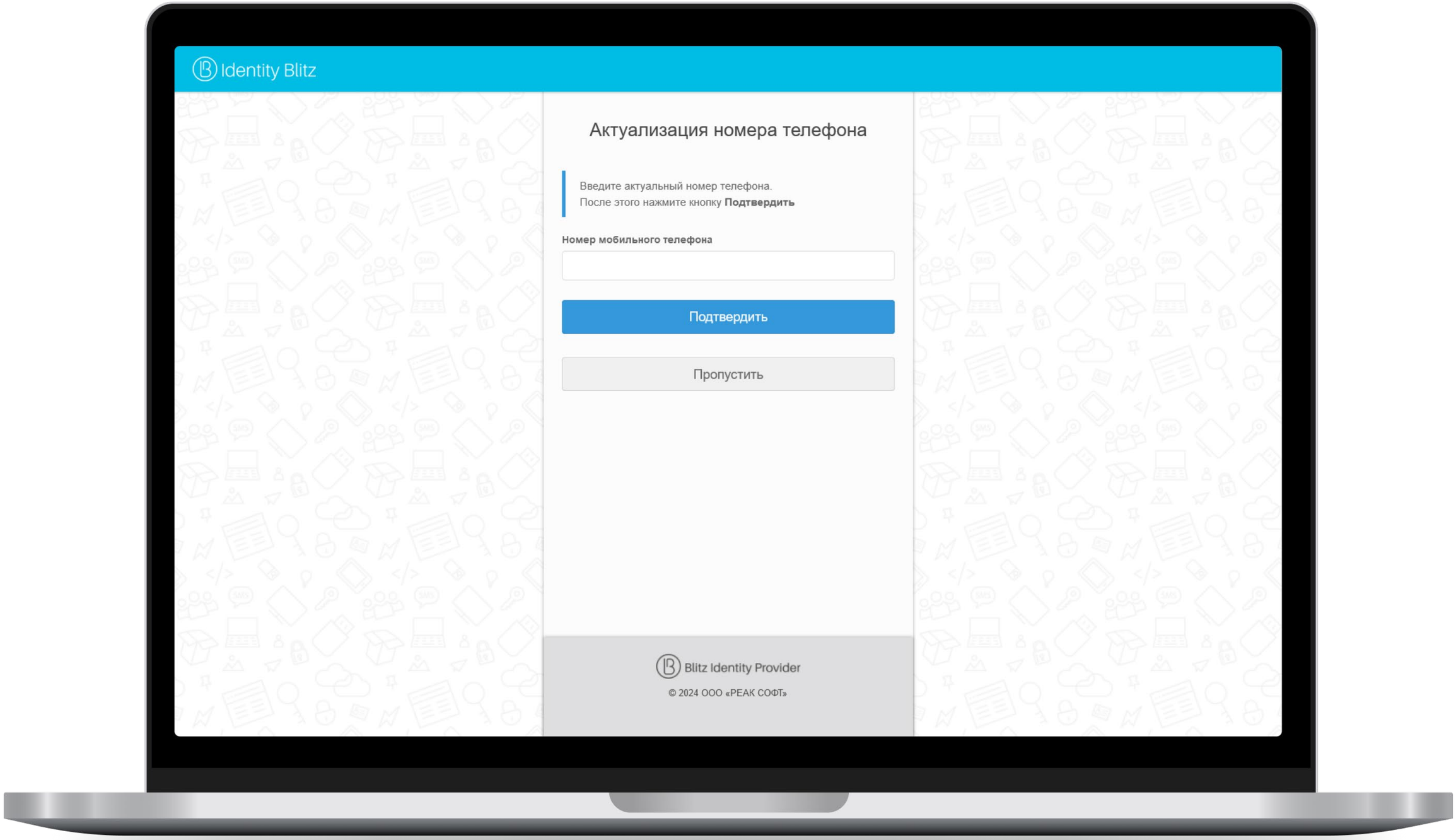

Identity Blitz
Русский (RU)
Вход в Личный кабинет
Срок действия вашего пароля истек. Пожалуйста, задайте новый пароль для вашей учетной
Новый пароль
Новый пароль
Подтвердите новый пароль
Новый пароль еще раз
Выйти со всех устройств
Изменить пароль
Вход по сеансу операционной системы
Вход по электронной подписи
Вход по ключу безопасности
Используйте инкогнито для входа с чужого устройства
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»

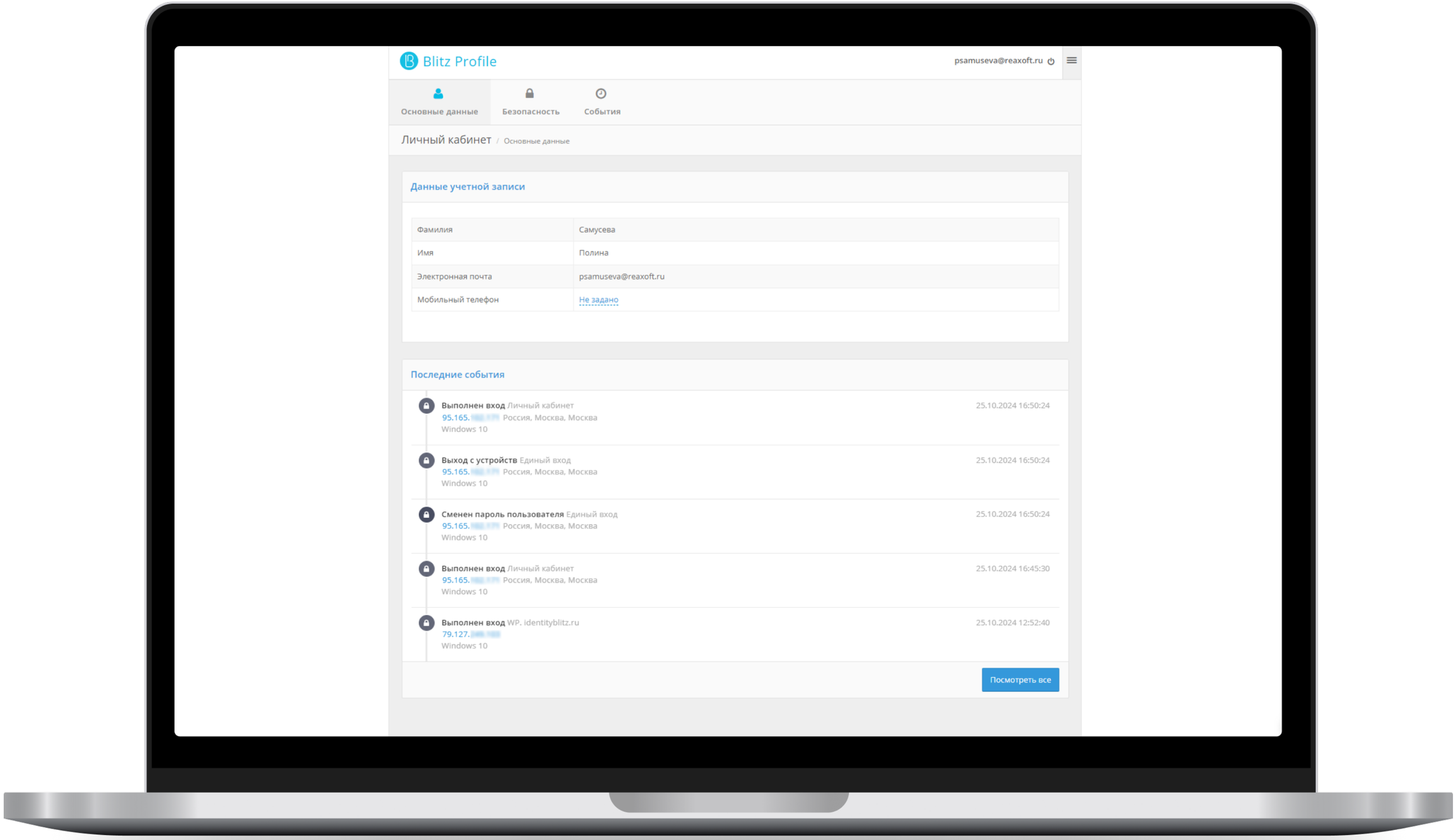

Identity Blitz
Русский (RU)
Доверять этому браузеру?
Если вы решили доверять этому браузеру, то при последующих входах с этого браузера не будет запрашиваться подтверждение
Доверять
Не доверять
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»

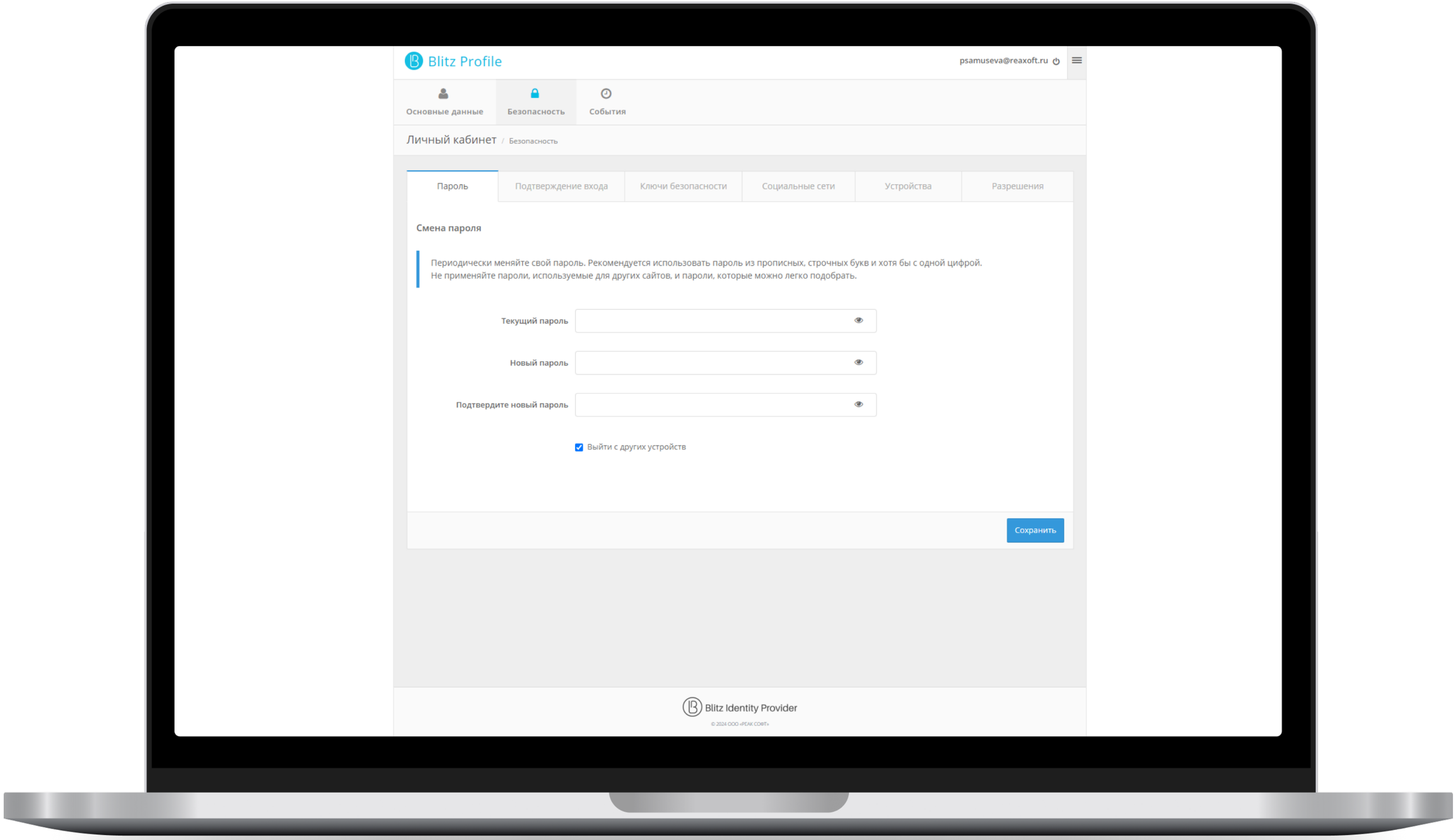

Вход
П
Пользователь
+7 910 *** ** 23
Введите код подтверждения из мобильного приложения разовых паролей.
Код подтверждения
Подтвердить
или
Подтвердить с помощью
Код по электронной почте
9:41
Котей kotey
Введите одноразовый пароль на другом устройстве
691 472
Скопировать код
Закрыть

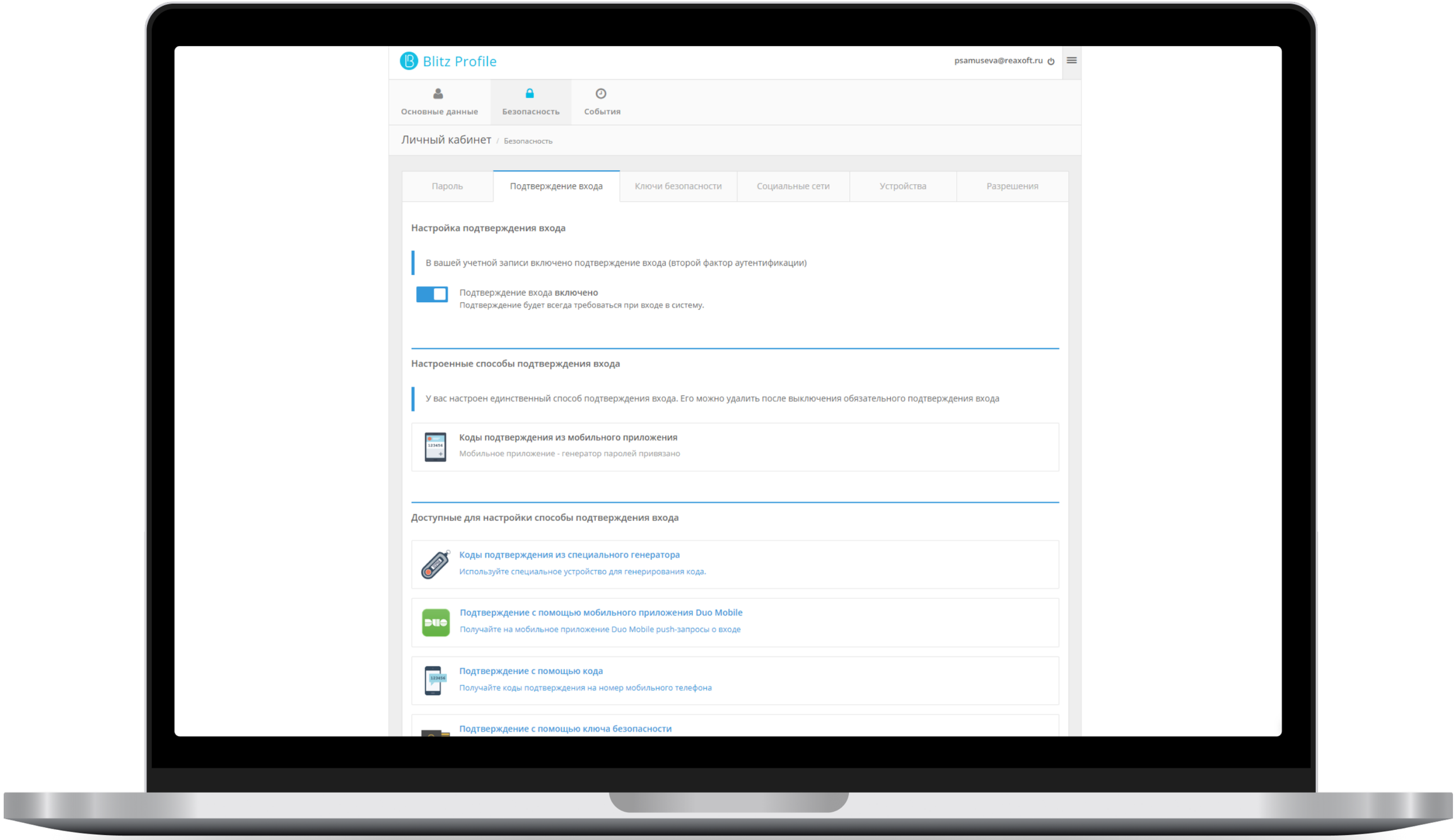

Вход
П
Пользователь
+7 910 *** ** 23
SMS с кодом подтверждения отправлено на номер 7910*****23
Код подтверждения
Отправить ещё раз через 3 мин 10 сек
Подтвердить
или
Подтвердить с помощью
Код по электронной почте
9:41
9:41
Tuesday, 23 June
СООБЩЕНИЯ
now
Код подтверждения: 254753

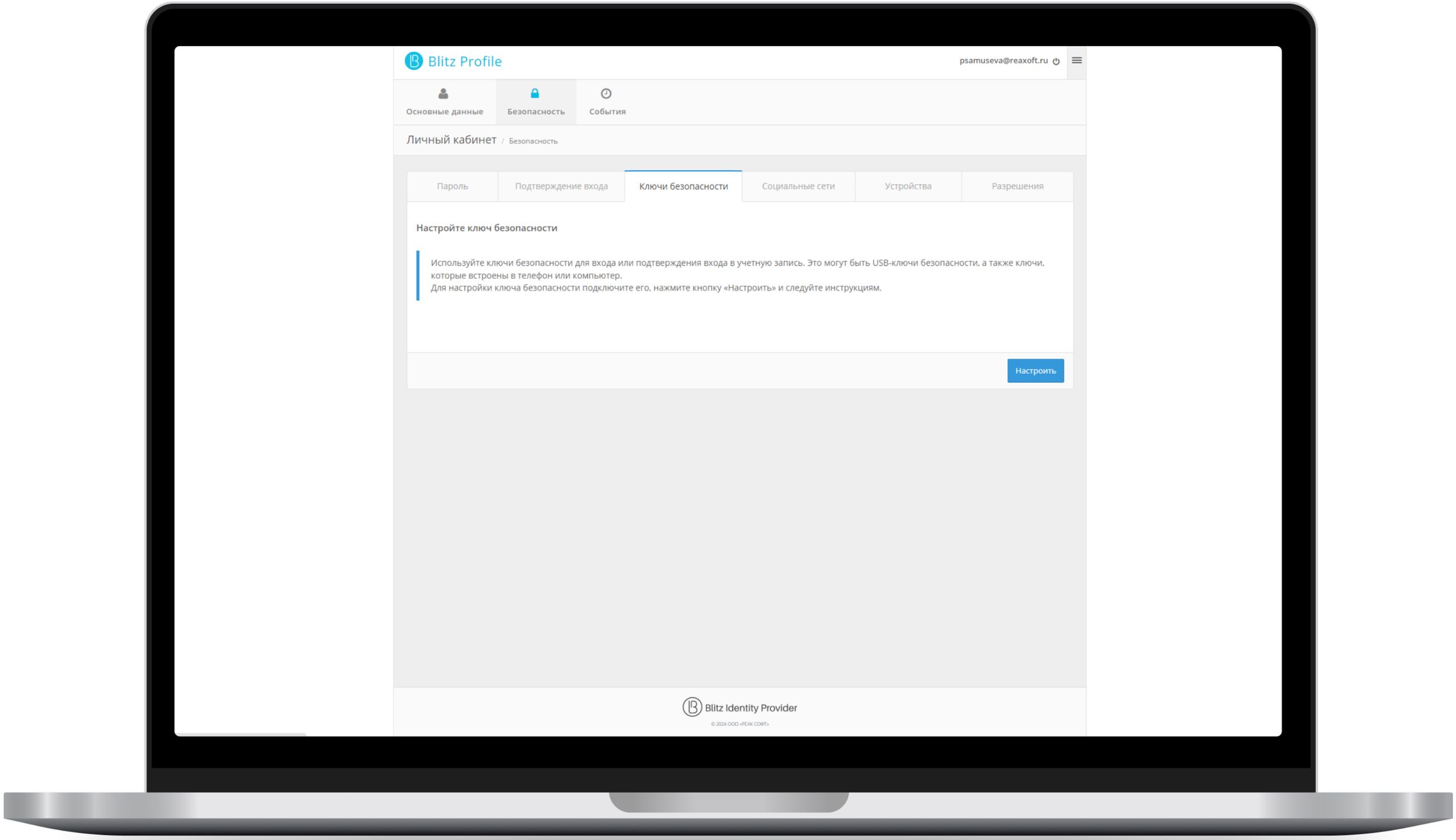

Identity Blitz
Обновление отсутствующих данных
В учетной записи не указаны данные, хотите указать их?
Да
Нет
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»

