



Aladdin 2FA. Руководство пользователя

Инструкция по работе с мобильным приложением Aladdin
2FA

Версия продукта	1.3.2
Статус	Публичный
Дата	04.04.2025
Листов	63

Оглавление

1. О документе.....	4
1.1 Назначение документа.....	4
1.2 На кого ориентирован документ.....	4
1.3 Обозначения и сокращения.....	4
2. Мобильное приложение Aladdin 2FA. Общая информация.....	5
2.1 Обозначения экранов, элементов интерфейса и терминов, используемых в работе с приложением.....	5
2.2 Регистрация аутентификатора.....	6
2.3 Что делать в случае возникновения ошибки.....	9
2.3.1 База знаний с описанием известных ошибок.....	9
2.3.2 Быстрая помощь.....	10
2.3.3 Обращение в техническую поддержку.....	11
3. Инструкция для пользователей Android.....	12
3.1 Первый запуск приложения Aladdin 2FA.....	12
3.2 Добавление аутентификатора.....	15
3.3 Редактирование аутентификатора.....	18
3.3.1 Удаление.....	19
3.3.2 Переименование.....	19
3.3.3 Перемещение.....	20
3.4 Использование одноразового пароля.....	20
3.5 PUSH-аутентификация.....	21
3.5.1 PUSH-аутентификация при закрытом приложении.....	21
3.5.2 PUSH-аутентификация в открытом приложении.....	24
3.6 Настройки приложения.....	24
3.7 Биометрия.....	26
3.7.1 Отключение регулярного ввода PIN-кода.....	26
3.8 Резервное копирование.....	27
3.9 Восстановление из копии.....	29
4. Инструкция для пользователей iOS.....	34
4.1 Первый запуск приложения Aladdin 2FA.....	34
4.2 Добавление аутентификатора.....	36
4.3 Редактирование аутентификатора.....	39
4.3.1 Удаление.....	39
4.3.2 Переименование.....	40
4.3.3 Перемещение.....	40
4.3.4 Просмотр информации об аутентификаторе.....	41
4.4 Использование одноразового пароля.....	41
4.5 PUSH-аутентификация.....	42
4.5.1 PUSH-аутентификация при закрытом приложении.....	42
4.5.2 PUSH-аутентификация в открытом приложении.....	44
4.6 Настройки приложения.....	44
4.7 Биометрия.....	45
4.7.1 Отключение напоминания пароля.....	46
4.8 Создание бэкапа.....	46
4.9 Восстановление из бэкапа.....	49
5. Настройки смартфонов, при которых приложение работает некорректно.....	52
5.1 Время смартфона переведено более, чем на 23 часа.....	52
5.2 На некоторых смартфонах не приходят PUSH-уведомления.....	52

Приложение А. Добавление сертификата в пользовательское хранилище на устройстве	53
Для устройств с ОС Android	53
Для устройств с ОС iOS	54
Приложение Б. Запуск телеграм-бота	57
Для устройств с ОС Android	57
Для устройств с ОС iOS	58
Контакты	61
Офис (общие вопросы)	61
Техническая поддержка	61
Список литературы	62
Регистрация изменений	63

1. О документе

1.1 Назначение документа

Настоящий документ представляет собой руководство пользователя по работе с мобильным приложением Aladdin 2FA.

1.2 На кого ориентирован документ

Документ предназначен для пользователей мобильного приложения Aladdin 2FA.

1.3 Обозначения и сокращения

- Aladdin 2FA – мобильное приложение, представляющее собой генератор одноразовых паролей (OTP), используемых в качестве второго фактора аутентификации (2FA);
- JAS – сервер усиленной аутентификации пользователей в информационных системах с применением второго фактора аутентификации (2FA);
- JMS – система управления средствами аутентификации, такими как электронные ключи, PUSH-, OTP-, U2F-аутентификаторы и сертификаты пользователей;
- OTP (One-Time Password) – одноразовый пароль. Действителен только для одного сеанса аутентификации;
- PIN-код – секретная последовательность, известная только пользователю, которую необходимо предъявить для аутентификации пользователя в мобильном приложении Aladdin 2FA;
- PUSH-аутентификация – метод аутентификации с помощью PUSH-уведомлений, используемый на мобильных устройствах;
- Аутентификация - действия по проверке подлинности субъекта (и/или объекта) доступа, а также по проверке принадлежности субъекту (и/или объекту) доступа предъявленного идентификатора доступа и аутентификационной информации.

2. Мобильное приложение Aladdin 2FA. Общая информация

Мобильное приложение Aladdin 2FA представляет собой генератор одноразовых паролей (OTP), используемых в качестве второго фактора аутентификации.

С помощью мобильного приложения Aladdin 2FA можно войти в учетную запись на компьютере, на корпоративном портале или на общедоступных интернет-ресурсах, используя в качестве второго фактора аутентификации одноразовый пароль или PUSH-аутентификацию.

Мобильное приложение поддерживает работу со всеми совместимыми сервисами и ресурсами, предоставляющими возможность использовать одноразовые пароли в качестве второго фактора аутентификации.

В мобильном приложении Aladdin 2FA предусмотрена защита биометрией (опционально), доступной на используемом мобильном устройстве, или PIN-кодом.

Мобильное приложение можно свободно загружать для операционных систем iOS и Android из магазинов приложений (введя в строке поиска **Aladdin 2FA**), также доступно для скачивания [на сайте Алладин](#) для разных версий ОС.

2.1 Обозначения экранов, элементов интерфейса и терминов, используемых в работе с приложением

Для удобства работы с мобильным приложением Aladdin 2FA и документом условимся по обозначениям элементов интерфейса и терминам:

1. Аутентификатор – элемент интерфейса мобильного приложения, с помощью которого пользователь получает возможность входа в определенный сервис или систему с использованием второго фактора;
2. Мобильное приложение Aladdin 2FA поддерживает следующие виды аутентификаторов:
 - TOTP-аутентификатор – аутентификатор, реализующий стандарт формирования одноразового пароля TOTP (RFC 6238). Пример отображения TOTP-аутентификатора приведен ниже (см. Рисунок 1);



Рисунок 1 - Aladdin 2FA. Отображение TOTP-аутентификатора

- HOTP-аутентификатор – аутентификатор, реализующий стандарт формирования одноразового пароля HOTP (RFC 4226). Пример отображения HOTP -аутентификатора приведен ниже (см. Рисунок 2);



Рисунок 2 - Aladdin 2FA. Отображение HOTP-аутентификатора

- PUSH-аутентификатор – аутентификатор, позволяющий использовать PUSH-аутентификацию. Пример отображения PUSH-аутентификатора приведен ниже (см. Рисунок 3);

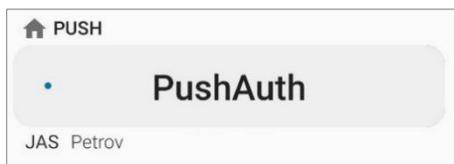


Рисунок 3 - Aladdin 2FA. Отображение PUSH-аутентификатора

3. Главный экран – приведен ниже (Рисунок 4). На нем отображаются зарегистрированные аутентификаторы, методы добавления аутентификаторов, кнопка вызова настроек мобильного приложения;
4. Пустой экран – приведен выше (см. Рисунок 5). На нем отображается информация о том, каким образом добавить аутентификатор. Пустой экран отображается при первом запуске мобильного приложения либо в случае, если все аутентификаторы были удалены.

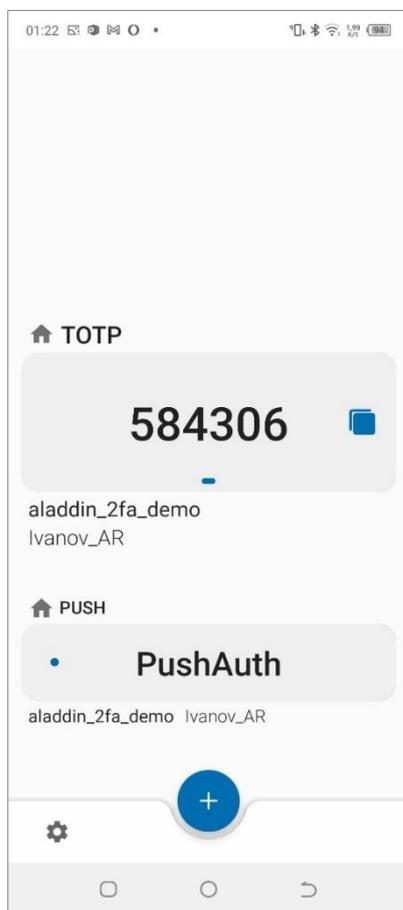


Рисунок 4 – Aladdin 2FA. Главный экран с добавленными аутентификаторами

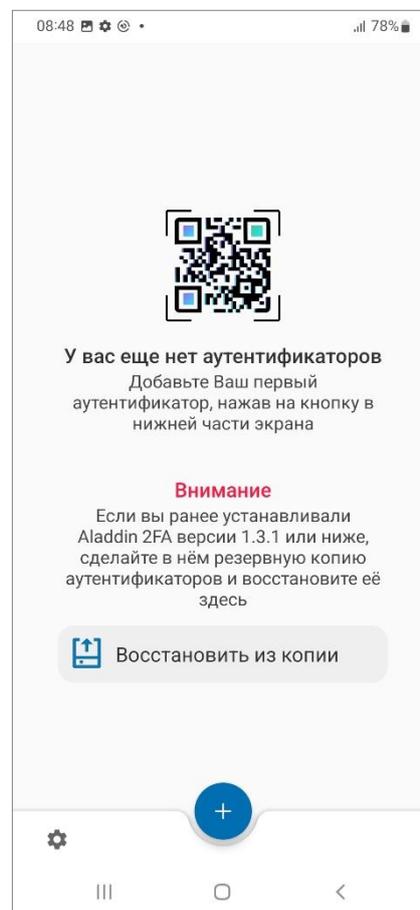


Рисунок 5 - Aladdin 2FA. Главный экран без аутентификаторов

2.2 Регистрация аутентификатора

Для регистрации аутентификатора можно воспользоваться следующими способами:

1. Отсканировать QR-код (см. подробнее подраздел 3.2 шаг 2);
2. Воспользоваться ссылкой для регистрации (подробное описание см. ниже);
3. Добавить аутентификатор вручную (см. подробнее подраздел 3.2 шаг 3).

При выборе второго варианта, на почтовый ящик придет письмо с вариантами регистрации аутентификаторов в мобильном приложении Aladdin 2FA. Пример письма приведен на рисунках (см. Рисунок 6 - Рисунок 8).

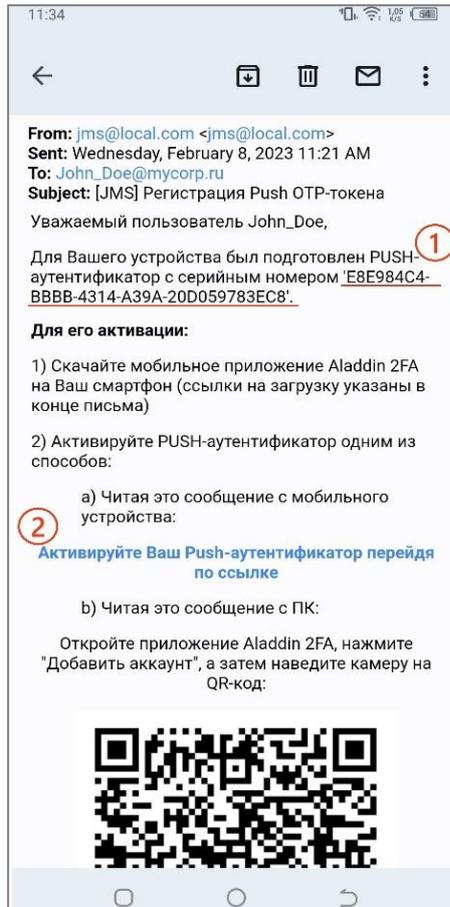


Рисунок 6 – Электронное письмо с вариантами регистрации в мобильном приложении Aladdin 2FA. Часть 1

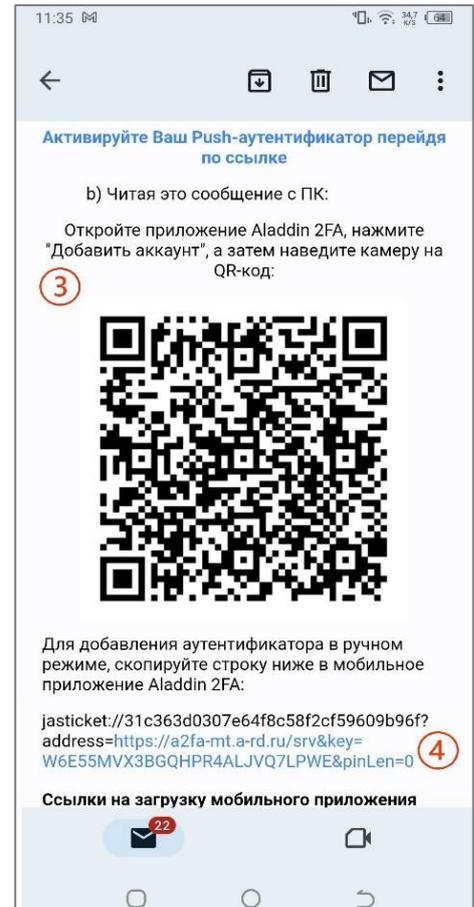


Рисунок 7 - Электронное письмо с вариантами регистрации в мобильном приложении Aladdin 2FA. Часть 2



Рисунок 8 - Электронное письмо с вариантами регистрации в мобильном приложении Aladdin 2FA. Часть 3

Подробнее про настройки и сценарии регистрации, представленные на рисунках выше, приведено в таблице ниже (см. Таблица 1).

Таблица 1 – Электронное письмо с вариантами регистрации в мобильном приложении Aladdin 2FA. Описание настроек

Элемент управления	Описание
1	Серийный номер PUSH-аутентификатора. Серийный номер может понадобиться при обращении в поддержку при возникновении сложностей в ходе регистрации в мобильном приложении
2	Ссылка для регистрации PUSH-аутентификатора. Данный сценарий применим в случае, если электронное письмо получено на том же устройстве, на котором установлено мобильное приложение Aladdin 2FA. Тогда, при нажатии на ссылку, будет открыто мобильное приложение, в котором после ввода PIN-кода или предъявления биометрии, будет зарегистрирован PUSH-аутентификатор
3	QR-код для регистрации PUSH-аутентификатора. В случае, если электронное письмо получено на компьютере, необходимо отсканировать QR-код из письма, совершив вход в мобильное приложение Aladdin 2FA

Элемент управления	Описание
4	Строка для ручного ввода в мобильном приложении. Данный сценарий применим в случае, если электронное письмо получено на том же смартфоне, на котором установлено мобильное приложение Aladdin 2FA. Необходимо скопировать строку с помощью долгого нажатия на нее и выбора пункта <Копировать> из контекстного меню. Скопированную строку вставить в окне [Ручное добавление]. Подробнее про добавление строки вручную см.п. 3.2 Добавление (для ОС Android) или п.4.2 Добавление аутентификатора (для ОС iOS)
5	Ссылки на страницу Aladdin 2FA на официальном сайте Аладдин с информацией о поддерживаемых ОС и на различные маркетплейсы для загрузки приложения

2.3 Что делать в случае возникновения ошибки

Иногда в приложении могут возникать непредвиденные ошибки или сбои. Данный раздел поможет с тем, чтобы понять, как поступить при возникновении таких ситуаций.

2.3.1 База знаний с описанием известных ошибок

В случае возникновения ошибки, если она уже известна, можно самостоятельно установить причину и попробовать ее устранить.

Если произошла ошибка в приложении и отображается кнопка <Помощь с этой ошибкой> (см. Рисунок 9) - это говорит о том, что ошибка известная и ее описание есть в базе знаний.

При нажатии на кнопку будет открыта страница в браузере устройства, на которой приведено описание данной ошибки (см. Рисунок 10): будут указаны причины ее возникновения и как ее исправить.

