ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «BLITZ IDENTITY PROVIDER»

Версия 5.31

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

1147746651733.62.01.000.001.И2

Москва, 2025

Оглавление

Глава 1

Введение

1.1 Общая информация

Система аутентификации Blitz Identity Provider предназначена для обеспечения возможности пользователям использовать единую учетную запись для входа в корпоративные веб-сайты и приложения без многократного ввода логина и пароля при переключении между различными формами входа.

> **Важно**
>
> Технология единого входа Blitz Identity Provider не требует установки специальных программ на устройства пользователя и работает с основными популярными клиентскими операционными системами и типами устройств (ПК, планшеты, смартфоны).

Система аутентификации Blitz Identity Provider предназначена для доступа пользователей к ресурсам как внутрикорпоративной сети, так и к внешним Интернет-ресурсам. Для каждой компании и сферы применения могут быть настроены свои правила доступа, внешний вид единой страницы входа и использоваться наиболее подходящие методы авторизации.

В стандартной конфигурации Blitz Identity Provider пользователи могут использовать свой корпоративный адрес электронной почты и пароль для доступа в Личный кабинет. При доступе из внутрикорпоративной сети со своего рабочего ПК возможен режим автоматического входа, когда доступ осуществляется на основе результатов входа в корпоративный домен в процессе включения ПК. В зависимости от конфигурации Blitz Identity Provider, помимо входа с помощью логина и пароля, возможен также вход с помощью кода подтверждения из SMS-сообщения или с использованием различных внешних сервисов идентификации, однако их перечень также зависит от настроек Blitz Identity Provider, установленных организацией.

При включенной двухфакторной аутентификации пользователю дополнительно к вводу логина и пароля может быть запрошен ввод кода подтверждения, полученного в SMS-сообщении или сгенерированного в специальном мобильном приложении. Привязка номера мобильного телефона и/или мобильного приложения осуществляется пользователем самостоятельно через Личный кабинет.

Безопасная работа Blitz Identity Provider обеспечивается посредством правильной установки и настройки, которые должны осуществляться в соответствии с Руководством администратора.

1.2 Режимы работы

Режим функционирования Blitz Identity Provider

24 часа/7 дней в неделю.

Периоды пиковой нагрузки

Зависят от графика работы, принятого внутри компании, но обычно это интервал 9:00 – 18:00, понедельник – пятница.

Продолжительность сервисного обслуживания

5 часов в месяц.

Предпочтительный интервал сервисного обслуживания

21:00 – 6:00.

Периодичность и сроки проведения регламентных работ на серверах ЦОД оператора Blitz Identity Provider

- ежедневно: с 22:00 до 22:20 – сбор статистики, автоматический анализ sql-запросов;
- ежедневно: с 02:00 до 03:00 – обновление аналитических данных в случае взаимодействия с информационными системами;
- ежедневно: с 3:00 до 5:00 – резервное копирование данных;
- периодически: с 19:00 до 21:00 – плановые работы, установка периодических обновлений;
- периодически: по необходимости – прочие работы по массовому изменению данных (выверка данных, приведение форматов к единому виду и т. п.) – после предварительного согласования с обслуживающим персоналом, выполняющим функции администрирования Blitz Identity Provider.

Режимы функционирования

- штатный режим, в котором компоненты исправно выполняют все свои основные функции;
- сервисный режим, в котором проводятся реконфигурация, обновления программного обеспечения (далее – ПО) и профилактическое обслуживание;
- аварийный режим, в котором один или несколько критических компонентов Blitz Identity Provider не выполняют свои функции.

Важно

Для обеспечения штатного режима функционирования Blitz Identity Provider необходимо выполнять требования и выдерживать условия эксплуатации ПО и комплекса технических средств, указанные в соответствующих документах (техническая документация, инструкции по эксплуатации и т. д.).

В сервисном режиме функционирования Blitz Identity Provider обеспечивается доступ уполномоченных работников для проведения следующих работ:

- регламентное обслуживание общесистемного и прикладного ПО, баз данных;
- обновление версий ПО и баз данных;
- восстановление после сбоев и аварийных ситуаций;
- проверка функций мониторинга;
- иные работы, необходимые для функционирования Blitz Identity Provider в соответствии с требованиями ТЗ и ЧТЗ, согласованные с Заказчиком.

Предупреждение

При нахождении Blitz Identity Provider в сервисном режиме возможно ограничение доступа пользователей к системе, некоторым модулям и/или функциям Blitz Identity Provider.

Аварийный режим функционирования характеризуется отказом одного или нескольких критических компонентов программного и (или) технического обеспечения.

Предупреждение

При нахождении в аварийном режиме доступ пользователей к Blitz Identity Provider будет невозможен.

Уполномоченным работникам и/или администраторам необходимо будет выполнить комплекс мероприятий по устранению причины перехода Blitz Identity Provider в аварийный режим.

1.3 Ошибки и способы их устранения

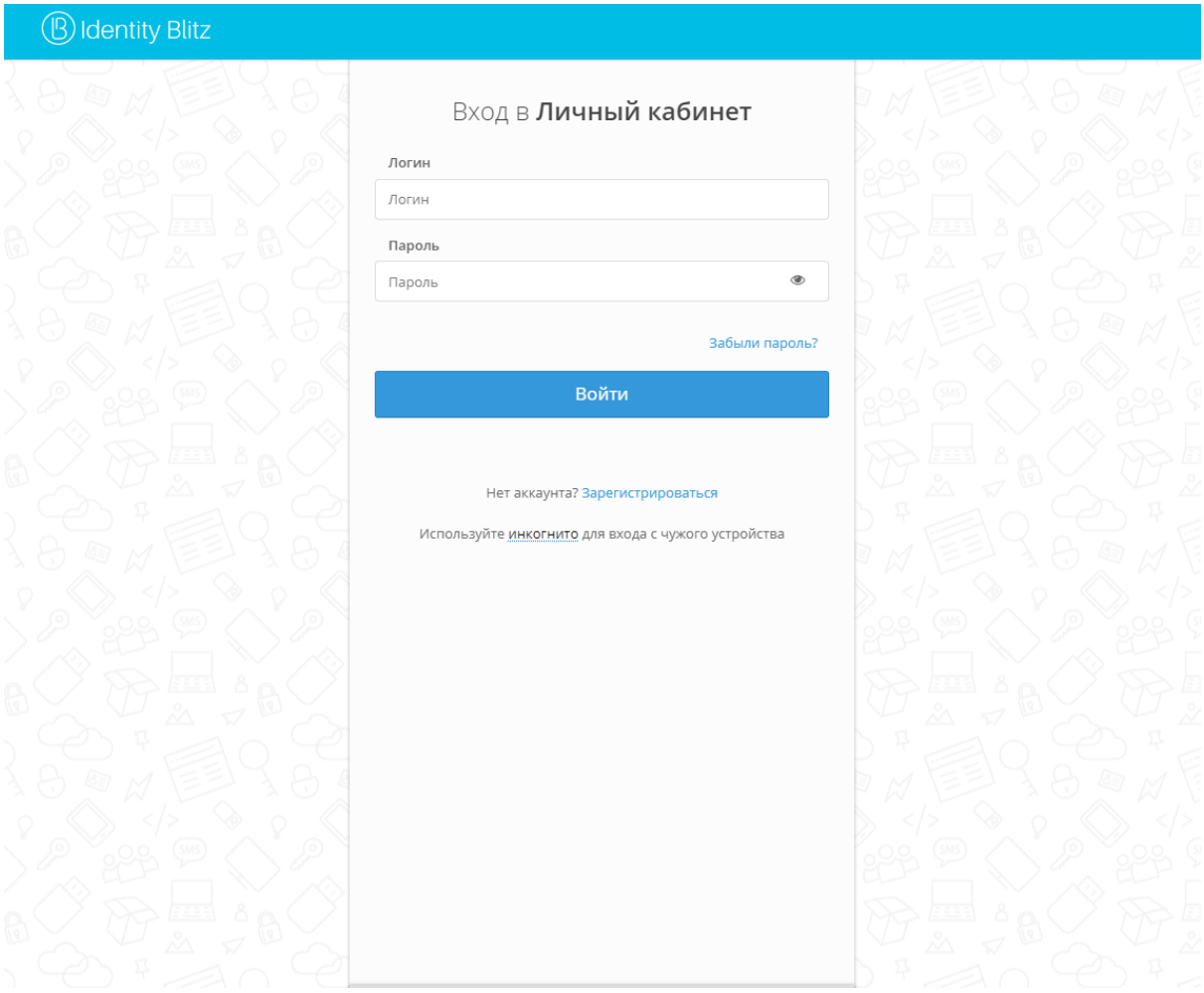
№	Ситуация	Способ устранения ошибки
1	Ошибка ввода при указании логина и/или пароля.	Заново ввести логин и пароль, проверив на отсутствие лишних символов и пробелов.
2	Ошибка входа с использованием сеанса операционной системы.	Убедиться, что ПК входит в домен, вход осуществляется из корпоративной сети, с момента аутентификации на ПК не прошло много времени (например, не более 8 часов), настройки браузера не препятствуют использованию режима автоматического входа. Если все условия соблюдены, то попробовать войти повторно.
3	Ошибка входа с использованием сеанса операционной системы.	Авторизоваться по электронной почте и паролю.
4	Ошибка входа при включенной двухфакторной аутентификации.	Убедиться, что у пользователя настроен хотя бы один способ получения кода подтверждения. Если ни один способ не настроен, то необходимо обратиться к системному администратору организации.
5	Повторение ошибки входа, невозможность войти другими способами.	Необходимо обратиться к системному администратору организации.

Глава 2

Вход пользователя в Личный Кабинет

2.1 Вход с помощью логина и пароля

При входе в приложение, защищенное Blitz Identity Provider, обычно открывается страница входа Blitz Identity Provider. В стандартной конфигурации по умолчанию пользователю предлагается войти по логину и паролю. Стандартный вид единой страницы входа с помощью логина и пароля представлен на рисунке ниже, однако внешний вид единой страницы входа может отличаться в зависимости от настроек Blitz Identity Provider, установленных организацией.



В качестве логина в зависимости от конфигурации системы аутентификации, установленной организацией, пользователи могут использовать, например, свой адрес электронной почты, мобильный телефон или

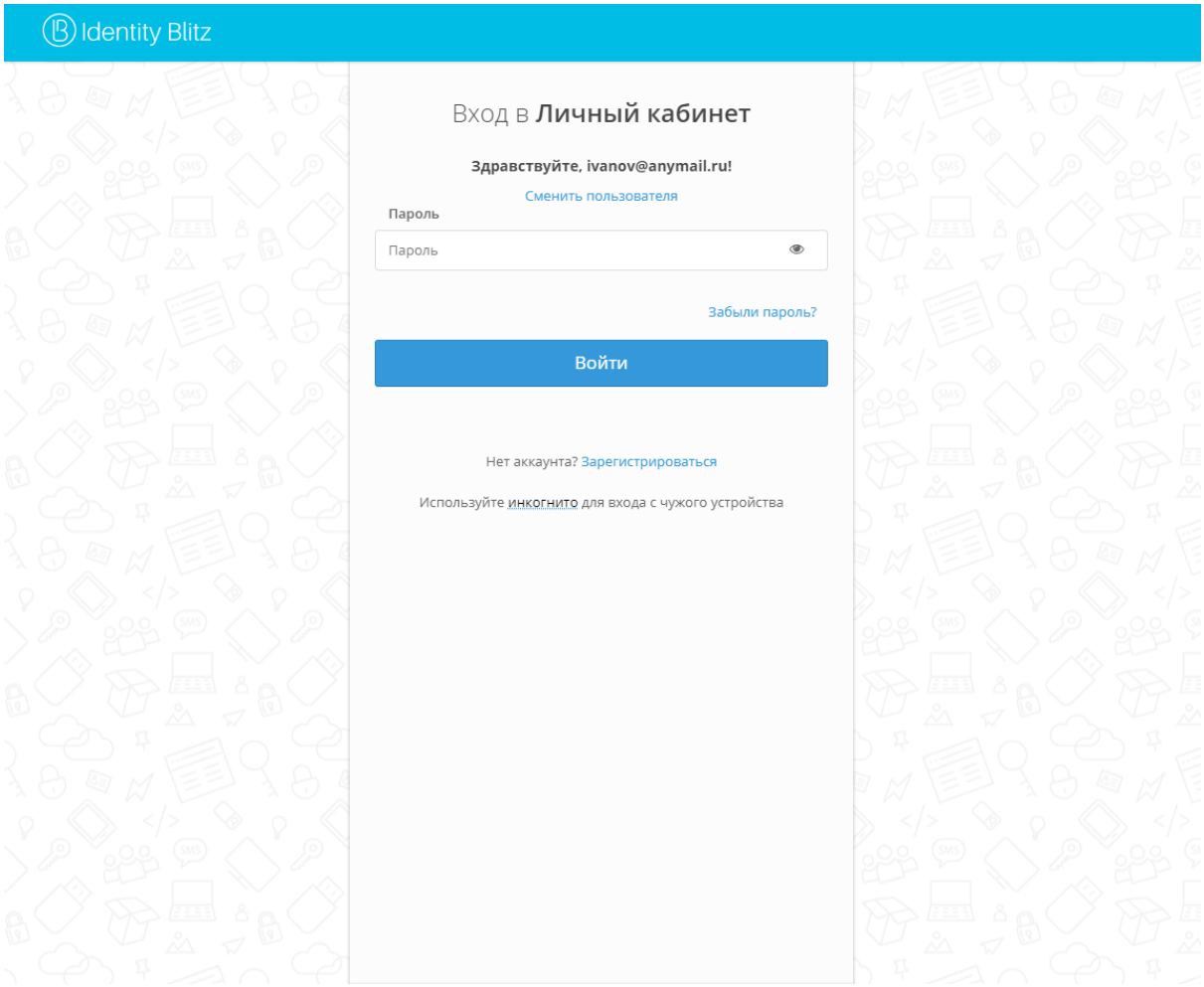
иной уникальный идентификатор.

В процессе входа по логину и паролю может возникнуть ситуация, что установленный парольной политикой безопасности срок действия пароля истекает. В этом случае система аутентификации может предложить пользователю задать новый пароль для его учетной записи.

В случае ошибки при вводе логина и/или пароля система выдаст сообщение об ошибке, и пользователю будет предложено войти повторно. Многократные неуспешные попытки входа могут быть расценены системой как попытка мошенничества. Система аутентификации протоколирует любые попытки входа (успешные и неуспешные). *Просмотреть события безопасности* (страница 33) за выбранный период, связанные с учетной записью пользователя, можно в Личном кабинете пользователя.

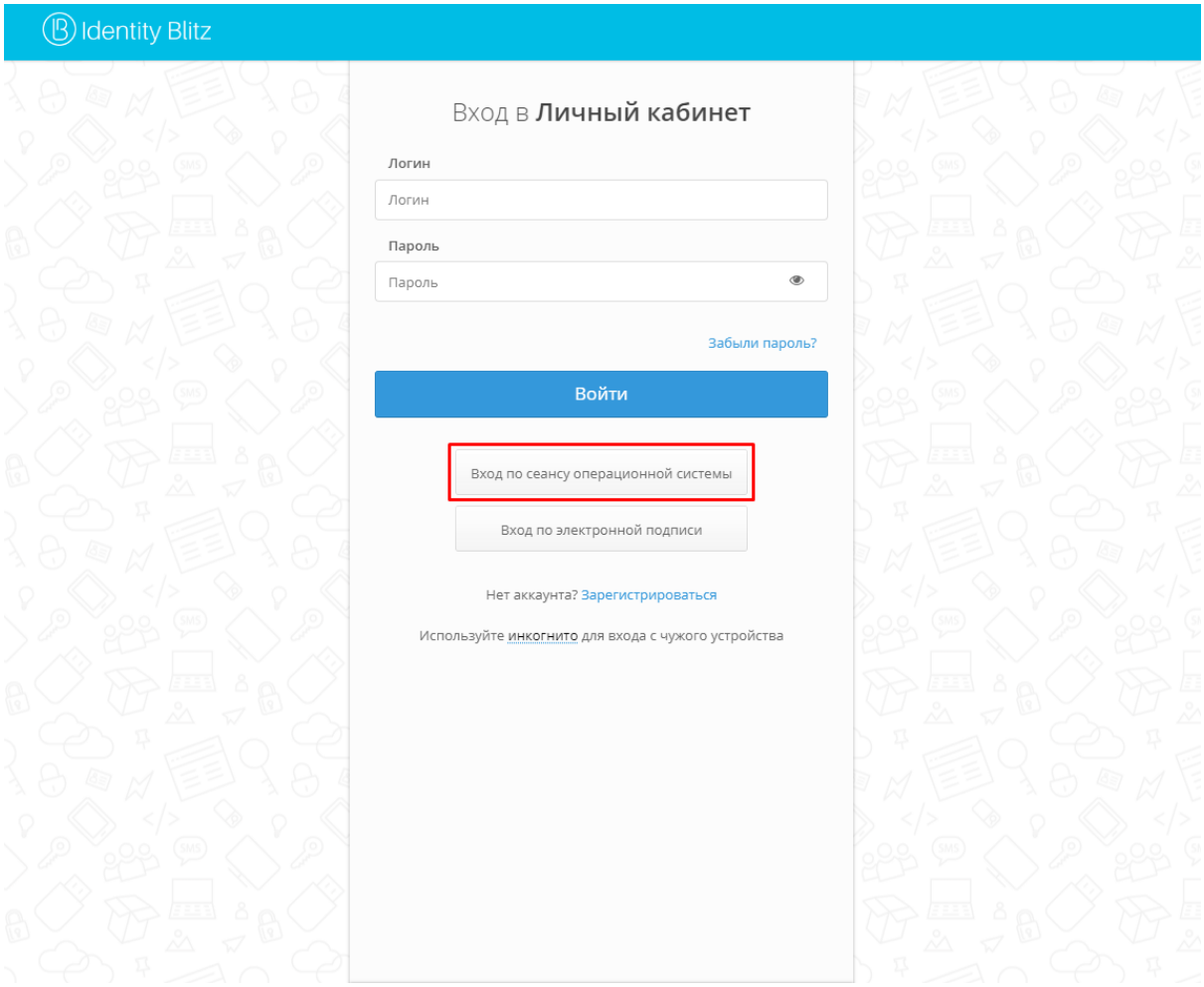
2.2 Вход с известного устройства

Вход с известного устройства позволяет не запрашивать вход пользователя, если ранее в течение определенного времени данный пользователь уже входил в систему с данного устройства и с использованием того же браузера. В этом случае ввод логина в этом браузере на этом ПК будет запомнен системой. При повторном входе на портал при использовании того же самого компьютера и браузера не потребуется вновь вводить электронную почту – достаточно ввести только пароль.