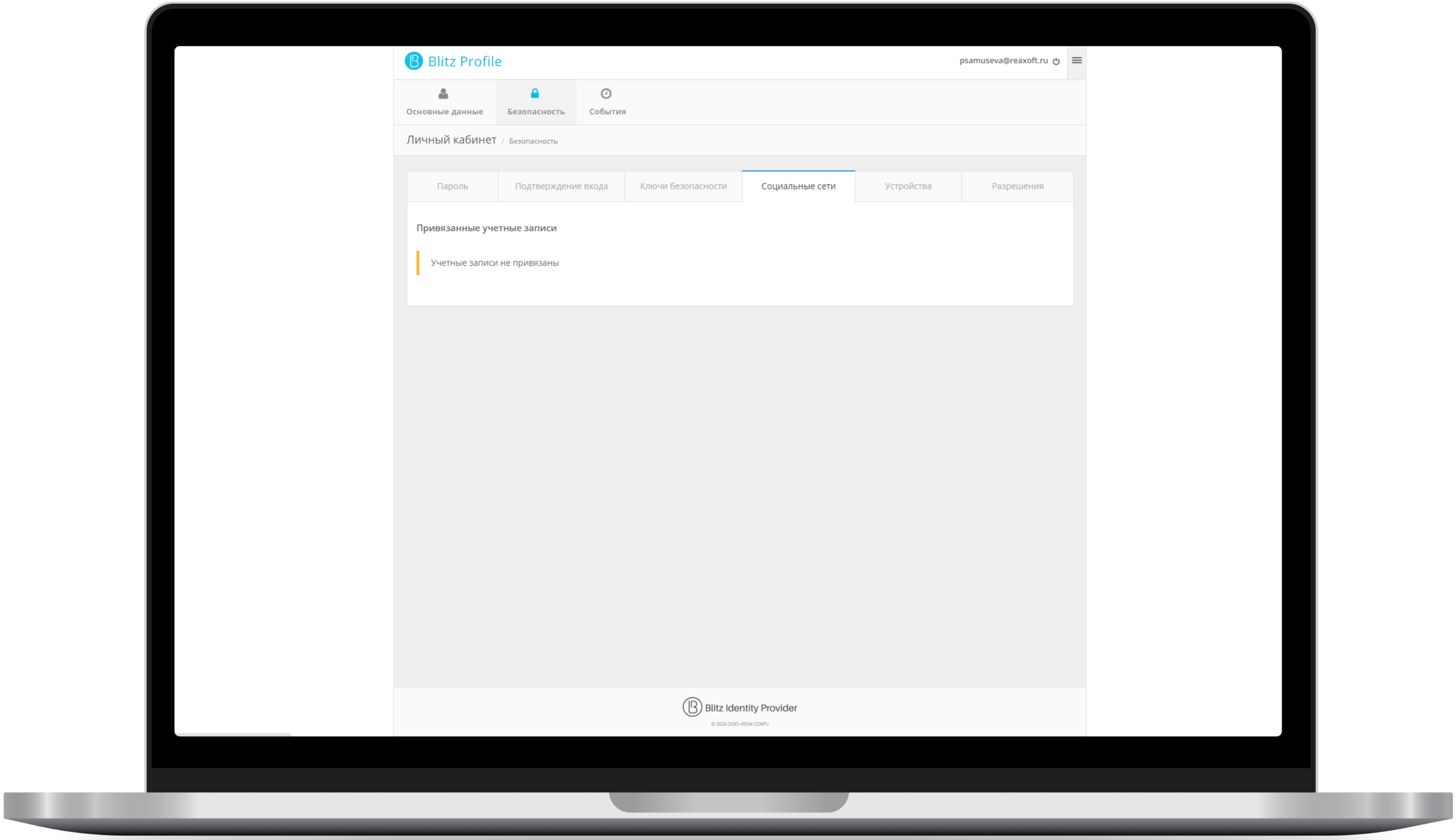

Identity Blitz
Актуализация номера телефона
Введите актуальный номер телефона.
После этого нажмите кнопку Подтвердить
Номер мобильного телефона
Подтвердить
Пропустить
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»

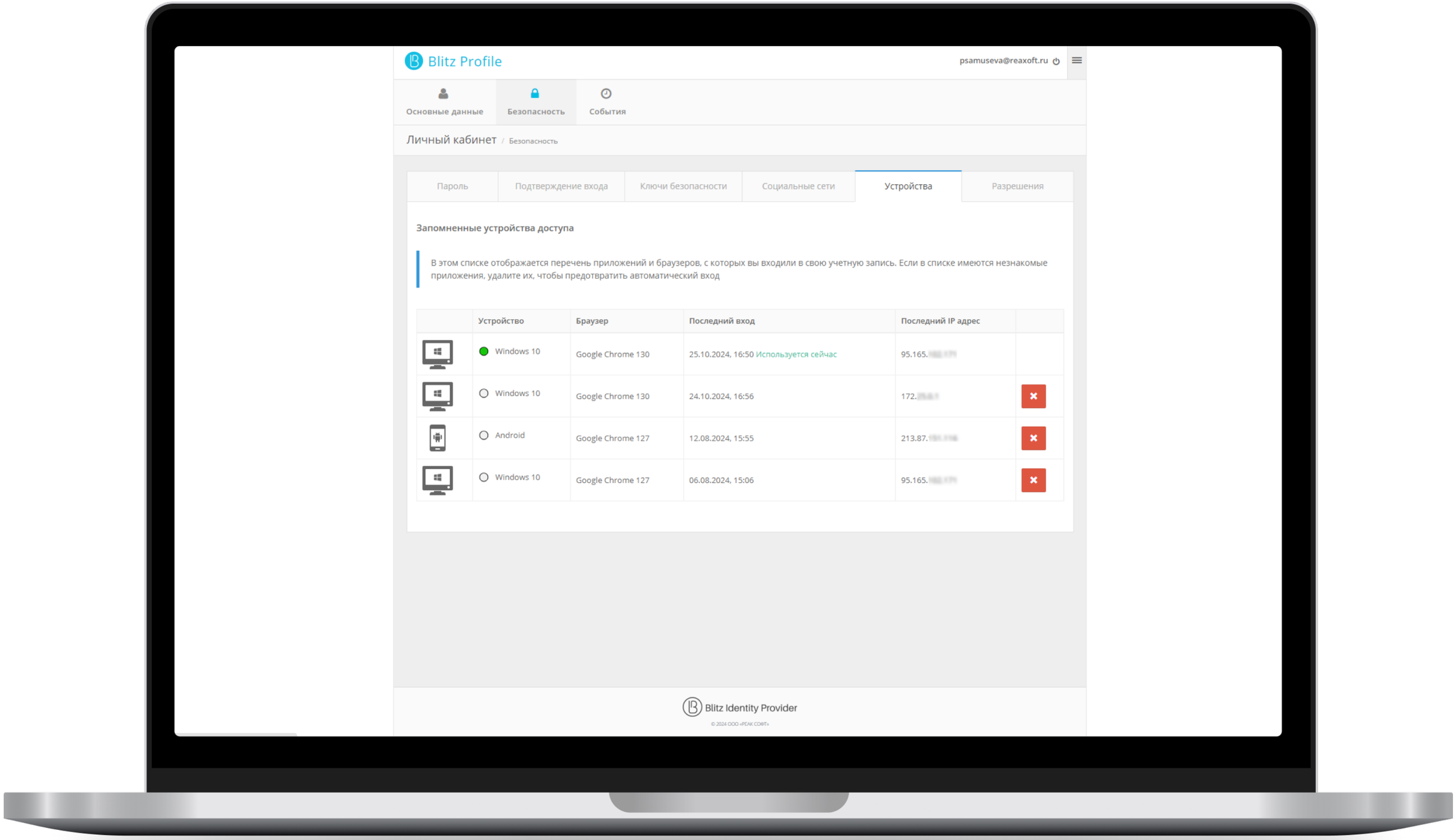

Blitz Profile
psamuseva@reaxoft.ru
Основные данные
Безопасность
События
Личный кабинет / Основные данные
Данные учетной записи
Фамилия
Самусева
Имя
Полина
Электронная почта
psamuseva@reaxoft.ru
Мобильный телефон
Не задано
Последние события
Выполнен вход Личный кабинет
95.165. Россия, Москва, Москва
Windows 10
25.10.2024 16:50:24
Выход с устройств Единый вход
95.165. Россия, Москва, Москва
Windows 10
25.10.2024 16:50:24
Сменен пароль пользователя Единый вход
95.165. Россия, Москва, Москва
Windows 10
25.10.2024 16:50:24
Выполнен вход Личный кабинет
95.165. Россия, Москва, Москва
Windows 10
25.10.2024 16:45:30
Выполнен вход WP. identityblitz.ru
79.127.
Windows 10
25.10.2024 12:52:40
Посмотреть все

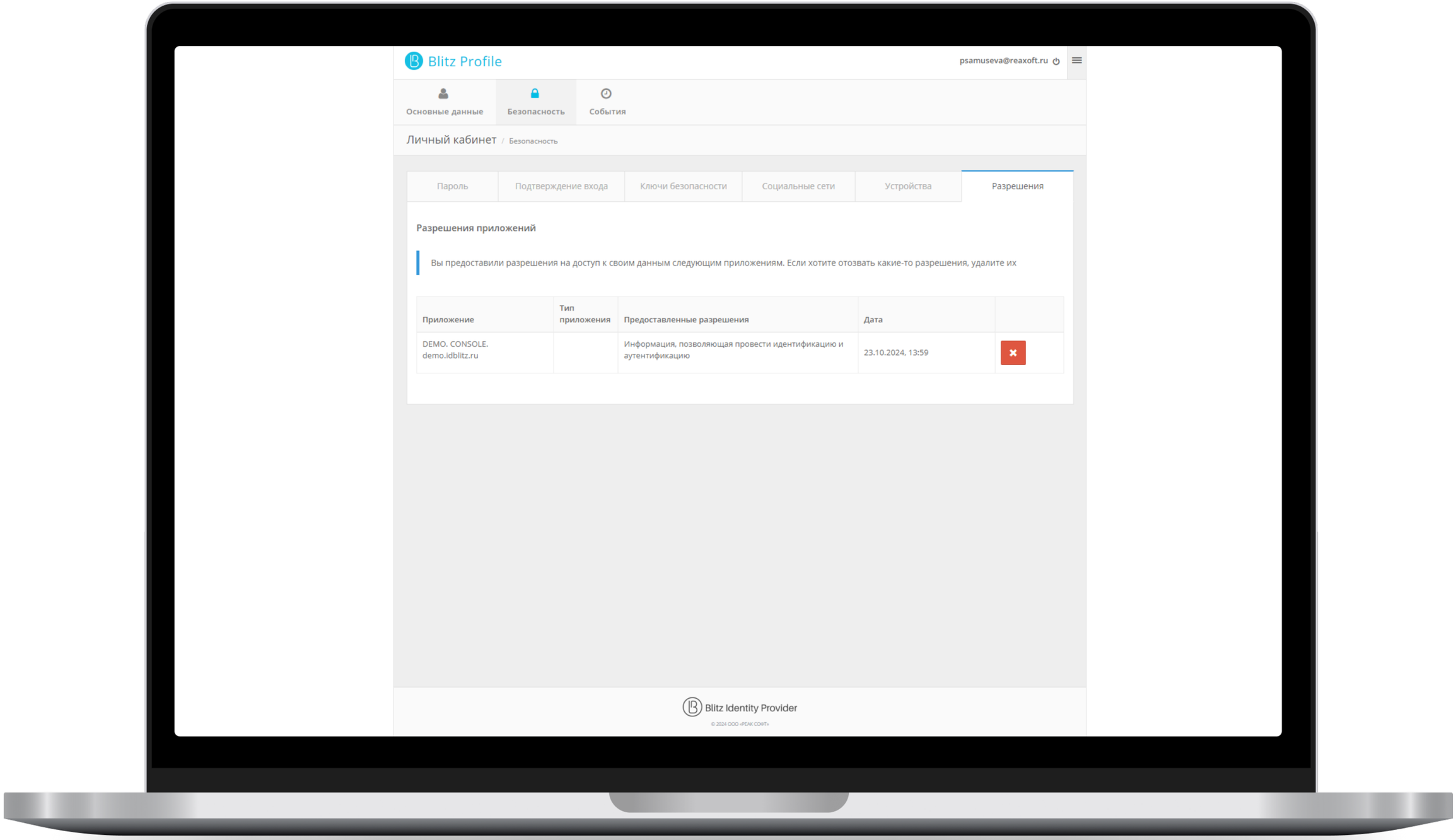

Blitz Profile
psamuseva@reaxoft.ru
Основные данные
Безопасность
События
Личный кабинет / Безопасность
Пароль
Подтверждение входа
Ключи безопасности
Социальные сети
Устройства
Разрешения
Смена пароля
Периодически меняйте свой пароль. Рекомендуется использовать пароль из прописных, строчных букв и хотя бы с одной цифрой.
Не применяйте пароли, используемые для других сайтов, и пароли, которые можно легко подобрать.
Текущий пароль
Новый пароль
Подтвердите новый пароль
Выйти с других устройств
Сохранить
Blitz Identity Provider

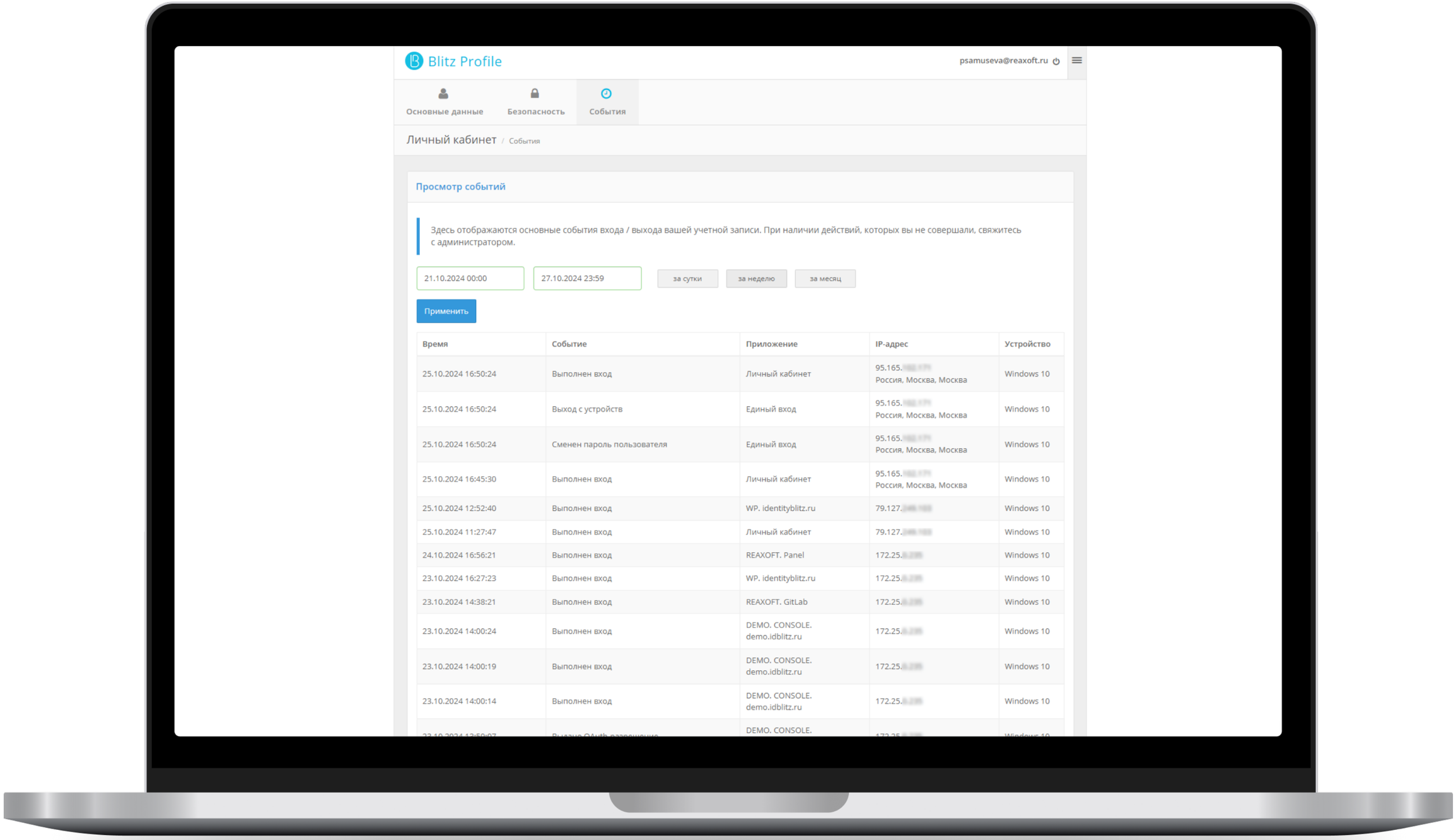

Blitz Profile
psamuseva@reaxoft.ru
Основные данные
Безопасность
События
Личный кабинет / Безопасность
Пароль
Подтверждение входа
Ключи безопасности
Социальные сети
Устройства
Разрешения
Настройка подтверждения входа
В вашей учетной записи включено подтверждение входа (второй фактор аутентификации)
Подтверждение входа включено
Подтверждение будет всегда требоваться при входе в систему.
Настроенные способы подтверждения входа
У вас настроен единственный способ подтверждения входа. Его можно удалить после выключения обязательного подтверждения входа
Коды подтверждения из мобильного приложения
Мобильное приложение - генератор паролей привязано
Доступные для настройки способы подтверждения входа
Коды подтверждения из специального генератора
Используйте специальное устройство для генерирования кода.
Подтверждение с помощью мобильного приложения Duo Mobile
Получайте на мобильное приложение Duo Mobile push-запросы о входе
Подтверждение с помощью кода
Получайте коды подтверждения на номер мобильного телефона
Подтверждение с помощью ключа безопасности