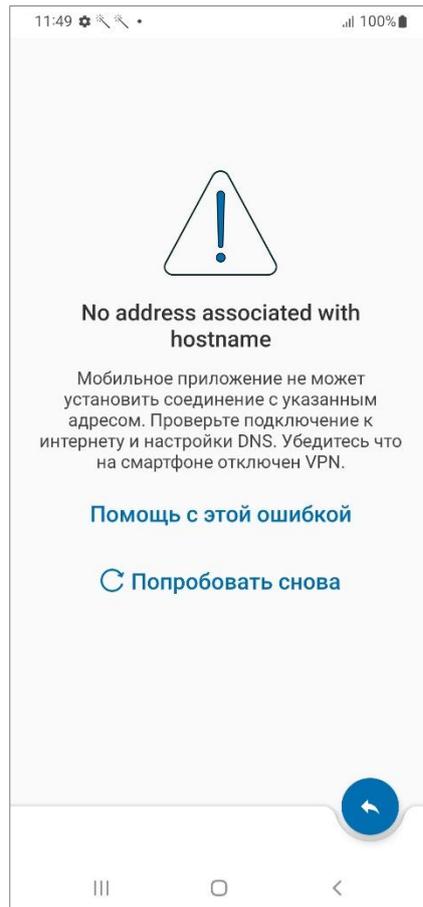


Рисунок 9 - Aladdin 2FA. Отображение окна с известной ошибкой



Рисунок 10 – Страница с описанием ошибки в базе знаний

2.3.2 Быстрая помощь

В случае если ошибка не описана в базе знаний, то будет открыт экран с быстрой помощью (см. Рисунок 11) – действиями, которые иногда помогают исправить ошибку.

Можно самостоятельно поискать ошибку в базе знаний, перейдя по ссылке <в нашей базе знаний> или написать команде разработчиков, нажав на <напишите нам>.



Рисунок 11 - Aladdin 2FA. Отображения окна [Быстрая помощь]

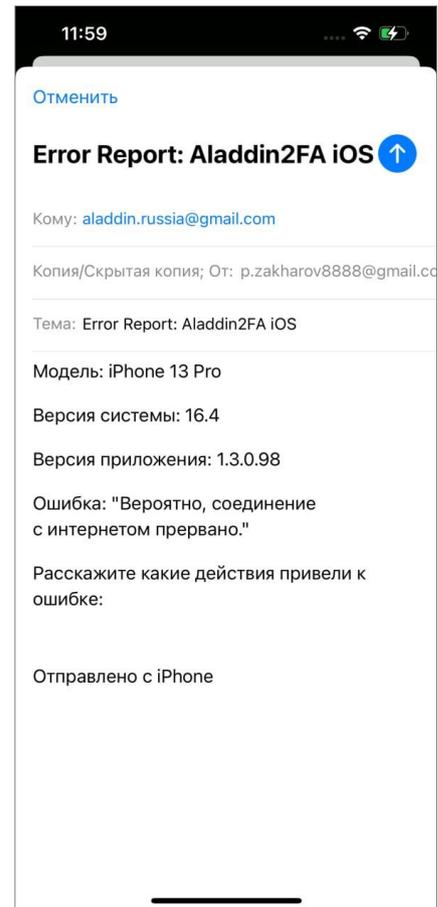


Рисунок 12 – Форма письма в техподдержку

2.3.3 Обращение в техническую поддержку

При переходе по ссылке <напишите нам> будет открыта форма создания нового письма в почтовом агенте (см. Рисунок 12) с предзаполненными полями. В письме необходимо описать действия, которые привели к ошибке.

3. Инструкция для пользователей Android

Внимание! Мобильное приложение «Aladdin 2FA» запрещено устанавливать и использовать на эмуляторах Android. Пример запуска приложения на эмуляторе приведен на рисунке (см. Рисунок 13).



Рисунок 13 – Запуск на эмуляторе

После установки мобильного приложения на смартфон с ОС Android, доступны сценарии работы, приведенные в данном разделе.

3.1 Первый запуск приложения Aladdin 2FA



1. Нажмите на иконку приложения для его запуска - ;
2. Будет открыто окно (см. Рисунок 14), где необходимо придумать PIN-код из четырех символов, с помощью которого будет осуществляться вход в приложение;
3. На следующем шаге необходимо повторно ввести PIN-код для подтверждения (см. Рисунок 15). После установки PIN-кода, если на устройстве используется биометрия, будет предложено включить возможность входа, используя биометрию (см. Рисунок 16);

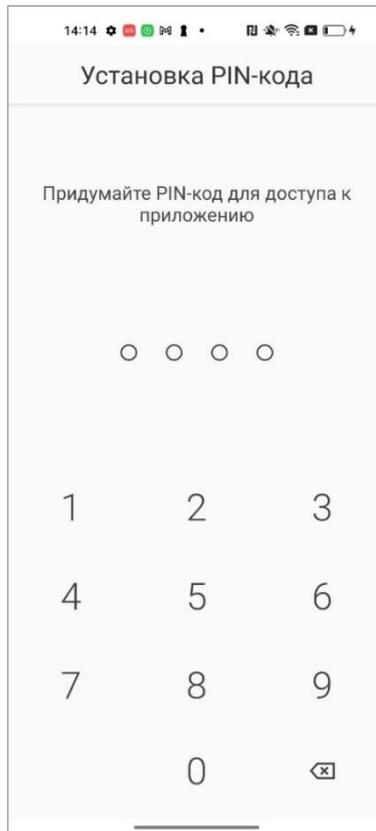


Рисунок 14 - Aladdin 2FA. Установка PIN-кода

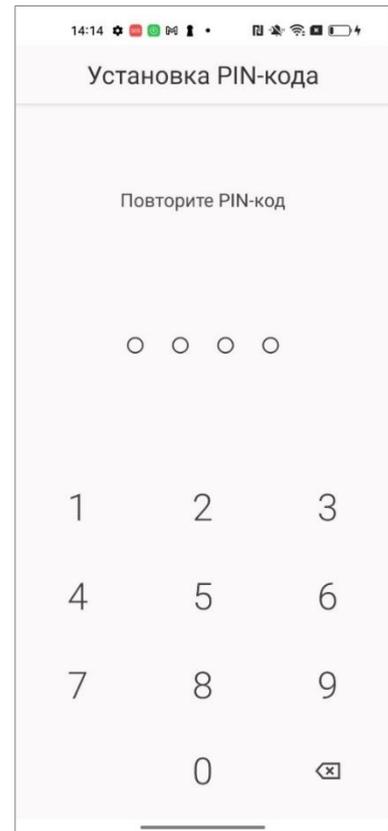


Рисунок 15 - Aladdin 2FA. Подтверждение PIN-кода

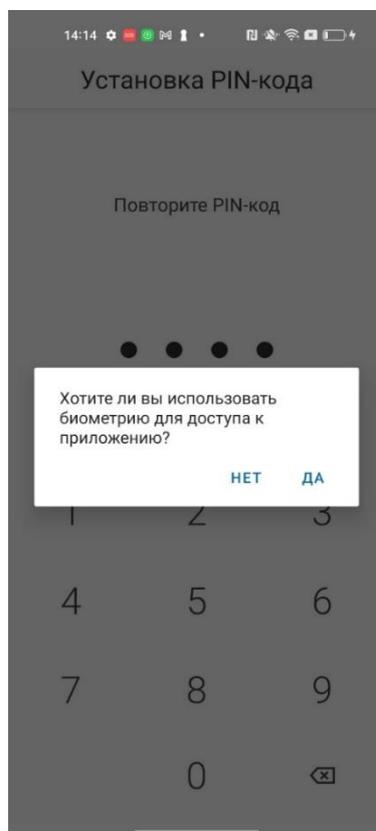


Рисунок 16 - Aladdin 2FA. Подключение биометрии

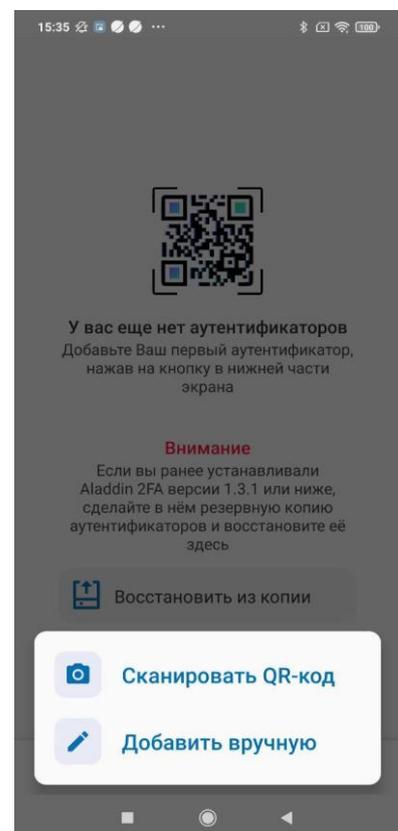


Рисунок 17 - Aladdin 2FA. Добавление аутентификатора

4. При первом входе в приложение на экране, приведенном выше (см. Рисунок 15), добавить аутентификатор с помощью кнопки . При нажатии на кнопку будет доступен выбор способа добавления аутентификатора:
- <Сканировать QR-код> - добавление аутентификатора с помощью камеры устройства;
 - <Добавить вручную> - добавить скопированную строку из электронного письма;
5. Самым распространенным способом регистрации аутентификатора является сканирование QR-кода с помощью камеры устройства. Для этого необходимо нажать <Сканировать QR-код>, после чего будет открыто окно, приведенное на Рисунок 18.

В зависимости от настроек смартфона может понадобиться предоставить разрешение для использования камеры

Необходимо просканировать QR-код, разместив его внутри квадратной области. Кнопка  осуществляет переключение между камерами на устройстве. В случае необходимости можно использовать фронтальную камеру для считывания QR-кода;

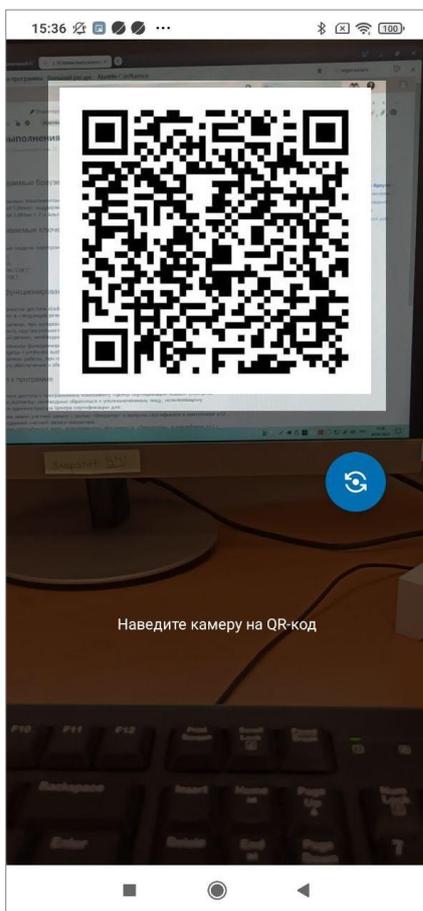


Рисунок 18 - Aladdin 2FA. Сканирование QR-кода



Рисунок 19 - Aladdin 2FA. Добавленный аутентификатор

6. После добавления аутентификатора главный экран приложения имеет вид, приведенный на рисунке (Рисунок 19), где цифрами обозначены следующие элементы:
- 1) – тип аутентификатора. Для одноразового пароля тип по умолчанию - TOTP или HOTP, для PUSH-аутентификации тип будет PUSH. Заданные по умолчанию иконку и тип аутентификатора можно изменить, подробнее описано в п. 3.3.2;

- 2) – сгенерированный одноразовый пароль. Скопировать значение можно с помощью кнопки ;
- 3) – индикатор – убывающий к центру отрезок, который показывает время, в течение которого пароль будет действителен. По истечении этого времени будет сгенерирован новый одноразовый пароль;
- 4) – учетные данные пользователя;
- 5) – кнопка добавления аутентификатора (см. п. 3.2);
- 6) – переход к меню с настройками приложения (см. п. 3.6);

3.2 Добавление аутентификатора

После каждого добавленного аутентификатора данных рекомендуется совершать процедуру резервного копирования (см. п. 3.8)

На главном экране мобильного приложения отображается перечень всех добавленных аутентификаторов (см. Рисунок 20).

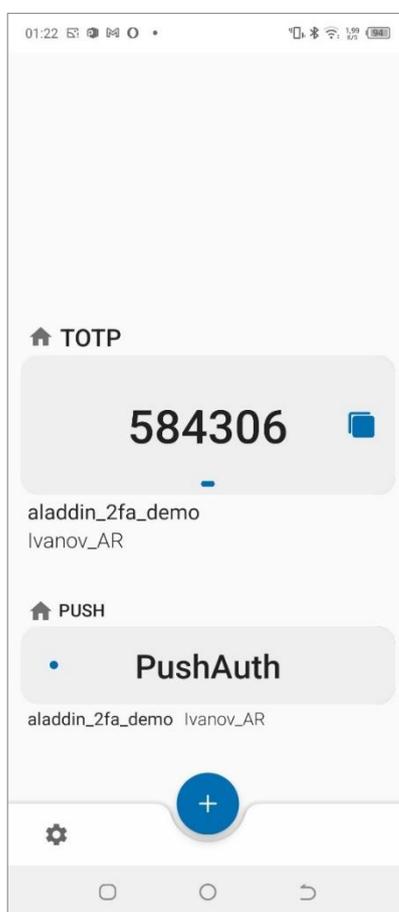


Рисунок 20 - Aladdin 2FA. Главный экран

Для добавления нового аутентификатора необходимо:

1. Нажать кнопку , выбрать способ добавления: <Сканировать QR-код> или <Добавить вручную>;
2. При выборе <Сканировать QR-код> будет открыта камера для сканирования QR-кода (см. Рисунок 18).

При добавлении нескольких одноразовых паролей одного типа, приложение предложит «Дублировать» или «Перезаписать» код:

- При выборе «Дублировать» - на главном экране появится ещё одна запись аутентификатора с присвоенным одноразовым паролем;
 - При выборе «Перезаписать» - перезапишется первая запись в списке добавленных аутентификаторов
3. При выборе «Добавить вручную» будет осуществлен переход на экран [Ручное добавление]. В поле надо вставить скопированную строку из электронного письма с присланным аутентификатором (см. Рисунок 21) и нажать кнопку «Добавить аутентификатор».

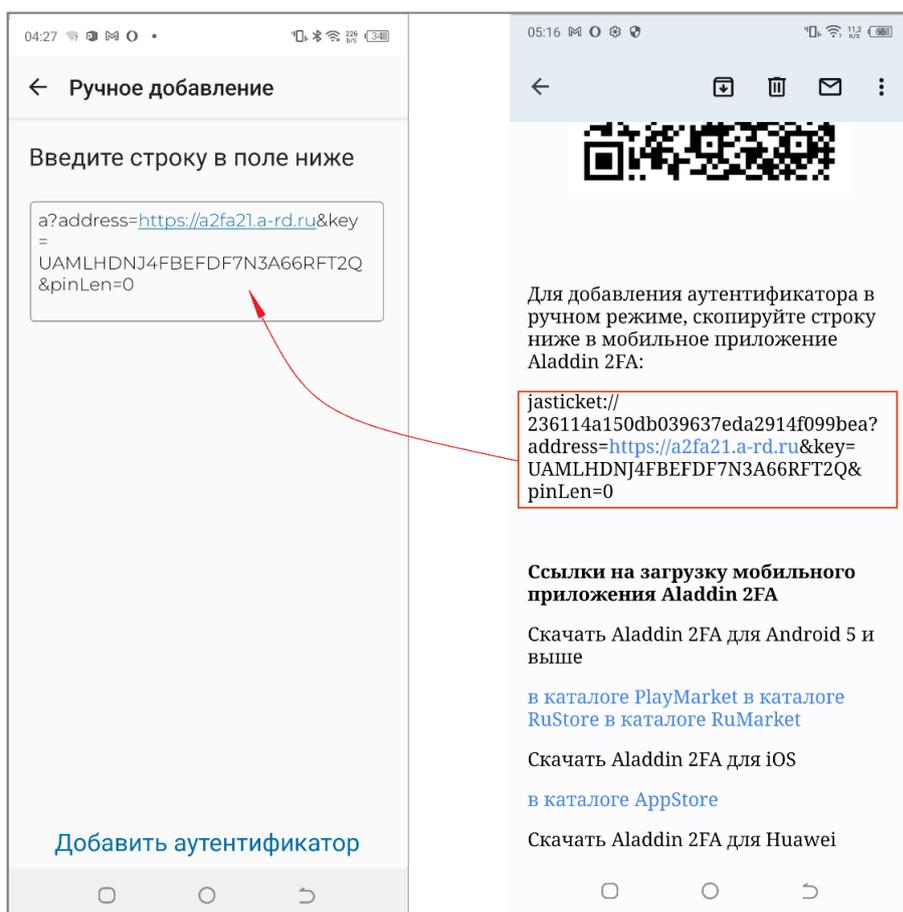


Рисунок 21 - Aladdin 2FA. Добавление аутентификатора вручную

В случае успешного добавления, аутентификатор появится в списке аутентификаторов на главном экране.