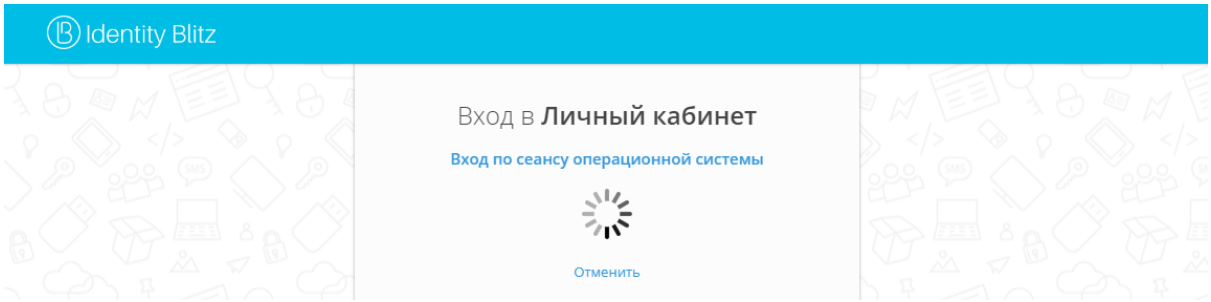


2.3 Вход с помощью сеанса операционной системы

Для входа в систему с помощью сеанса операционной системы необходимо на странице аутентификации нажать на кнопку *Вход по сеансу операционной системы*.



В некоторых установках Blitz Identity Provider вход по сеансу ОС может запускаться автоматически, например, если будет обнаружено, что вход осуществляется из внутренней сети компании.



В процессе входа с использованием сеанса операционной системы предусмотрено время задержки в несколько секунд, в течение которых пользователь может нажать на кнопку *Отменить*, чтобы отказаться от автоматического входа.

Данный способ входа может использоваться в случае, если с компьютера, на котором пользователь вошел в домен, нужно временно предоставить возможность войти в Личный кабинет другому пользователю под его учетной записью, не завершая сеанса в операционной системе.

Вход с использованием сеанса операционной системы может завершиться ошибкой. В этом случае пользователю предложат войти по электронной почте и паролю. Можно воспользоваться предложенным способом входа или разобраться с причинами ошибки. Возможны следующие причины возникновения ошибки:

- Вход осуществляется с ПК, не введенного в домен.
- Вход осуществляется извне корпоративной сети компании.
- С момента включения ПК и идентификации/аутентификации пользователя прошло существенное

время (более 8 часов), и выданное доменом разрешение для автоматической аутентификации устарело.

- Настройки браузера на ПК пользователя препятствуют использованию режима автоматического входа.

Пользователю обычно не требуется самостоятельно менять настройки браузера для автоматического входа – данные настройки применяются через обновление корпоративных доменных политик. Однако пользователь может проверить правильность настроек по следующей инструкции:

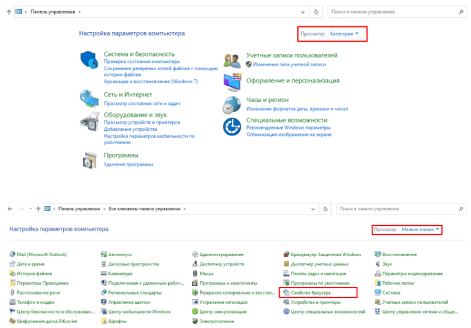
Для браузеров под операционной системой Windows нужно задать следующие настройки:

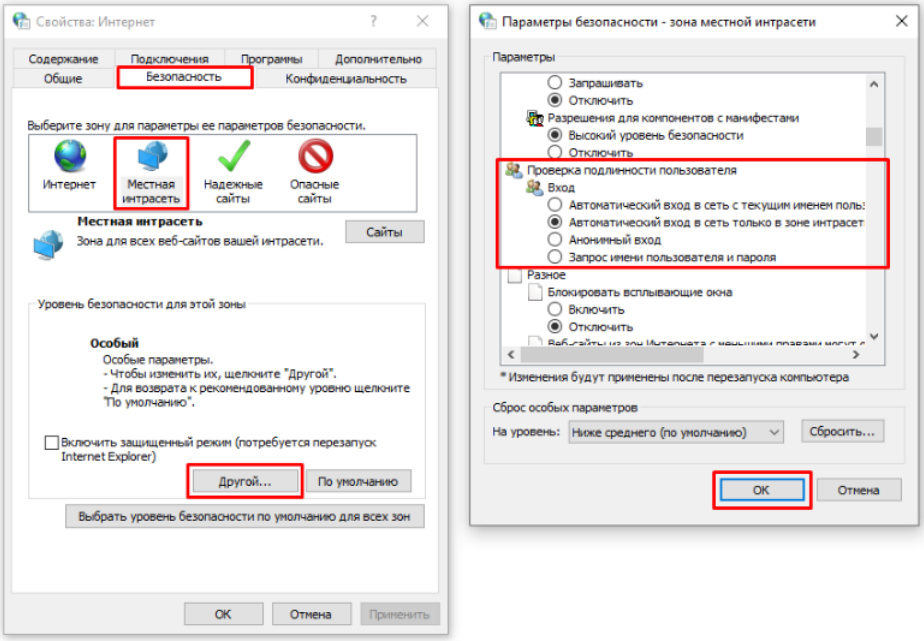
- открыть «Пуск → Панель управления», изменить вариант просмотра с «Категория» на «Мелкие значки», в открывшихся настройках выбрать «Свойства браузера»;
- в новом окне выбрать «Безопасность → Местная интрасеть» и нажать кнопку «Сайты». В открывшемся окне нажать кнопку «Дополнительно» и внести сайт с Blitz Identity Provider в список сайтов «Местная интрасеть», нажав «Добавить»;
- в окне «Свойства: Интернет → Безопасность → Местная интрасеть» нажать кнопку «Другой…». В открывшемся окне найти настройку «Проверка подлинности пользователя → Вход». Установить ее в значение «Автоматический вход в сеть только в зоне интрасети».

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

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

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





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

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

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

```
"/Applications/Google Chrome.app/Contents/MacOS/Google Chrome" --args --auth-
↪server-whitelist="auth.cscentr.com" --auth-negotiate-delegate-whitelist="auth.
↪cscentr.com"
```

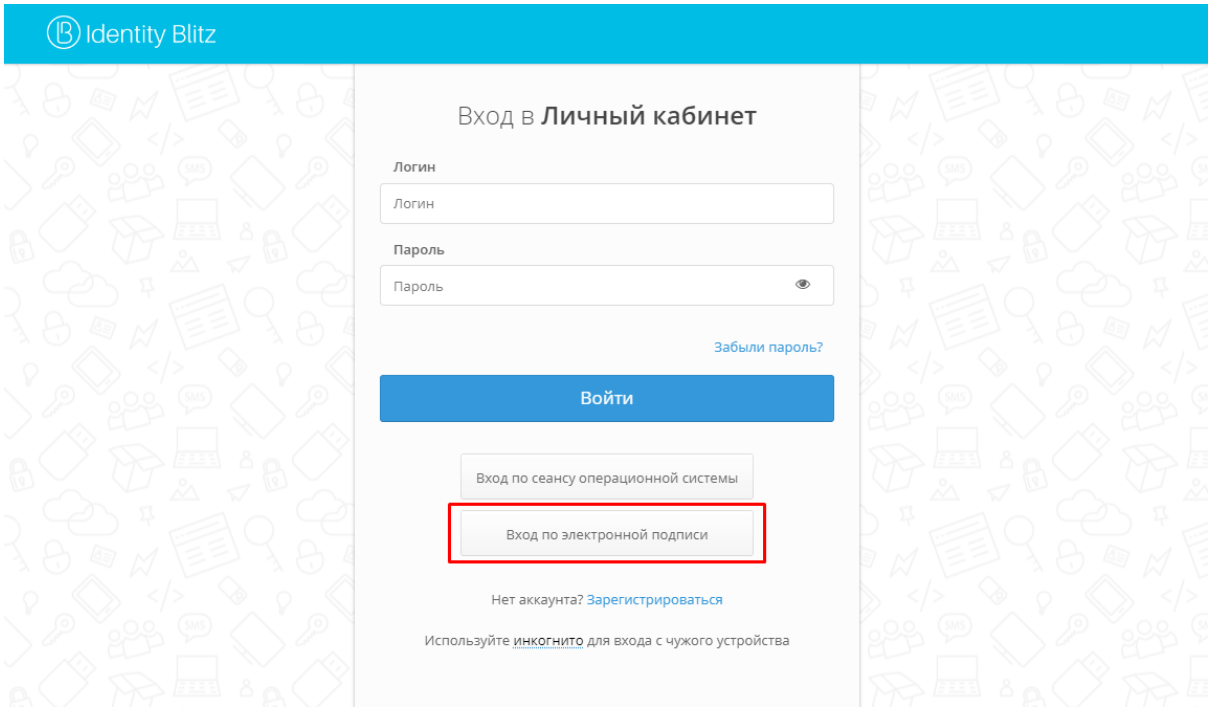
Где в качестве idp.domain.ru нужно указать URL сайта с Blitz Identity Provider.

Для Apple Safari в macOS отдельная настройка не требуется.

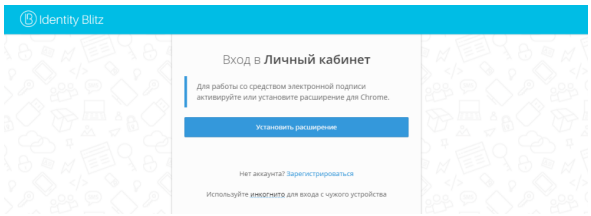
В случае повторения ошибки пользователю следует обратиться к системному администратору организации.

2.4 Вход с помощью средства электронной подписи

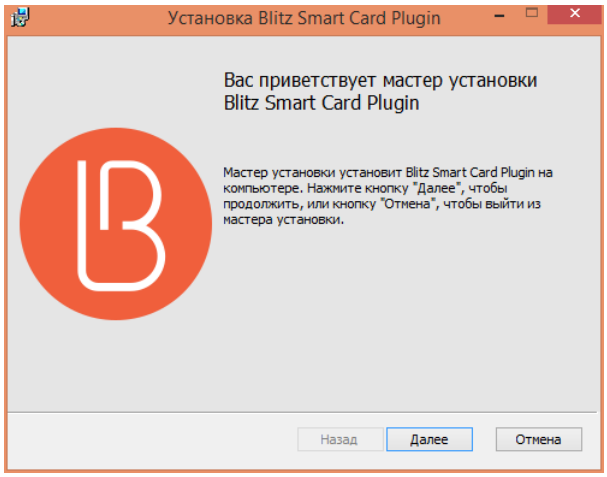
В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход с помощью средства электронной подписи.



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.

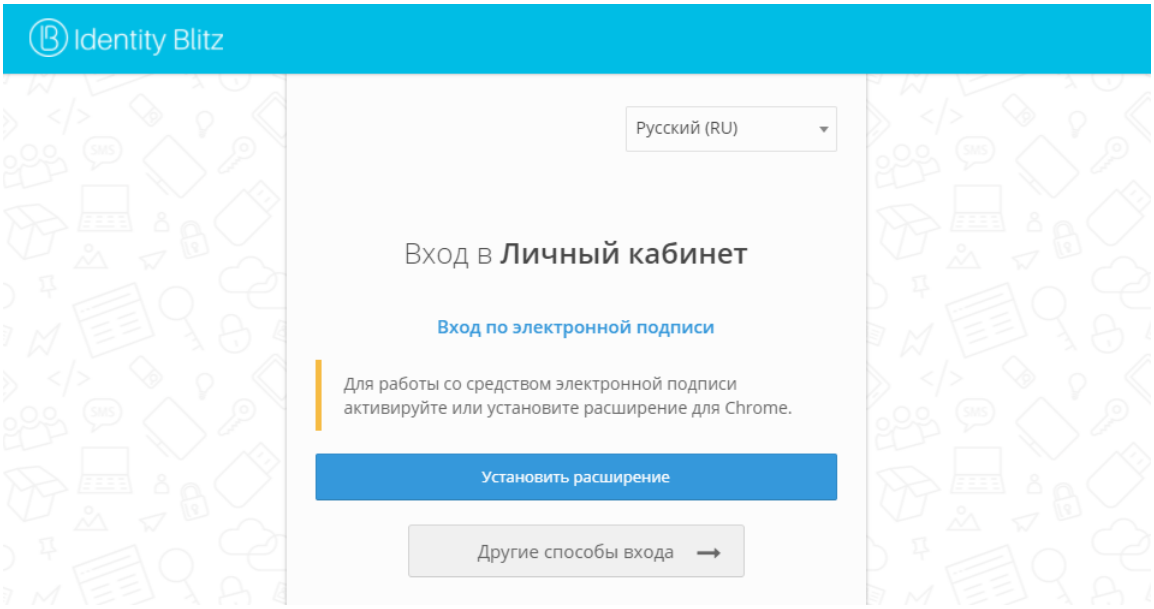


После загрузки установочного файла Blitz Smart Card Plugin и его запуска пользователю следует пройти все шаги установки плагина. При повторном входе с данного устройства не потребуется устанавливать плагин заново.



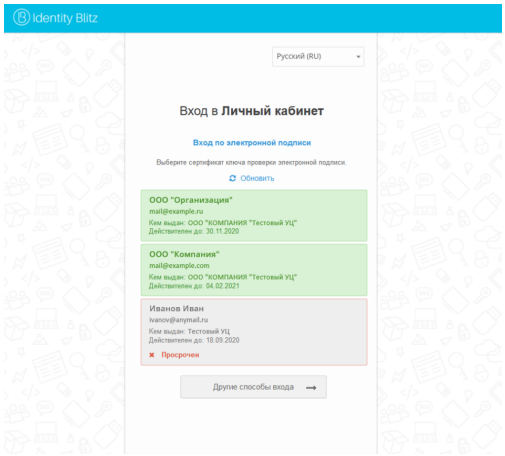
Дополнительно для веб-браузеров Google Chrome и Mozilla Firefox требуется установка специального расширения. О необходимости этого действия будет свидетельствовать предупреждение со ссылкой.

- для веб-браузера Google Chrome необходимо установить расширение. При нажатии кнопки «Установить расширение» открывается интернет-магазин Google Chrome с открытым расширением «Адаптер плагина Blitz Smart Card Plugin». Его необходимо установить.

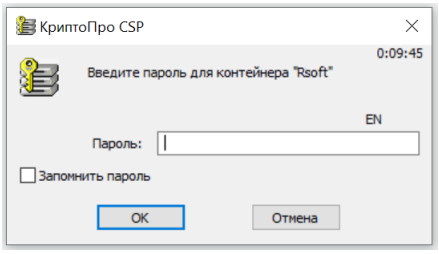


- для веб-браузера Mozilla Firefox требуется установить расширение. При нажатии кнопки «Установить расширение» необходимо разрешить установку программного обеспечения. Для этого требуется нажать кнопку «Разрешить». При необходимости расширение можно загрузить по ссылке и установить вручную с помощью веб-браузера Mozilla Firefox.

После успешной установки плагина пользователю необходимо подсоединить средство электронной подписи к ПК. Далее на странице входа в браузере будут отображены доступные сертификаты ключа электронной подписи, который подсоединен к ПК. Необходимо выбрать из списка тот сертификат, ключ которого подсоединен.



При необходимости потребуется ввести ПИН-код, чтобы осуществить вход в систему.



Если был введен корректный ПИН-код, вход будет успешно выполнен. При некорректном вводе ПИН-кода три раза подряд или при нажатии кнопки «Отмена» будет отображено сообщение об ошибке.

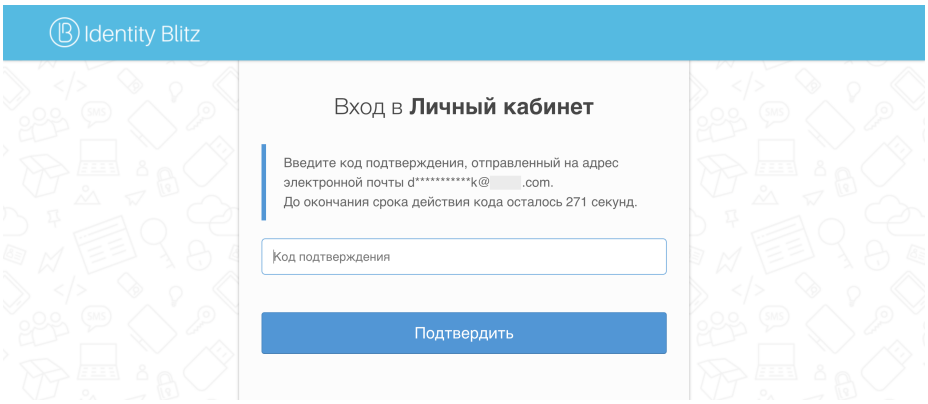
Если при авторизации использованием средства электронной подписи в Blitz Identity Provider не найдена зарегистрированная учетная запись пользователя с уникальным идентификатором из сертификата элек-

тронной подписи, то Blitz Identity Provider предложит ее зарегистрировать. Для этого пользователь перенаправляется на форму регистрации пользователя с предварительно заполненными из сертификата данными (фамилия, имя, отчество, уникальный идентификатор), вводит адрес электронной почты и номер телефона, после чего следует инструкциям на экране. В случае успешной регистрации будет создана учетная запись Blitz Identity Provider и пользователь будет направлен в систему, в рамках которой производился вход.