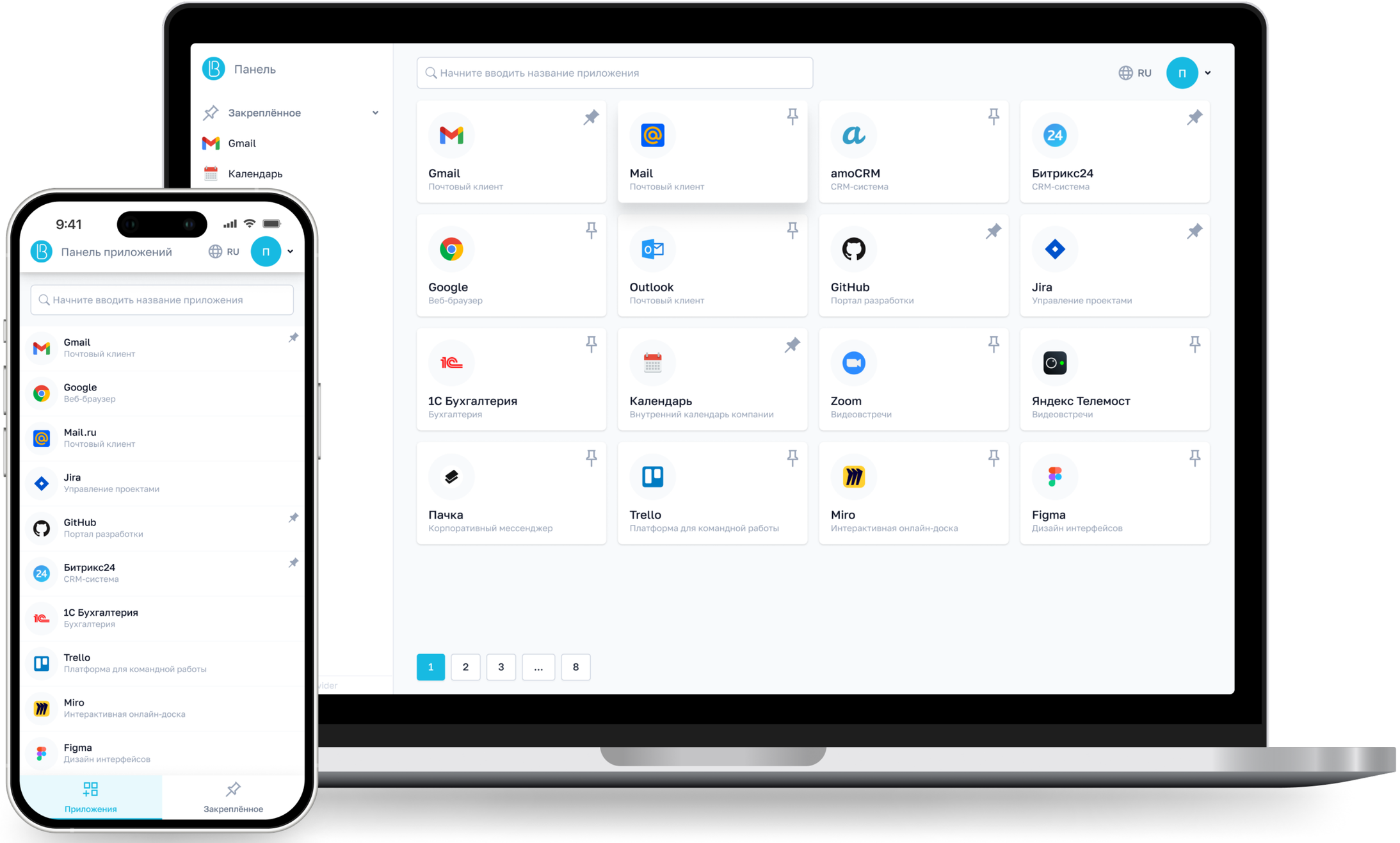

Blitz Profile
psamuseva@reaxoft.ru
Основные данные
Безопасность
События
Личный кабинет / Безопасность
Пароль
Подтверждение входа
Ключи безопасности
Социальные сети
Устройства
Разрешения
Настройте ключ безопасности
Используйте ключи безопасности для входа или подтверждения входа в учетную запись. Это могут быть USB-ключи безопасности, а также ключи, которые встроены в телефон или компьютер.
Для настройки ключа безопасности подключите его, нажмите кнопку «Настроить» и следуйте инструкциям.
Настроить
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»

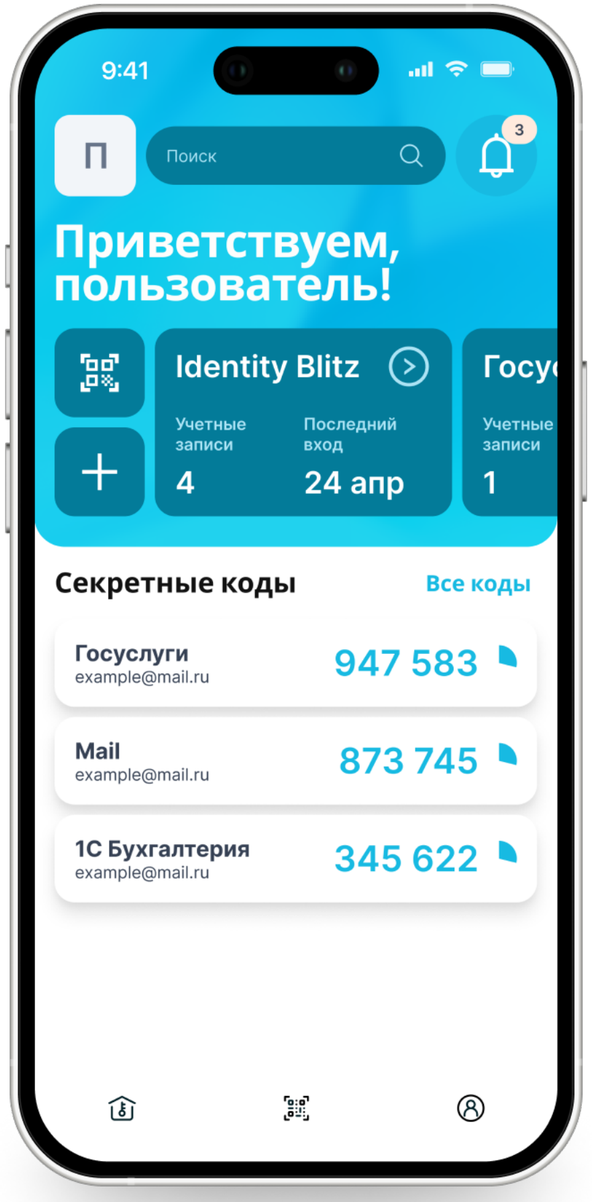

Blitz Profile
psamuseva@reaxoft.ru
Основные данные
Безопасность
События
Личный кабинет / Безопасность
Пароль
Подтверждение входа
Ключи безопасности
Социальные сети
Устройства
Разрешения
Привязанные учетные записи
Учетные записи не привязаны
Blitz Identity Provider

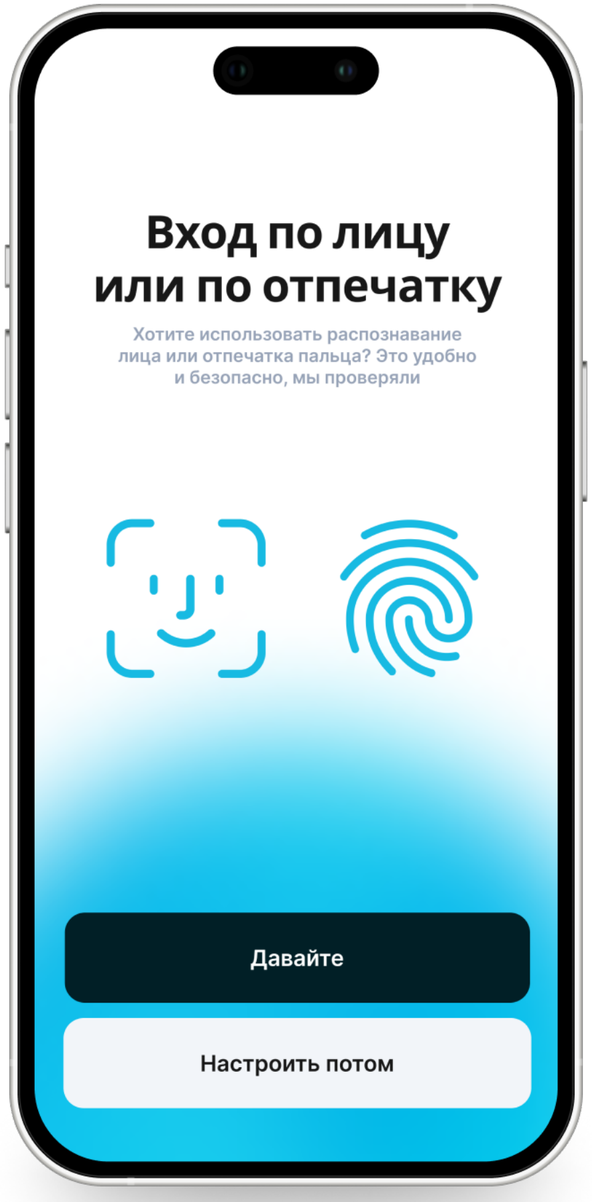

Blitz Profile
psamuseva@reaxoft.ru
Основные данные
Безопасность
События
Личный кабинет / Безопасность
Пароль
Подтверждение входа
Ключи безопасности
Социальные сети
Устройства
Разрешения
Запомненные устройства доступа
В этом списке отображается перечень приложений и браузеров, с которых вы входили в свою учетную запись. Если в списке имеются незнакомые приложения, удалите их, чтобы предотвратить автоматический вход
Устройство
Браузер
Последний вход
Последний IP адрес
Windows 10
Google Chrome 130
25.10.2024, 16:50 Используется сейчас
95.165.
Windows 10
Google Chrome 130
24.10.2024, 16:56
172.
Android
Google Chrome 127
12.08.2024, 15:55
213.87.
Windows 10
Google Chrome 127
06.08.2024, 15:06
95.165.
Blitz Identity Provider

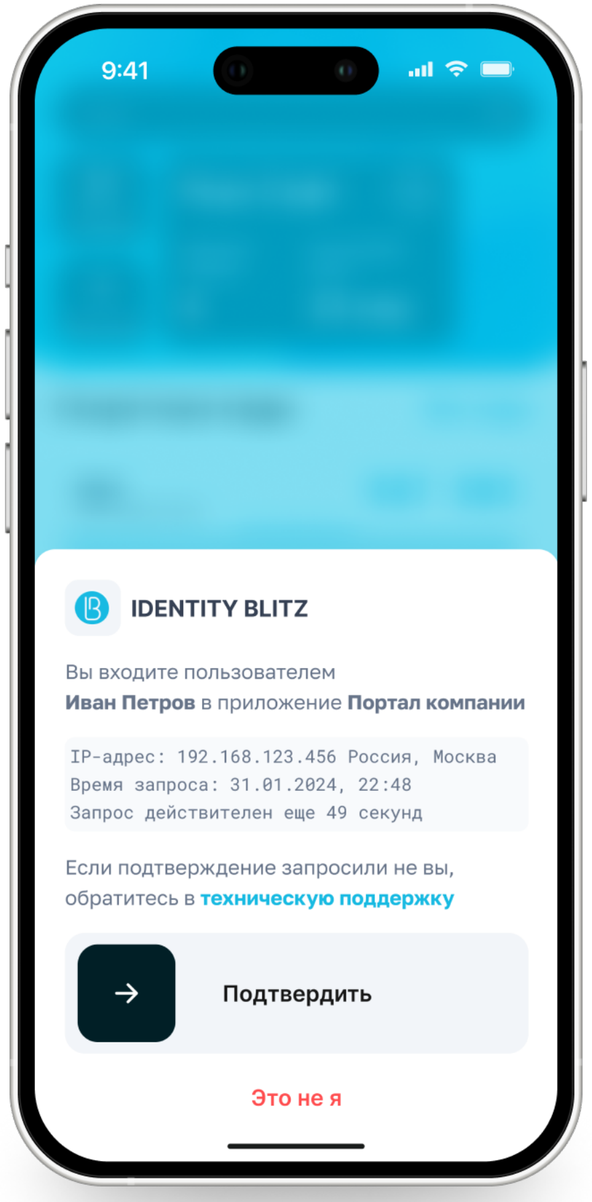

Blitz Profile
psamuseva@reaxoft.ru
Основные данные
Безопасность
События
Личный кабинет / Безопасность
Пароль
Подтверждение входа
Ключи безопасности
Социальные сети
Устройства
Разрешения
Разрешения приложений
Вы предоставили разрешения на доступ к своим данным следующим приложениям. Если хотите отозвать какие-то разрешения, удалите их
Приложение
Тип приложения
Предоставленные разрешения
Дата
DEMO. CONSOLE. demo.idblitz.ru
Информация, позволяющая провести идентификацию и аутентификацию
23.10.2024, 13:59
Blitz Identity Provider


Blitz Profile
psamuseva@reaxoft.ru
Основные данные
Безопасность
События
Личный кабинет / События
Просмотр событий
Здесь отображаются основные события входа / выхода вашей учетной записи. При наличии действий, которых вы не совершали, свяжитесь с администратором.
21.10.2024 00:00
27.10.2024 23:59
за сутки
за неделю
за месяц
Применить
Время
Событие
Приложение
IP-адрес
Устройство
25.10.2024 16:50:24
Выполнен вход
Личный кабинет
95.165.
Россия, Москва, Москва
Windows 10
25.10.2024 16:50:24
Выход с устройств
Единый вход
95.165.
Россия, Москва, Москва
Windows 10
25.10.2024 16:50:24
Сменен пароль пользователя
Единый вход
95.165.
Россия, Москва, Москва
Windows 10
25.10.2024 16:45:30
Выполнен вход
Личный кабинет
95.165.
Россия, Москва, Москва
Windows 10
25.10.2024 12:52:40
Выполнен вход
WP. identityblitz.ru
79.127.
Windows 10
25.10.2024 11:27:47
Выполнен вход
Личный кабинет
79.127.
Windows 10
24.10.2024 16:56:21
Выполнен вход
REAXOFT. Panel
172.25.
Windows 10
23.10.2024 16:27:23
Выполнен вход
WP. identityblitz.ru
172.25.
Windows 10
23.10.2024 14:38:21
Выполнен вход
REAXOFT. GitLab
172.25.
Windows 10
23.10.2024 14:00:24
Выполнен вход
DEMO. CONSOLE.
demo.idblitz.ru
172.25.
Windows 10
23.10.2024 14:00:19
Выполнен вход
DEMO. CONSOLE.
demo.idblitz.ru
172.25.
Windows 10
23.10.2024 14:00:14
Выполнен вход
DEMO. CONSOLE.
demo.idblitz.ru
172.25.
Windows 10
DEMO. CONSOLE.