Для добавления аутентификатора с поддержкой геолокации необходимо предоставить разрешение на использование данных о местоположении (см. Рисунок 22 - Рисунок 23).



Рисунок 22 - Aladdin 2FA. Ошибка GPS

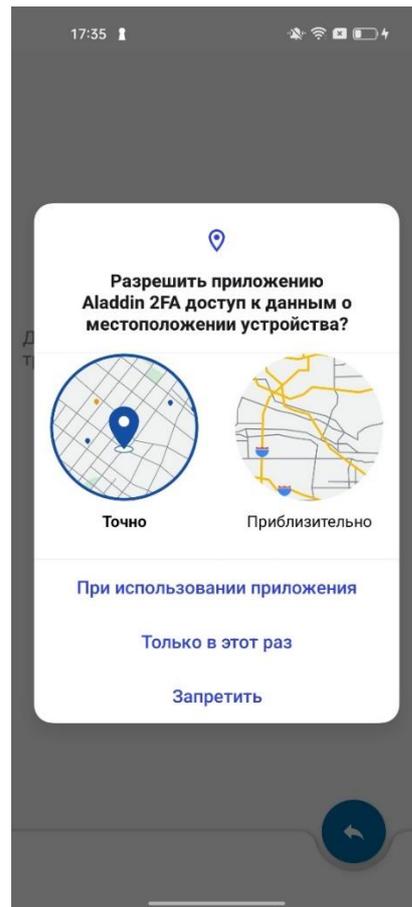


Рисунок 23 - Aladdin 2FA. Запрос на предоставление доступа к данным о местоположении

В случае, если при нажатии на кнопку «Добавить аутентификатор» на экране появилась ошибка (см. Рисунок 24), необходимо обратиться к администратору, выдавшему аутентификатор, и сообщить об ошибке (подробнее про возможные ошибки приведено в приложении см. подраздел 2.3).

При регистрации PUSH OTP аутентификатора в мобильном приложении «Aladdin 2FA» без Google-сервисов на экране отображается соответствующее уведомление (см. Рисунок 25).

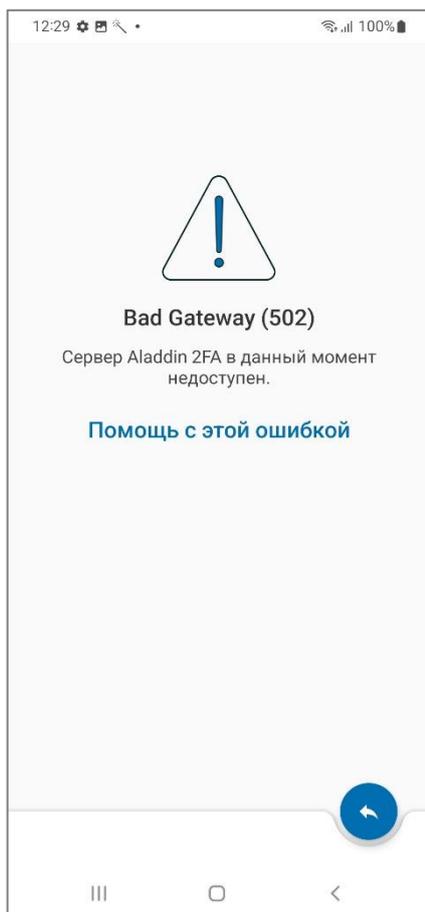


Рисунок 24 - Aladdin 2FA. Не удалось активировать аутентификатор вручную

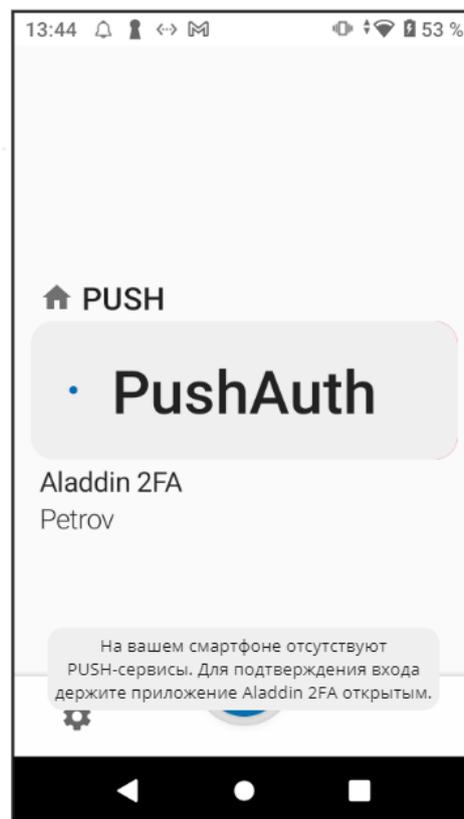


Рисунок 25 - Aladdin 2FA. Уведомление об отсутствии Google-сервисов

3.3 Редактирование аутентификатора

При долгом нажатии на выбранный аутентификатор становится доступен режим редактирования (см. Рисунок 26), в котором доступны следующие действия:

- удаление аутентификатора (п. 3.3.1);
- переименовать аутентификатора (п. 3.3.2);
- изменение местоположения аутентификатора, в случае если их два и больше (п. 3.3.3).

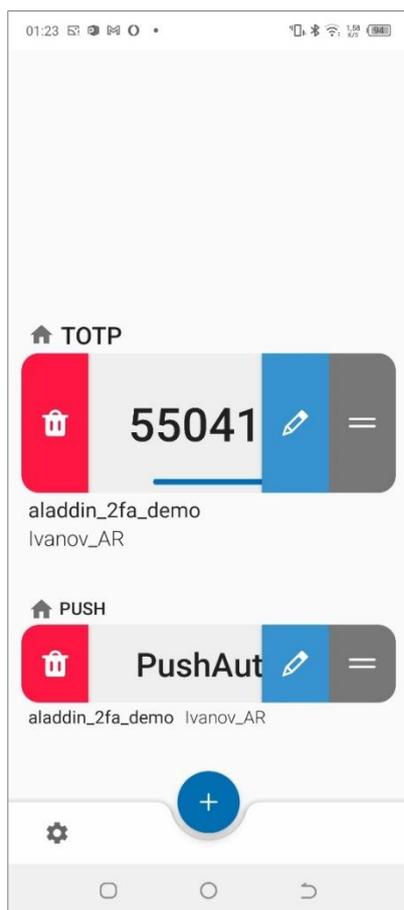


Рисунок 26 - Aladdin 2FA. Режим редактирования аутентификатора

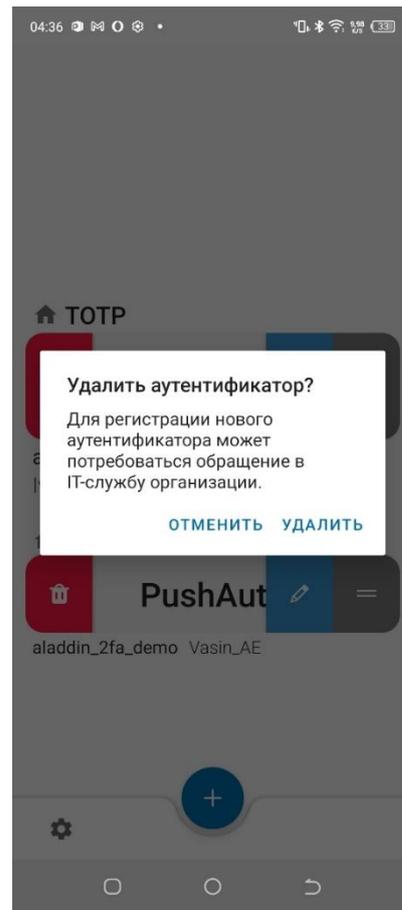


Рисунок 27 - Aladdin 2FA. Информационное сообщение при удалении аутентификатора

3.3.1 Удаление

Для удаления аутентификатора необходимо выполнить следующие действия:

1. Перейти в режим редактирования и нажать кнопку . Появится окно с информацией об удалении (см. Рисунок 27);
2. Подтвердить удаление аутентификатора с помощью кнопки <Удалить>.

В случае, если операция удаления применяется к единственному аутентификатору, то после удаления будет отображен пустой экран (см. Рисунок 5).

3.3.2 Переименование

1. Перейти в режим редактирования и нажать кнопку ;
2. В открытом окне [Лейбл аутентификатора] (см. Рисунок 28) в поле [Введите имя аутентификатора] ввести новое имя и выбрать иконку. Изменения сохраняются автоматически после каждого нажатия по экрану.

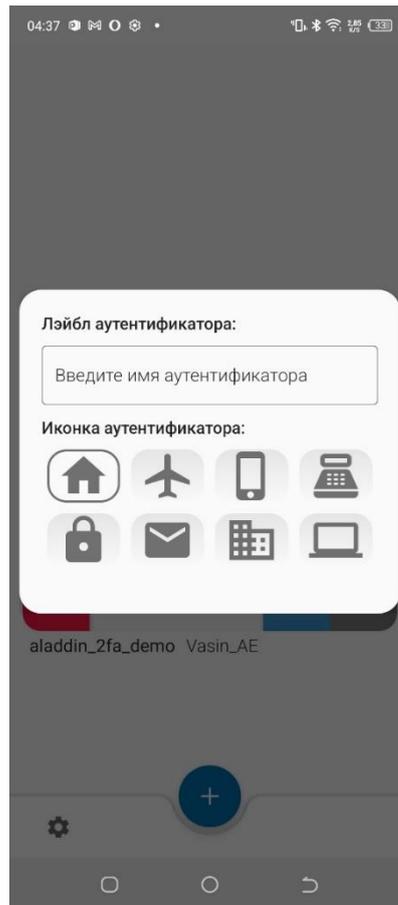


Рисунок 28 - Aladdin 2FA. Задание нового имени для аутентификатора

3.3.3 Перемещение

Аутентификатор можно перемещать по экрану или менять его местоположение: перемещать выше или переносить в конец списка.

Для этого необходимо кнопку  нажать пальцем и переместить аутентификатор.

3.4 Использование одноразового пароля

При использовании одноразового пароля для входа на свой ресурс (личный кабинет, почту и т.д.) необходимо ввести одноразовый пароль (вставить, если он был скопирован) в нужное поле в качестве второго фактора аутентификации (см. Рисунок 29).

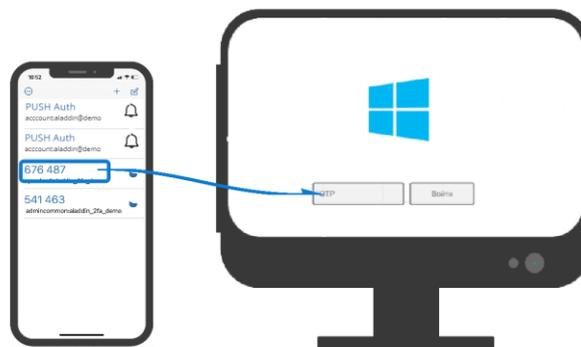


Рисунок 29 – Ввод сгенерированного одноразового кода в соответствующее поле

3.5 PUSH-аутентификация

Работа мобильного приложения с PUSH-аутентификацией осуществляется следующим образом: при попытке входа на своей ресурс (личный кабинет, почту и т.д.), пользователь получает запрос на авторизацию на смартфон. Для подтверждения или отказа входа необходимо нажать соответствующую кнопку в уведомлении.

Необходимо убедиться, что в настройках смартфона для приложения Aladdin 2FA включены PUSH-уведомления

У аутентификатора, зарегистрированного с помощью PUSH-аутентификации, отображается индикатор в виде маленького круга. В штатном режиме индикатор синего цвета - 

Красный цвет индикатора -  - говорит о недоступности сервера в данный момент. Рекомендуется выйти из приложения и зайти повторно

Сценарий PUSH-аутентификации в мобильном приложении Aladdin 2FA осуществляется в двух вариантах: при закрытом приложении и при открытом приложении.

Оба варианта описаны подробно в данном разделе.

На некоторых Android-смартфонах не приходят PUSH-уведомления, подробнее описано в подразделе 5.2

3.5.1 PUSH-аутентификация при закрытом приложении

Если приложение Aladdin 2FA закрыто, то порядок работы с PUSH-аутентификацией следующий:

1. Дождаться получения уведомления с запросом об авторизации (см. Рисунок 30);

Для пользователей Android версии 11 и ниже доступна функция

раскрыть уведомление с помощью кнопки  . Будут доступны кнопки <Принять> и <Отклонить

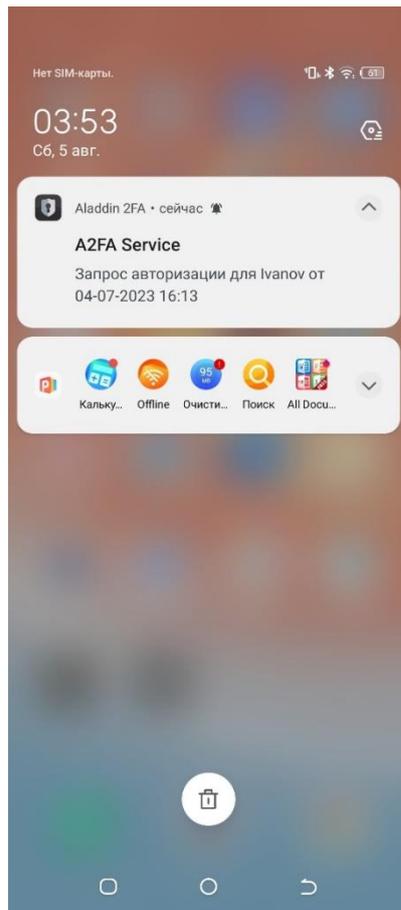


Рисунок 30 - Aladdin 2FA. Уведомление с запросом на авторизацию

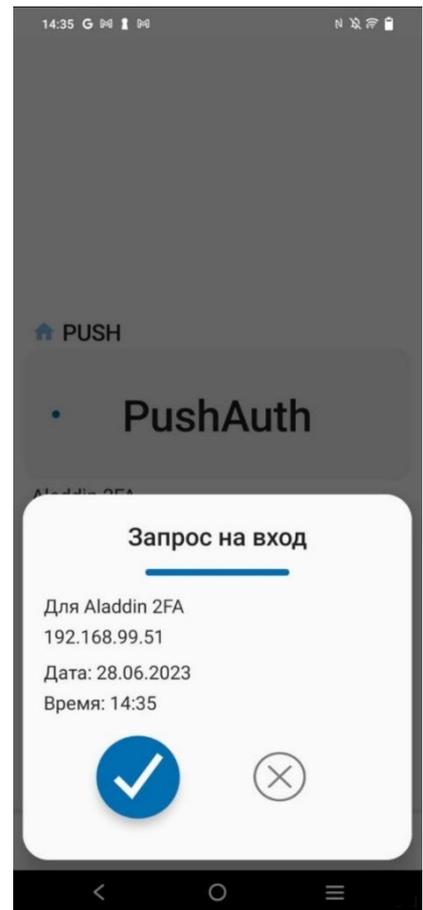


Рисунок 31 - Aladdin 2FA. Запрос на авторизацию в приложении

2. Раскрыть уведомление с помощью кнопки  и нажать на него. Будет осуществлен автоматический вход в приложение Aladdin 2FA;
3. Войти в приложение с помощью пароля или биометрии;
4. В приложении будет открыто окно [Запрос на вход] с информацией и кнопками  -  - <Принять> и  - <Отклонить> (см. Рисунок 31);
5. После нажатия на любую из кнопок будет отображаться окно [Проверка] (см. Рисунок 32), пока происходит процесс подтверждения/отклонения авторизации;
6. При нажатии на кнопку <Принять> авторизация будет подтверждена (см. Рисунок 33). Окно с подтверждением закроется автоматически;

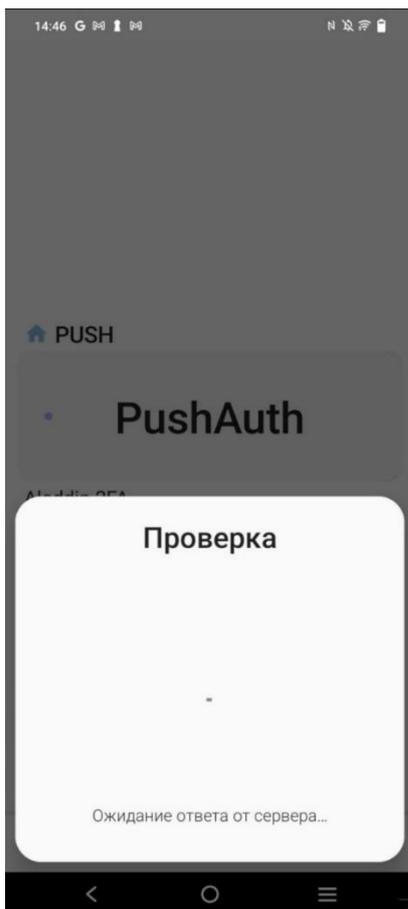


Рисунок 32 - Aladdin 2FA. Проверка ответа на запрос авторизации

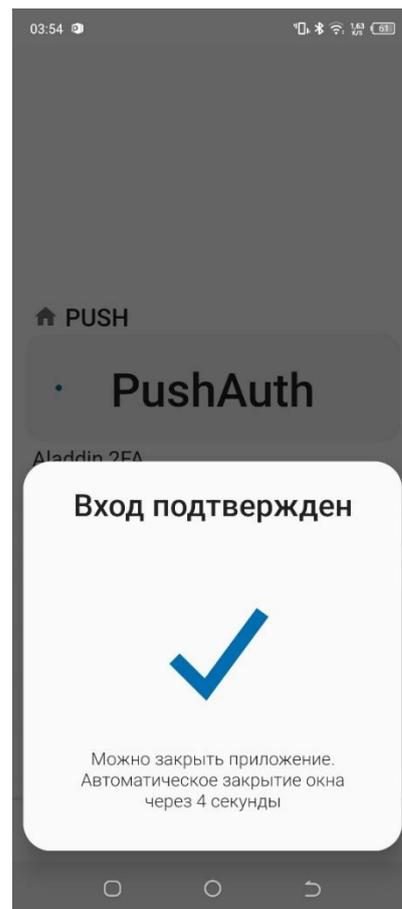


Рисунок 33 - Aladdin 2FA. Запрос на авторизацию подтвержден

7. При нажатии на кнопку <Отклонить> авторизация будет отклонена (см. Рисунок 34). Окно [Вход отклонен] закроется автоматически.