2.5 Вход с помощью электронной почты

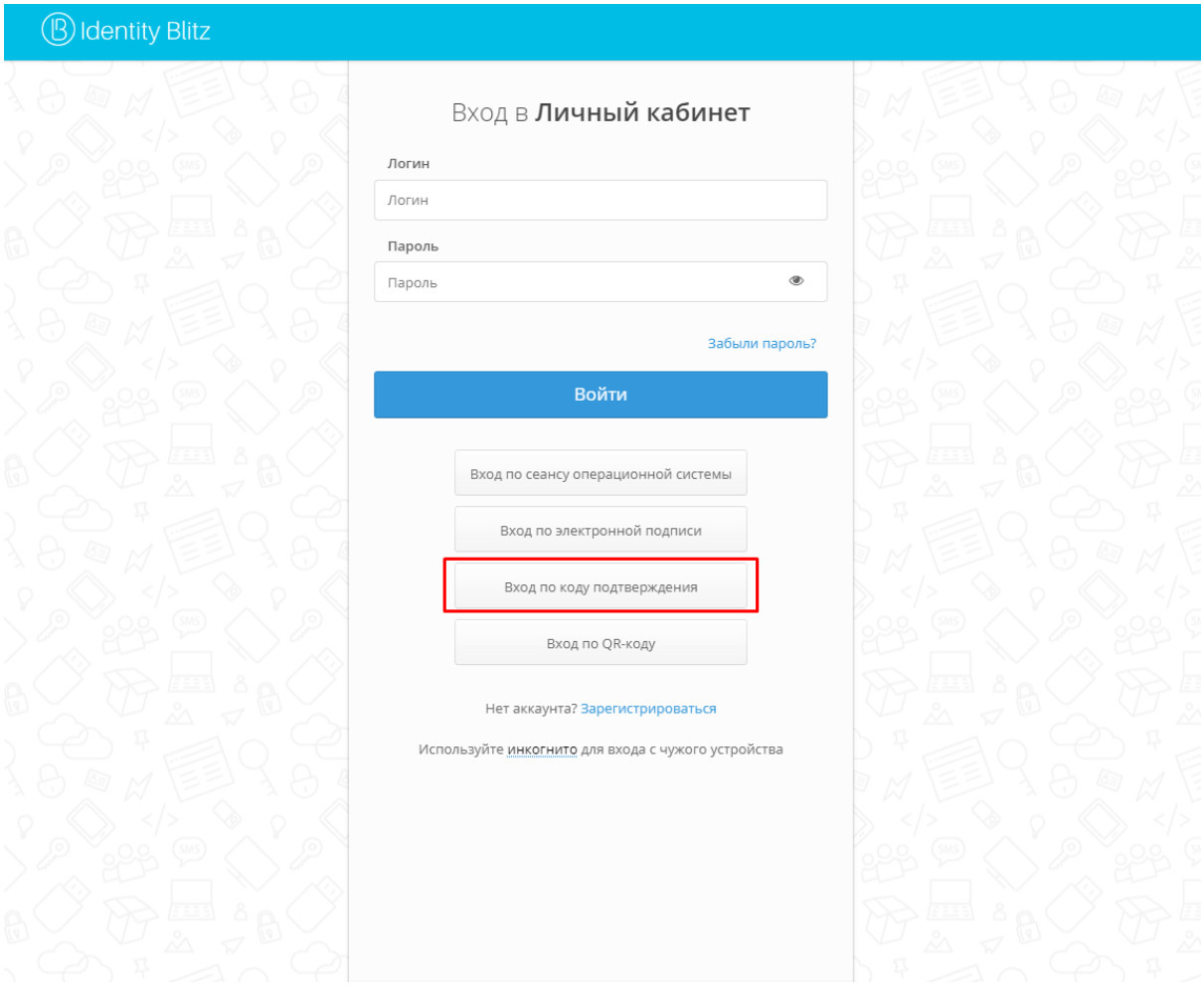
В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход с помощью кода подтверждения, отправляемого по электронной почте.

Пользователю необходимо указать адрес электронной почты, на который будет отправлен код подтверждения. После получения кода его необходимо ввести полученный код в соответствующее поле на странице, чтобы выполнить вход в Личный кабинет.

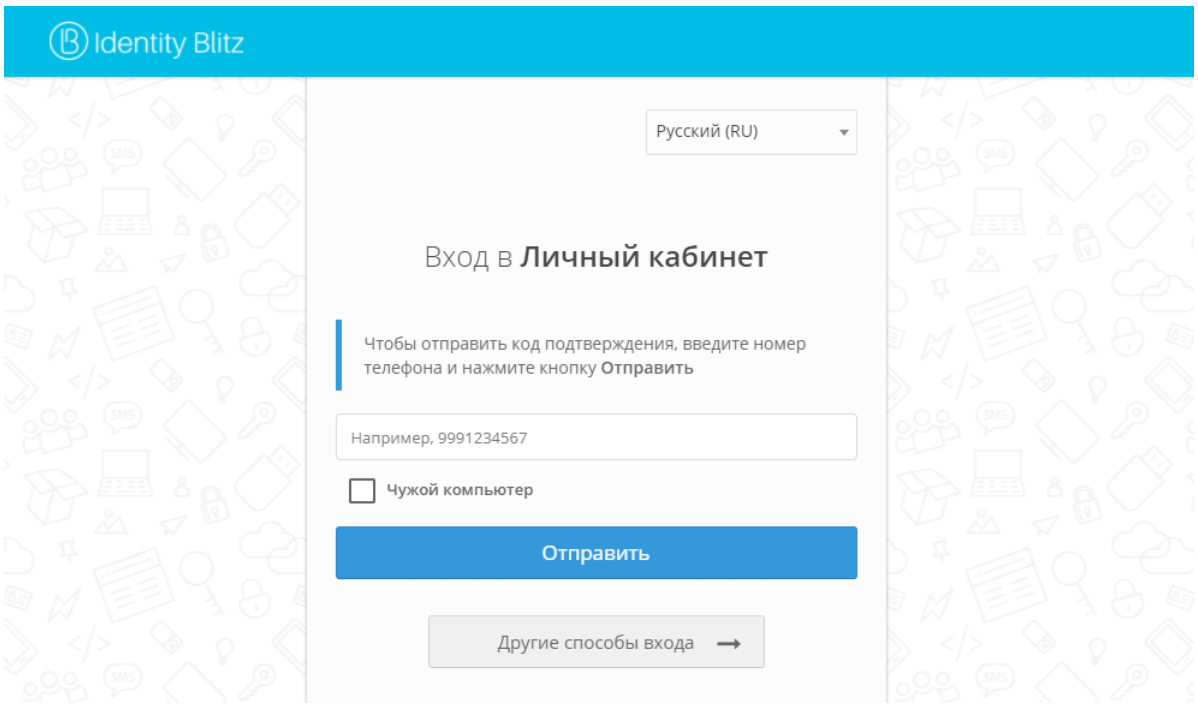


2.6 Вход с помощью кода подтверждения, отправляемого по SMS или PUSH

В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход с помощью кода подтверждения. Внешний вид единой страницы входа может отличаться в зависимости от настроек, установленных организацией.



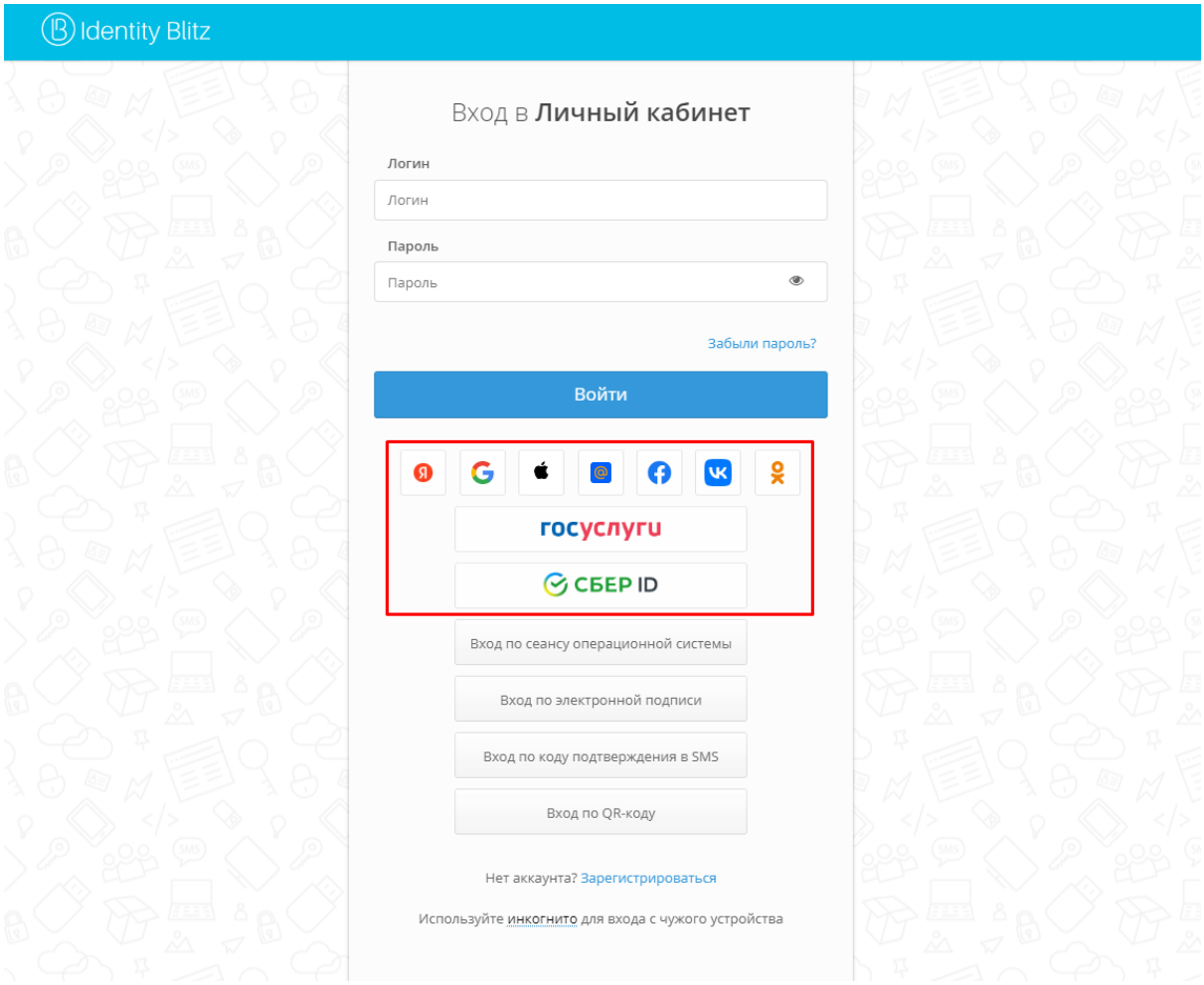
Пользователю необходимо указать номер телефона, на который будет отправлен код подтверждения в виде SMS-сообщения или push-уведомления. После получения кода необходимо ввести полученный код в соответствующее поле на странице, чтобы выполнить вход в Личный кабинет.



Следует учесть, что если у пользователя в Личном кабинете не задан номер мобильного телефона, то он не сможет использовать этот способ входа. В связи с этим привязка номера мобильного телефона к учетной записи должна осуществляться пользователем заранее – задать номер телефона пользователь может самостоятельно через Личный кабинет.

2.7 Вход с помощью внешних сервисов идентификации

В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход с использованием внешних сервисов идентификации. Внешний вид страницы входа при включенных внешних сервисах идентификации может отличаться в зависимости от настроек, установленных организацией.



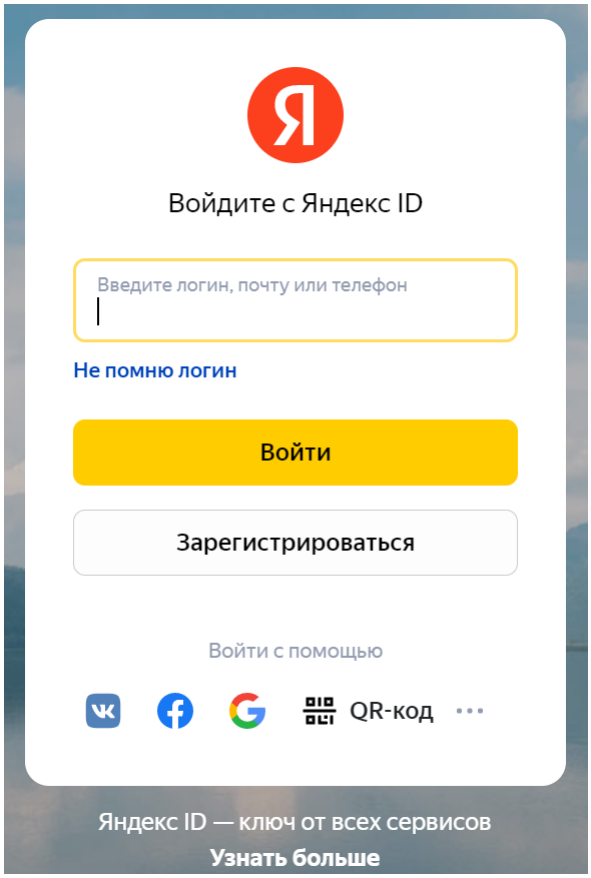
Blitz Identity Provider поддерживает следующие внешние сервисы идентификации:

- поставщика идентификации Apple ID;
- поставщика идентификации социальной сети Facebook[1];
- поставщика идентификации социальной сети ВКонтакте;
- поставщика идентификации Яндекс;
- поставщика идентификации Google;
- поставщика идентификации социальной сети Одноклассники;
- поставщика идентификации Mail.ru (Mail ID);

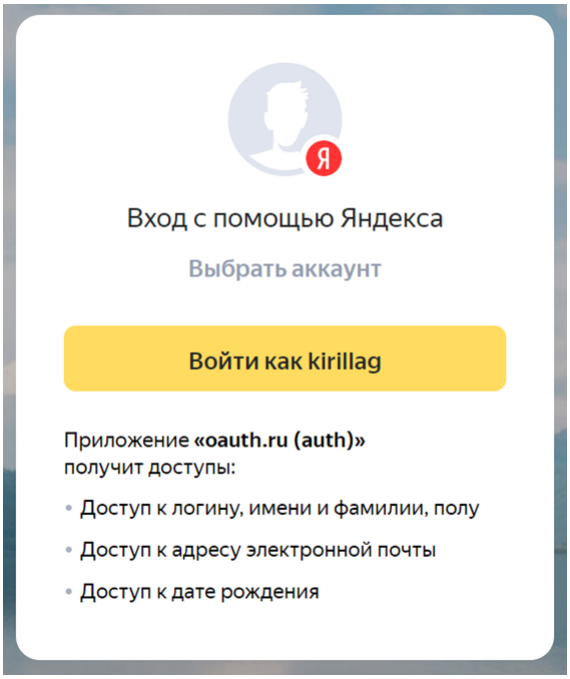
[1] Meta признана экстремистской организацией и запрещена на территории Российской Федерации, деятельность принадлежащих ей социальных сетей Facebook и Instagram также запрещена в РФ.

- поставщика идентификации VK ID;
- поставщика идентификации ЕСИА (gosuslugi.ru);
- поставщика идентификации ЕСИА в режиме «Цифровой профиль» (gosuslugi.ru);
- поставщика идентификации Сбер ID;
- поставщика идентификации T-ID;
- поставщика идентификации ВТБ ID;
- поставщика идентификации Альфа ID;
- поставщика идентификации СберБизнес ID;
- поставщика идентификации Mos ID (СУДИР);
- Blitz Identity Provider, установленного в партнерской организации.

Для осуществления входа пользователю необходимо выбрать подходящий внешний сервис идентификации. После чего в браузере загрузится страница входа выбранного сервиса идентификации. Далее на странице входа внешнего сервиса идентификации пользователю необходимо ввести логин и пароль, нажать кнопку входа.



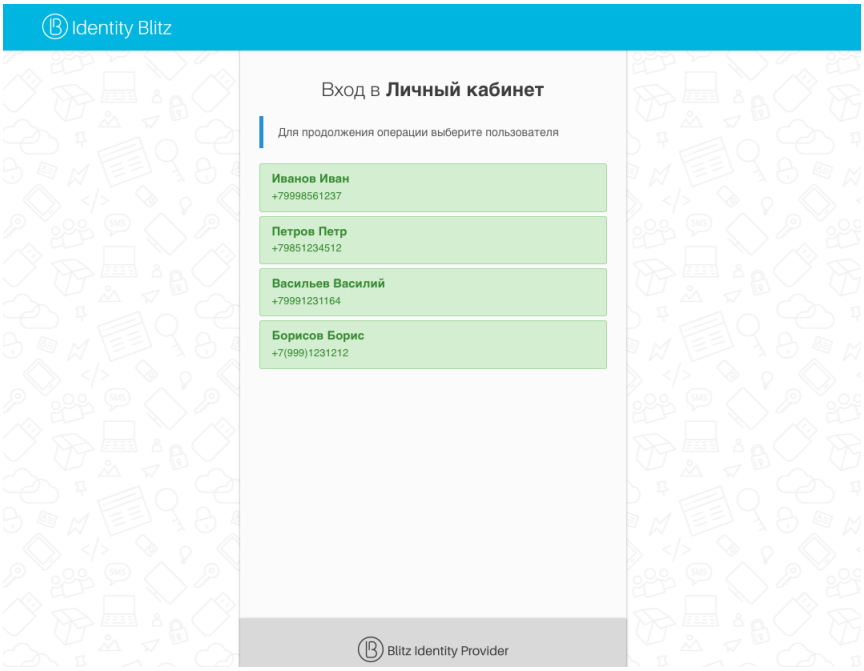
При первом входе через учетную запись пользователя внешний сервис идентификации может дополнительно запросить доступ к данным пользователя.



Если учетная запись пользователя внешнего сервиса идентификации не привязана ни к одной учетной записи в Blitz Identity Provider, то в процессе входа через внешний сервис возможно привязать учетную запись пользователя внешнего сервиса идентификации к уже имеющейся учетной записи. Для этого пользователю необходимо привязать учетную запись пользователя внешнего сервиса идентификации к учетной записи Blitz Identity Provider. Чтобы сделать это, нужно ввести пароль или логин и пароль от учетной записи Blitz Identity Provider на странице связывания учетных записей. Следует учесть, что если по данным из внешнего сервиса идентификации (например, по адресу электронной почты, была найдена учетная запись в Blitz Identity Provider, то для связывания нужно ввести только пароль от этой учетной записи.

Также пользователь может осуществить *предварительное привязывание* (страница 27) учетной записи внешнего сервиса идентификации к Blitz Identity Provider в Личном кабинете через раздел *Настройки безопасности*.

Если пользователь входит с помощью такой учетной записи внешнего сервиса идентификации, которая одновременно привязана к нескольким учетным записям в Blitz Identity Provider, то пользователю будет показан экран выбора учетной записи для входа.