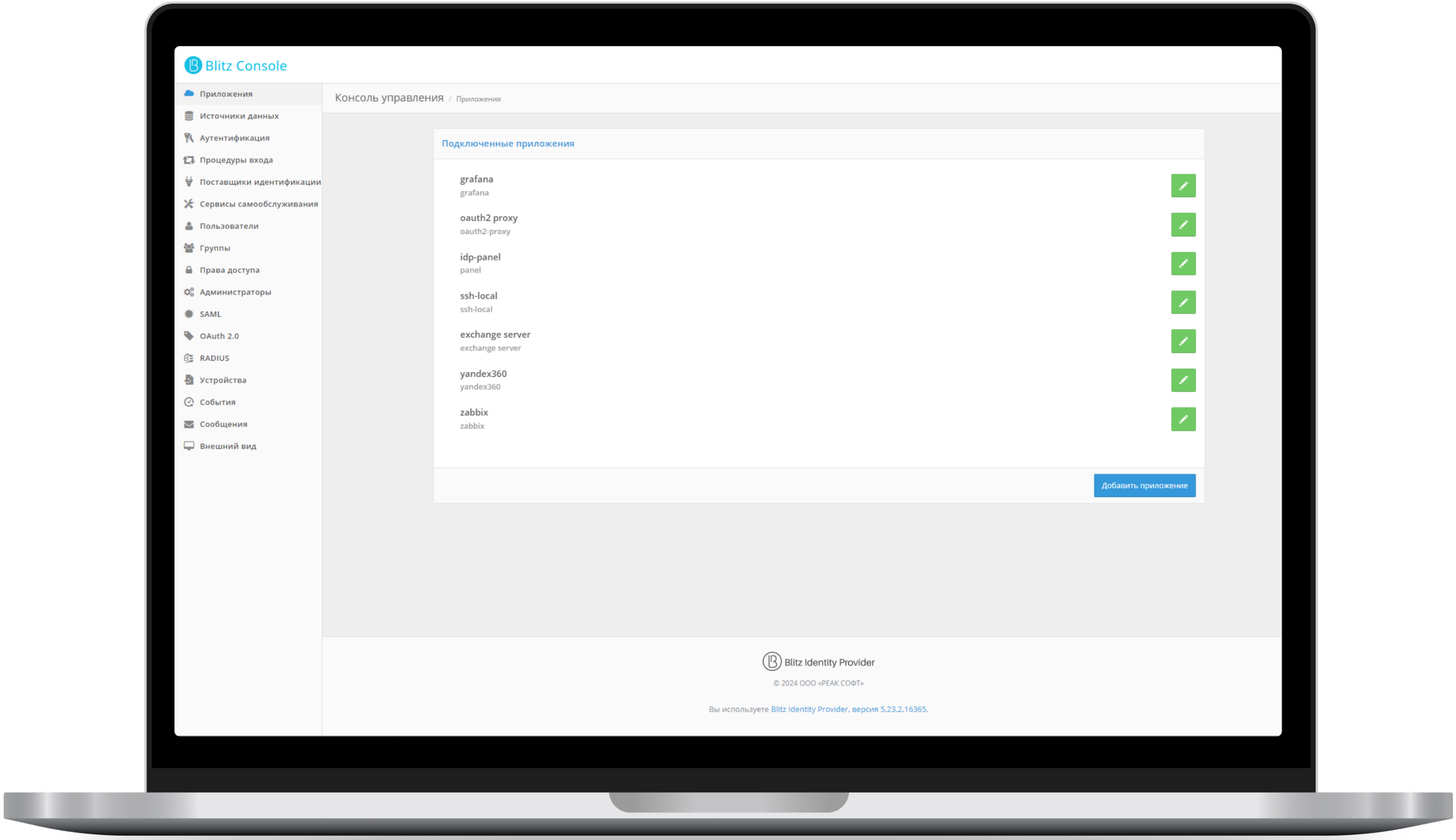

Панель
Закреплённое
Gmail
Календарь
Начните вводить название приложения
RU
П
Gmail
Почтовый клиент
Mail
Почтовый клиент
amoCRM
CRM-система
Битрикс24
CRM-система
Google
Веб-браузер
Outlook
Почтовый клиент
GitHub
Портал разработки
Jira
Управление проектами
1С Бухгалтерия
Бухгалтерия
Календарь
Внутренний календарь компании
Zoom
Видеовстречи
Яндекс Телемост
Видеовстречи
Пачка
Корпоративный мессенджер
Trello
Платформа для командной работы
Miro
Интерактивная онлайн-доска
Figma
Дизайн интерфейсов
1
2
3
...
8
9:41
Панель приложений
RU
П
Начните вводить название приложения
Gmail
Почтовый клиент
Google
Веб-браузер
Mail.ru
Почтовый клиент
Jira
Управление проектами
GitHub
Портал разработки
Битрикс24
CRM-система
1С Бухгалтерия
Бухгалтерия
Trello
Платформа для командной работы
Miro
Интерактивная онлайн-доска
Figma
Дизайн интерфейсов
Приложения
Закреплённое