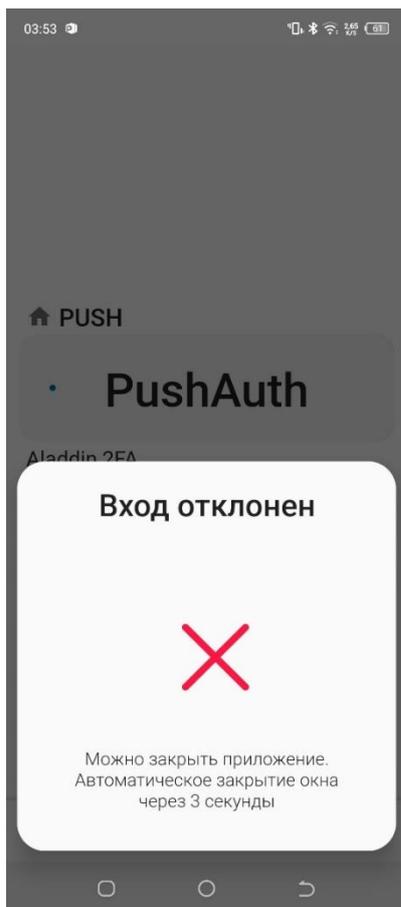


Рисунок 34 - Aladdin 2FA. Запрос на авторизацию отклонен

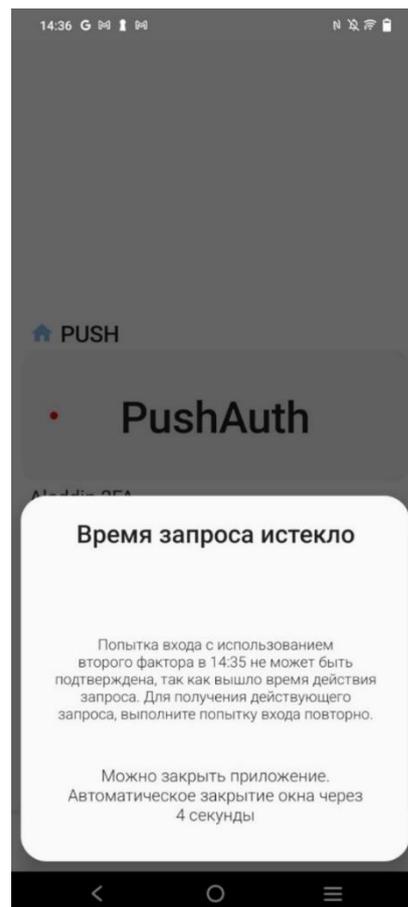


Рисунок 35 - Aladdin 2FA. Запрос на авторизацию отклонен

8. Если при переходе от уведомления в приложение возникли ошибки (серверу не удалось подтвердить запрос, сервер недоступен в текущий момент) и индикатор PUSH-аутентификации красного цвета, то отобразится окно [Время запроса истекло] (см. Рисунок 35). Рекомендуется осуществить повторный вход в приложение Aladdin 2FA.

3.5.2 PUSH-аутентификация в открытом приложении

Если приложение Aladdin 2FA открыто, то запрос на авторизацию появится автоматически (см. Рисунок 31). Дальнейшая работа полностью аналогична предыдущему пункту (п. 3.5.1), начиная с шага 4.

3.6 Настройки приложения

При нажатии на кнопку  в левом нижнем углу главного экрана будет открыто меню с настройками (см. Рисунок 36).

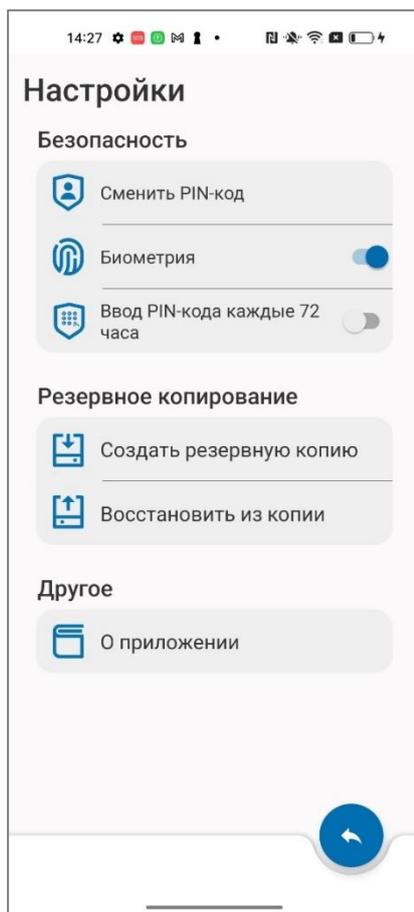


Рисунок 36 - Aladdin 2FA. Настройки приложения



Рисунок 37 - Aladdin 2FA. О приложении

Таблица 2 – Настройки приложения

	<Сменить PIN-код> - при нажатии на кнопку будет открыто окно для смены PIN-кода (см. Рисунок 14). Нужно ввести новый PIN-код и его подтверждение
	<Биометрия> - кнопка для переключения режима входа в приложение с помощью отпечатка пальца. <i>Если смартфон не поддерживает биометрию, данной кнопки в меню опций не будет</i>
	<Ввод PIN-код каждые 72 часа> - переключатель для включения и выключения повторения ввода PIN-кода каждые 72 часа
	<Создать резервную копию> - кнопка для перехода к процедуре создания резервной копии данных приложения. Подробнее см. п. 3.8
	<Восстановить из копии> - кнопка для перехода к процедуре восстановления данных из ранее созданной резервной копии. Подробнее см. п. 3.9
	<О приложении> - при нажатии на кнопку будет открыто информационное окно с номером версии приложения, лицензионным соглашением, политикой конфиденциальности и соглашением о ПО третьих сторон (см. Рисунок 37)

3.7 Биометрия

Если используемое устройство поддерживает аутентификацию по биометрии, то вход в приложение Aladdin 2FA можно осуществлять с помощью биометрии.

Биометрия настраивается в настройках устройства

Для включения или выключения функции необходимо:



1. На главном экране, открыть настройки приложения, нажав на кнопку ;
2. У настройки <Биометрия> включить или отключить тумблер.

Если, при включенной опции <Биометрия>, на устройстве настройки биометрии были изменены, то, при входе, приложение выведет предупреждение (см. Рисунок 38). Войти в приложение можно будет только по заданному паролю

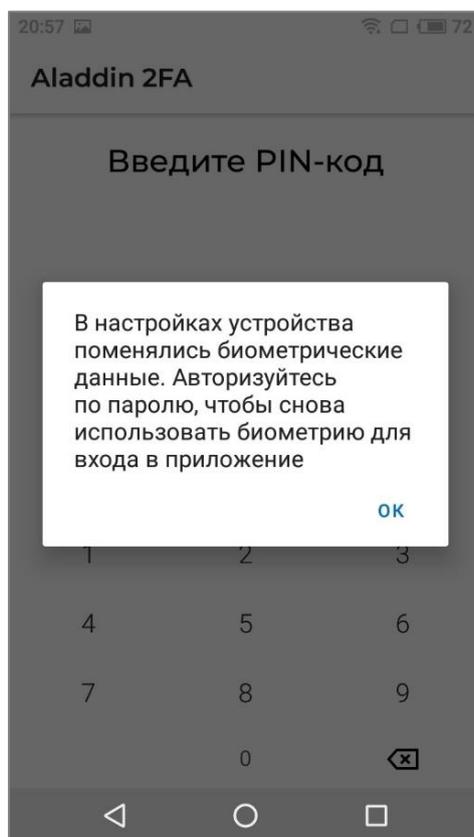


Рисунок 38 - Aladdin 2FA. Настройки приложения

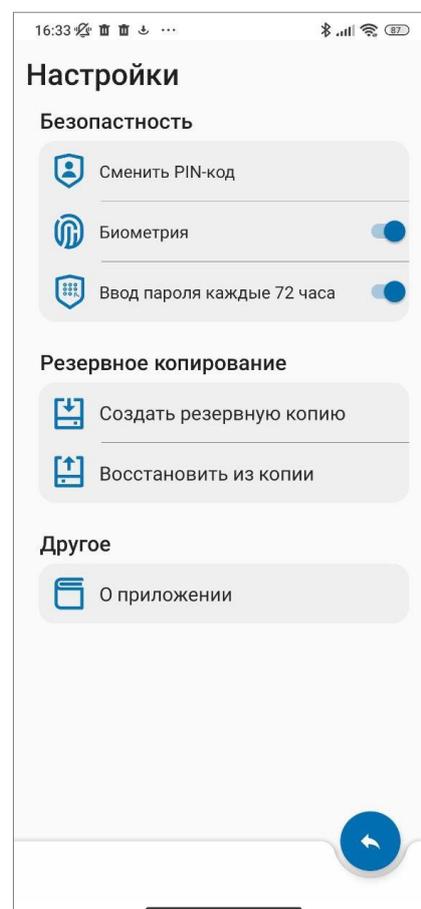


Рисунок 39 - Aladdin 2FA. Отключение регулярного ввода PIN-кода

3.7.1 Отключение регулярного ввода PIN-кода

При включенной опции <Биометрия> есть возможность отключить регулярный ввод PIN-кода.

После включения тумблера <Биометрия> появляется опция <Ввод пароля каждые 72 часа> (см. Рисунок 39), которая по умолчанию включена. При выключении тумблера <Ввод пароля каждые 72 часа> приложение перестает запрашивать ввод PIN-кода раз в 72 часа. В таком случае ответственность за запоминание PIN-кода остается за пользователем, так как восстановить его не получится.

3.8 Резервное копирование

Для безопасности данных рекомендуется совершать процедуру резервного копирования после каждого добавленного аутентификатора

Для создания резервной копии необходимо:

1. Нажмите на иконку приложения для его запуска - ;
2. На главном экране мобильного приложения отображается перечень всех добавленных аутентификаторов (см. Рисунок 40);
3. Нажать на кнопку  в левом нижнем углу главного экрана, в результате будет открыто меню с настройками (см. Рисунок 41).

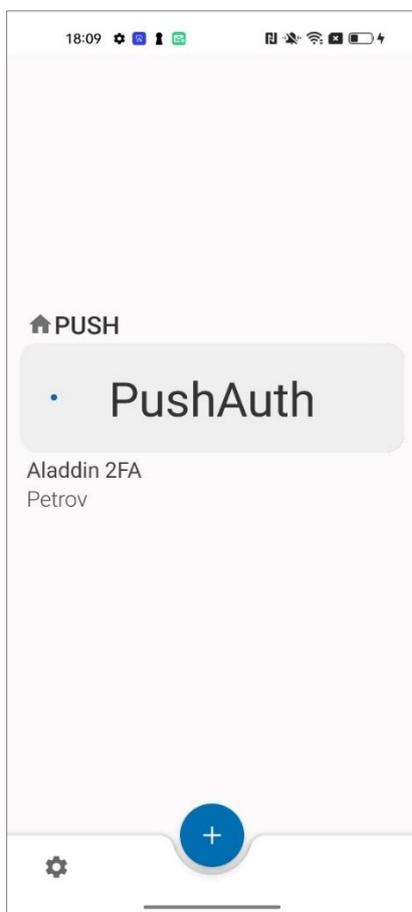


Рисунок 40 - Aladdin 2FA. Главный экран

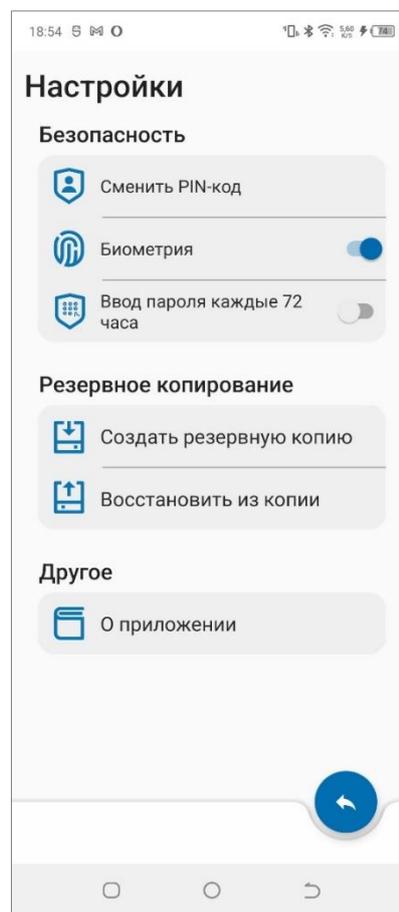


Рисунок 41 - Aladdin 2FA. Настройки приложения

4. Нажать кнопку <Создать резервную копию> (см. Рисунок 41), ввести PIN-код для создания резервной копии (см. Рисунок 42);
5. Далее будет открыт экран [Создание], на котором приведена справочная информация о процессе создания резервной копии (см. Рисунок 43).