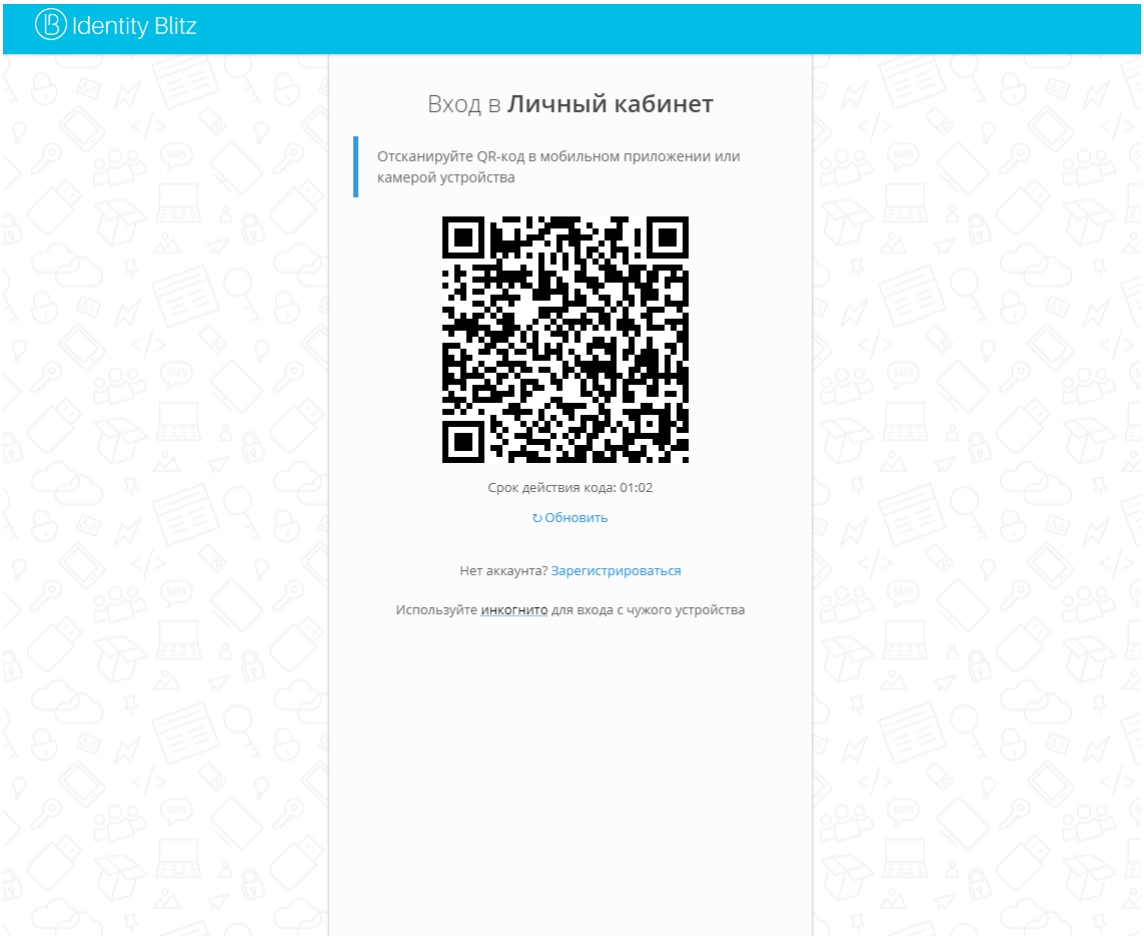
2.8 Вход по разовой ссылке

В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход по разовой ссылке.

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

2.9 Вход по QR-коду

В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход по QR-коду. Внешний вид единой страницы входа может отличаться в зависимости от настроек, установленных организацией.



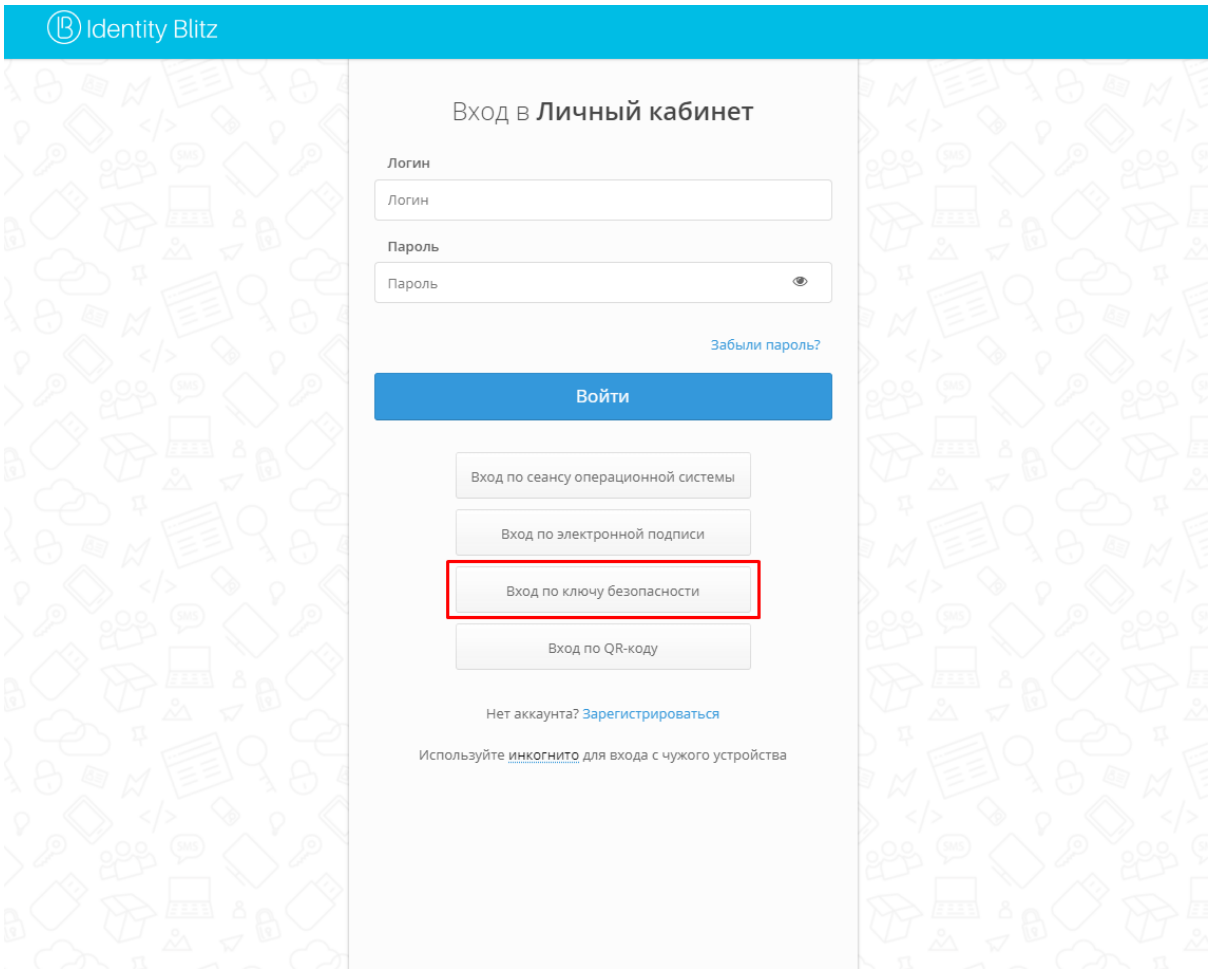
Для осуществления входа по QR-коду пользователю необходимо выполнить следующие действия:

- на странице входа пользователю необходимо выбрать «Войти по QR коду»;
- на странице входа отображается QR-код и инструкция. QR-код имеет ограниченный срок действия (пользователю показывается таймер со сроком действия QR-кода);
- пользователь запускает мобильное приложение компании, в которое встроена поддержка режима входа по QR-коду, и считывает с помощью этого приложения QR код;
- мобильное приложение показывает пользователю детальную информацию о входе, полученную от Blitz Identity Provider (имя приложения, в которое осуществляется вход, IP-адрес, браузер и имя операционной системы устройства, на котором осуществляется вход);
- пользователь в мобильном приложении принимает решение, разрешить или запретить вход;

- в зависимости от решения пользователя на компьютере происходит успешный вход пользователя в приложение или запрос входа отклоняется.

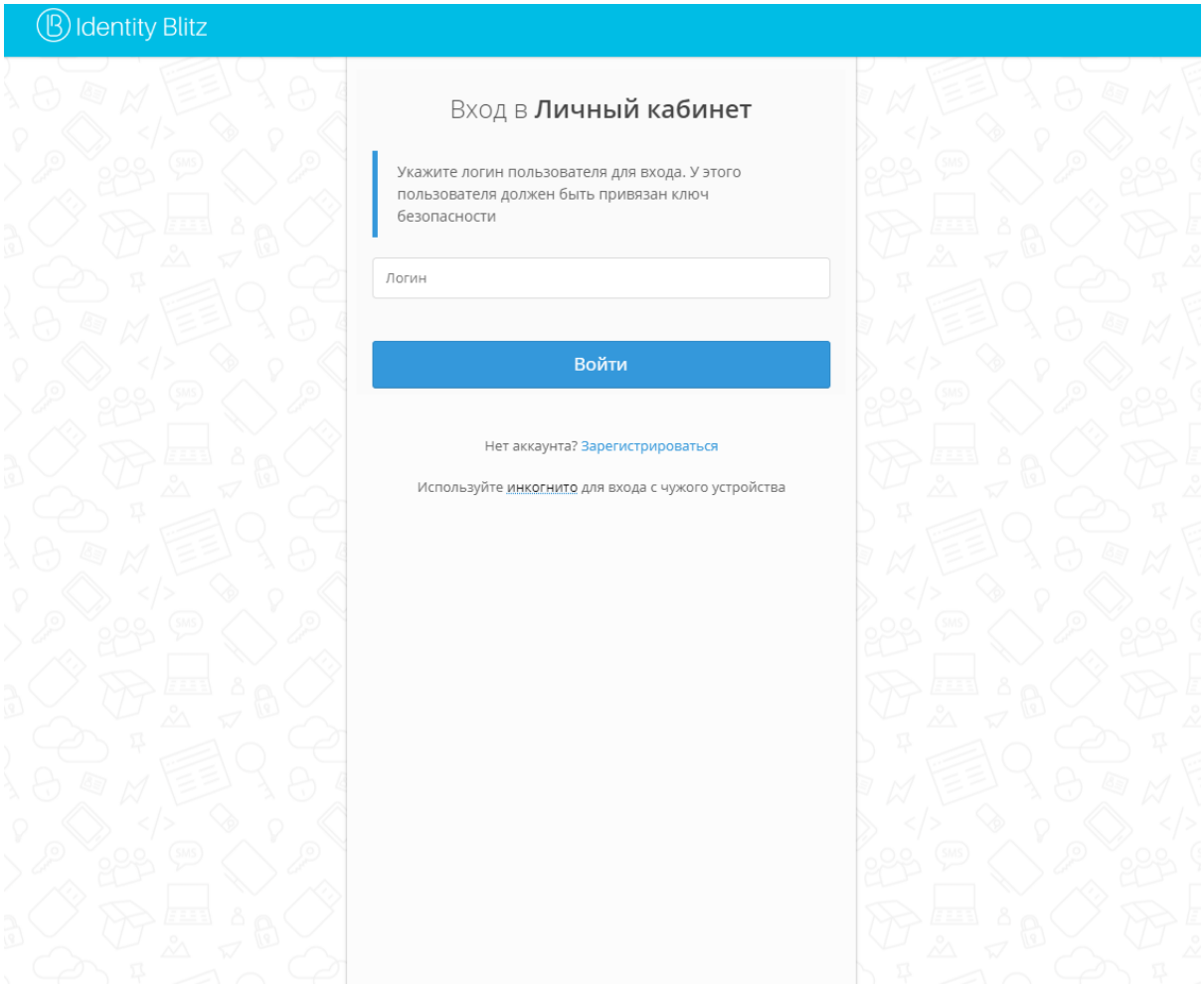
2.10 Вход с помощью ключей безопасности

В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход с помощью ключей безопасности (WebAuthn, Passkey, FIDO2). Внешний вид единой страницы входа может отличаться в зависимости от настроек, установленных организацией.



Поддерживаются следующие типы ключей:

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

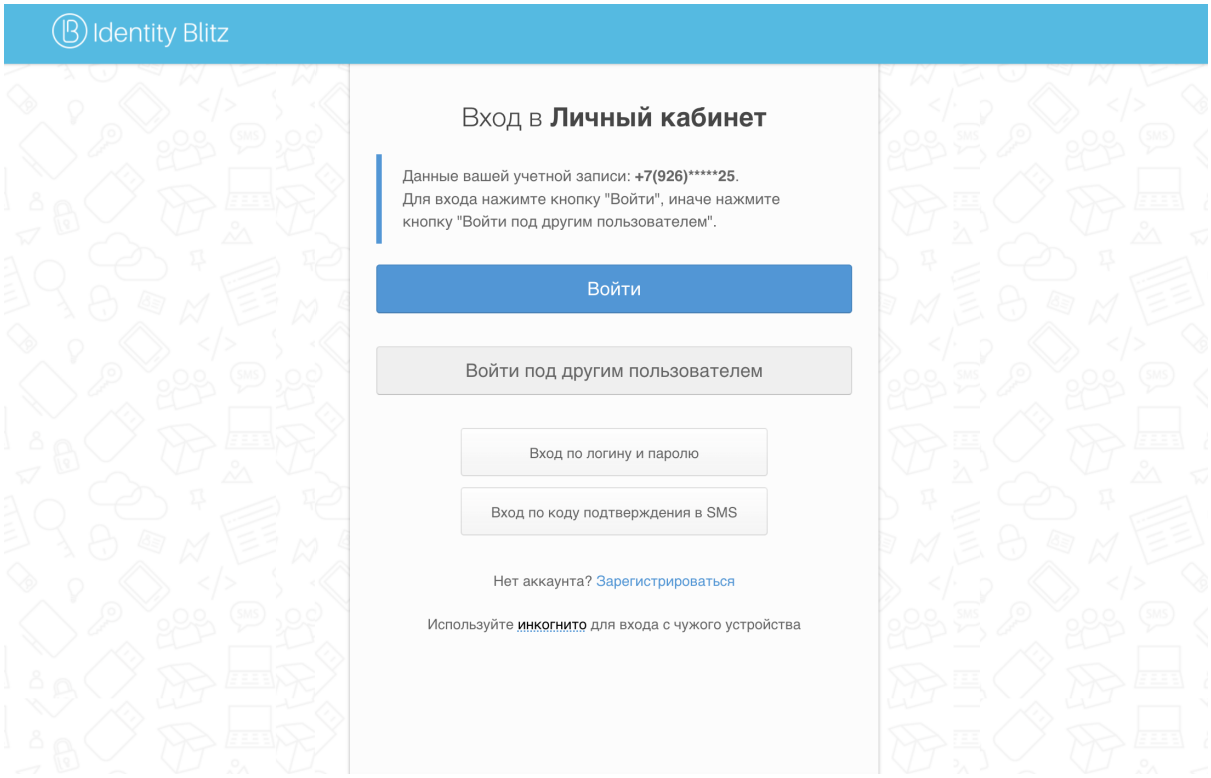


Следует учесть, что если у пользователя в Личном кабинете не привязан ключ безопасности, то он не сможет использовать этот способ входа. В связи с этим привязка ключа безопасности к учетной записи должна осуществляться пользователем заранее – сделать это пользователь может самостоятельно через Личный кабинет.

2.11 Вход с помощью автоматической идентификации пользователя по свойствам сессии

В зависимости от настроек Blitz Identity Provider, установленных организацией, пользователю может быть доступен вход с помощью автоматической идентификации. В этом случае одно или несколько свойств сессии пользователя будут автоматически вычислены Blitz Identity Provider, по ним найдена соответствующая учетная запись и предоставлен доступ в систему. Частным случаем входа с помощью автоматической идентификации является вход по номеру телефона, автоматически определенному по IP-адресу пользователя мобильного интернета.

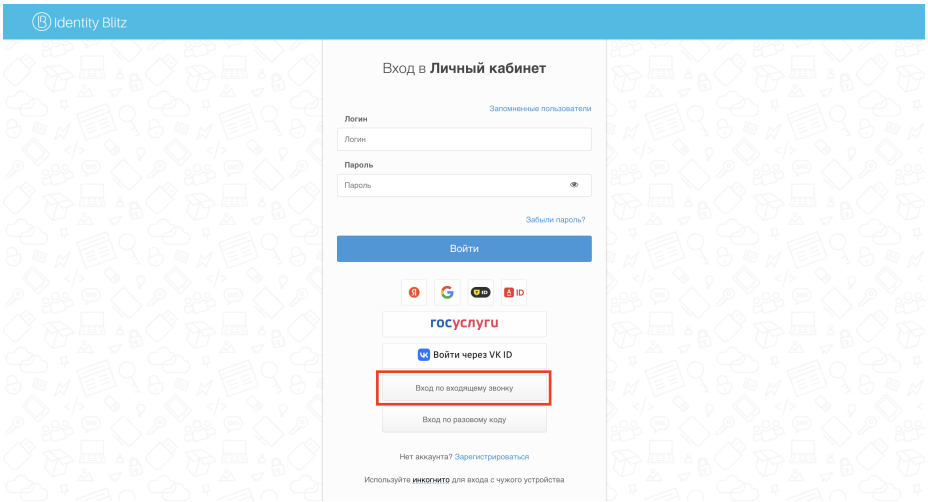
В зависимости от настроек Blitz Identity Provider, при данном типе входа может отображаться экран подтверждения входа. В случае если пользователь не подтверждает вход, ему будет предложен другой метод аутентификации.



Внешний вид страницы входа может отличаться в зависимости от настроек, установленных организацией.

2.12 Вход с помощью входящего звонка

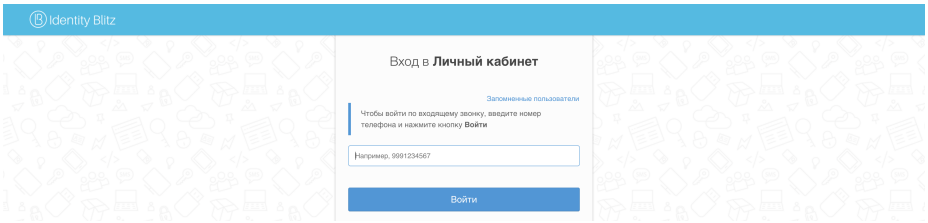
В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход с помощью входящего звонка. Внешний вид единой страницы входа может отличаться в зависимости от настроек, установленных организацией.