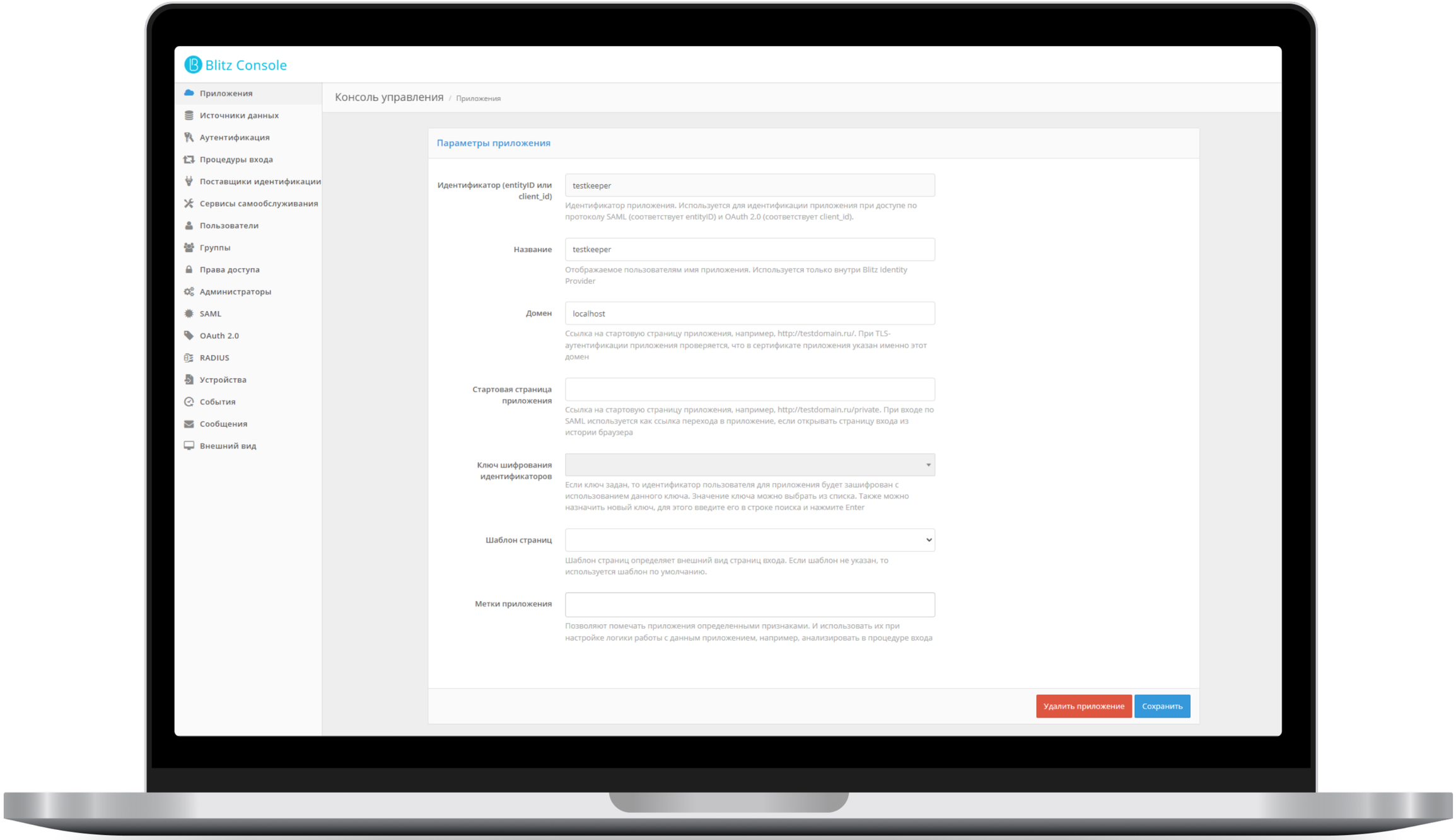


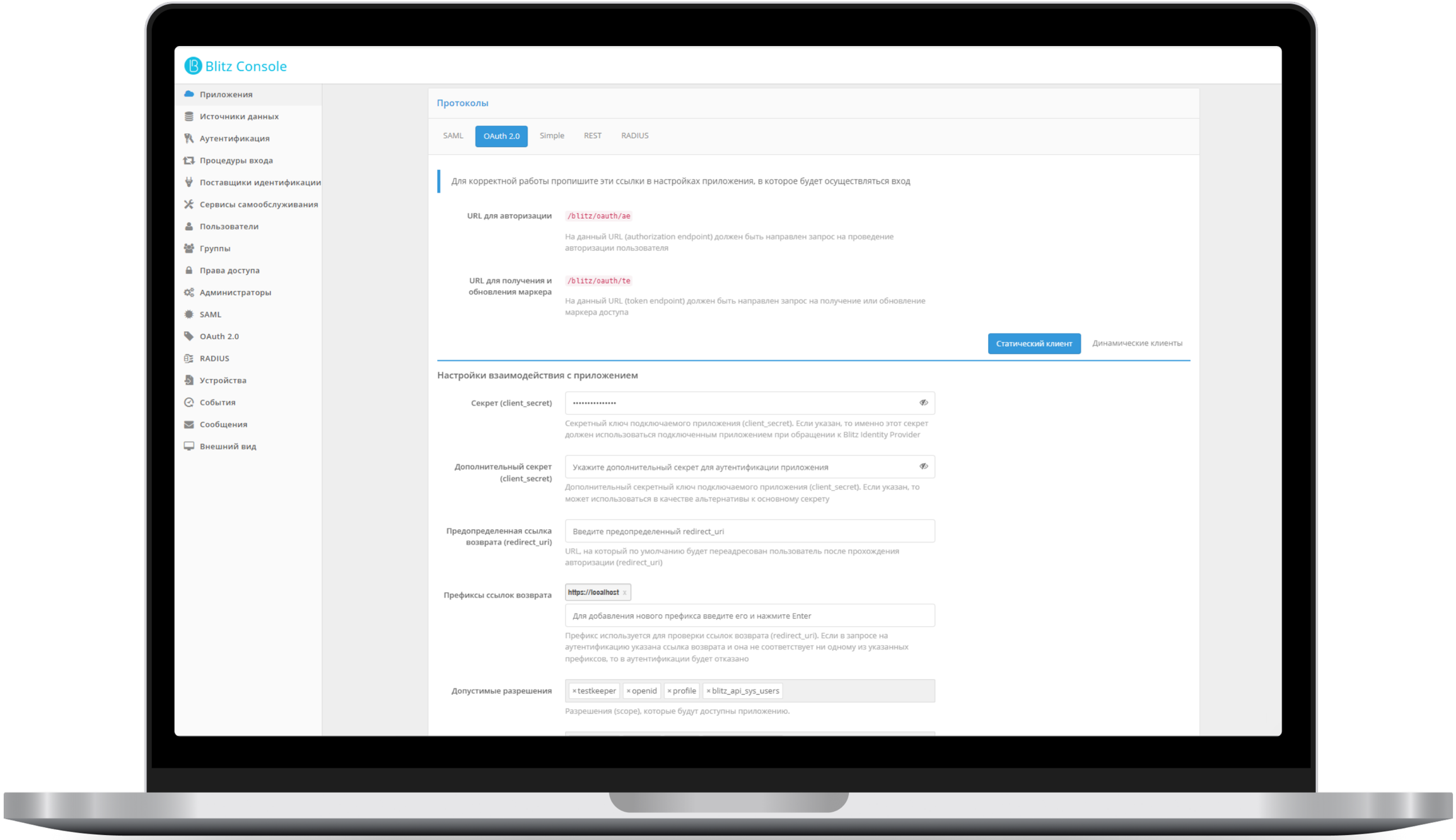


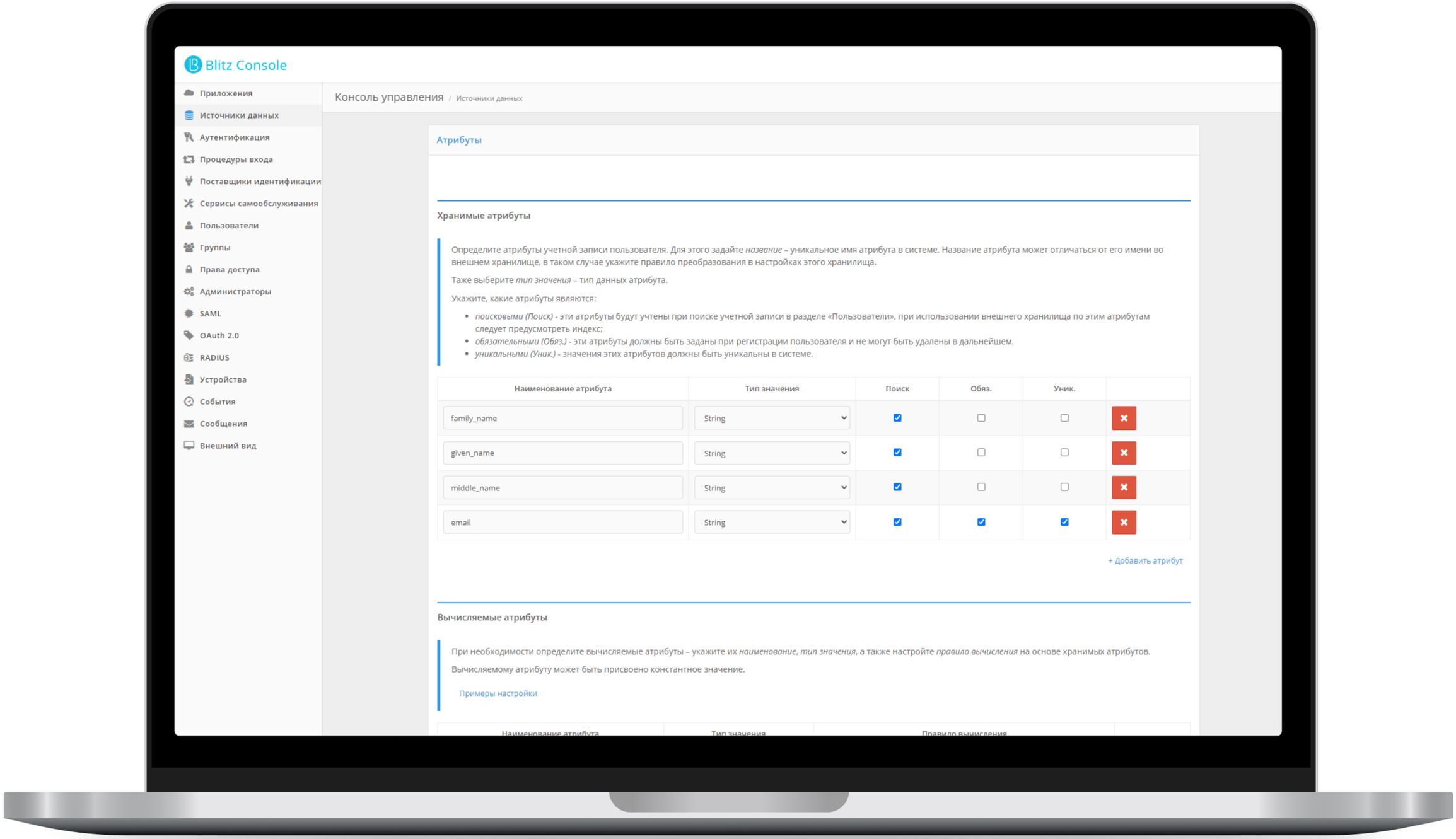


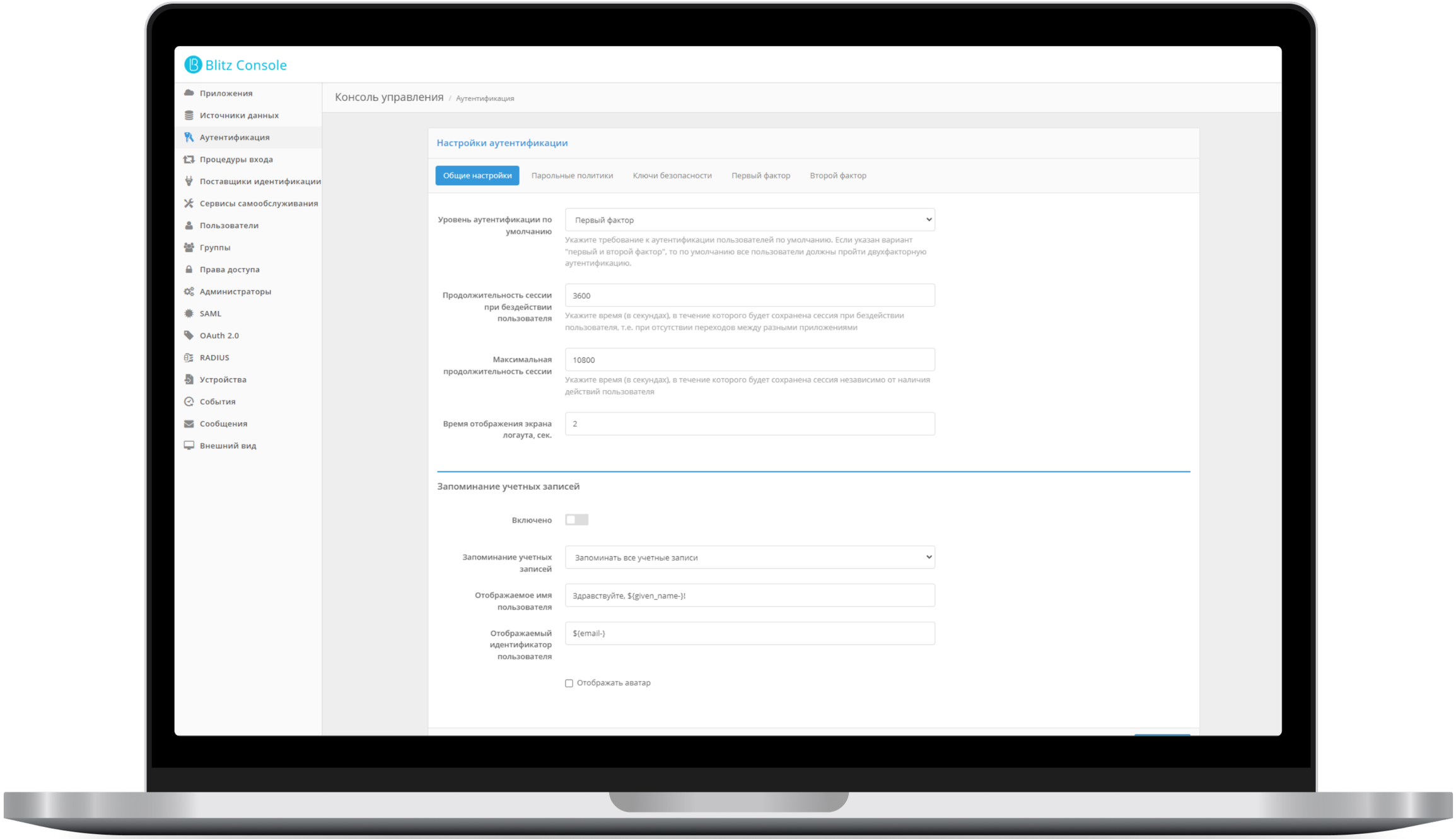
*в разработке

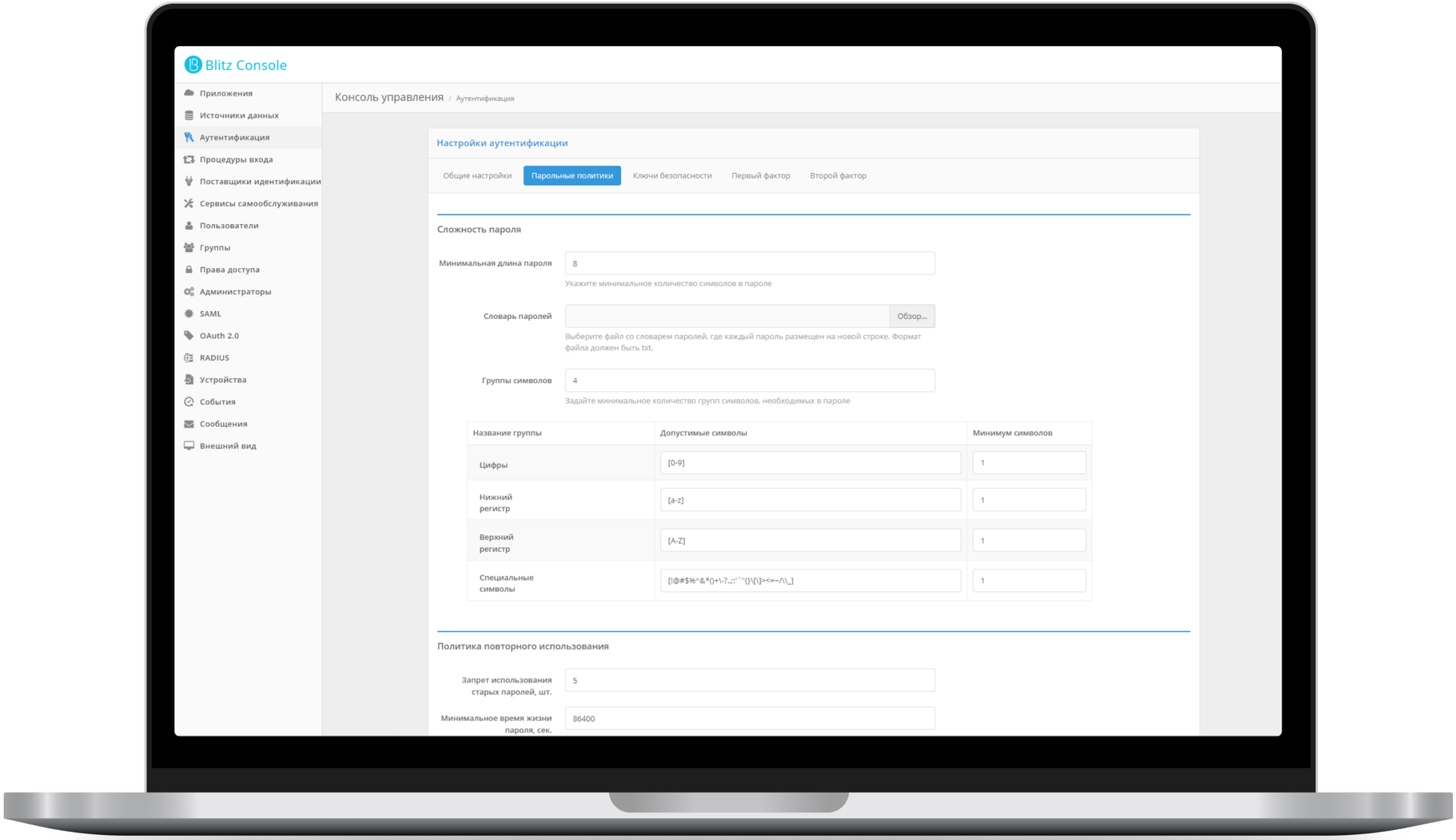

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Приложения
Подключенные приложения
grafana
grafana
oauth2 proxy
oauth2-proxy
idp-panel
panel
ssh-local
ssh-local
exchange server
exchange server
yandex360
yandex360
zabbix
zabbix
Добавить приложение
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»
Вы используете Blitz Identity Provider, версия 5.23.2.16365.

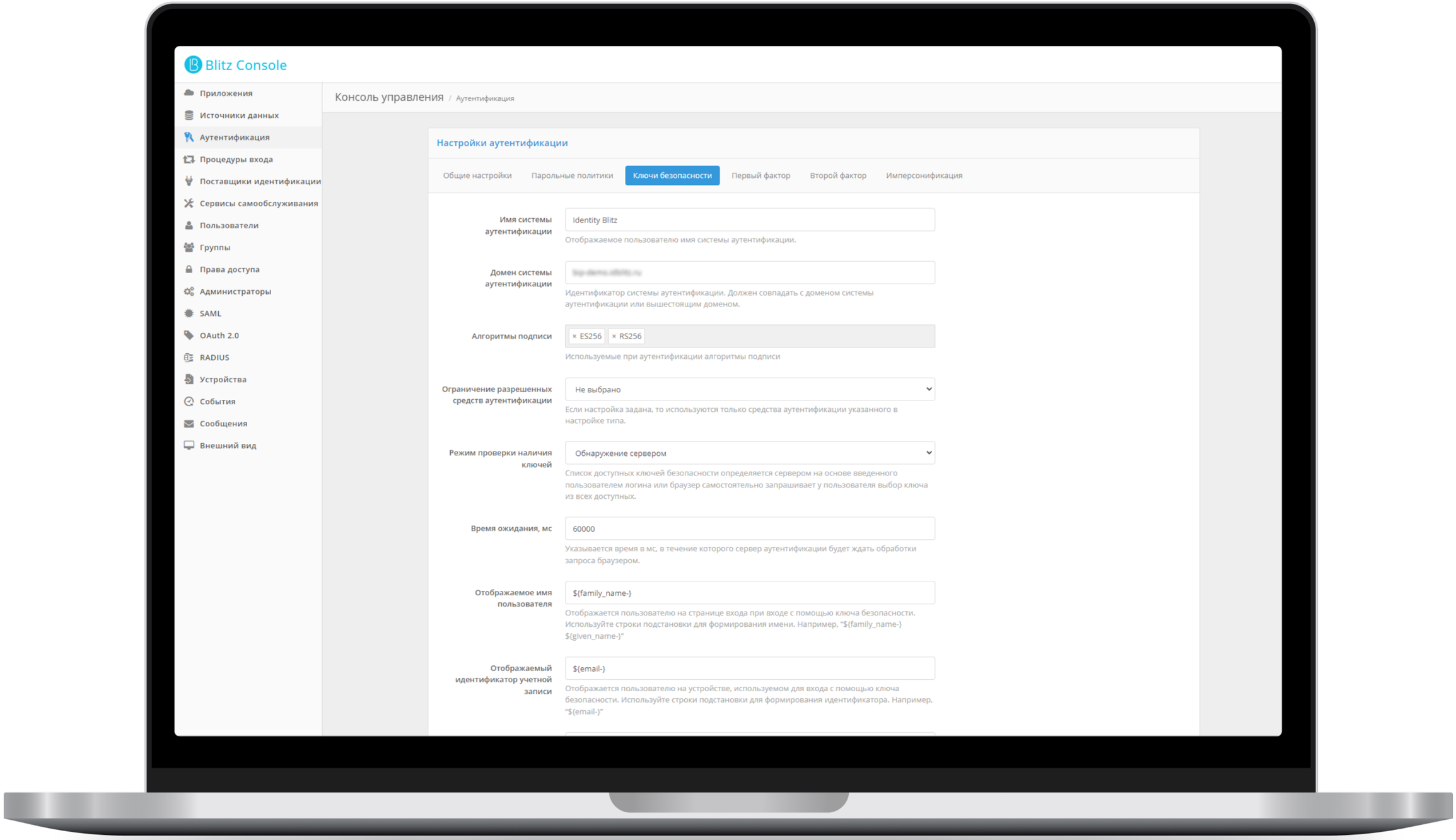

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Приложения
Параметры приложения
Идентификатор (entityID или client_id)
testkeeper
Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).
Название
testkeeper
Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider
Домен
localhost
Ссылка на стартовую страницу приложения, например, http://testdomain.ru/. При TLS-аутентификации приложения проверяется, что в сертификате приложения указан именно этот домен
Стартовая страница приложения
Ссылка на стартовую страницу приложения, например, http://testdomain.ru/private. При входе по SAML используется как ссылка перехода в приложение, если открывать страницу входа из истории браузера
Ключ шифрования идентификаторов
Если ключ задан, то идентификатор пользователя для приложения будет зашифрован с использованием данного ключа. Значение ключа можно выбрать из списка. Также можно назначить новый ключ, для этого введите его в строке поиска и нажмите Enter
Шаблон страниц
Шаблон страниц определяет внешний вид страниц входа. Если шаблон не указан, то используется шаблон по умолчанию.
Метки приложения
Позволяют помечать приложения определенными признаками. И использовать их при настройке логики работы с данным приложением, например, анализировать в процедуре входа
Удалить приложение
Сохранить

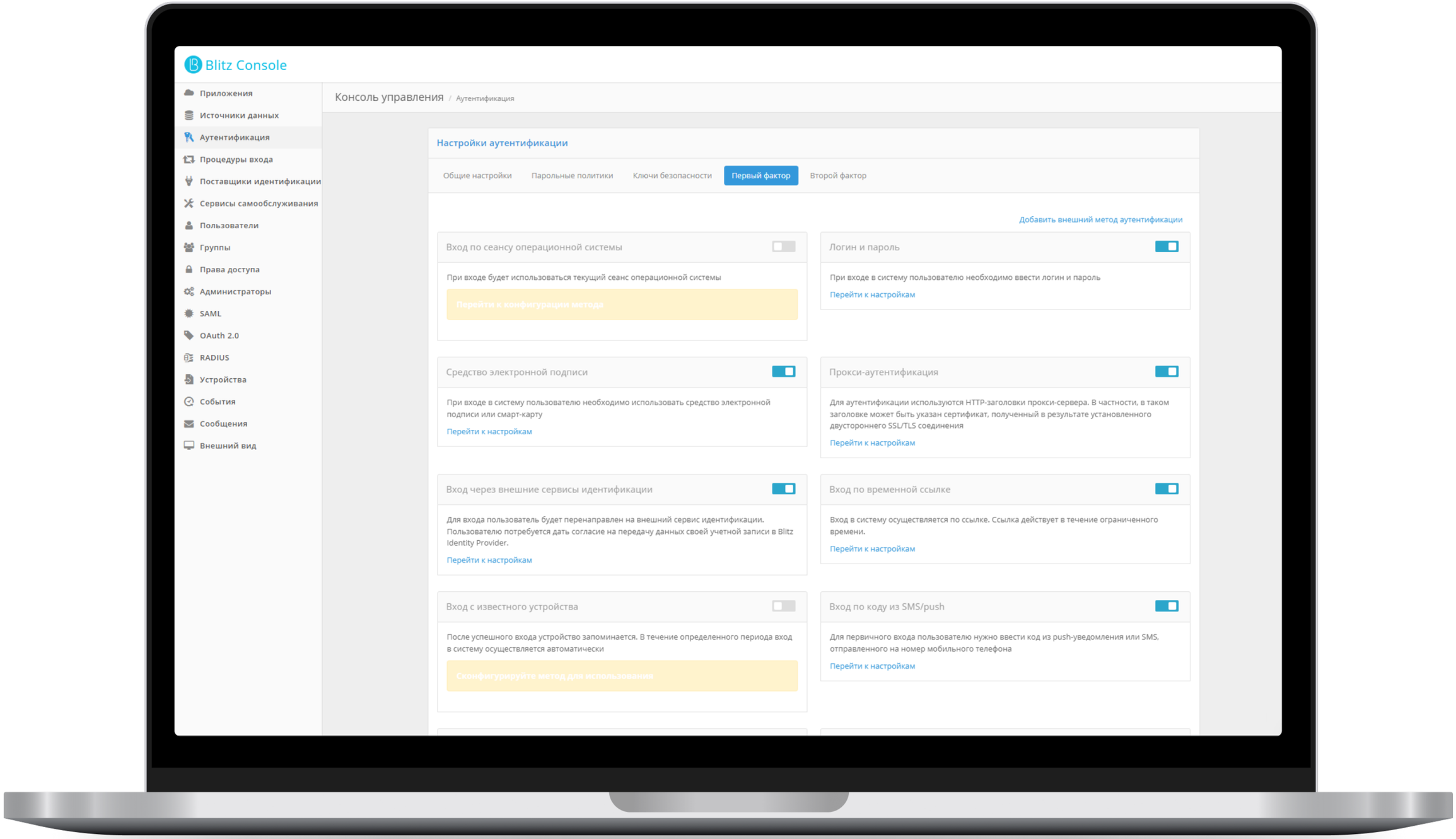

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Протоколы
SAML
OAuth 2.0
Simple
REST
RADIUS
Для корректной работы пропишите эти ссылки в настройках приложения, в которое будет осуществляться вход
URL для авторизации
/blitz/oauth/ae
На данный URL (authorization endpoint) должен быть направлен запрос на проведение авторизации пользователя
URL для получения и обновления маркера
/blitz/oauth/te
На данный URL (token endpoint) должен быть направлен запрос на получение или обновление маркера доступа
Статический клиент
Динамические клиенты
Настройки взаимодействия с приложением
Секрет (client_secret)
Секретный ключ подключаемого приложения (client_secret). Если указан, то именно этот секрет должен использоваться подключенным приложением при обращении к Blitz Identity Provider
Дополнительный секрет (client_secret)
Укажите дополнительный секрет для аутентификации приложения
Дополнительный секретный ключ подключаемого приложения (client_secret). Если указан, то может использоваться в качестве альтернативы к основному секрету
Предопределенная ссылка возврата (redirect_uri)
Введите предопределенный redirect_uri
URL, на который по умолчанию будет переадресован пользователь после прохождения авторизации (redirect_uri)
Префиксы ссылок возврата
https://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
testkeeper
openid
profile
blitz_api_sys_users
Разрешения (scope), которые будут доступны приложению.

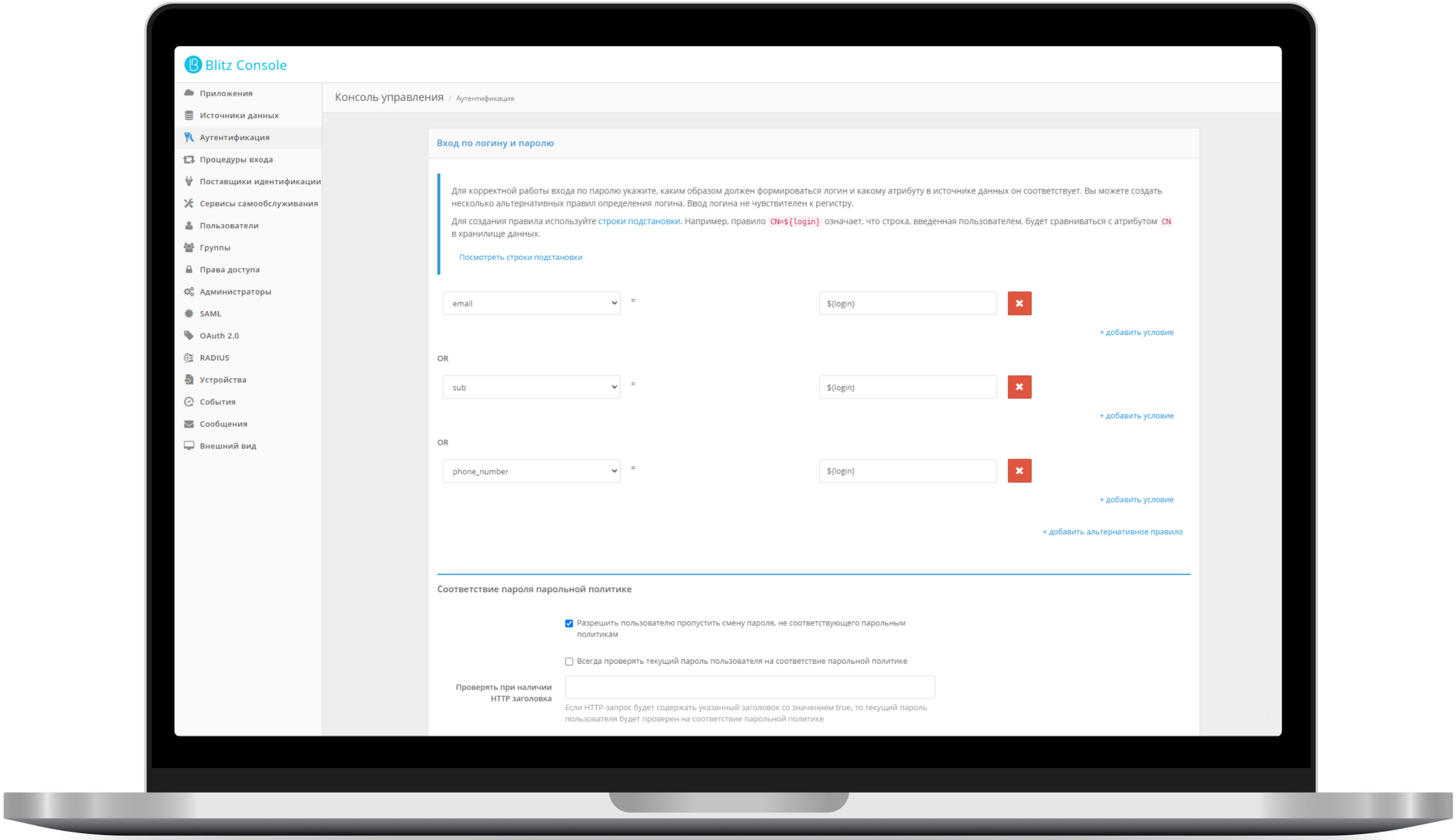

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Источники данных
Атрибуты
Хранимые атрибуты
Определите атрибуты учетной записи пользователя. Для этого задайте название – уникальное имя атрибута в системе. Название атрибута может отличаться от его имени во внешнем хранилище, в таком случае укажите правило преобразования в настройках этого хранилища.
Таже выберите тип значения – тип данных атрибута.
Укажите, какие атрибуты являются:
поисковыми (Поиск) - эти атрибуты будут учтены при поиске учетной записи в разделе «Пользователи», при использовании внешнего хранилища по этим атрибутам следует предусмотреть индекс;
обязательными (Обяз.) - эти атрибуты должны быть заданы при регистрации пользователя и не могут быть удалены в дальнейшем.
уникальными (Уник.) - значения этих атрибутов должны быть уникальны в системе.
Наименование атрибута
Тип значения
Поиск
Обяз.
Уник.
family_name
String
given_name
String
middle_name
String
email
String
+ Добавить атрибут
Вычисляемые атрибуты
При необходимости определите вычисляемые атрибуты – укажите их наименование, тип значения, а также настройте правило вычисления на основе хранимых атрибутов.
Вычисляемому атрибуту может быть присвоено константное значение.
Примеры настройки
Наименование атрибута
Тип значения
Правило вычисления