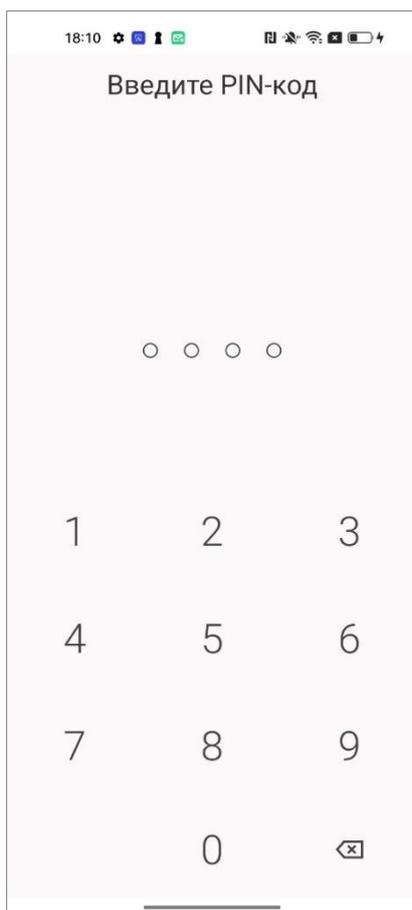


Рисунок 42 - Aladdin 2FA. Ввод PIN-кода приложения

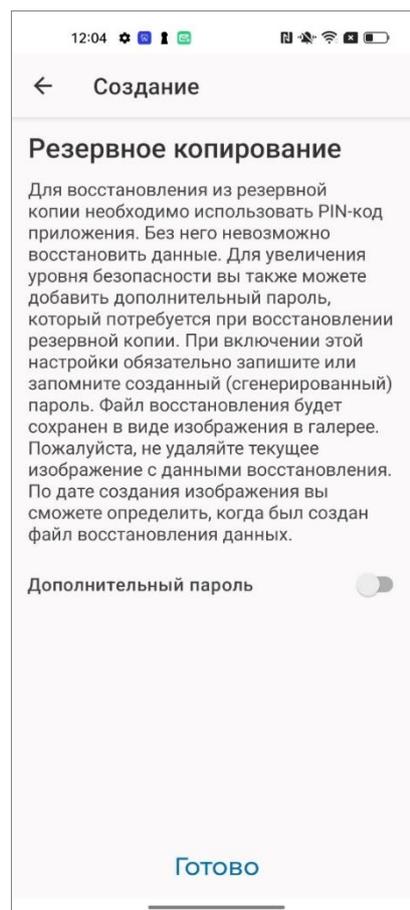


Рисунок 43 - Aladdin 2FA. Создание резервной копии без ввода 16-значного кода

Для повышения уровня безопасности можно воспользоваться дополнительным паролем, для этого необходимо включить тумблер <Дополнительный пароль> (см. Рисунок 44);

- 5.1. Если тумблер <Дополнительный пароль> не включен, то при нажатии на кнопку <Готово> будет создана резервная копия;
- 5.2. Если тумблер <Дополнительный пароль> включен, появятся дополнительные поля. В поле [Пароль восстановления] отображается автоматически сгенерированный 16-значный код, который надо скопировать и вставить в поле [Повторить пароль восстановления] (см. Рисунок 44). После нажатия на кнопку <Готово> будет создана резервная копия (см. Рисунок 45).

Данный пароль необходимо запомнить, так как восстановить его нельзя, но он понадобится на этапе восстановления данных из резервной копии

Резервная копия хранится на устройстве в виде изображения с логотипом компании Аладдин Р.Д. в галерее устройства (см. Рисунок 45). Изображение нельзя удалять и переименовывать.



Рисунок 44 - Aladdin 2FA. Создание резервной копии с вводом 16-значного кода



Рисунок 45 - Файл резервной копии в виде логотипа

3.9 Восстановление из копии

Для восстановления данных из резервной копии необходимо убедиться, что изображение, представляющее собой резервную копию данных, находится на устройстве

Для восстановления данных из резервной копии необходимо:

1. Нажмите на иконку приложения для его запуска - ;
2. На главном экране мобильного приложения отобразится пустой экран без аутентификаторов (см. Рисунок 46);
3. Нажать на кнопку  в левом нижнем углу главного экрана (см. Рисунок 46) в результате будет открыто меню с настройками (см. Рисунок 47);

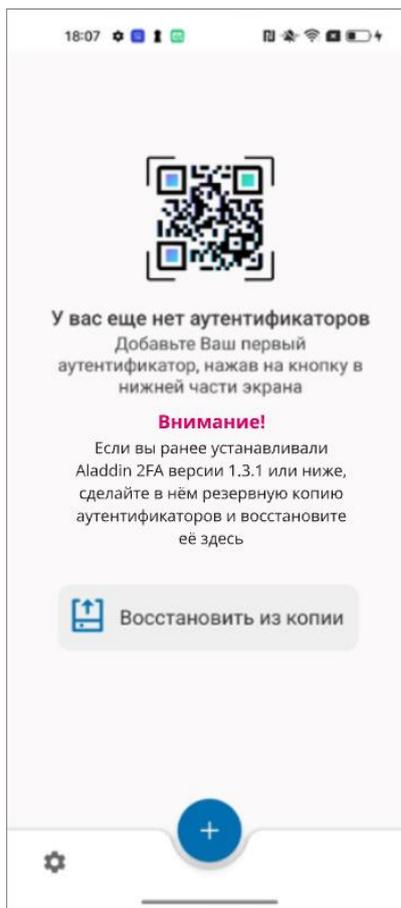


Рисунок 46 - Aladdin 2FA. Главный экран приложения после резервного копирования

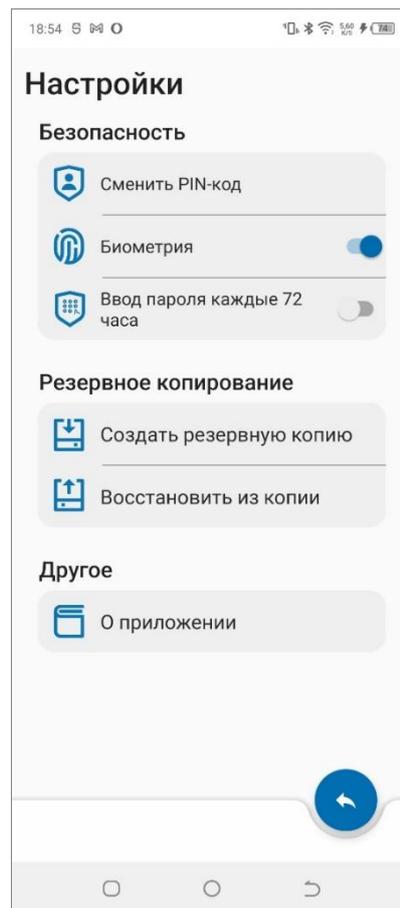


Рисунок 47 - Aladdin 2FA. Настройки приложения

4. Нажать на кнопку <Восстановление из копии> (см. Рисунок 47) ввести PIN-код для восстановления данных из резервной копии (см. Рисунок 48);
5. Далее будет открыт экран [Восстановление], на котором приведена справочная информация о восстановлении данных из резервной копии (см. Рисунок 49);



Рисунок 48 - Aladdin 2FA. Ввод PIN-кода приложения

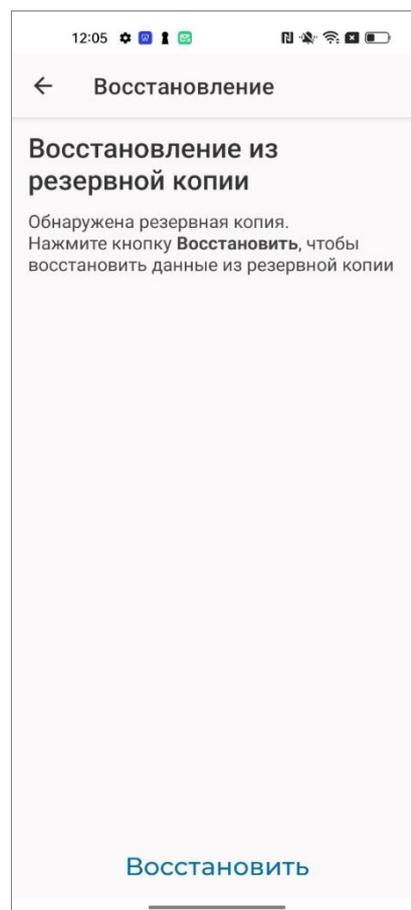


Рисунок 49 - Aladdin 2FA. Восстановление данных из резервной копии без ввода 16-значного кода

6. В случае, если при создании резервной копии был включен тумблер «Дополнительный пароль», то после ввода PIN-кода необходимо ввести 16-значный код, сохраненный при резервном копировании (см. Рисунок 50). Нажать кнопку <Восстановить>.

В зависимости от настроек смартфона может потребоваться предоставить разрешение для доступа к галерее устройства

Если вы не помните 16-значный код, к сожалению, расшифровать резервную копию будет невозможно

Если был введен неправильный пароль или изображение с резервной копией было создано на другом устройстве, после нажатия на кнопку <Восстановить>, будет отображаться ошибка (см. Рисунок 51).

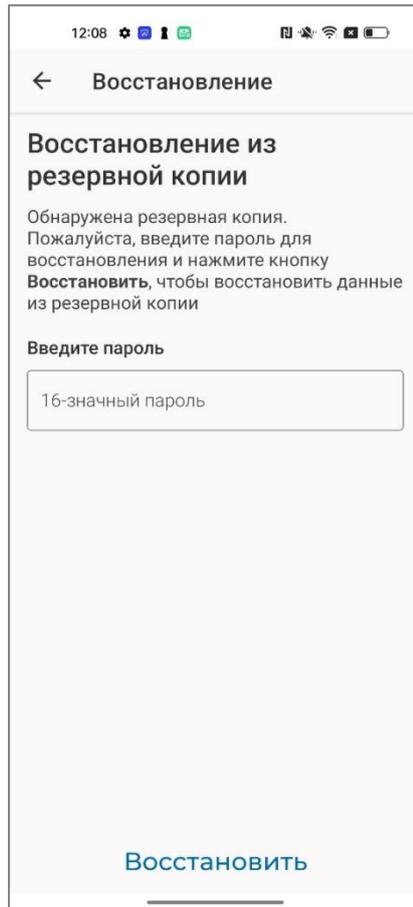


Рисунок 50 - Aladdin 2FA. Восстановление данных из резервной копии с вводом 16-значного кода

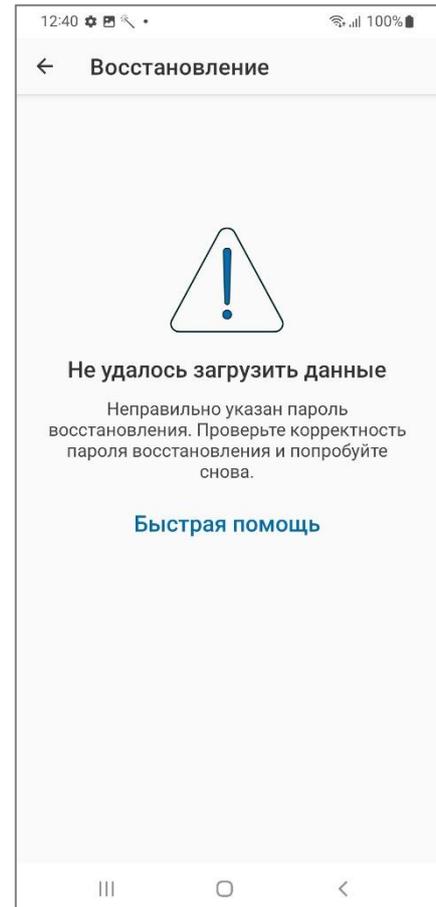


Рисунок 51 - Aladdin 2FA. Ошибка при восстановлении из резервной копии

Если на устройстве, на котором было произведено резервное копирование данных, производилась переустановка приложения Aladdin 2FA, то при первом запуске приложение предложит восстановить данные из резервной копии с PIN-кодом и 16-значным паролем (см. Рисунок 53) или без 16-значного пароля (см. Рисунок 52) (зависит от того какой тип пароля был задан при создании резервной копии) .

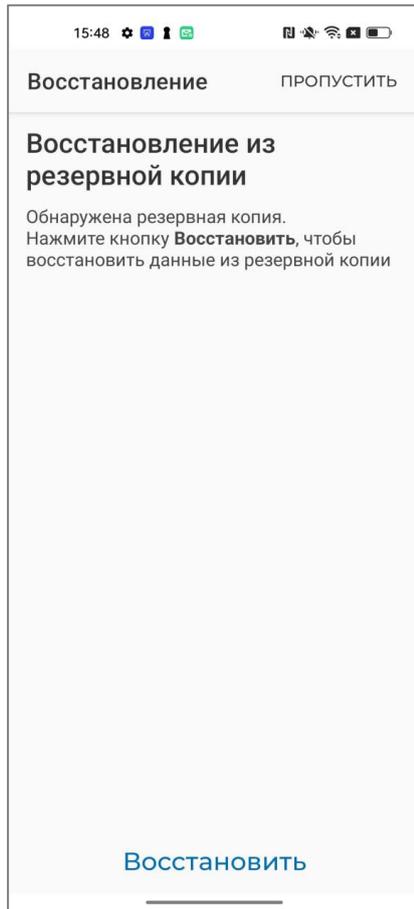


Рисунок 52 - Aladdin 2FA. Восстановление из резервной копии при переустановке приложения без ввода 16-значного пароля

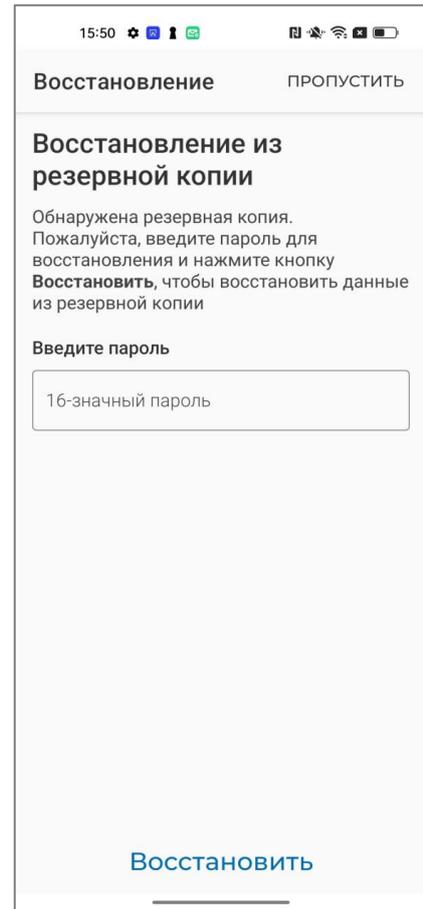


Рисунок 53 - Aladdin 2FA. Восстановление из резервной копии при переустановке приложения с вводом 16-значного пароля

4. Инструкция для пользователей iOS

После установки мобильного приложения на устройство с ОС iOS, доступны сценарии работы, приведенные ниже в данном разделе.

4.1 Первый запуск приложения Aladdin 2FA



1. Нажмите на иконку приложения для его запуска - ;
2. Будет открыто окно, где необходимо придумать PIN-код из четырех символов, с помощью которого будет осуществляться вход в приложение (см. Рисунок 54);
3. На следующем шаге ввести подтверждение пароля (см. Рисунок 55). После установки пароля, если на устройстве используется биометрия, будет предложено включить возможность входа, используя биометрию (см. Рисунок 56);



Рисунок 54 - Aladdin 2FA. Установка PIN-кода

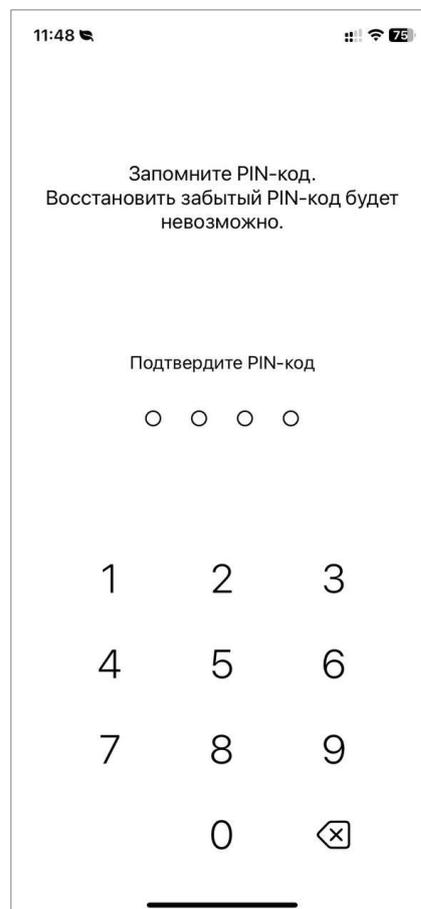


Рисунок 55 - Aladdin 2FA. Подтверждение PIN-кода

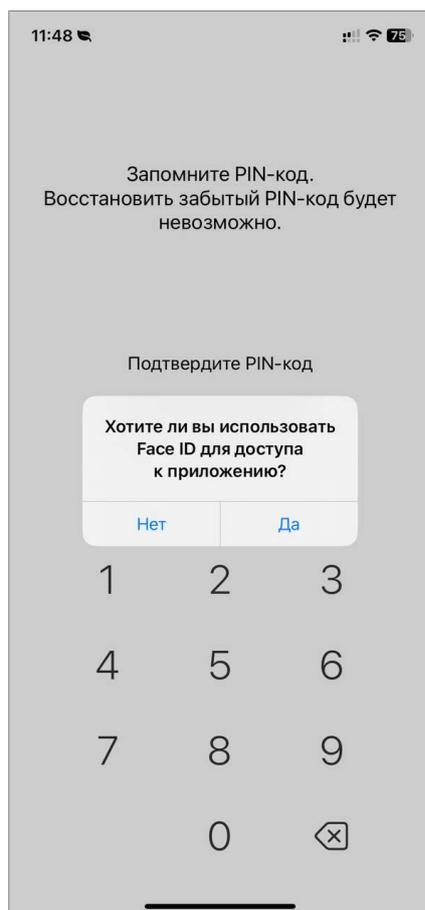


Рисунок 56 - Aladdin 2FA. Подключение биометрии

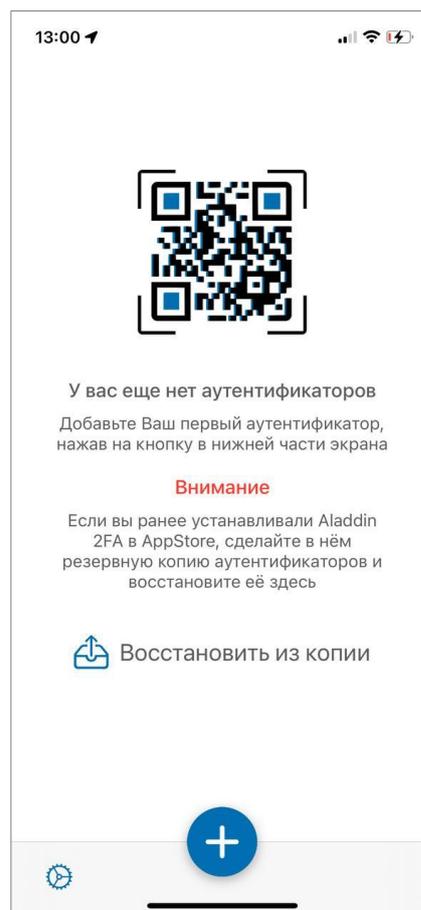


Рисунок 57 - Aladdin 2FA. Добавление аутентификатора

4. При первом входе в приложение на экране, приведенном выше (см. Рисунок 55), добавить