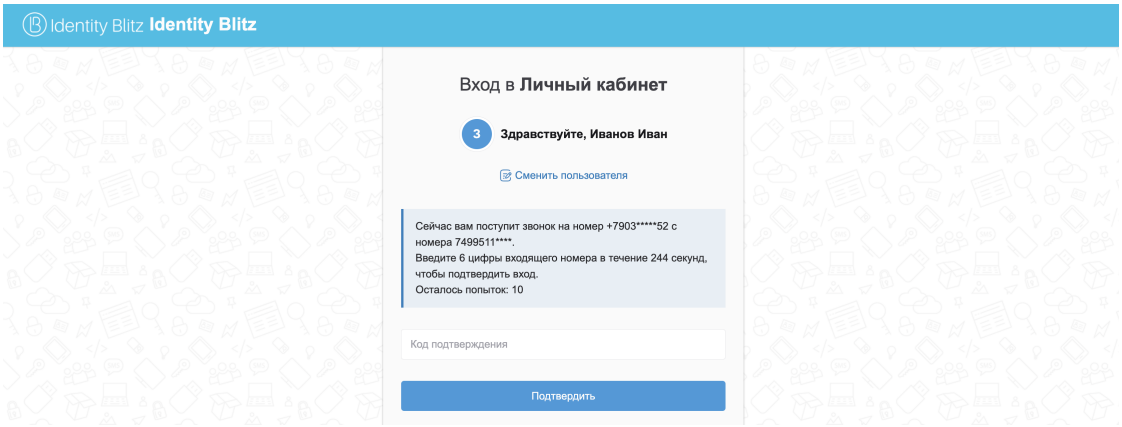
Внешний вид страницы входа может отличаться в зависимости от настроек, установленных организацией.

Для осуществления входа с помощью разового пароля на основе времени пользователю необходимо выполнить следующие действия:

- на странице входа пользователю необходимо выбрать «Вход по входящему звонку»;
- на странице входа отображается поле для ввода номера мобильного телефона. Введите номер мобильного телефона;



- звонок поступит на номер введенного телефона;
- пользователь вводит последние 6 цифр входящего номера телефона;

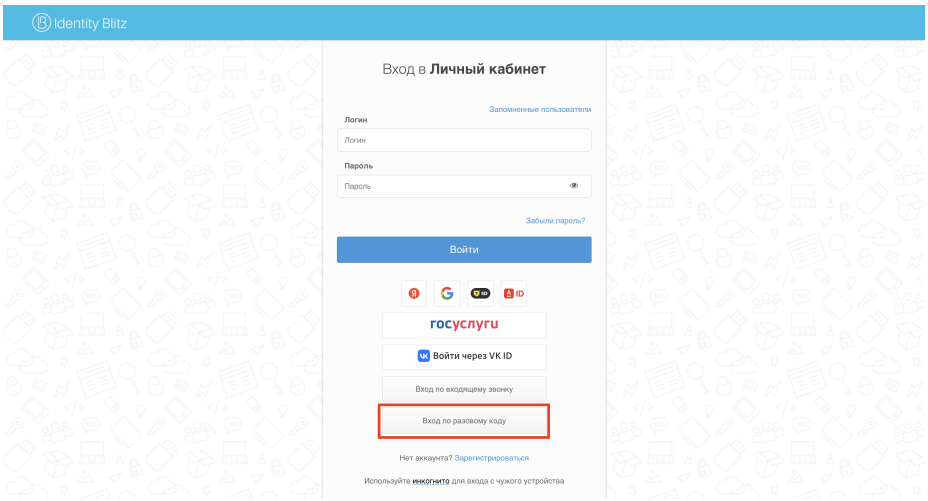


- в зависимости от решения пользователя на компьютере происходит успешный вход пользователя в приложение или запрос входа отклоняется.

2.13 Вход с помощью разового пароля на основе времени (TOTP)

В зависимости от настроек Blitz Identity Provider, установленных организацией, помимо входа по логину и паролю, пользователю может быть доступен вход с помощью разового пароля на основе времени (TOTP).

> **Примечание**
>
> Внешний вид единой страницы входа может отличаться в зависимости от настроек, установленных организацией.



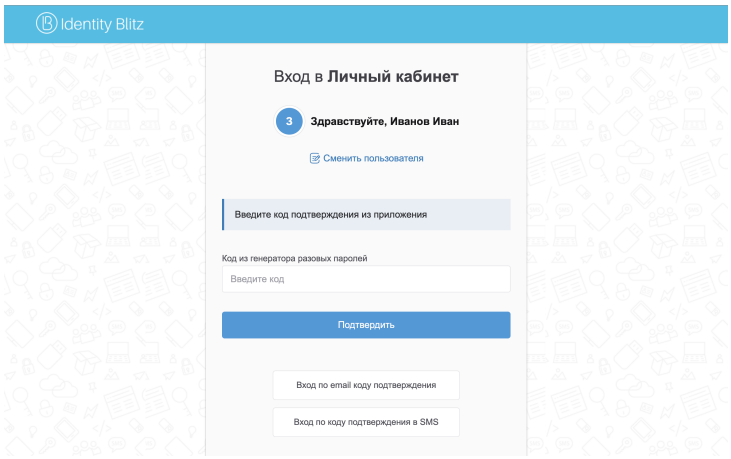
Для осуществления входа с помощью разового пароля на основе времени выполните следующие действия:

1. На странице входа выберите Войти по разовому коду. В результате отобразится поле `Код из генератора разовых паролей`.

2. Введите код подтверждения из приложения-генератора разовых паролей, привязанного к вашей учетной записи.

> **Примечание**
>
> Наиболее известные приложения для выработки TOTP-кодов: Twilio Authy, FreeOTP Authenticator, Microsoft Authenticator, Яндекс.Ключ.

> **Совет**
>
> Вы также можете использовать мобильное приложение Blitz Key.



Глава 3

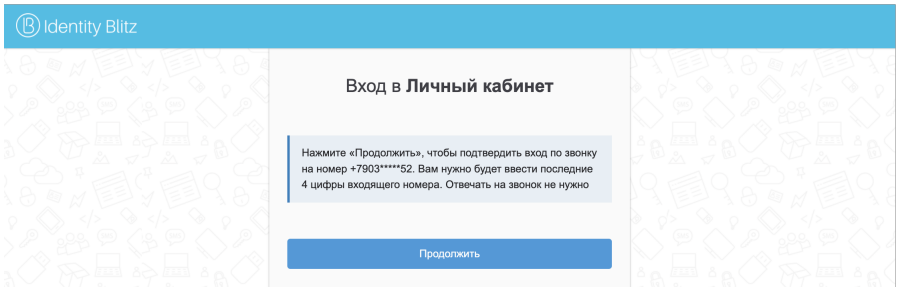
Двухфакторная аутентификация и вход в сетевые службы

3.1 Вход при включенной двухфакторной аутентификации

При включенной двухфакторной аутентификации пользователю после выполнения входа по логину и паролю или любым другим доступным способом потребуется дополнительное подтверждение, например, с помощью кода подтверждения, полученного в SMS-сообщении, push-уведомлении, по электронной почте, сгенерированного в специальном мобильном приложении или доставленного в виде последних цифр входящего звонка.

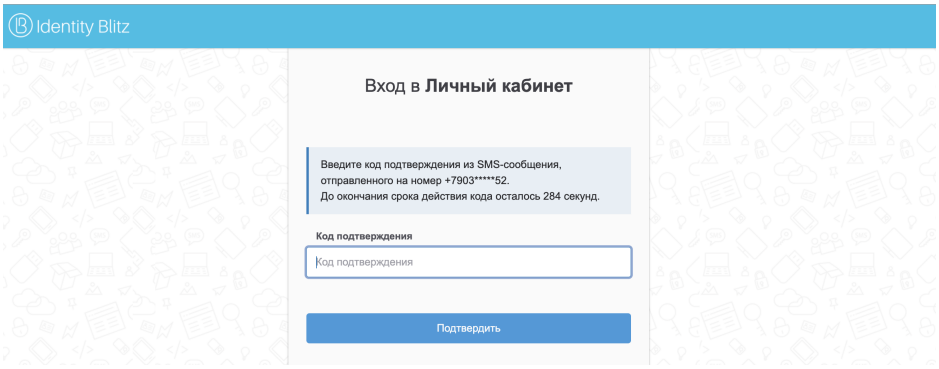
Привязка номера мобильного телефона осуществляется пользователем самостоятельно через Личный кабинет, либо выполняется в иной системе управления данными пользователя, используемой в организации.

> **Внимание**
>
> Если у пользователя в Личном кабинете не задан номер мобильного телефона, то он не сможет использовать подтверждение входа через SMS или по входящему звонку.

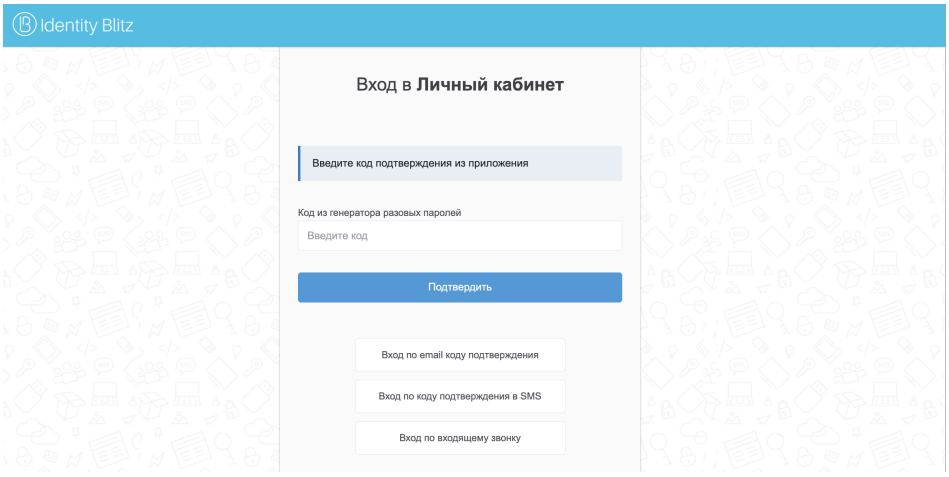


Для подтверждения входа с помощью кода подтверждения, пользователю необходимо:

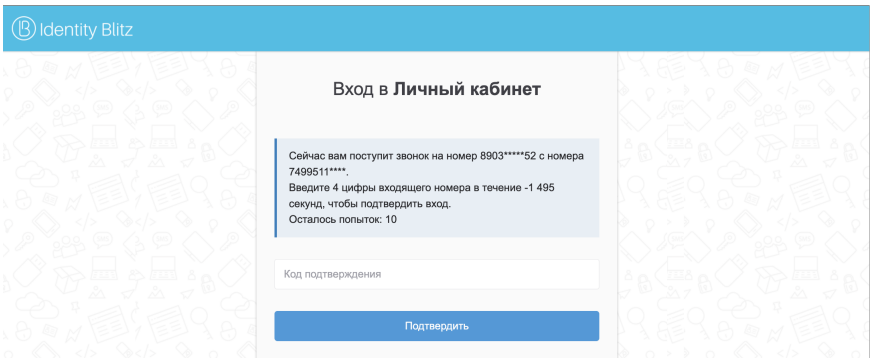
1. Выполнить вход в приложение, защищенное Blitz Identity Provider, по логину и паролю или любым другим доступным способом;
2. Выбрать предпочтительный способ подтверждения входа, если настроено несколько способов, нажатием кнопки «Другие способы подтверждения». По умолчанию предлагается ввести код подтверждения из SMS-сообщения или push-уведомления, которое можно получить через мобильное приложение.
3. Подтвердить вход в учетную запись в зависимости от выбранного способа:
    - вводом кода, полученного SMS-сообщением или push-уведомлением;



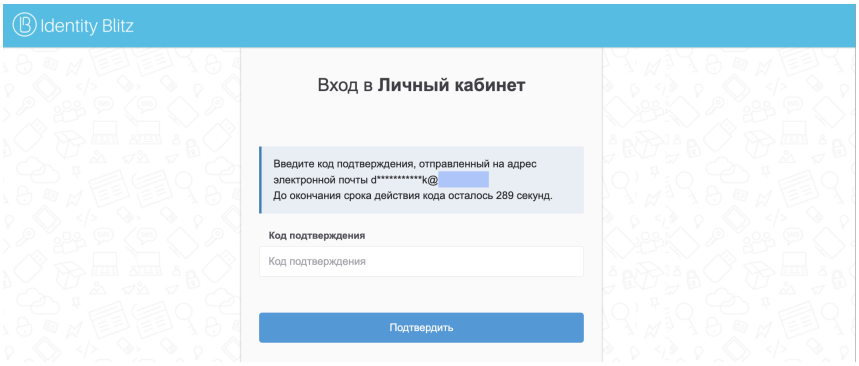
- вводом кода из мобильного приложения, генерирующего коды подтверждения.



- вводом кода, доставленного в виде последних цифр входящего звонка.



- вводом кода, полученным на адрес электронной почты.



- подтверждением через доверенное приложение, например, Blitz Key. Подробнее.

Если у пользователя не настроен ни одного способа получения кодов подтверждения, то будет отображен

экран с ошибкой.

Срок действия кода, отправленного SMS-сообщением, по умолчанию ограничен 300 секундами. Срок действия кода, сгенерированного мобильным приложением, ограничен 30 секундами.

При последующих входах с данного устройства и браузера можно пропустить этап ввода кода подтверждения. В этом случае, если вход в портал пройдет успешно, то будет запомнено устройство и браузер пользователя: при последующих входах не потребуется логин, а также подтверждать вход при помощи кода из мобильного приложения.

3.2 Вход в сетевые службы

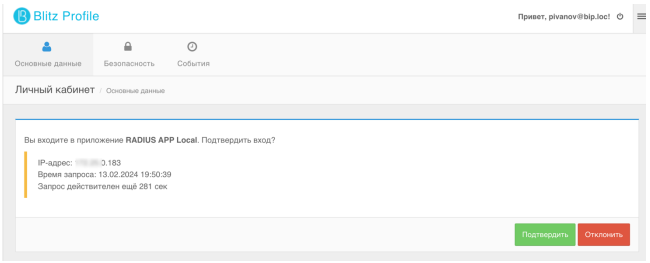
Если система настроена соответствующим образом, пользователи могут входить в сетевые службы через Blitz Identity Provider как по первому, так и второму фактору аутентификации.

В случае первичного входа последовательность действий пользователя не отличается от стандартного ввода логина и пароля в окне доступа к службе. При этом идентификацию пользователя осуществляет не служба, а Blitz Identity Provider.

В случае подтверждении входа на втором факторе возможны следующие сценарии:

1. Подтверждение по коду из SMS, push, TOTP, HOTP, email – после первичного входа по логину и паролю пользователю необходимо ввести код в окне доступа к службе.
2. Подтверждение в Личном кабинете пользователя – пользователь сначала входит в свой Личный кабинет с обязательным прохождением двухфакторной аутентификации. Далее пользователь выполняет первичный вход в сетевую службу, после чего служба переходит в режим ожидания подтверждения. В Личном кабинете появляется сообщение о попытке входа, в котором пользователю необходимо нажать кнопку *Подтвердить*.

> **Предупреждение**
>
> Подтверждение в Личном кабинете не поддерживается в браузере Internet Explorer 11.



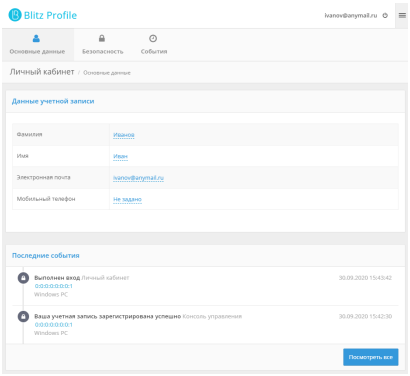
Глава 4

Как пользоваться Личным Кабинетом

4.1 Управление настройками учетной записи пользователя

Управление данными учетной записи в системе Blitz Identity Provider осуществляется пользователем через приложение – Личный кабинет. Для доступа к Личному кабинету пользователь может воспользоваться ссылкой, например: `https://idp.domain.ru/blitz/profile`.

Внешний вид Личного кабинета может отличаться в зависимости от настроек, установленных организацией.



Личный кабинет пользователя – веб-приложение, в котором пользователь может выполнить следующие действия с учетной записью:

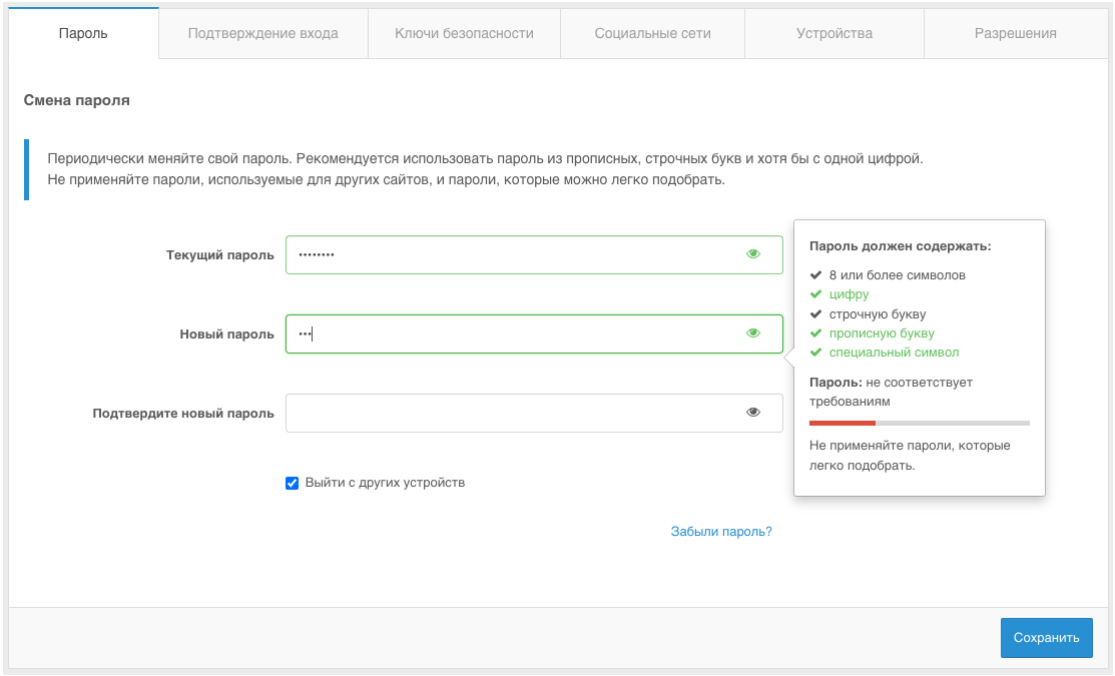
- посмотреть или изменить данные своей учетной записи;
- посмотреть последние события безопасности (например, события входа);
- сменить пароль;
- посмотреть и настроить способы подтверждения входа (двухфакторной аутентификации);
- посмотреть и настроить ключи безопасности;
- посмотреть привязанные учетные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

4.2 Смена пароля

Для смены пароля авторизованному пользователю необходимо осуществить следующие действия:

- на странице Личного кабинета перейти в раздел «Безопасность» и выбрать вкладку «Пароль»;
- на странице «Смена пароля» необходимо ввести текущий и новый пароль;
- если одновременно со сменой пароля необходимо сбросить сессии пользователя и выйти с других устройств, то необходимо отметить чекбокс «Выйти с других устройств»;
- нажать кнопку «Сохранить»;
- если текущий пароль утерян, необходимо воспользоваться функцией «Забыли пароль?»