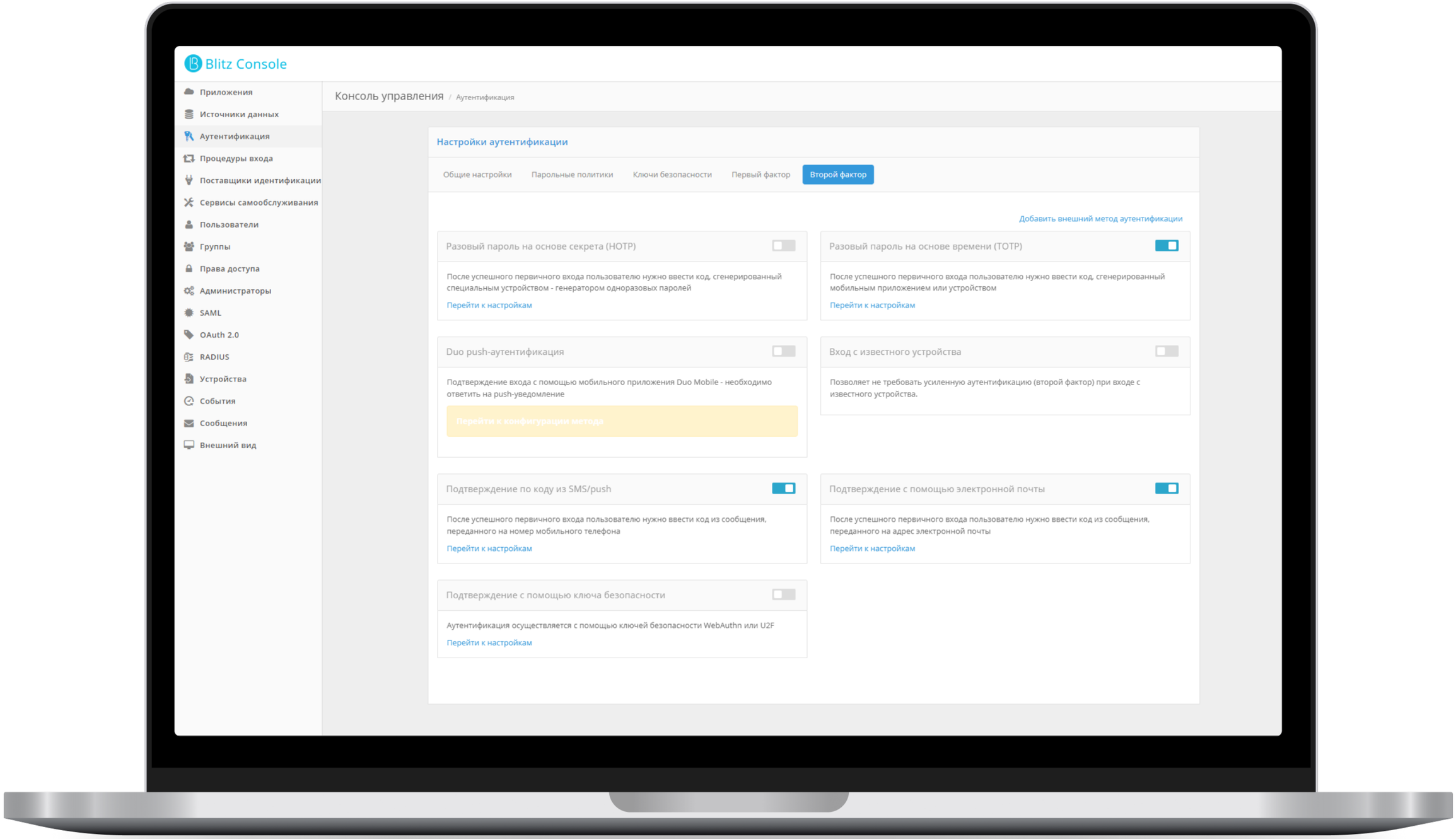

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Аутентификация
Настройки аутентификации
Общие настройки
Парольные политики
Ключи безопасности
Первый фактор
Второй фактор
Уровень аутентификации по умолчанию
Первый фактор
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 при бездействии пользователя
3600
Укажите время (в секундах), в течение которого будет сохранена сессия при бездействии пользователя, т.е. при отсутствии переходов между разными приложениями
Максимальная продолжительность сессии
10800
Укажите время (в секундах), в течение которого будет сохранена сессия независимо от наличия действий пользователя
Время отображения экрана логаута, сек.
2
Запоминание учетных записей
Включено
Запоминание учетных записей
Запоминать все учетные записи
Отображаемое имя пользователя
Здравствуйте, ${given_name-}!
Отображаемый идентификатор пользователя
${email-}
Отображать аватар

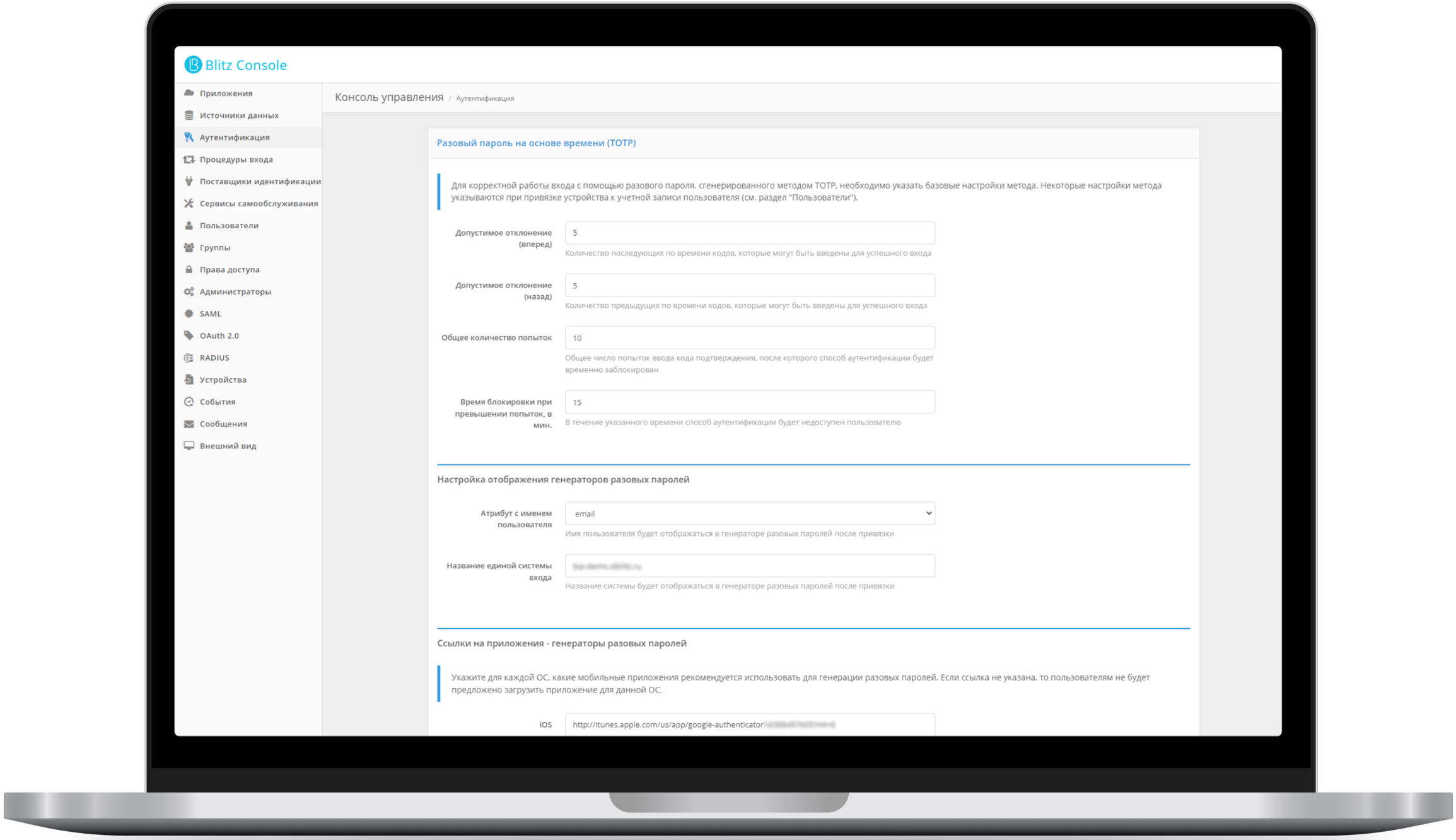

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Аутентификация
Настройки аутентификации
Общие настройки
Парольные политики
Ключи безопасности
Первый фактор
Второй фактор
Сложность пароля
Минимальная длина пароля
8
Укажите минимальное количество символов в пароле
Словарь паролей
Обзор...
Выберите файл со словарем паролей, где каждый пароль размещен на новой строке. Формат файла должен быть txt.
Группы символов
4
Задайте минимальное количество групп символов, необходимых в пароле
Название группы
Допустимые символы
Минимум символов
Цифры
[0-9]
1
Нижний регистр
[a-z]
1
Верхний регистр
[A-Z]
1
Специальные символы
[!@#$%^&.*()+\-?.,;:'`"{}\[\]><=~/_]
1
Политика повторного использования
Запрет использования старых паролей, шт.
5
Минимальное время жизни пароля, сек.
86400

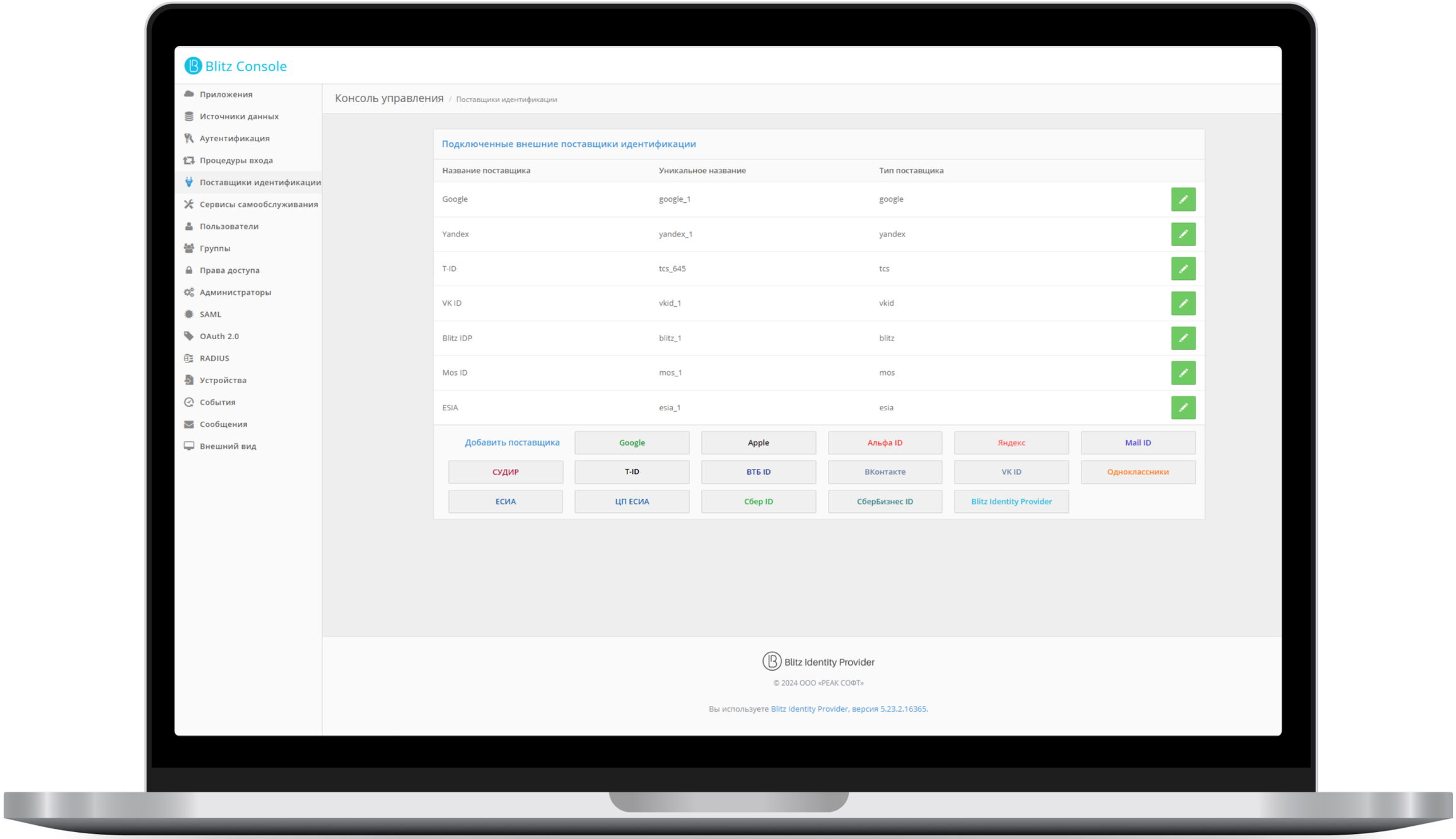

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Аутентификация
Настройки аутентификации
Общие настройки
Парольные политики
Ключи безопасности
Первый фактор
Второй фактор
Имперсонификация
Имя системы аутентификации
Identity Blitz
Отображаемое пользователю имя системы аутентификации.
Домен системы аутентификации
Идентификатор системы аутентификации. Должен совпадать с доменом системы аутентификации или вышестоящим доменом.
Алгоритмы подписи
× ES256 × RS256
Используемые при аутентификации алгоритмы подписи
Ограничение разрешенных средств аутентификации
Не выбрано
Если настройка задана, то используются только средства аутентификации указанного в настройке типа.
Режим проверки наличия ключей
Обнаружение сервером
Список доступных ключей безопасности определяется сервером на основе введенного пользователем логина или браузер самостоятельно запрашивает у пользователя выбор ключа из всех доступных.
Время ожидания, мс
60000
Указывается время в мс, в течение которого сервер аутентификации будет ждать обработки запроса браузером.
Отображаемое имя пользователя
${family_name-}
Отображается пользователю на странице входа при входе с помощью ключа безопасности. Используйте строки подстановки для формирования имени. Например, "${family_name-} ${given_name-}"
Отображаемый идентификатор учетной записи
${email-}
Отображается пользователю на устройстве, используемом для входа с помощью ключа безопасности. Используйте строки подстановки для формирования идентификатора. Например, "${email-}"

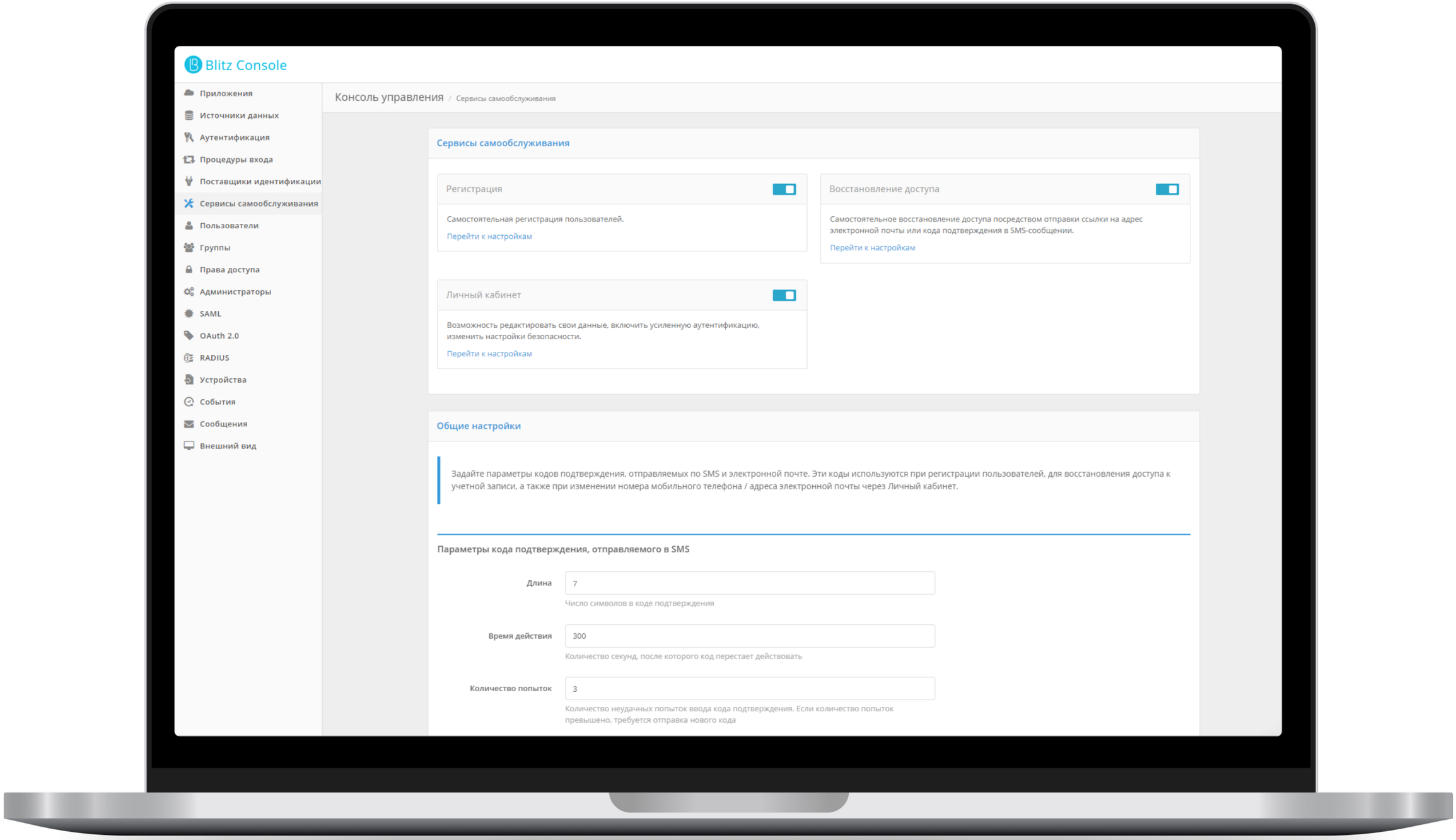

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Аутентификация
Настройки аутентификации
Общие настройки
Парольные политики
Ключи безопасности
Первый фактор
Второй фактор
Добавить внешний метод аутентификации
Вход по сеансу операционной системы
При входе будет использоваться текущий сеанс операционной системы
Перейти к конфигурации метода
Логин и пароль
При входе в систему пользователю необходимо ввести логин и пароль
Перейти к настройкам
Средство электронной подписи
При входе в систему пользователю необходимо использовать средство электронной подписи или смарт-карту
Перейти к настройкам
Прокси-аутентификация
Для аутентификации используются HTTP-заголовки прокси-сервера. В частности, в таком заголовке может быть указан сертификат, полученный в результате установленного двустороннего SSL/TLS соединения
Перейти к настройкам
Вход через внешние сервисы идентификации
Для входа пользователь будет перенаправлен на внешний сервис идентификации. Пользователю потребуется дать согласие на передачу данных своей учетной записи в Blitz Identity Provider.
Перейти к настройкам
Вход по временной ссылке
Вход в систему осуществляется по ссылке. Ссылка действует в течение ограниченного времени.
Перейти к настройкам
Вход с известного устройства
После успешного входа устройство запоминается. В течение определенного периода вход в систему осуществляется автоматически
Сконфигурируйте метод для использования
Вход по коду из SMS/push
Для первичного входа пользователю нужно ввести код из push-уведомления или SMS, отправленного на номер мобильного телефона
Перейти к настройкам