аутентификатор с помощью кнопки ;

В зависимости от настроек смартфона может понадобится предоставить разрешение для использования камеры

5. На следующем экране (см. Рисунок 58) происходит добавление аутентификатора с помощью сканирования QR-кода. Если такой способ в данный момент недоступен, добавить аутентификатор можно следующими способами (см. обозначения цифрами на Рисунок 58):

- 1) – кнопка переключения между камерами устройства. Позволяет считать QR-код с помощью фронтальной камеры;
- 2) – <Добавить вручную> - подробнее про функцию добавления в п. 4.2;

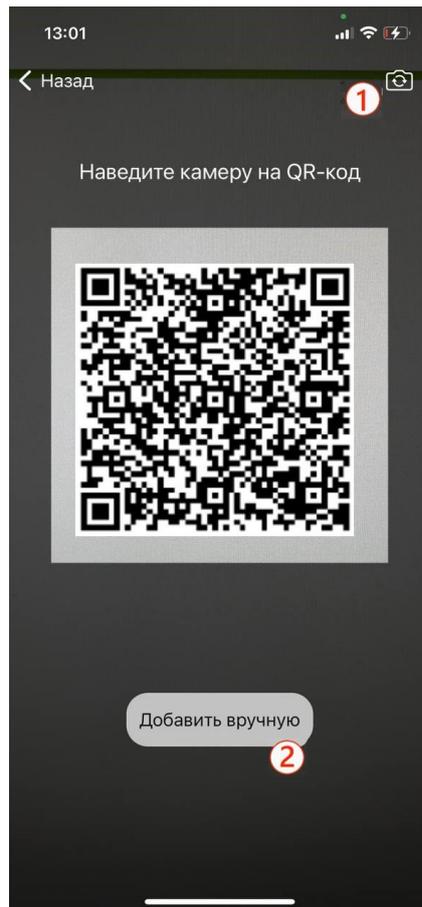


Рисунок 58 - Aladdin 2FA. Сканирование QR-кода

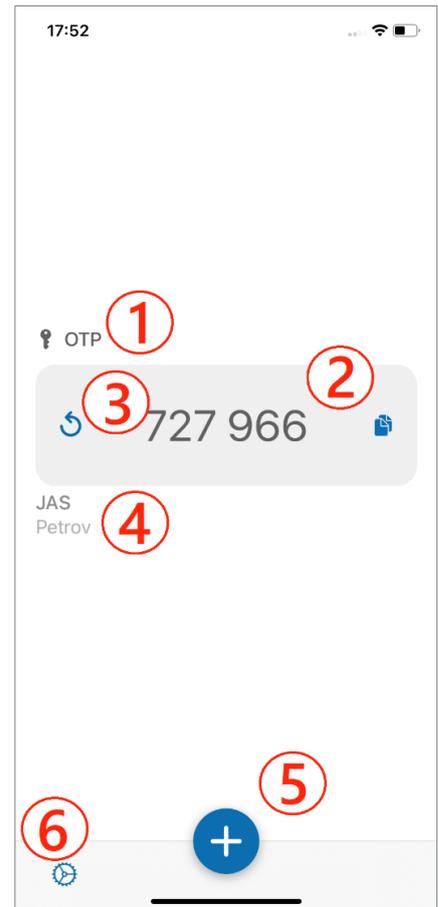


Рисунок 59 - Aladdin 2FA. Добавленный аккаунт

6. Будет добавлен аккаунт (см. Рисунок 59), где цифрами обозначены следующие элементы:
- 1) – тип аутентификатора. Для одноразового пароля тип по умолчанию - TOTP или HOTP, для PUSH-аутентификации тип будет PUSH. Заданные по умолчанию иконку и тип аккаунта можно изменить, подробнее описано в п. 4.3.2;
 - 2) – сгенерированный одноразовый пароль. Скопировать значение можно с помощью кнопки ; кнопки
 - 3) – элемент управления для обновления сгенерированного одноразового пароля;
 - 4) – учетные данные пользователя;
 - 5) – кнопка добавления аутентификатора (см. п. 4.2);
 - 6) – переход к меню с настройками приложения (см. п. 4.6).

4.2 Добавление аутентификатора

После каждого добавленного аутентификатора данных рекомендуется совершать процедуру резервного копирования (см. п. 4.8)

На главном экране мобильного приложения отображается перечень всех добавленных аутентификаторов (см. Рисунок 61).

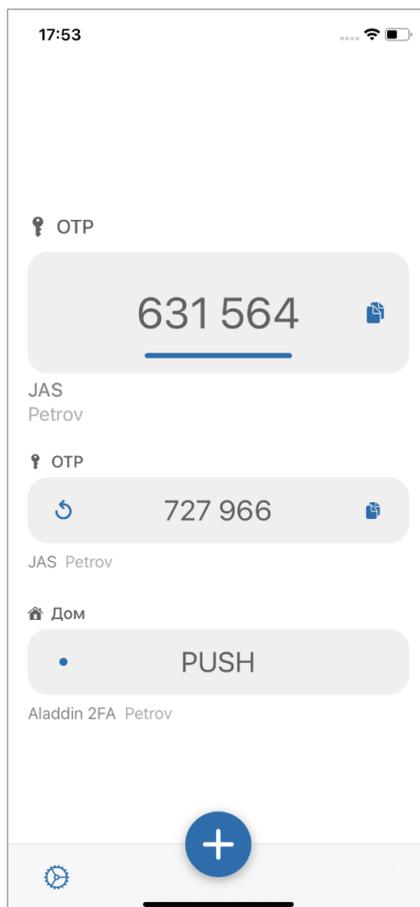


Рисунок 60 - Aladdin 2FA. Главный экран

Для добавления нового аутентификатора необходимо:

1. Нажать кнопку  внизу главного экрана;
2. Будет открыта камера для сканирования QR-кода (см. Рисунок 58), отсканировать QR-код.
При добавлении нескольких одноразовых паролей одного типа, приложение предложит «Дублировать» или «Перезаписать» код:
 - При выборе «Дублировать» - на главном экране появится ещё одна запись аккаунта с присвоенным одноразовым паролем;
 - При выборе «Перезаписать» - перезапишется первая запись в списке добавленных аутентификаторов
3. При выборе <Ввести секретный код> будет осуществлен переход на экран [Введите секретный код]. В поле надо вставить скопированную строку из электронного письма с присланным аутентификатором (см. Рисунок 61) и нажать кнопку <Добавить аутентификатор>.

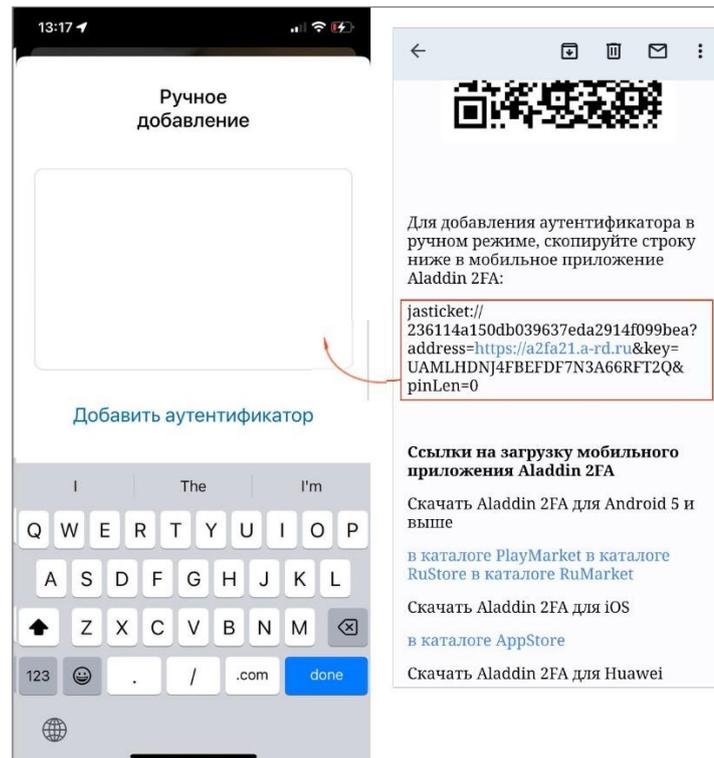


Рисунок 61 - Aladdin 2FA. Добавление аутентификатора вручную

Для добавления аутентификатора с поддержкой геолокации необходимо предоставить разрешение на использование геопозиции (см. Рисунок 62).

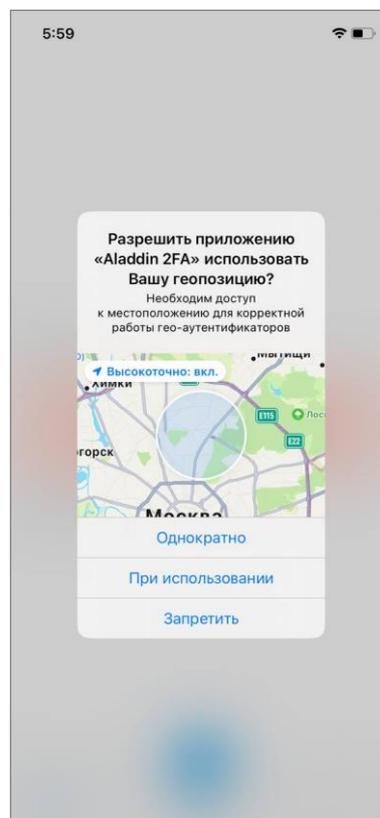


Рисунок 62 - Aladdin 2FA. Запрос на предоставление доступа к геопозиции

4.3 Редактирование аутентификатора

При долгом нажатии на выбранный аутентификатор становится доступен режим массового редактирования (см. Рисунок 63): можно удалить аутентификаторы, и изменить их местоположение. Что бы появилась возможность редактирования, получения информации и удаления нужно нажать на значок удаления.

Для редактирования конкретного аутентификатора необходимо сделать свайп на конкретном аутентификаторе, в результате чего появится возможность получения информации, редактирования и удаления.



Для сохранения изменения и выхода из редактирования необходимо нажать кнопку

Подробнее про каждую процедуру описано ниже.

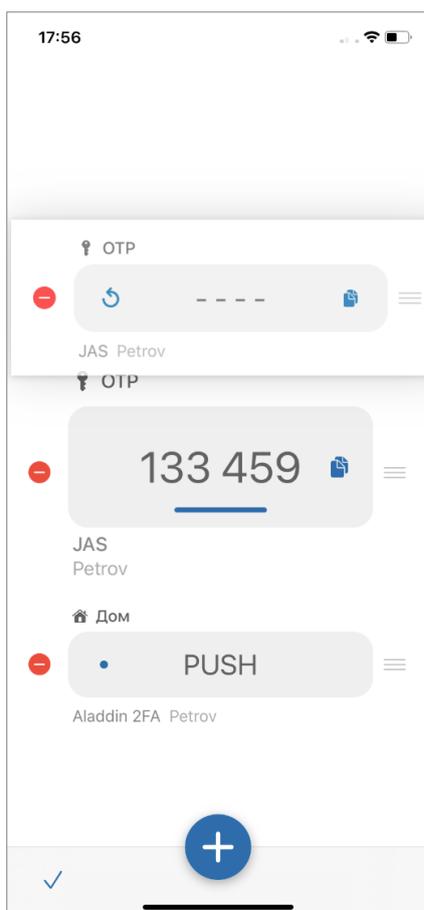


Рисунок 63 - Aladdin 2FA. Режим редактирования аутентификатора

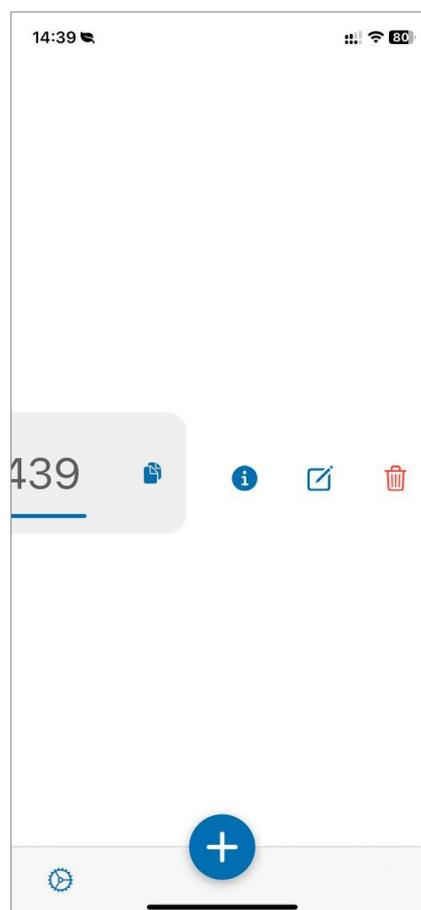


Рисунок 64 - Aladdin 2FA. Удаление аутентификатора

4.3.1 Удаление

Для удаления аутентификатора необходимо выполнить следующие действия:

1. Перейти в режим редактирования и нажать кнопку  (см. Рисунок 63). Также можно свайпнуть аутентификатор влево, тогда справа отобразится кнопка  - <Удалить> (см. Рисунок 64);

- Нажать на кнопку  или . Появится информационное сообщение (пример сообщения приведен на Рисунок 27 для ОС Android);
- Подтвердить удаление аутентификатора с помощью кнопки <Да>.

4.3.2 Переименование

- Свайпнуть аутентификатор влево, тогда справа отобразится кнопка ;
- Будет открыто окно [Лейбл аутентификатора] (см. Рисунок 65), в котором можно поменять название аутентификатора, заданное по умолчанию, на другое имя. Еще можно поменять иконку отображения аутентификатора;

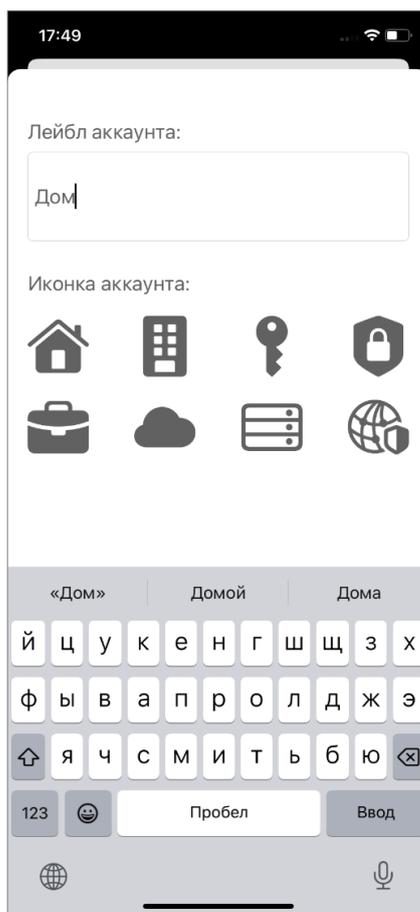


Рисунок 65 - Aladdin 2FA. Задание нового имени для аутентификатора

- В поле [Лейбл аккаунта] ввести новое имя и выбрать иконку. Изменения сохраняются автоматически после каждого нажатия по экрану.