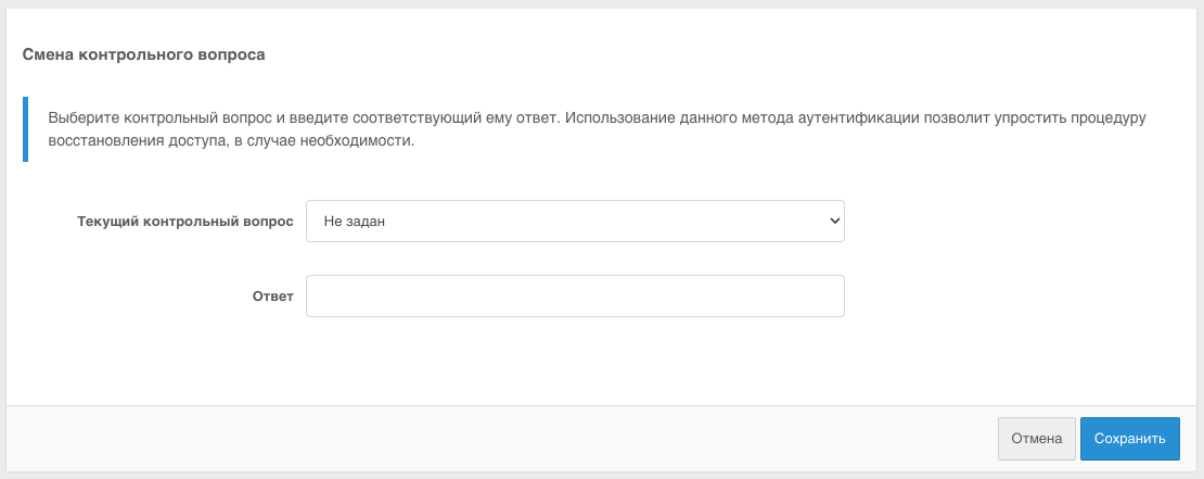
> **Примечание**
>
> См. *процедуру восстановления пароля* (страница 38).



4.3 Установка или изменение контрольного вопроса

Для установки или изменения контрольного вопроса и ответа на контрольный вопрос авторизованному пользователю необходимо осуществить следующие действия:

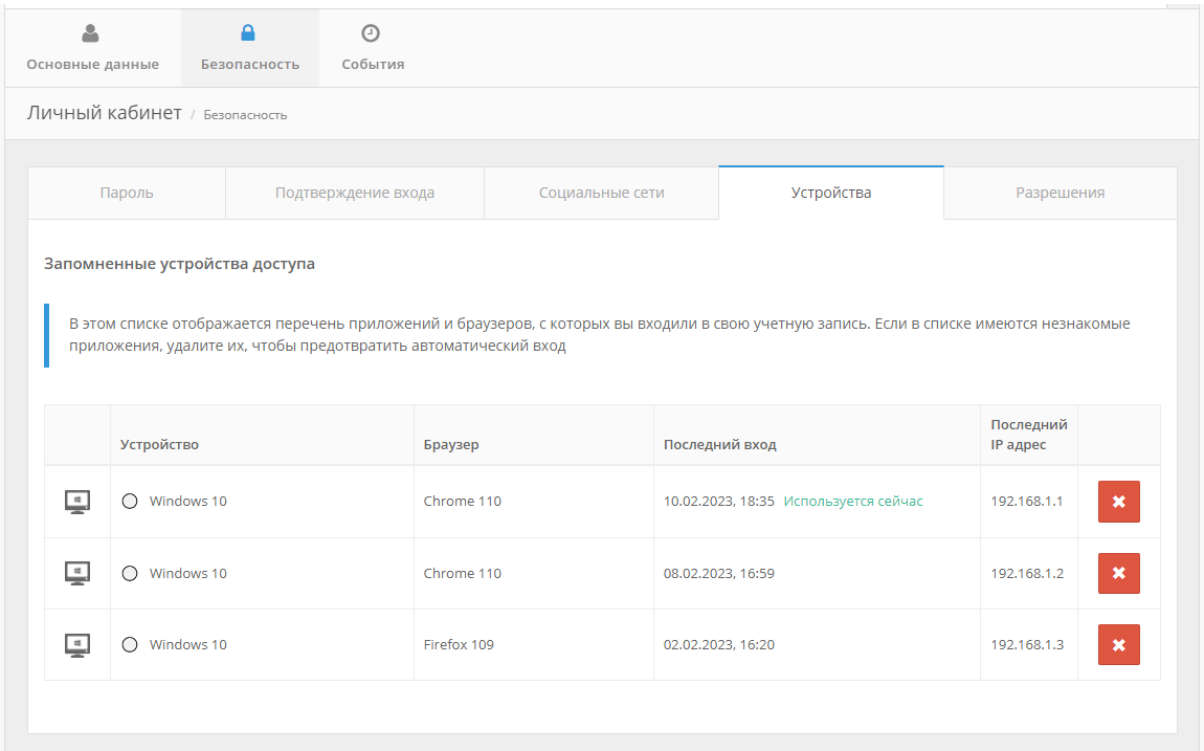
- на странице Личного кабинета перейти в раздел «Безопасность» и выбрать вкладку «Пароль». Перейти к блоку «Смена контрольного вопроса»;
- в поле «Текущий контрольный вопрос» необходимо выбрать вопрос из предлагаемого справочника
- в поле «Ответ» ввести ответ на выбранный вопрос и нажать кнопку «Сохранить».
- Если нужно сменить ранее заданный вопрос, то надо нажать на ссылку с текущим вопросом, и выбрать новый вопрос и задать ответ на него.



4.4 Удаление запомненного устройства

Для удаления запомненного устройства необходимо выполнить следующие шаги:

- на странице Личного кабинета перейти в раздел «Безопасность» и выбрать вкладку «Устройства»;

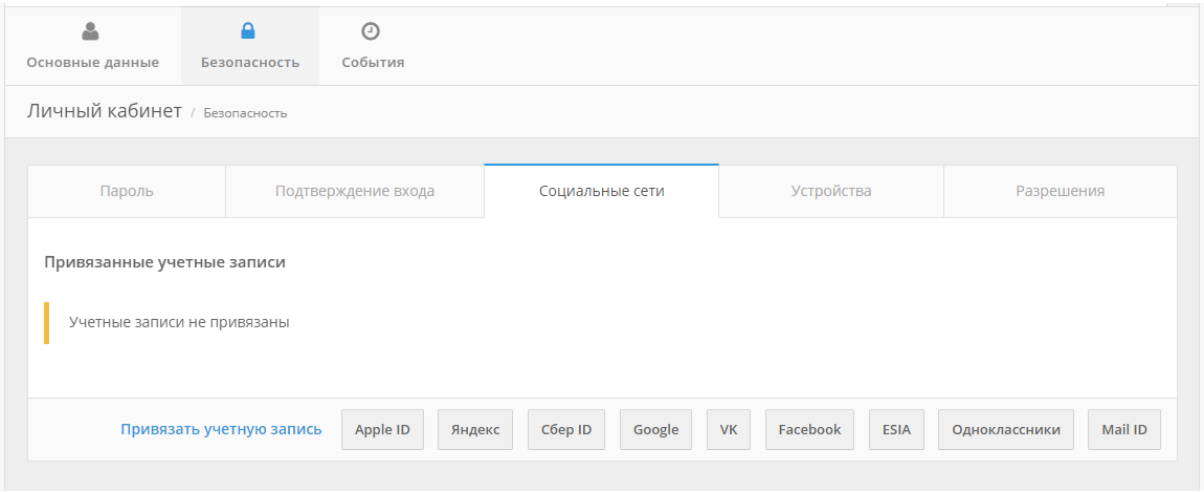


- на странице «Запомненные устройства доступа» найти устройство, которое необходимо удалить, и нажать значок «Удалить» ( ) напротив названия данного устройства.

4.5 Просмотр и управление привязанными учетными записями социальных сетей

Для просмотра списка аккаунтов социальных сетей, связанных с учетной записью, авторизованному пользователю необходимо осуществить следующие действия:

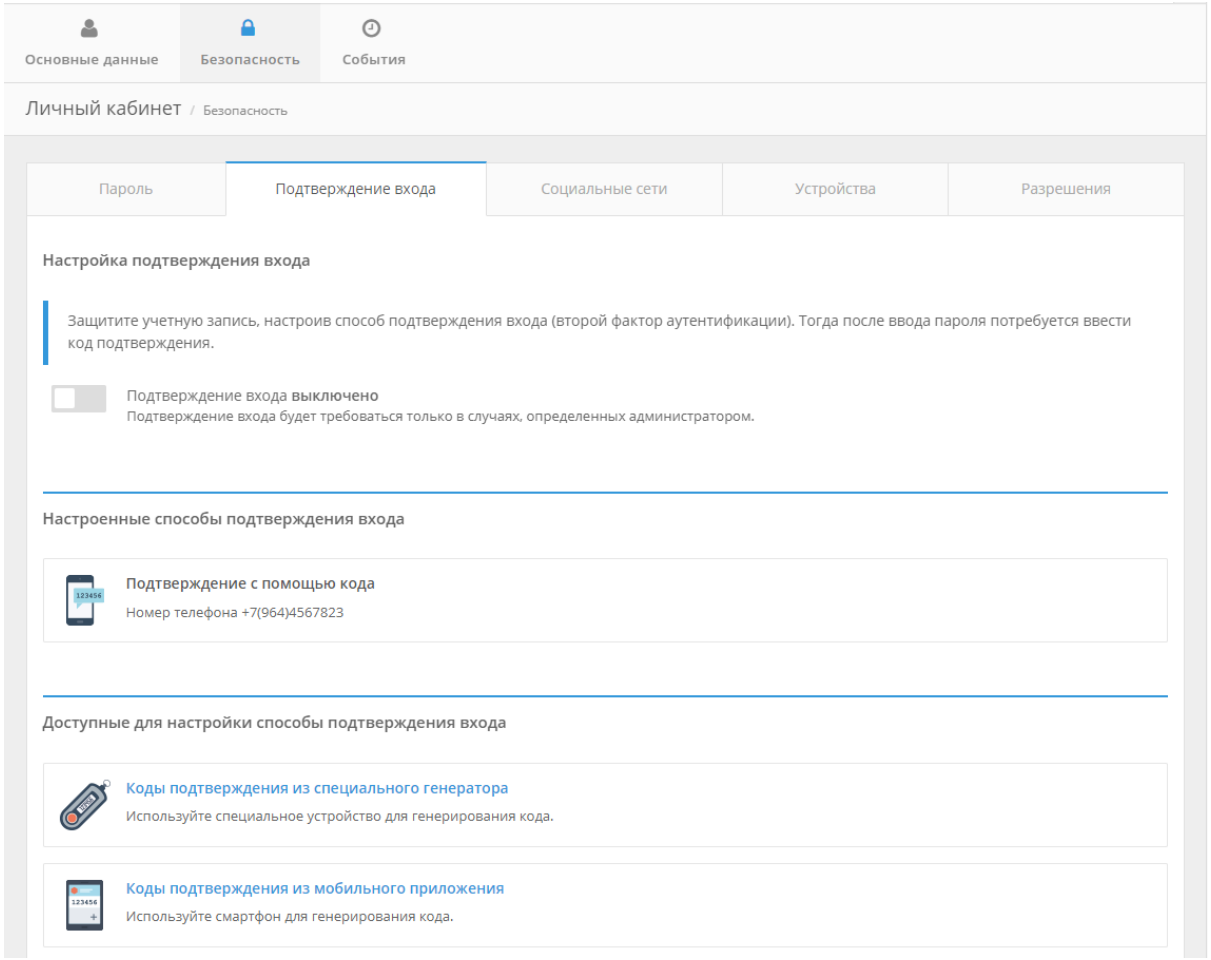
- на странице Личного кабинета перейти в раздел «Безопасность» и выбрать вкладку «Социальные сети»;



- в случае необходимости удаления связки с аккаунтом социальной сети следует нажать значок «Удалить» ( ) напротив названия соответствующей записи. Приложение пропадет из списка.

4.6 Настройка способов подтверждения входа (двухфакторной аутентификации)

Для включения второго фактора аутентификации авторизованному пользователю необходимо на странице Личного кабинета перейти в раздел «Безопасность» и выбрать вкладку «Подтверждение входа», где представлена возможность настройки методов подтверждения входа.



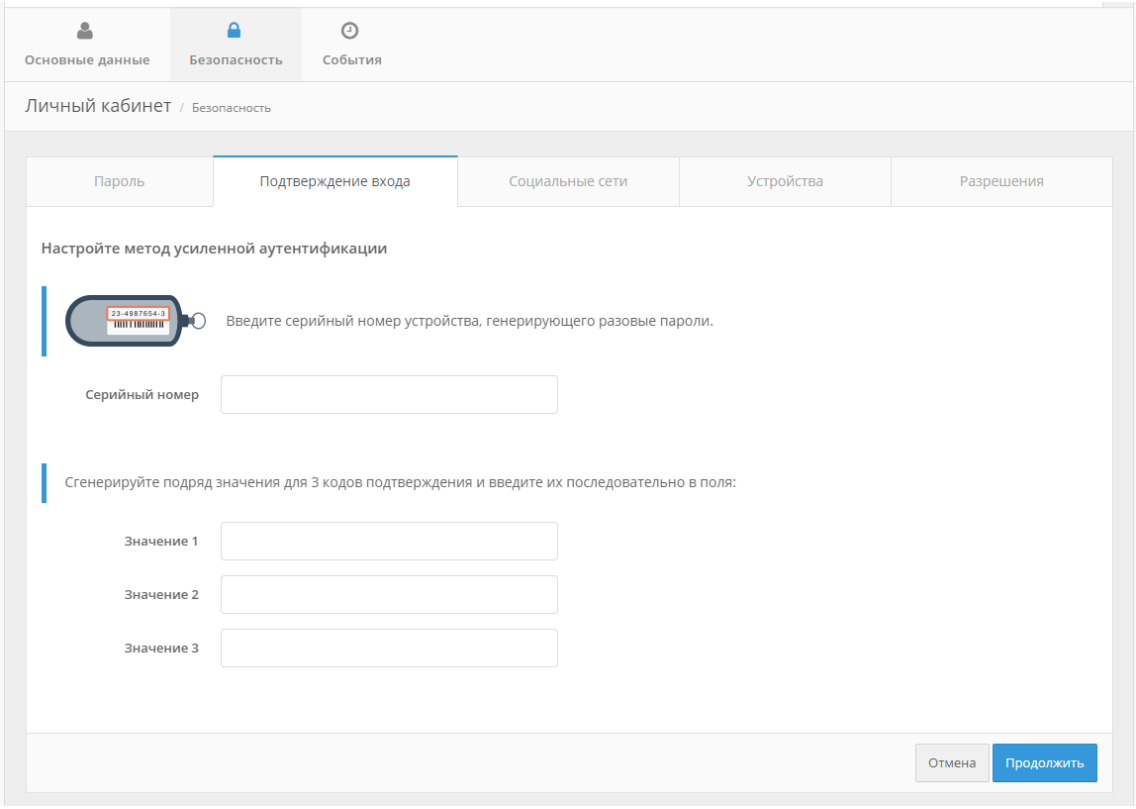
Доступны следующие способы подтверждения входа:

1. С помощью разовых паролей, полученных SMS-сообщением или через push-уведомление.
2. С помощью кодов подтверждения из специального устройства, генерирующего разовые пароли.
3. С помощью кодов подтверждения, генерируемых в специальном мобильном приложении.

Первый вариант предполагает наличие привязанного номера мобильного телефона в учетной записи пользователя. Второй способ может использоваться при наличии специального устройства, генерирующего разовые пароли. Третий способ предполагает наличие установленного специального мобильного приложения.

Для настройки подтверждения входа с помощью специального генератора пользователю необходимо выполнить следующие действия:

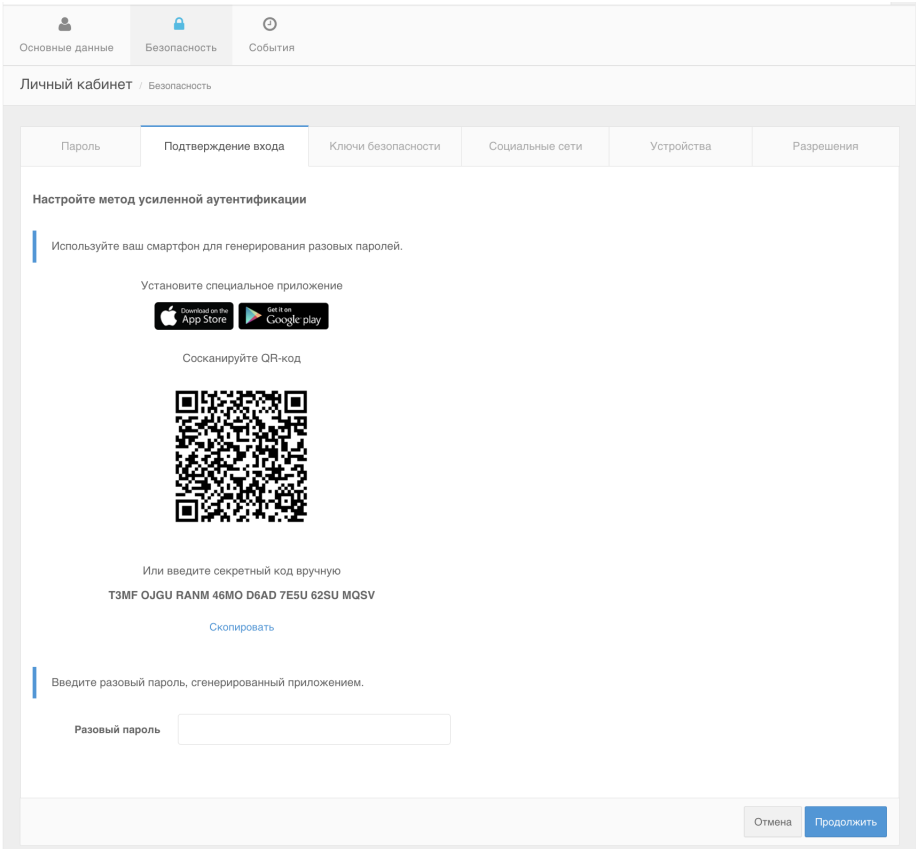
- на вкладке «Подтверждение входа» в разделе «Доступные для настройки способы подтверждения входа» нажать на кнопку «Коды подтверждения из специального генератора», в результате чего откроется привязка устройства для генерации кодов в качестве способа двухфакторной аутентификации;



- ввести серийный номер устройства, генерирующего разовые пароли, в соответствующее поле на странице;
- сгенерировать подряд значения для 3 кодов подтверждения и вести их последовательно в соответствующие поля, приведенные на странице.