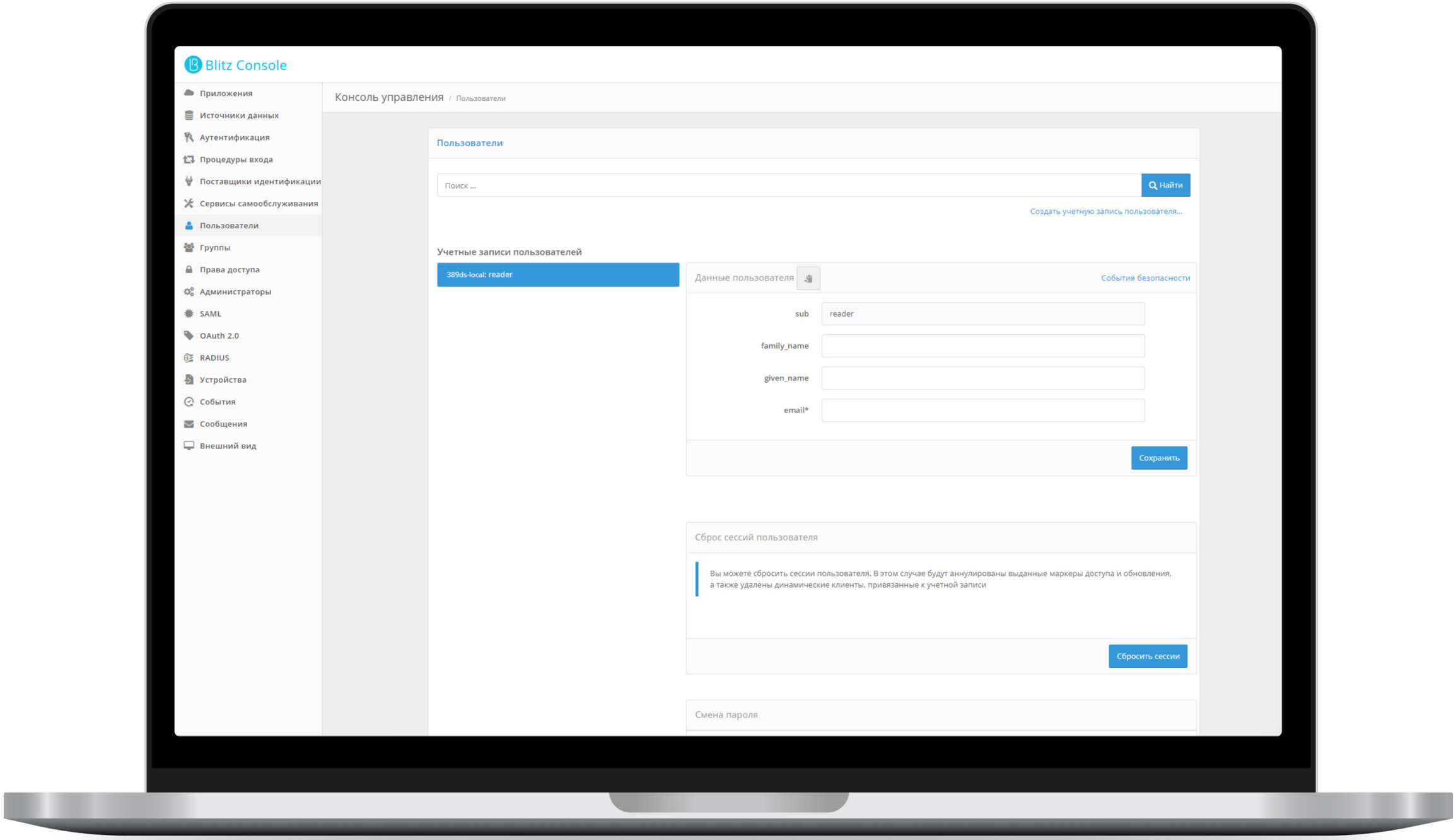

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Аутентификация
Вход по логину и паролю
Для корректной работы входа по паролю укажите, каким образом должен формироваться логин и какому атрибуту в источнике данных он соответствует. Вы можете создать несколько альтернативных правил определения логина. Ввод логина не чувствителен к регистру.
Для создания правила используйте строки подстановки. Например, правило CN=${login} означает, что строка, введенная пользователем, будет сравниваться с атрибутом CN в хранилище данных.
Посмотреть строки подстановки
email = ${login}
+ добавить условие
OR
sub = ${login}
+ добавить условие
OR
phone_number = ${login}
+ добавить условие
+ добавить альтернативное правило
Соответствие пароля парольной политике
Разрешить пользователю пропустить смену пароля, не соответствующего парольным политикам
Всегда проверять текущий пароль пользователя на соответствие парольной политике
Проверять при наличии HTTP заголовка
Если HTTP-запрос будет содержать указанный заголовок со значением true, то текущий пароль пользователя будет проверен на соответствие парольной политике

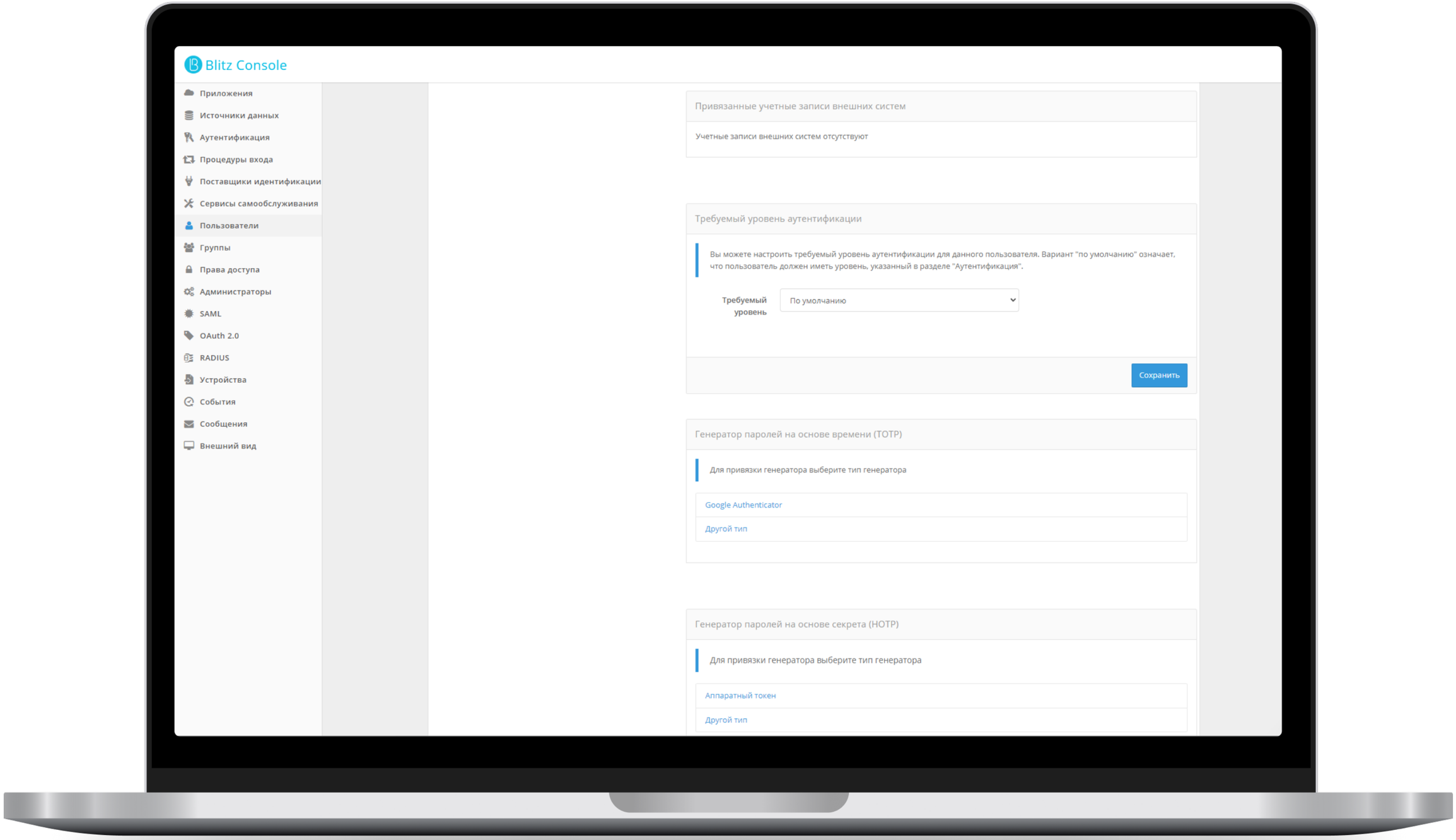

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Аутентификация
Настройки аутентификации
Общие настройки
Парольные политики
Ключи безопасности
Первый фактор
Второй фактор
Добавить внешний метод аутентификации
Разовый пароль на основе секрета (HOTP)
После успешного первичного входа пользователю нужно ввести код, сгенерированный специальным устройством - генератором одноразовых паролей
Перейти к настройкам
Разовый пароль на основе времени (TOTP)
После успешного первичного входа пользователю нужно ввести код, сгенерированный мобильным приложением или устройством
Перейти к настройкам
Duo push-аутентификация
Подтверждение входа с помощью мобильного приложения Duo Mobile - необходимо ответить на push-уведомление
Перейти к конфигурации метода
Вход с известного устройства
Позволяет не требовать усиленную аутентификацию (второй фактор) при входе с известного устройства.
Подтверждение по коду из SMS/push
После успешного первичного входа пользователю нужно ввести код из сообщения, переданного на номер мобильного телефона
Перейти к настройкам
Подтверждение с помощью электронной почты
После успешного первичного входа пользователю нужно ввести код из сообщения, переданного на адрес электронной почты
Перейти к настройкам
Подтверждение с помощью ключа безопасности
Аутентификация осуществляется с помощью ключей безопасности WebAuthn или U2F
Перейти к настройкам

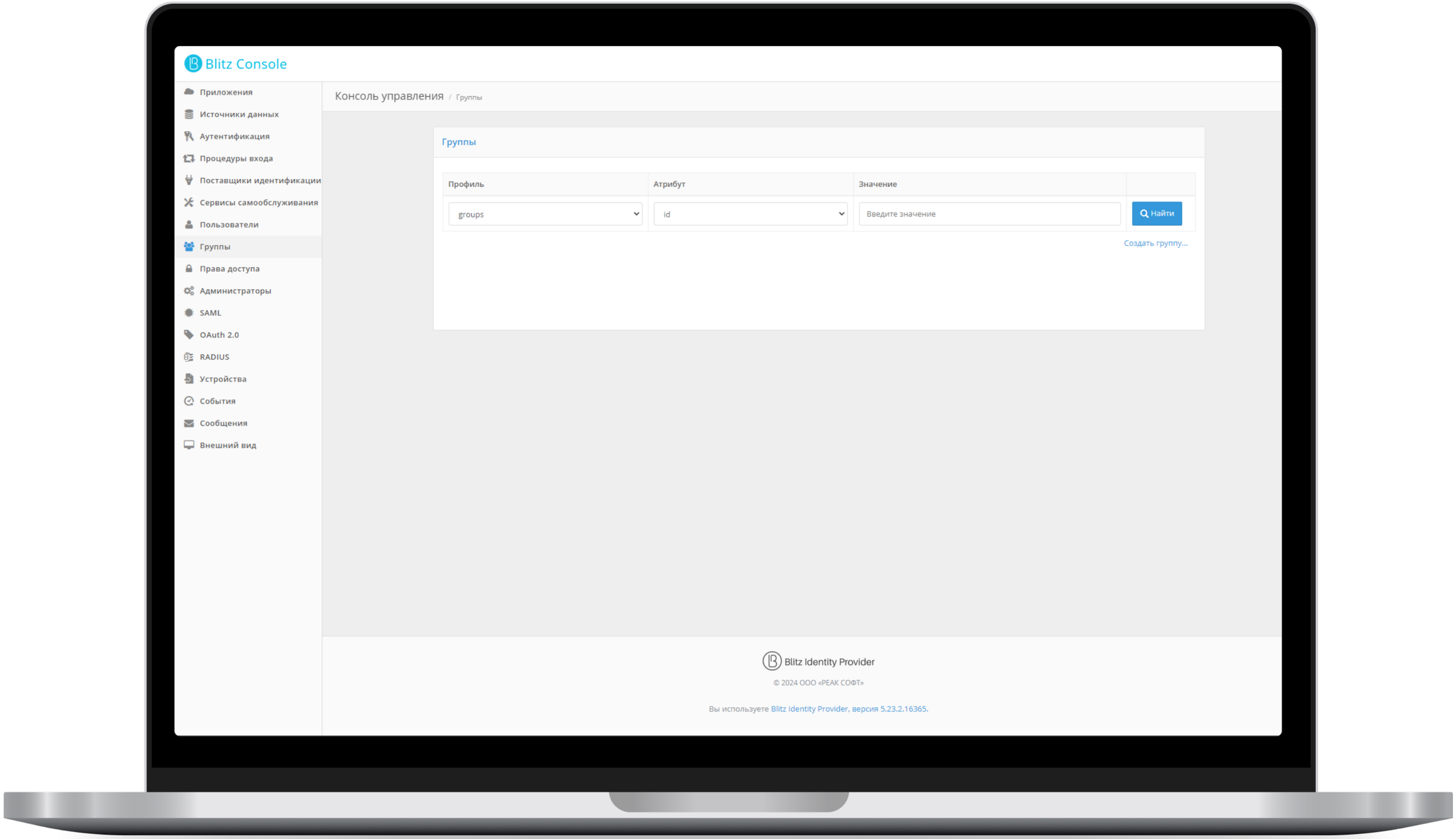

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Аутентификация
Разовый пароль на основе времени (TOTP)
Для корректной работы входа с помощью разового пароля, сгенерированного методом TOTP, необходимо указать базовые настройки метода. Некоторые настройки метода указываются при привязке устройства к учетной записи пользователя (см. раздел "Пользователи").
Допустимое отклонение (вперед)
5
Количество последующих по времени кодов, которые могут быть введены для успешного входа
Допустимое отклонение (назад)
5
Количество предыдущих по времени кодов, которые могут быть введены для успешного входа
Общее количество попыток
10
Общее число попыток ввода кода подтверждения, после которого способ аутентификации будет временно заблокирован
Время блокировки при превышении попыток, в мин.
15
В течение указанного времени способ аутентификации будет недоступен пользователю
Настройка отображения генераторов разовых паролей
Атрибут с именем пользователя
email
Имя пользователя будет отображаться в генераторе разовых паролей после привязки
Название единой системы входа
Название системы будет отображаться в генераторе разовых паролей после привязки
Ссылки на приложения - генераторы разовых паролей
Укажите для каждой ОС, какие мобильные приложения рекомендуется использовать для генерации разовых паролей. Если ссылка не указана, то пользователям не будет предложено загрузить приложение для данной ОС.
iOS
http://itunes.apple.com/us/app/google-authenticator

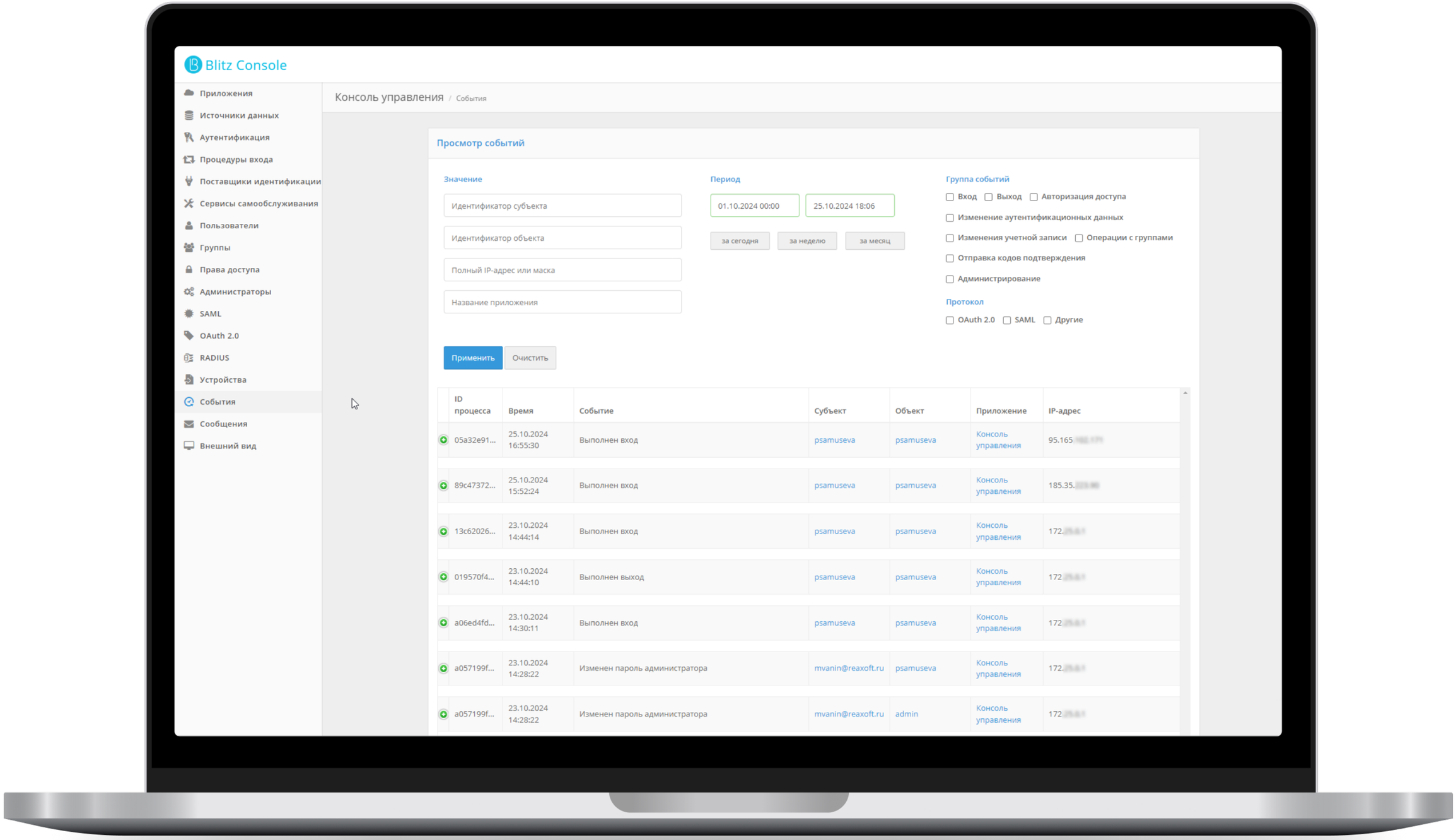

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Поставщики идентификации
Подключенные внешние поставщики идентификации
Название поставщика
Уникальное название
Тип поставщика
Google
google_1
google
Yandex
yandex_1
yandex
T-ID
tcs_645
tcs
VK ID
vkid_1
vkid
Blitz IDP
blitz_1
blitz
Mos ID
mos_1
mos
ESIA
esia_1
esia
Добавить поставщика
Google
Apple
Альфа ID
Яндекс
Mail ID
СУДИР
T-ID
ВТБ ID
ВКонтакте
VK ID
Одноклассники
ЕСИА
ЦП ЕСИА
Сбер ID
СберБизнес ID
Blitz Identity Provider
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»
Вы используете Blitz Identity Provider, версия 5.23.2.16365.