4.3.3 Перемещение

Аутентификатор можно перемещать по экрану или менять его местоположение: перемещать выше или переносить в конец списка.

Для этого необходимо кнопку  зажать пальцем и переместить аккаунт.

4.3.4 Просмотр информации об аутентификаторе

Для просмотра информации об аутентификаторе необходимо свайпнуть аутентификатор



влево и нажать на кнопку , в результате отобразится страница с информацией об аутентификаторе (см. Рисунок 66).

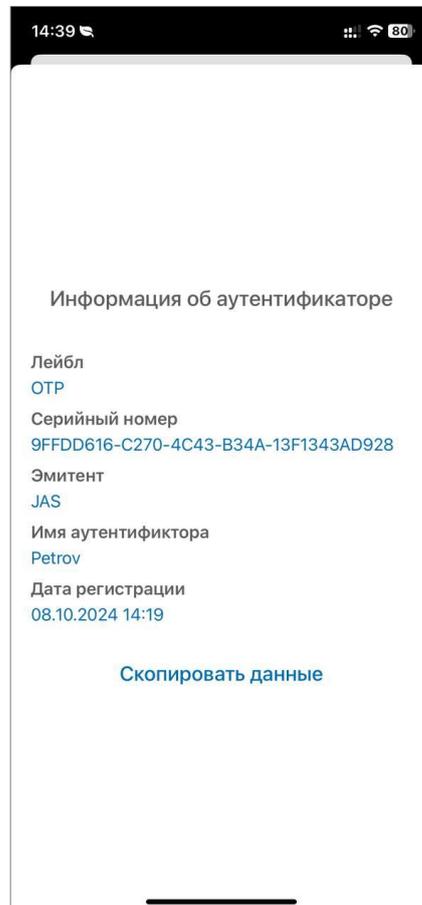


Рисунок 66 - Aladdin 2FA. Информация об аутентификаторе

4.4 Использование одноразового пароля

При использовании одноразового пароля для входа на свой ресурс (личный кабинет, почту и т.д.) необходимо ввести одноразовый пароль (вставить, если он был скопирован) в нужное поле в качестве второго фактора аутентификации (см. Рисунок 67).

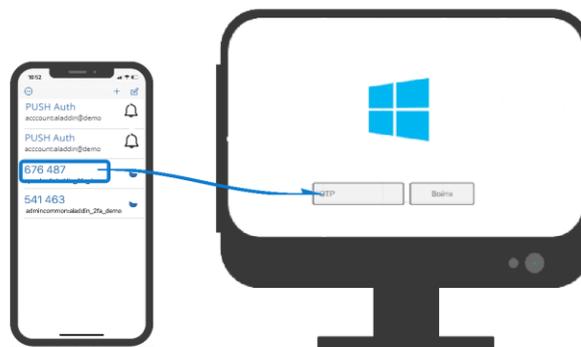


Рисунок 67 – Ввод сгенерированного одноразового кода в соответствующее поле

4.5 PUSH-аутентификация

Работа мобильного приложения с PUSH-аутентификацией осуществляется следующим образом: при попытке входа на своей ресурс (личный кабинет, почту и т.д.), пользователь получает запрос на авторизацию на смартфон. Для подтверждения или отказа входа необходимо нажать соответствующую кнопку в уведомлении.

Необходимо убедиться, что в настройках смартфона для приложения Aladdin 2FA включены PUSH-уведомления

У аутентификатора, зарегистрированного с помощью PUSH-аутентификации, отображается

индикатор в виде маленького круга. В штатном режиме индикатор синего цвета - 

Красный цвет индикатора -  - говорит о недоступности сервера в данный момент. Рекомендуется выйти из приложения и зайти повторно

Сценарий PUSH-аутентификации в мобильном приложении Aladdin 2FA осуществляется в двух вариантах: при закрытом приложении и при включенном приложении.

Оба варианта описаны подробно в данном разделе.

4.5.1 PUSH-аутентификация при закрытом приложении

Если приложение Aladdin 2FA закрыто, то порядок работы с PUSH-аутентификацией следующий:

1. Дождаться получения уведомления с запросом авторизации (см. Рисунок 68);
2. Нажать на полученное уведомление. Будет осуществлен переход в приложение Aladdin 2FA либо нажать и удерживать уведомление до отображения кнопок «Подтвердить»/«Отклонить» (см. Рисунок 69);

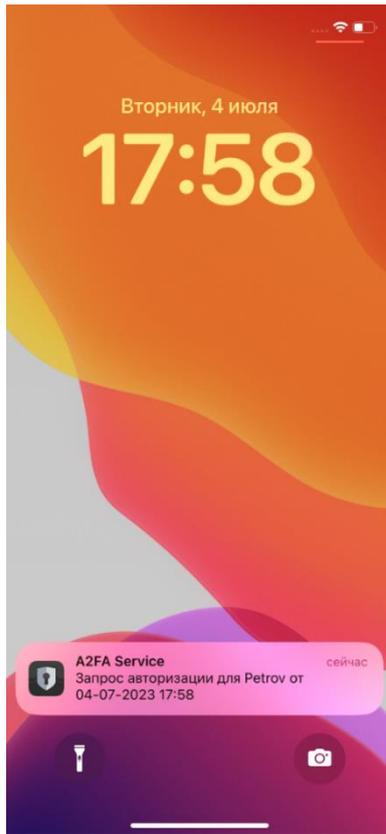


Рисунок 68 - Aladdin 2FA. Уведомление с запросом на авторизацию

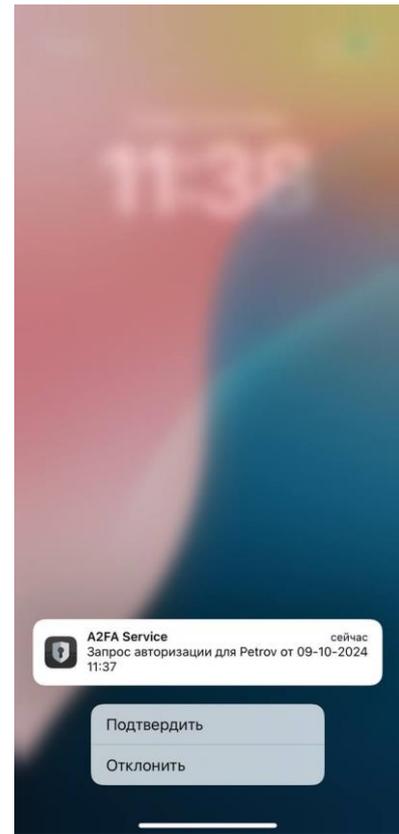


Рисунок 69 - Aladdin 2FA. Отображение кнопок на уведомлении с запросом на авторизацию

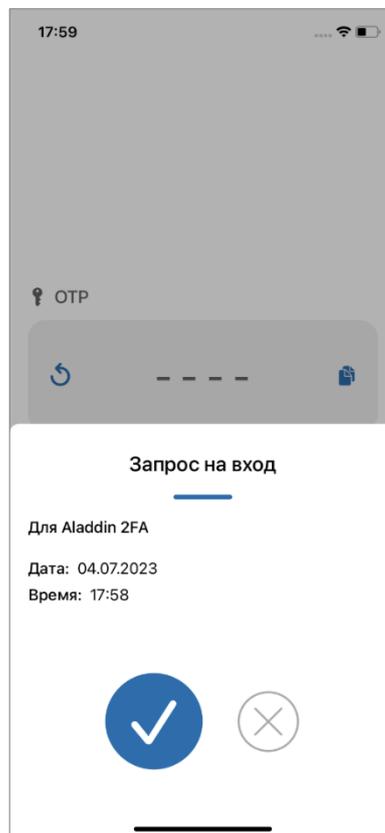


Рисунок 70 - Aladdin 2FA. Запрос на авторизацию в приложении

3. Войти в приложение с помощью PIN-кода или биометрии;



4. В приложении будет открыто окно [Запрос на вход] с информацией и кнопками



<Принять> и <Отклонить> (см. Рисунок 70);

5. При нажатии на кнопку <Принять> авторизация будет подтверждена (см. Рисунок 71).
Окно с подтверждением закроется автоматически;

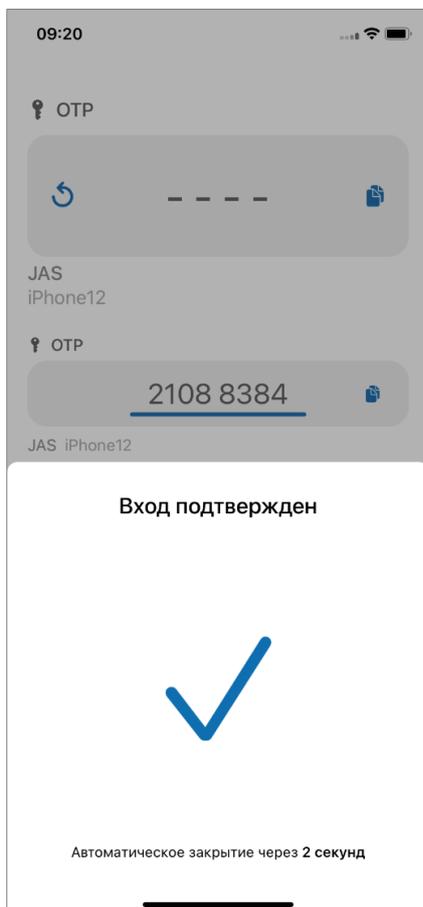


Рисунок 71 - Aladdin 2FA. Подтверждение входа

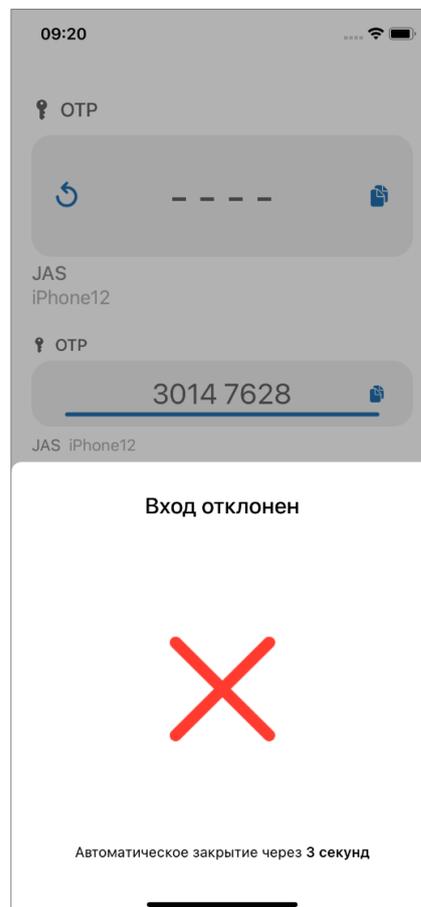


Рисунок 72 - Aladdin 2FA. Запрос на авторизацию отклонен

6. При нажатии на кнопку <Отклонить> авторизация будет отклонена (см. Рисунок 72). Окно [Вход отклонен] закроется автоматически.

4.5.2 PUSH-аутентификация в открытом приложении

Если приложение Aladdin 2FA открыто, то запрос на авторизацию появится автоматически (см. Рисунок 70). Дальнейшая работа полностью аналогична предыдущему пункту (п. 4.5.1), начиная с шага 4.

4.6 Настройки приложения



При нажатии на кнопку  в левом верхнем углу главного экрана будет открыто меню с настройками (см. Рисунок 73):

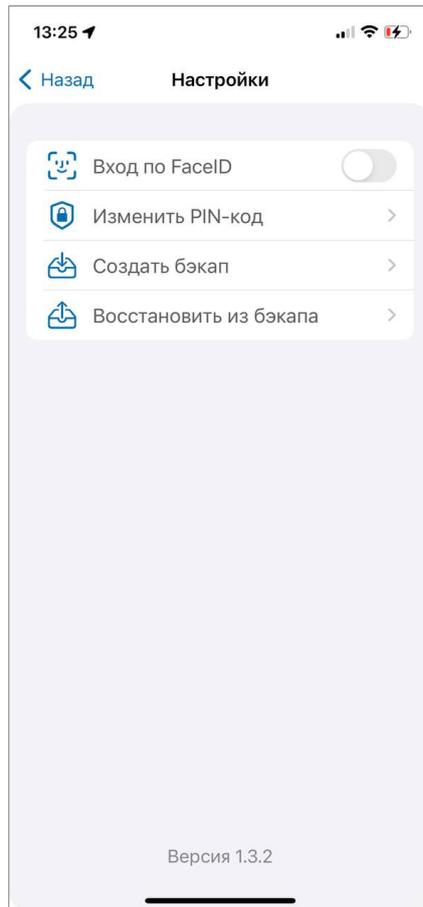


Рисунок 73 - Aladdin 2FA. Настройки приложения

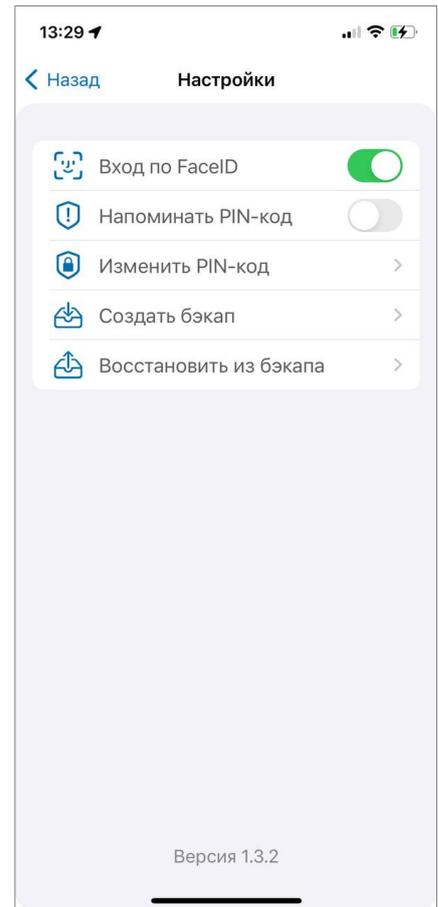


Рисунок 74 - Aladdin 2FA. Отображение пункта «Напомнить PIN-код» после активации пункта «Вход по FaceID»

Таблица 3 – Настройки приложения

	<p><Вход по FaceID> - кнопка для переключения режима входа в приложение с помощью функции распознавания лица FaceID.</p> <p><i>Если смартфон не поддерживает биометрию, данной кнопки в меню опций не будет</i></p>
	<p><Напомнить PIN-код> - переключатель для включения и выключения напоминания ввода PIN-кода</p>
	<p><Изменить PIN-код> - при нажатии на кнопку будет открыто окно для смены пароля. Нужно ввести новый пароль и его подтверждение</p>
	<p><Создать бэкап> - кнопка для перехода к процедуре создания резервной копии данных приложения. Подробнее см. п.4.8</p>
	<p><Восстановить из бэкапа> - кнопка для перехода к процедуре восстановления данных из ранее созданной резервной копии. Подробнее см. п.4.9</p>

4.7 Биометрия

Если используемое устройство поддерживает аутентификацию по биометрии, то вход в приложение Aladdin 2FA можно осуществлять с помощью биометрии.

Биометрия настраивается в настройках устройства

Для включения или выключения функции необходимо:

1. На главном экране, открыть настройки приложения, нажав на кнопку ;
2. У настройки <Вход по FaceID> включить или отключить тумблер.

Если, при включенной опции <Биометрия>, на устройстве настройки биометрии были изменены, то войти в приложение можно будет только по заданному паролю

4.7.1 Отключение напоминания пароля

При включенной опции <Вход по FaceID> есть возможность отключить регулярный ввод PIN-кода.

После включения тумблера <Вход по FaceID> появляется опция <Напоминать PIN-код> (см. Рисунок 74), которая по умолчанию включена. При выключении тумблера <Напоминать PIN-код> приложение перестает запрашивать ввод пароля раз в 72 часа. В таком случае ответственность за запоминание пароля остается за пользователем, так как восстановить его не получится.