Для настройки мобильного приложения для получения кодов подтверждения, пользователю необходимо выполнить следующие действия:

- на вкладке «Подтверждение входа» в разделе «Доступные для настройки способы подтверждения входа» нажать на кнопку «Мобильное приложение», в результате чего откроется окно установки и настройки мобильного приложения в качестве способа двухфакторной аутентификации;

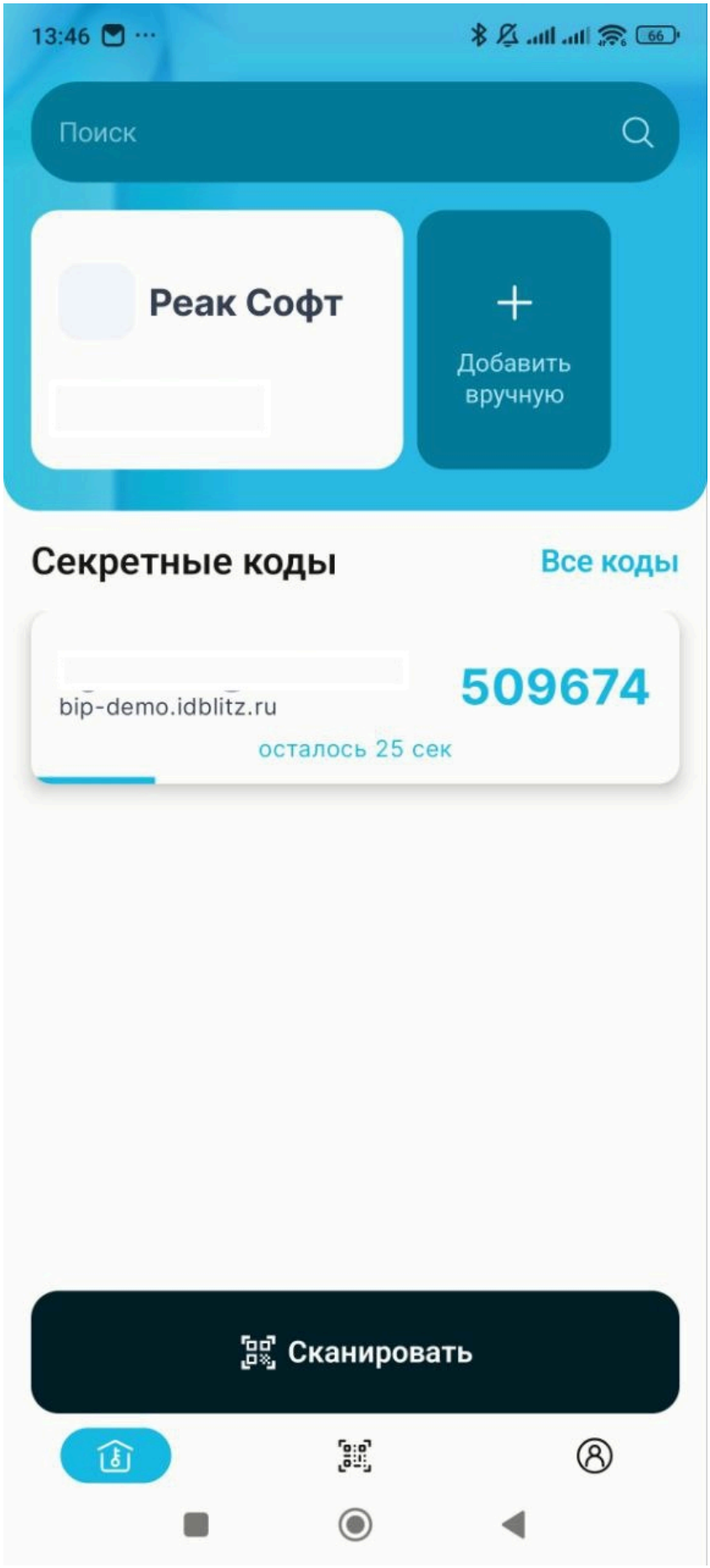


- скачать на смартфон мобильное приложение для генерации паролей. На странице настройки этого метода представлены ссылки, по которым можно загрузить данное приложения для различных мобильных ОС:

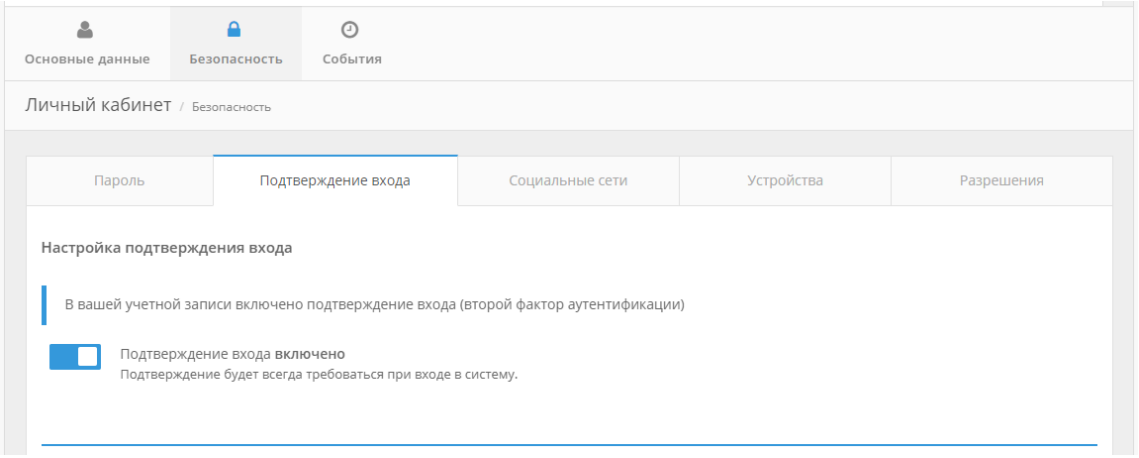
  – для iOS;

  – для Android.

- связать мобильное приложение, например, Blitz Key и учетную запись пользователя. Для этого необходимо открыть мобильное приложение Blitz Key и сфотографировать QR-код, или вручную ввести в приложение секретный код, отображенный на экране.

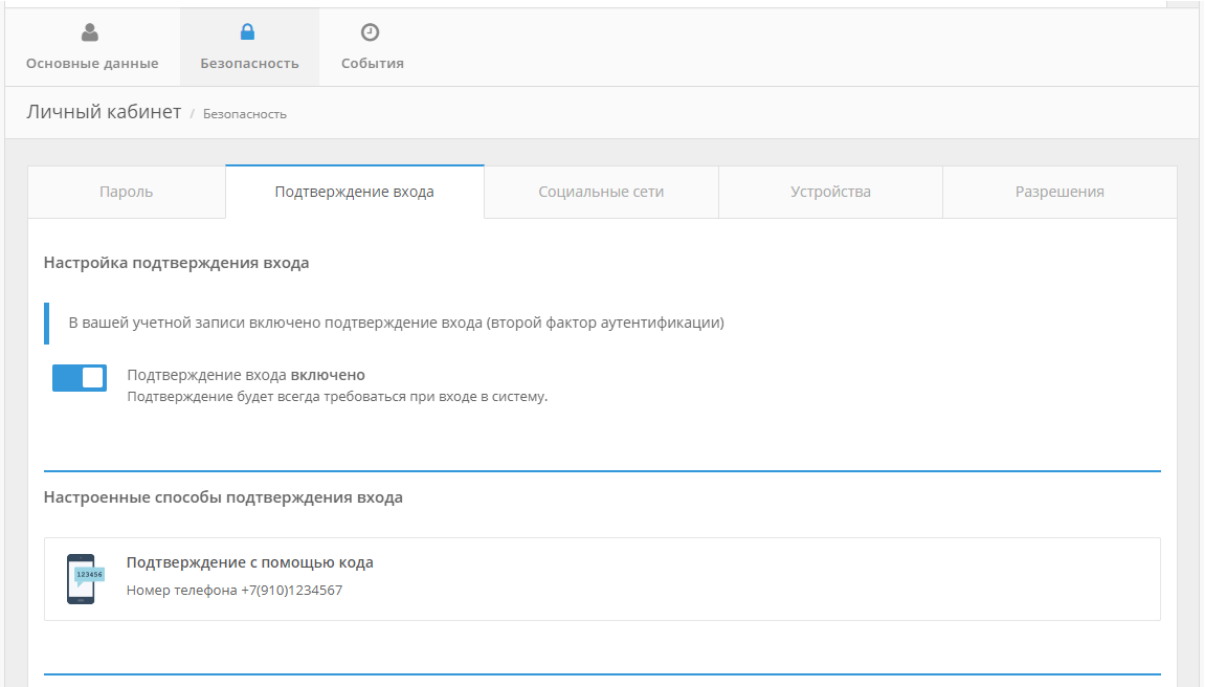

13:46
Поиск
Реак Софт
Добавить вручную
Секретные коды
Все коды
509674
bip-demo.idblitz.ru
осталось 25 сек
Сканировать

- ввести разовый код подтверждения, сгенерированный мобильным приложением, в соответствующее поле в браузере для подтверждения связки учетной записи и мобильного приложения.
- убедиться, что в Личном кабинете в разделе Настроенные способы подтверждения входа появится соответствующий способ, и подтверждение входа включено – переключатель «Подтверждение входа» включен.



Чтобы использовать второй фактор подтверждения входа – доставка кодов подтверждения, достаточно привязать номер мобильного телефона к учетной записи.

Далее необходимо осуществить переход в раздел «Безопасность» и убедиться, что на вкладке «Подтверждение входа» данный способ подтверждения входа настроен успешно и переключатель «Подтверждение входа» включен.



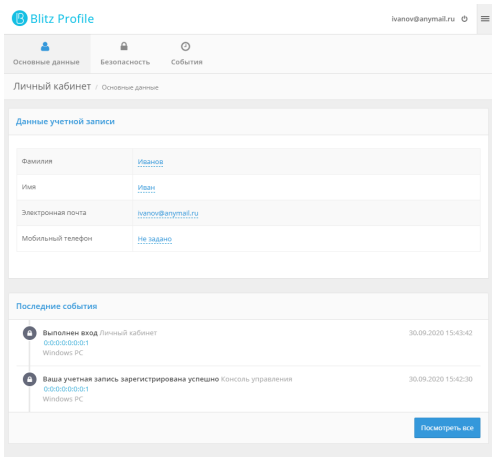
Для отключения двухфакторной аутентификации необходимо перейти в Личный кабинет в раздел «Подтверждение входа» и выключить переключатель «Подтверждение входа».

4.7 Просмотр событий безопасности

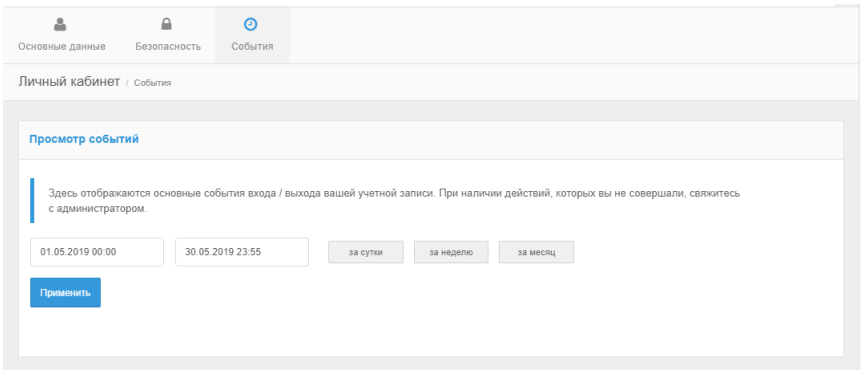
Пользователю доступен просмотр основных событий, связанных с действиями учетной записи. Например, информация о входе и/или выходе в Личный кабинет из-под учетной записи пользователя. Чтобы просмотреть основные события безопасности, связанные с действиями пользователя, необходимо выполнить

следующие действия:

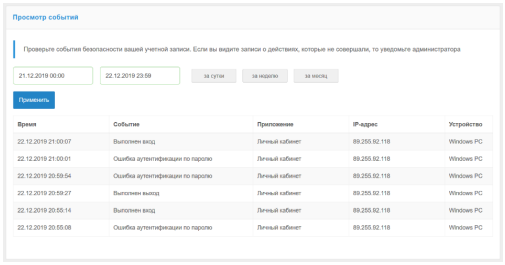
- на странице Личного кабинета в разделе «Основные данные» и перейти к блоку «Последние события». В нем содержится следующая информация о последних действиях пользователя учетной записи:
- тип события;
- система, в контексте которой совершено действие;
- IP-адрес устройства;
- устройство, с которого совершено действие;
- дата и время события.



При необходимости посмотреть расширенный перечень событий или более ранние события можно нажать на кнопку «Посмотреть все» или перейти в раздел «События».



В этом разделе необходимо указать время, за которое следует отобразить события и нажать на кнопку «Применить» (либо выбрать один из предусмотренных вариантов – за сутки, за неделю или за месяц). В результате будут показаны события за выбранный период.