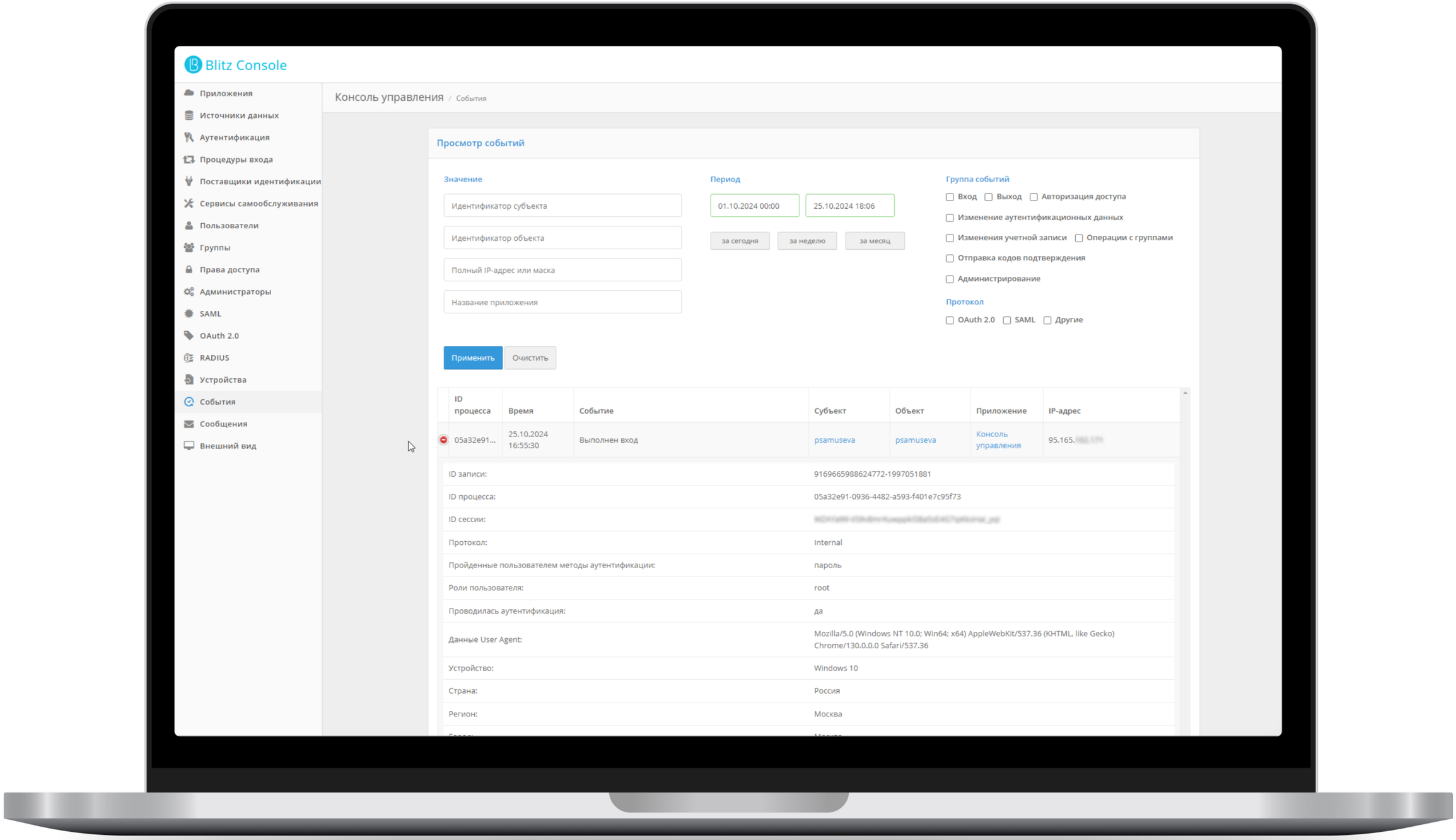

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Сервисы самообслуживания
Сервисы самообслуживания
Регистрация
Самостоятельная регистрация пользователей.
Перейти к настройкам
Восстановление доступа
Самостоятельное восстановление доступа посредством отправки ссылки на адрес электронной почты или кода подтверждения в SMS-сообщении.
Перейти к настройкам
Личный кабинет
Возможность редактировать свои данные, включить усиленную аутентификацию, изменить настройки безопасности.
Перейти к настройкам
Общие настройки
Задайте параметры кодов подтверждения, отправляемых по SMS и электронной почте. Эти коды используются при регистрации пользователей, для восстановления доступа к учетной записи, а также при изменении номера мобильного телефона / адреса электронной почты через Личный кабинет.
Параметры кода подтверждения, отправляемого в SMS
Длина
7
Число символов в коде подтверждения
Время действия
300
Количество секунд, после которого код перестает действовать
Количество попыток
3
Количество неудачных попыток ввода кода подтверждения. Если количество попыток превышено, требуется отправка нового кода

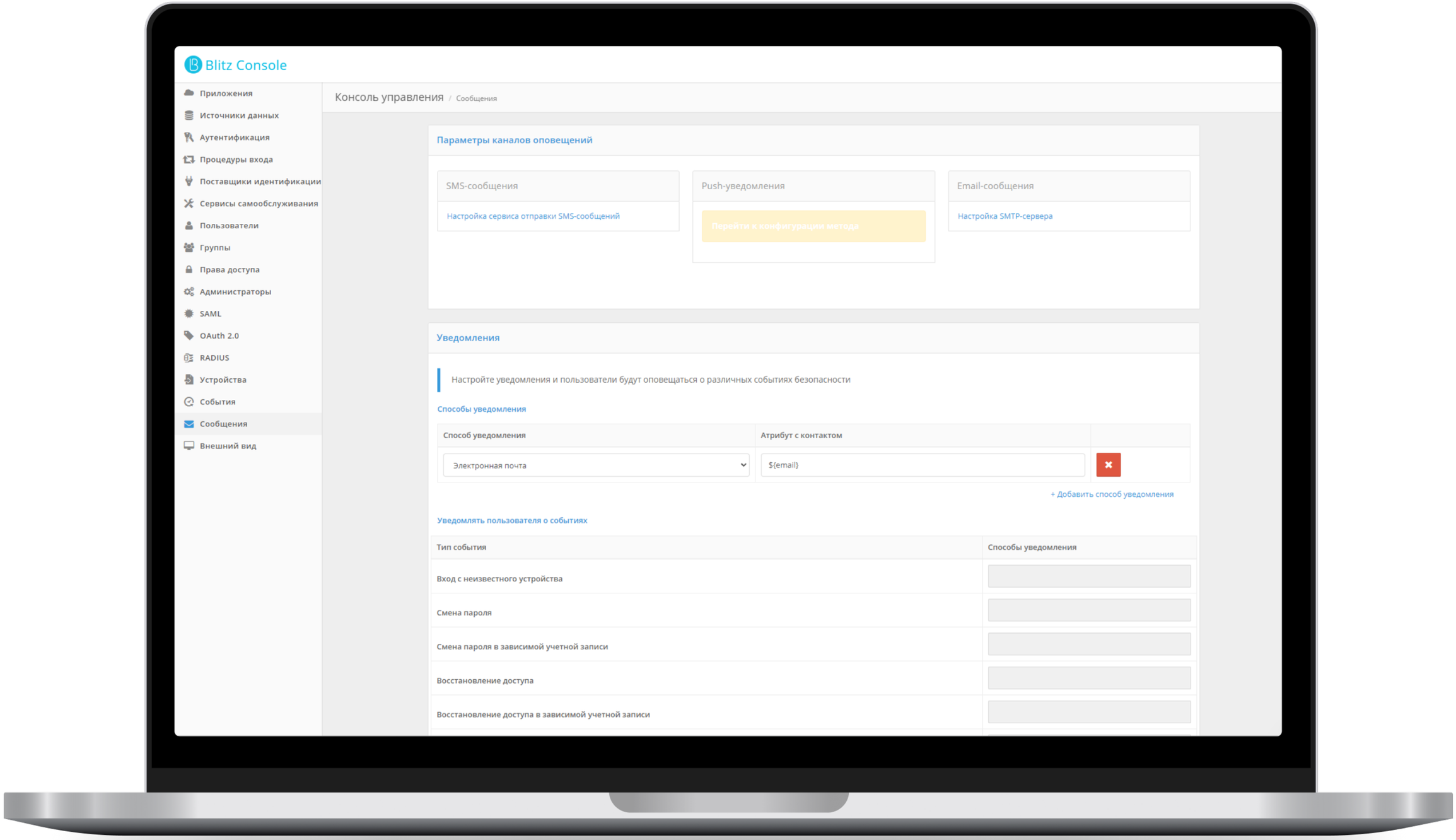

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Пользователи
Пользователи
Поиск ...
Найти
Создать учетную запись пользователя...
Учетные записи пользователей
389ds-local: reader
Данные пользователя
События безопасности
sub
reader
family_name
given_name
email*
Сохранить
Сброс сессий пользователя
Вы можете сбросить сессии пользователя. В этом случае будут аннулированы выданные маркеры доступа и обновления, а также удалены динамические клиенты, привязанные к учетной записи
Сбросить сессии
Смена пароля

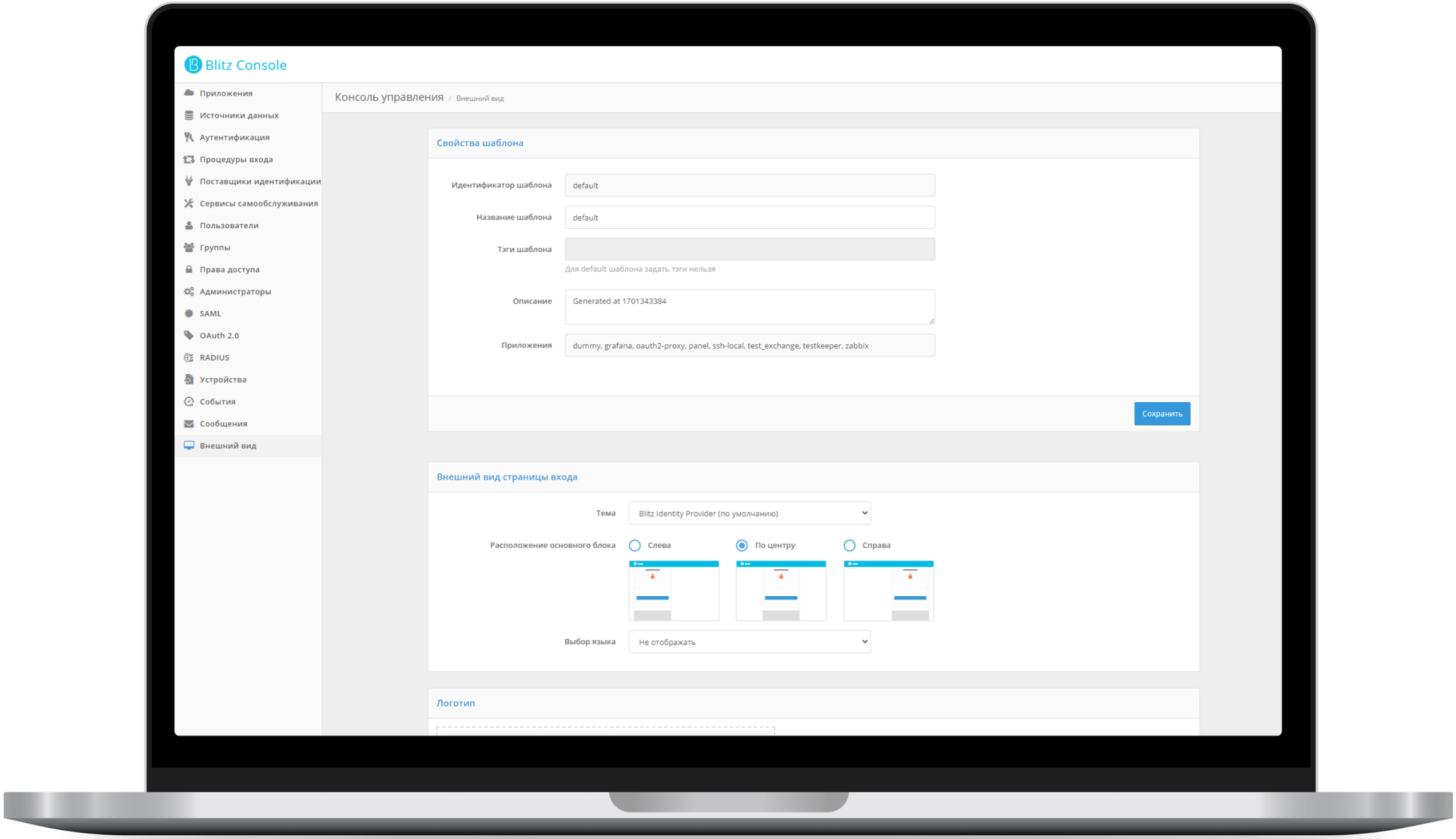

Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Привязанные учетные записи внешних систем
Учетные записи внешних систем отсутствуют
Требуемый уровень аутентификации
Вы можете настроить требуемый уровень аутентификации для данного пользователя. Вариант "по умолчанию" означает, что пользователь должен иметь уровень, указанный в разделе "Аутентификация".
Требуемый уровень
По умолчанию
Сохранить
Генератор паролей на основе времени (TOTP)
Для привязки генератора выберите тип генератора
Google Authenticator
Другой тип
Генератор паролей на основе секрета (HOTP)
Для привязки генератора выберите тип генератора
Аппаратный токен
Другой тип


Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Группы
Группы
Профиль
Атрибут
Значение
groups
id
Введите значение
Найти
Создать группу...
Blitz Identity Provider
© 2024 ООО «РЕАК СОФТ»
Вы используете Blitz Identity Provider, версия 5.23.2.16365.


Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / События
Просмотр событий
Значение
Идентификатор субъекта
Идентификатор объекта
Полный IP-адрес или маска
Название приложения
Период
01.10.2024 00:00
25.10.2024 18:06
за сегодня
за неделю
за месяц
Группа событий
Вход
Выход
Авторизация доступа
Изменение аутентификационных данных
Изменения учетной записи
Операции с группами
Отправка кодов подтверждения
Администрирование
Протокол
OAuth 2.0
SAML
Другие
Применить
Очистить
ID процесса
Время
Событие
Субъект
Объект
Приложение
IP-адрес
05a32e91...
25.10.2024 16:55:30
Выполнен вход
psamuseva
psamuseva
Консоль управления
95.165
89c47372...
25.10.2024 15:52:24
Выполнен вход
psamuseva
psamuseva
Консоль управления
185.35.
13c62026...
23.10.2024 14:44:14
Выполнен вход
psamuseva
psamuseva
Консоль управления
172.
019570f4...
23.10.2024 14:44:10
Выполнен выход
psamuseva
psamuseva
Консоль управления
172.
a06ed4fd...
23.10.2024 14:30:11
Выполнен вход
psamuseva
psamuseva
Консоль управления
172.
a057199f...
23.10.2024 14:28:22
Изменен пароль администратора
mvanin@reaxoft.ru
psamuseva
Консоль управления
172.
a057199f...
23.10.2024 14:28:22
Изменен пароль администратора
mvanin@reaxoft.ru
admin
Консоль управления
172.


Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / События
Просмотр событий
Значение
Идентификатор субъекта
Идентификатор объекта
Полный IP-адрес или маска
Название приложения
Период
01.10.2024 00:00
25.10.2024 18:06
за сегодня
за неделю
за месяц
Группа событий
Вход
Выход
Авторизация доступа
Изменение аутентификационных данных
Изменения учетной записи
Операции с группами
Отправка кодов подтверждения
Администрирование
Протокол
OAuth 2.0
SAML
Другие
Применить
Очистить
ID процесса
Время
Событие
Субъект
Объект
Приложение
IP-адрес
05a32e91...
25.10.2024 16:55:30
Выполнен вход
psamuseva
psamuseva
Консоль управления
95.165.
ID записи:
9169665988624772-1997051881
ID процесса:
05a32e91-0936-4482-a593-f401e7c95f73
ID сессии:
Протокол:
Internal
Пройденные пользователем методы аутентификации:
пароль
Роли пользователя:
root
Проводилась аутентификация:
да
Данные User Agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36
Устройство:
Windows 10
Страна:
Россия
Регион:
Москва


Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Сообщения
Параметры каналов оповещений
SMS-сообщения
Настройка сервиса отправки SMS-сообщений
Push-уведомления
Перейти к конфигурации метода
Email-сообщения
Настройка SMTP-сервера
Уведомления
Настройте уведомления и пользователи будут оповещаться о различных событиях безопасности
Способы уведомления
Способ уведомления
Атрибут с контактом
Электронная почта
${email}
+ Добавить способ уведомления
Уведомлять пользователя о событиях
Тип события
Способы уведомления
Вход с неизвестного устройства
Смена пароля
Смена пароля в зависимой учетной записи
Восстановление доступа
Восстановление доступа в зависимой учетной записи


Blitz Console
Приложения
Источники данных
Аутентификация
Процедуры входа
Поставщики идентификации
Сервисы самообслуживания
Пользователи
Группы
Права доступа
Администраторы
SAML
OAuth 2.0
RADIUS
Устройства
События
Сообщения
Внешний вид
Консоль управления / Внешний вид
Свойства шаблона
Идентификатор шаблона
default
Название шаблона
default
Тэги шаблона
Для default шаблона задать тэги нельзя
Описание
Generated at 1701343384
Приложения
dummy, grafana, oauth2-proxy, panel, ssh-local, test_exchange, testkeeper, zabbix
Сохранить
Внешний вид страницы входа
Тема
Blitz Identity Provider (по умолчанию)
Расположение основного блока
Слева
По центру
Справа
Выбор языка
Не отображать
Логотип

identityblitz.ru