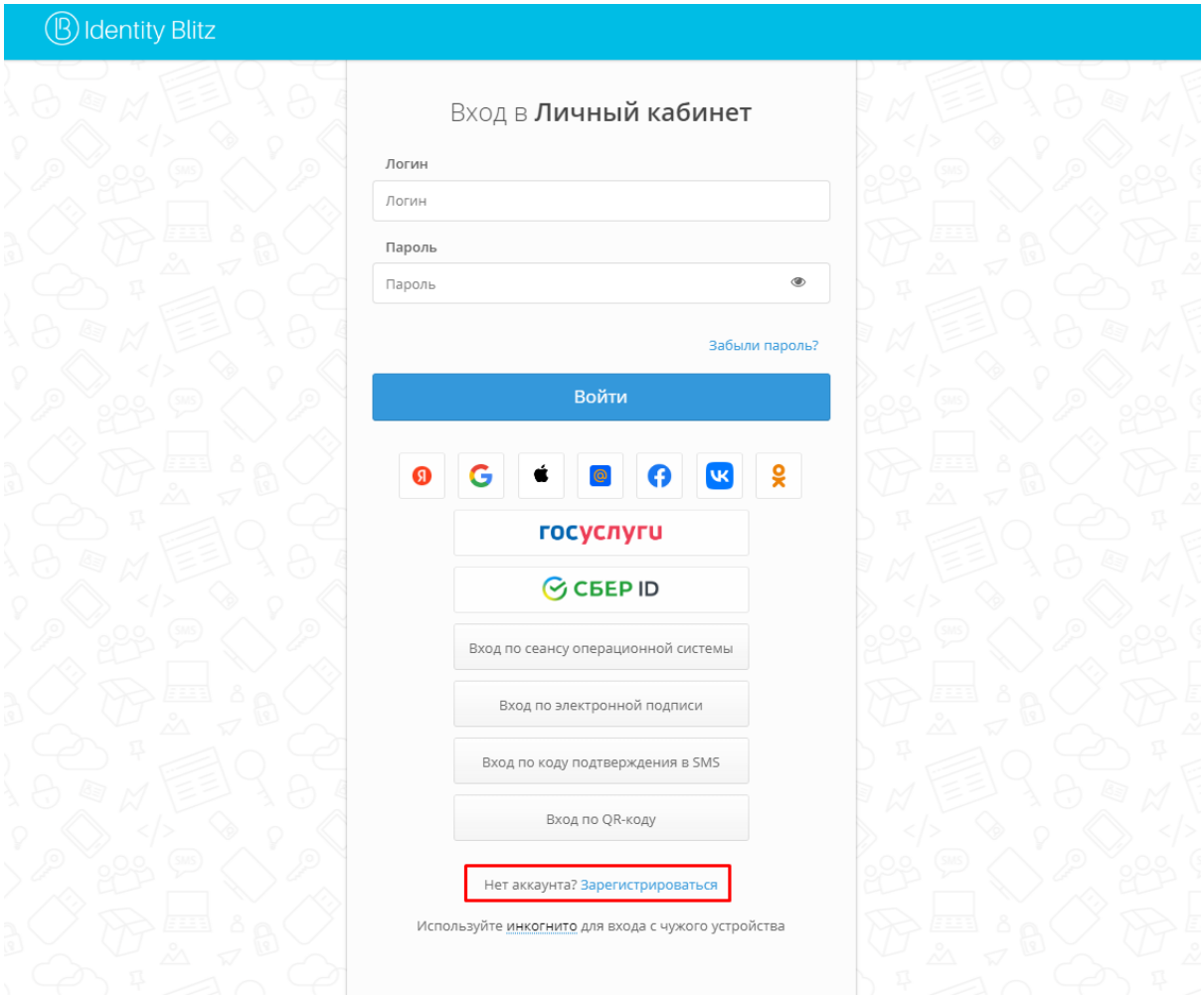
Глава 5

Регистрация и восстановление доступа

5.1 Регистрация нового пользователя

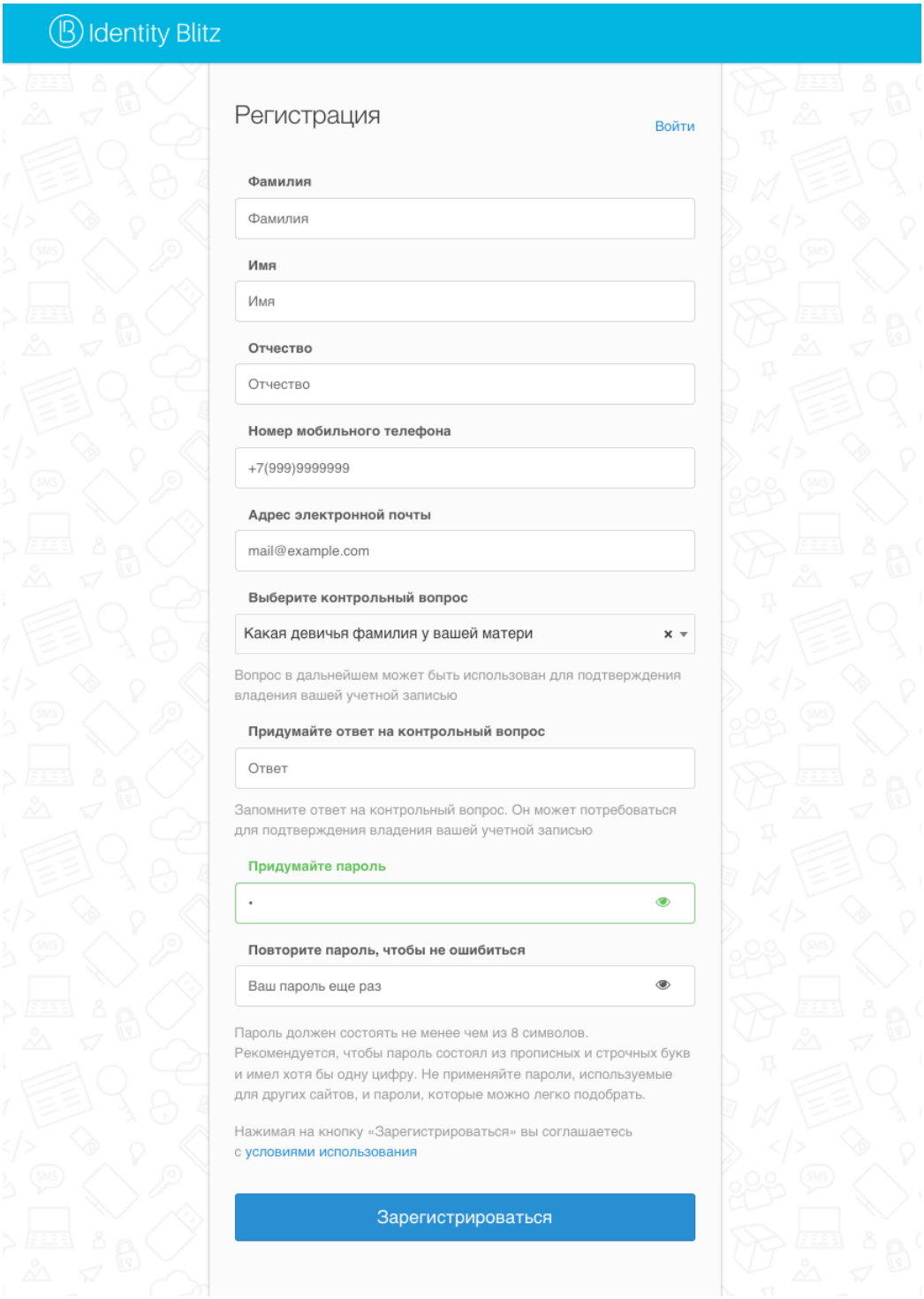
Регистрация пользователя в Blitz Identity Provider является обязательным условием работы пользователя в подключенных веб-сайтах и приложениях. Для регистрации пользователя необходимо выполнить следующие действия.

- запустить веб-браузер;
- в адресной строке веб-браузера ввести ссылку портала, подключенного к Blitz Identity Provider, и инициировать вход;
- на открывшейся странице входа перейти по ссылке «Зарегистрироваться».



Внешний вид страницы регистрации пользователей может отличаться в зависимости от настроек Blitz Identity Provider, установленных организацией. На странице регистрации пользователю необходимо ввести свои данные в соответствующие поля, например:

- фамилия;
- имя;
- номер мобильного телефона. на указанный номер будет отправлено SMS с кодом для подтверждения мобильного телефона.
- адрес электронной почты. На указанный адрес будет отправлено письмо с кодом подтверждения почты;
- пароль и подтверждение пароля;



Далее пользователю может потребоваться ввести кода подтверждения, который был отправлен в SMS-сообщении на указанный при регистрации номер мобильного телефона. После получения кода подтверждения на мобильный телефон необходимо вставить его в соответствующее поле.

Далее также может потребоваться дополнительное подтверждение адреса электронной почты, указанного при регистрации, на который будет отправлен код подтверждения и ссылка. Необходимо прочитать письмо, скопировать полученный код и вставить его в поле ввода или перейти по ссылке из письма.

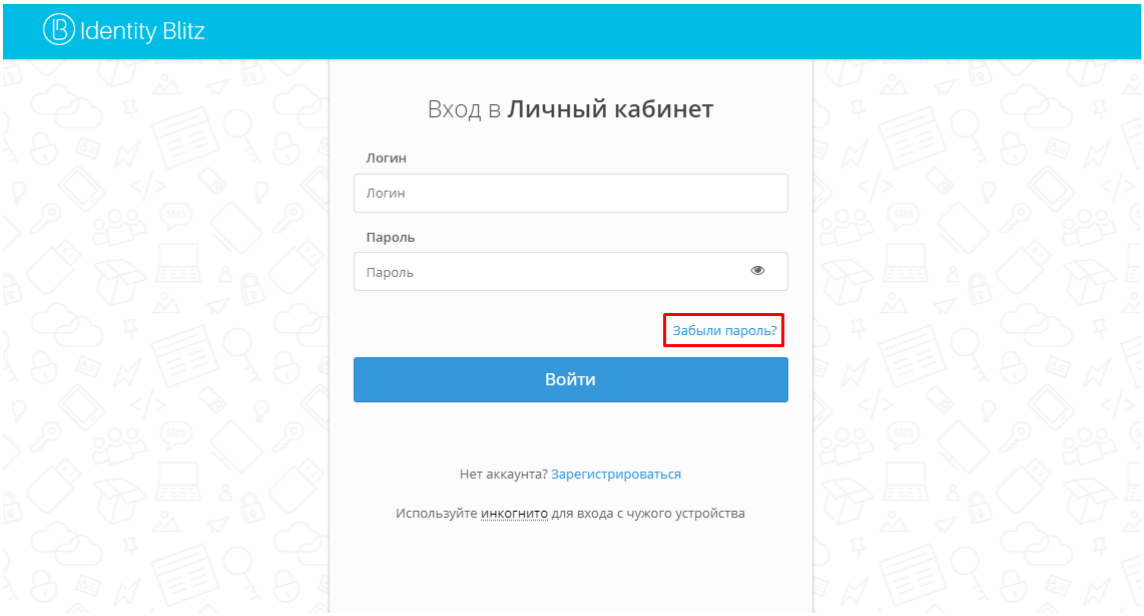
После успешной регистрации произойдёт автоматический вход в систему, куда пользователь изначально инициировал вход.

5.2 Восстановление пароля по логину

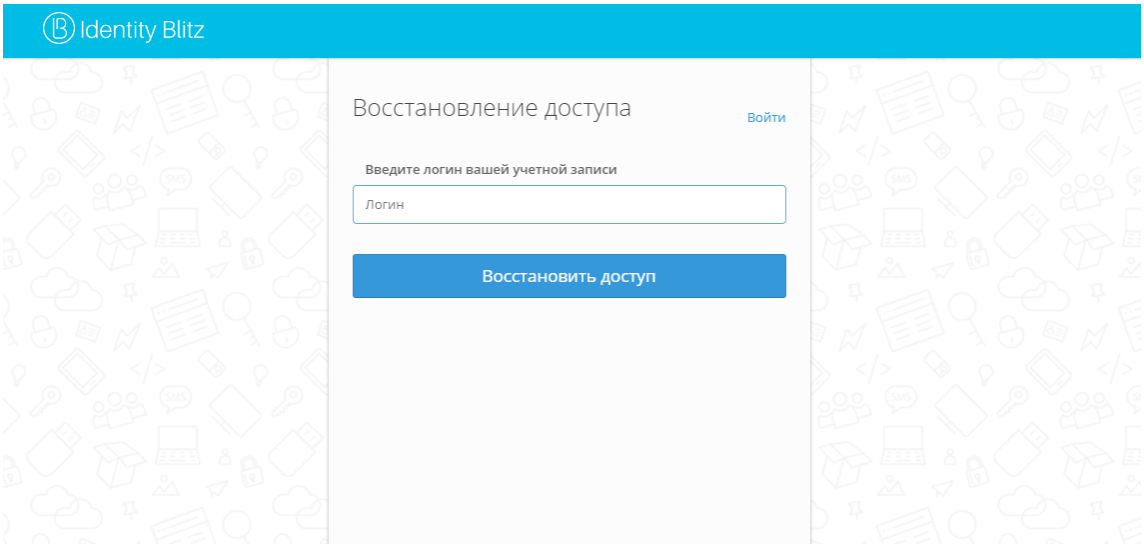
Восстановить пароль учетной записи пользователя можно уникальному идентификатору. В качестве идентификатора в зависимости от конфигурации системы аутентификации, установленной в организации, могут выступать адрес электронной почты, номер мобильного телефона, табельный номер и др.

Для восстановления пользователю необходимо выполнить следующие действия:

- на странице входа перейти по ссылке «Забыли пароль?». В результате откроется страница восстановления пароля.



- на странице «Восстановления доступа» ввести уникальный идентификатор:
- при вводе адреса электронной почты, указанного при регистрации, письмом придет инструкция по восстановлению пароля;
- при вводе номера мобильного телефона, указанного при регистрации, на указанный номер поступит сообщение с одноразовым паролем;
- ввести в качестве логина уникальный идентификатор, указанный при регистрации, откроется страница для выбора способа получения кода для восстановления пароля (при наличии альтернативных каналов доставки кода восстановления);
- опционально система может предложить ввести проверочный атрибут (например, фамилию) – если по указанному идентификатору будет найдена учетная запись, то для восстановления значение проверочного атрибута должно соответствовать тому, что хранится в учетной записи;
- нажать кнопку «Восстановить доступ».



Если данные введены верно и в системе найден зарегистрированный пользователь, в учетной записи которого указаны соответствующие данные (мобильный телефон и/или электронная почта и/или уникальный идентификатор), то далее необходимо следовать инструкциям для перехода на страницу ввода нового пароля. Примеры экранов приведены на следующих рисунках.

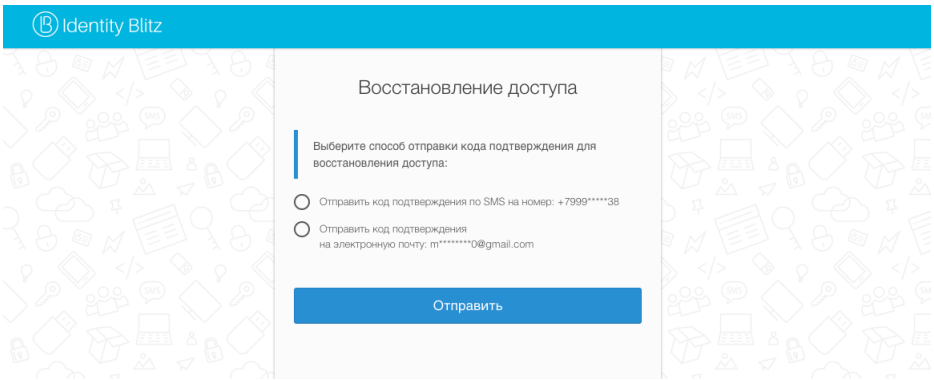


Рис. 1: Экран выбора способа отправки кода подтверждения для восстановления доступа

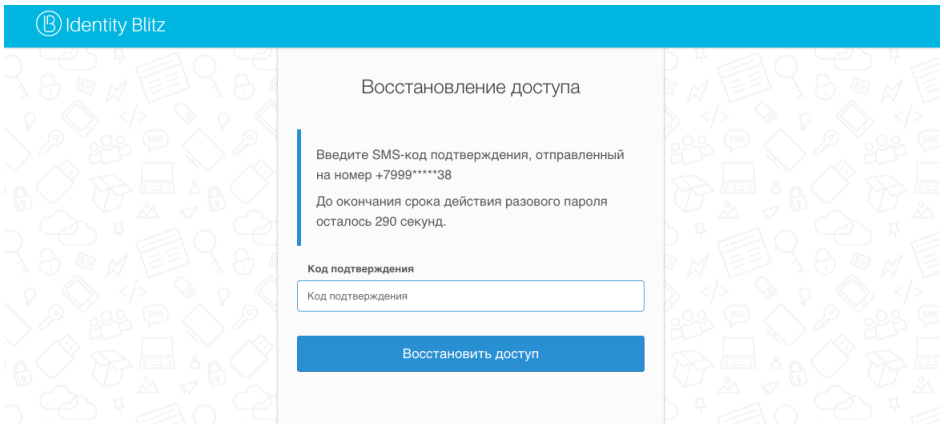


Рис. 2: Экран ввода SMS-кода подтверждения

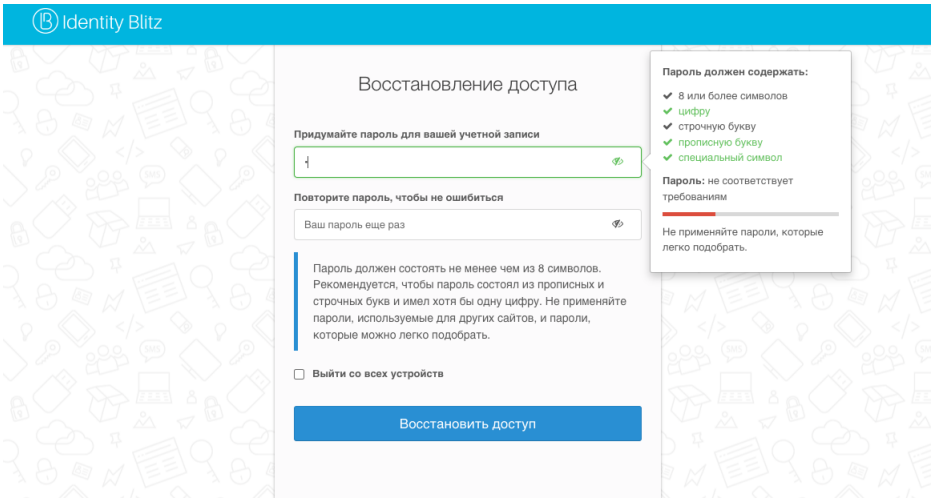


Рис. 3: Экран ввода пароля для восстановления доступа

При задании нового пароля будет отображаться степень его надежности. Чтобы повысить надежность пароля, необходимо увеличить его длину или использовать специальные символы. На этой странице пользователю необходимо дважды ввести новый пароль, отметить при необходимости чекбокс «Выйти со всех устройств» и нажать «Восстановить доступ». После успешного изменения пароля осуществится автоматический вход в систему, куда пользователь изначально инициировал вход.

В случае появления сообщений о том, что пользователь не был найден, или отсутствии каких-либо личных данных, необходимо осуществить восстановление доступа с использованием другого контакта.

5.3 Восстановление пароля при включенной двухфакторной аутентификации

При восстановлении пароля от учетной записи, для которой включен режим двухфакторной аутентификации, требуется дополнительное подтверждение. Например, после ввода кода подтверждения из SMS система потребует выбор одного из предусмотренных дополнительных способов подтверждения:

- код подтверждения, отправляемый на адрес электронной почты (при наличии в учетной записи адреса электронной почты);
- код подтверждения, генерируемых в специальном мобильном приложении (если настроен);
- ответ на контрольный вопрос.

Примеры экранов приведены на рисунках.

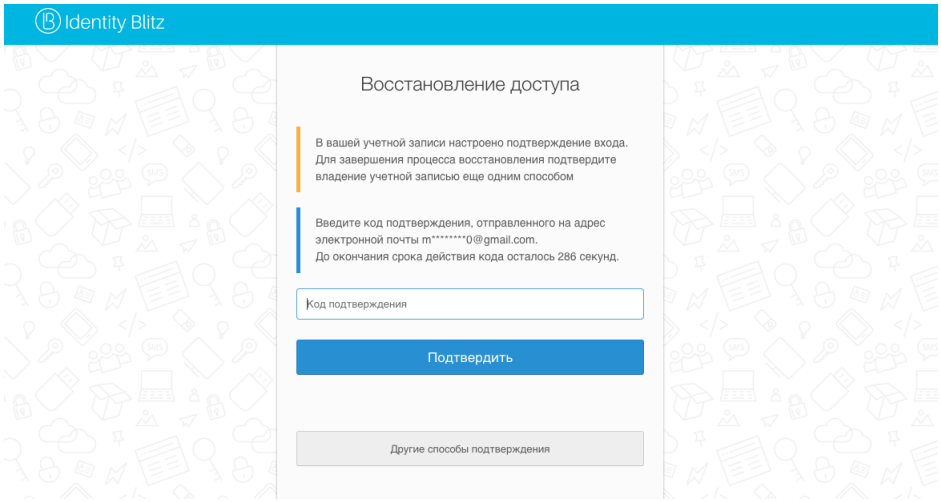


Рис. 4: Экран ввода кода подтверждения, отправленного на электронную почту

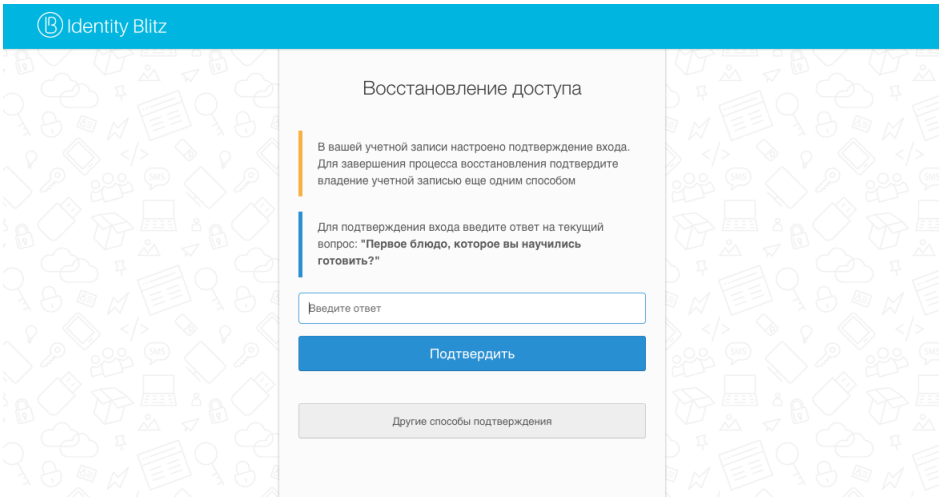


Рис. 5: Экран ввода ответа на секретный вопрос

Следует учесть, что в случае отсутствия дополнительного способа подтверждения сброс пароля и доступ к учетной записи будет невозможен.