4.8 Создание бэкапа

Для безопасности данных рекомендуется производить процедуру резервного копирования после каждого добавленного аутентификатора

Для создания резервной копии необходимо:

1. Нажать кнопку <Создать бэкап>, ввести PIN-код для создания резервной копии (см. Рисунок 77);
2. На экране [Создать бэкап] приведена справочная информация о процессе создания резервной копии (см. Рисунок 78).

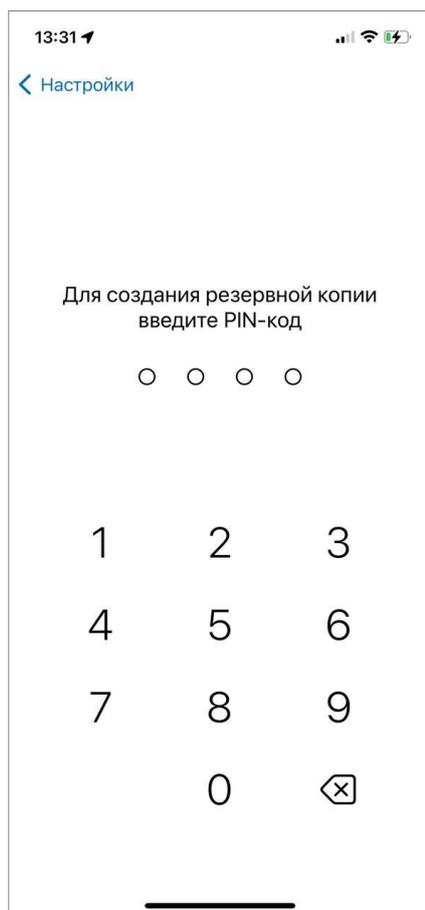


Рисунок 75 - Aladdin 2FA. Создание резервной копии

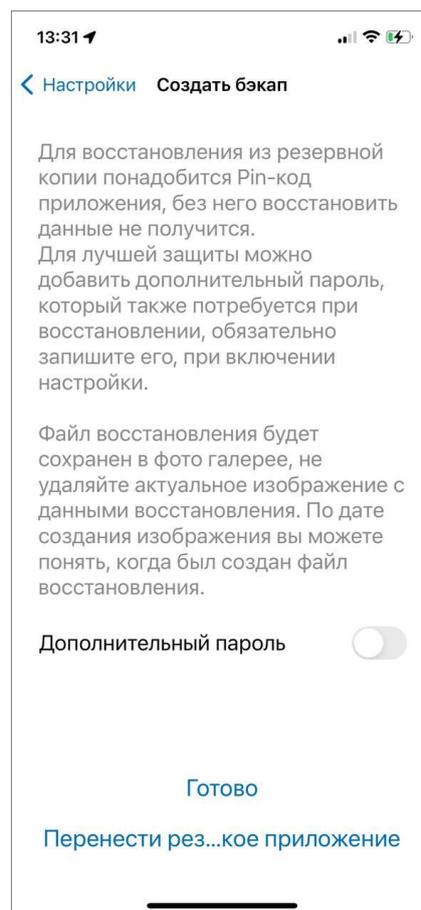


Рисунок 76 - Aladdin 2FA. Файл резервной копии в виде логотипа

Для повышения уровня безопасности можно воспользоваться дополнительным паролем, для этого необходимо включить тумблер <Дополнительный пароль>;

- 2.1. Если тумблер <Дополнительный пароль> не включен, то при нажатии на кнопку <Готово> будет создана резервная копия (см. Рисунок 77);
- 2.2. Если тумблер <Дополнительный пароль> включен, появятся дополнительные поля. В поле [Пароль восстановления] отображается автоматически сгенерированный 16-значный код, который надо скопировать и вставить в поле [Повторить пароль восстановления] (см. Рисунок 78). После нажатия на кнопку <Готово> будет создана резервная копия (см. Рисунок 79).

В зависимости от настроек смартфона может понадобиться предоставить разрешение на добавление фото в Галерею

Данный пароль необходимо запомнить так как восстановить его нельзя, но он понадобится на этапе восстановления бэкапа

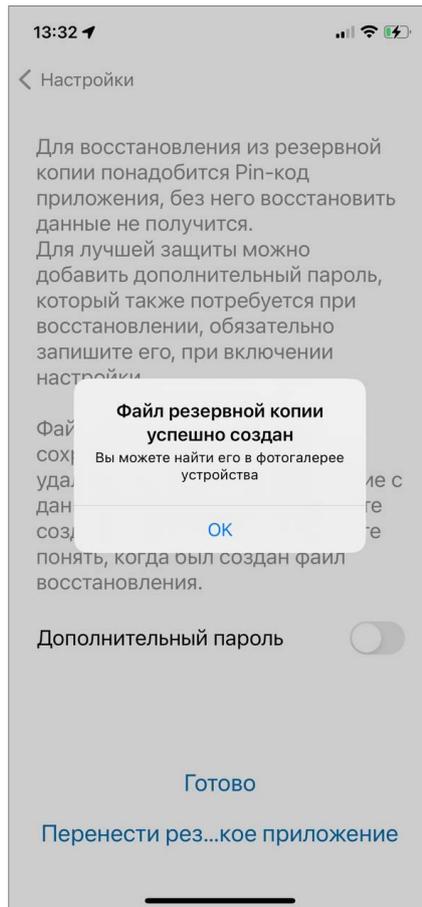


Рисунок 77 - Aladdin 2FA. Информационное сообщение о созданном бэкапе

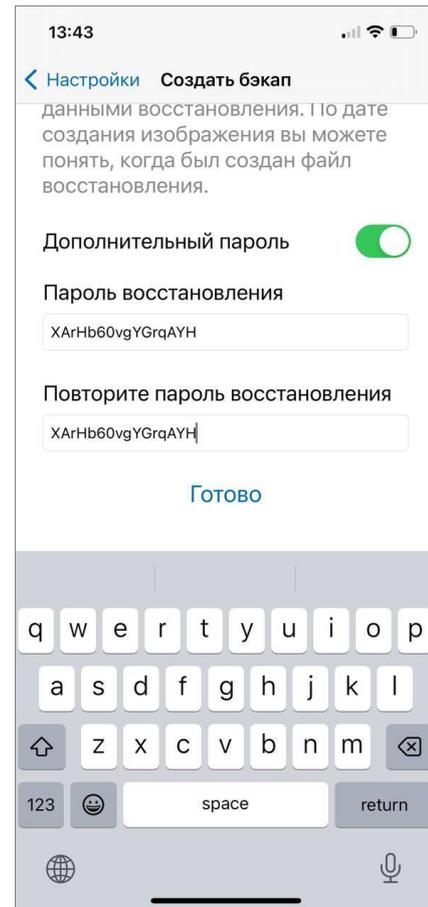


Рисунок 78 - Aladdin 2FA. Дополнительный пароль при создании бэкапа

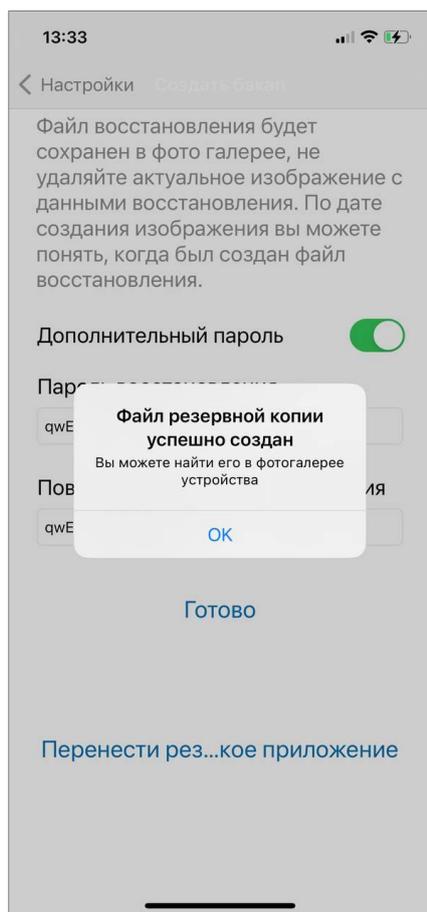


Рисунок 79 - Aladdin 2FA. Информационное сообщение о созданном бэкапе

Резервная копия хранится на устройстве в виде изображения с логотипом компании Аладдин Р.Д. в галерее устройства (см. Рисунок 80). Изображение нельзя удалять и переименовывать.

4.9 Восстановление из бэкапа

Для восстановления данных из резервной копии необходимо убедиться, что изображение, представляющее собой бэкап данных, находится на устройстве

При нажатии на кнопку <Восстановить из бэкапа> будет открыт экран для выбора изображения с резервной копией (см. Рисунок 81). Необходимо нажать кнопку <Выбрать файл восстановления> и указать файл, содержащий бэкап (см. Рисунок 82).



Рисунок 80 - Файл резервной копии в виде логотипа



Рисунок 81 - Aladdin 2FA. Восстановление из резервной копии



Рисунок 82 – Выбор изображения, представляющего собой бэкап

При восстановлении из бэкапа отображается окно, в котором необходимо ввести 16-значный пароль, если он был установлен при создании бэкапа и нажать кнопку <Восстановить>(см. Рисунок 83).

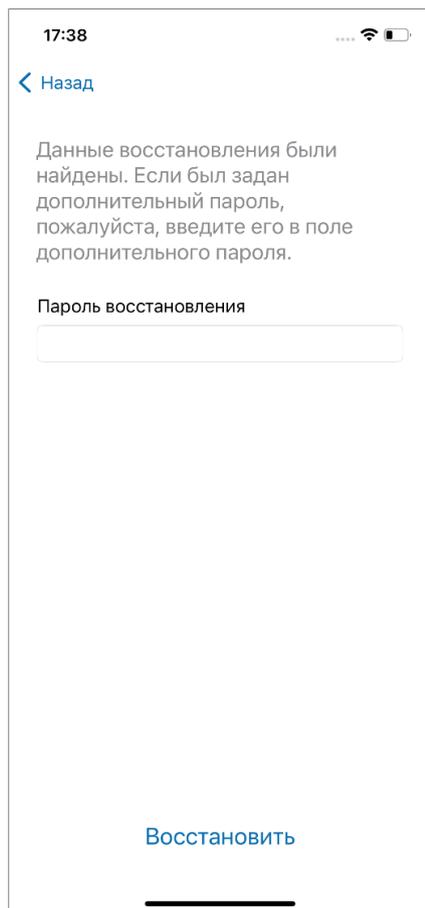


Рисунок 83 - Aladdin 2FA. Восстановление из резервной копии. Ввод дополнительного пароля

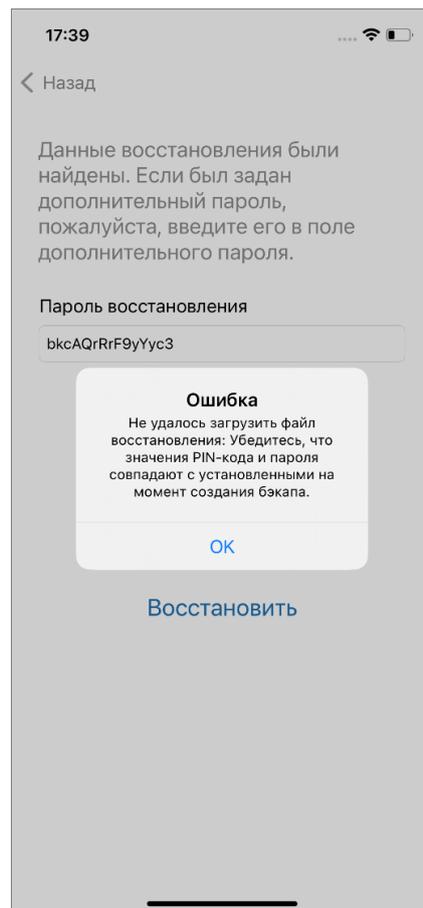


Рисунок 84 – Aladdin 2FA. Ошибка при восстановлении бэкапа

Если вы не помните 16-значный код, к сожалению, расшифровать резервную копию будет невозможно

Если был введен неправильный пароль или PIN-код, то после нажатия на кнопку <Восстановить>, будет отображаться ошибка (см. Рисунок 84).

5. Настройки смартфонов, при которых приложение работает некорректно

5.1 Время смартфона переведено более, чем на 23 часа

Если время смартфона переведено, функции бэкапирования будут работать некорректно.

5.2 На некоторых смартфонах не приходят PUSH-уведомления

На ряде Android-смартфонов имеются проблемы с доставкой PUSH-уведомлений (см. Рисунок 85). Если PUSH-уведомления не приходят в течение 10 секунд, необходимо зайти в приложение и дождаться окна подтверждения (см. Рисунок 86).

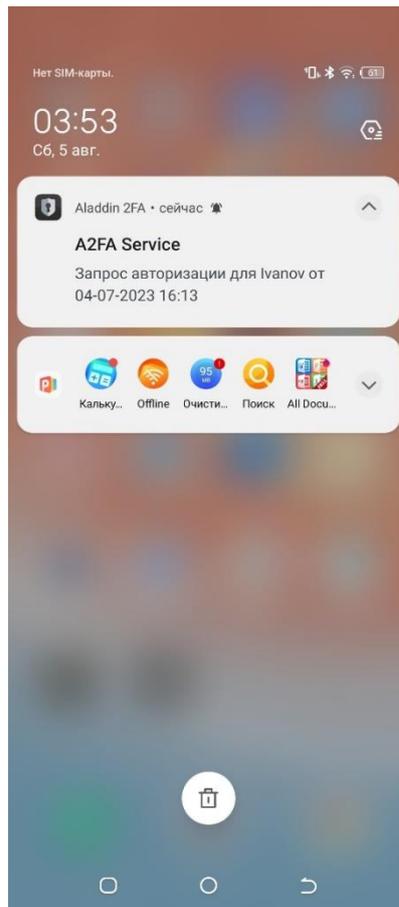


Рисунок 85 - Aladdin 2FA. Уведомление с запросом на авторизацию

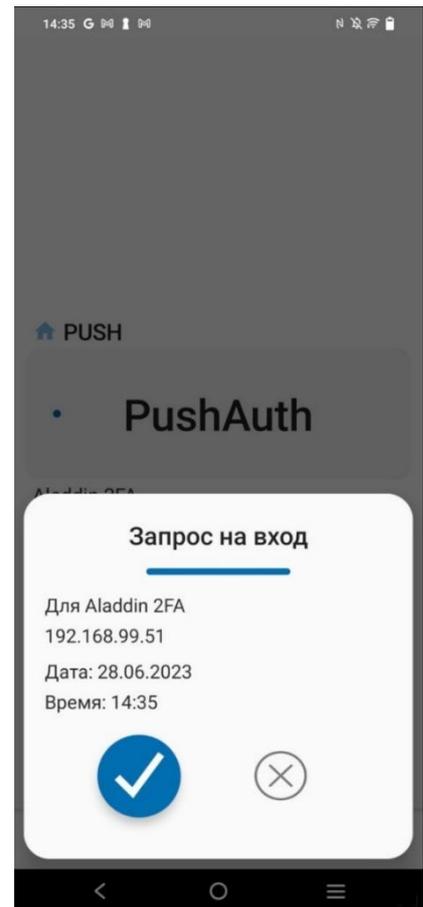


Рисунок 86 - Aladdin 2FA. Запрос на авторизацию в приложении

Приложение А. Добавление сертификата в пользовательское хранилище на устройстве

При использовании TLS для обеспечения безопасного соединения между сервером Aladdin 2FA Service и мобильными приложениями Aladdin 2FA может возникнуть необходимость использования корпоративных сертификатов. Для обеспечения безопасности и правильной работы системы необходимо добавить эти сертификаты в пользовательское хранилище на устройстве. Это позволит убедиться в подлинности идентификационных данных, использованных для TLS-соединения с сервером Aladdin 2FA Service, и обеспечит безопасность передачи данных между сервером и мобильным приложением.

Для устройств с ОС Android

Для добавления сертификата в пользовательское хранилище необходимо:

1. Запросить сертификат у администратора A2FA;
2. На устройстве перейти в <Настройки>;
3. <Установить сертификаты из памяти>, далее <Сертификат центра сертификации>;
4. Будет открыт экран [Конфиденциальность ваших данных будет нарушена] с информацией, нажать кнопку <Все равно установить> (см. Рисунок 88). Подтвердить действие паролем или предъявлением биометрии;

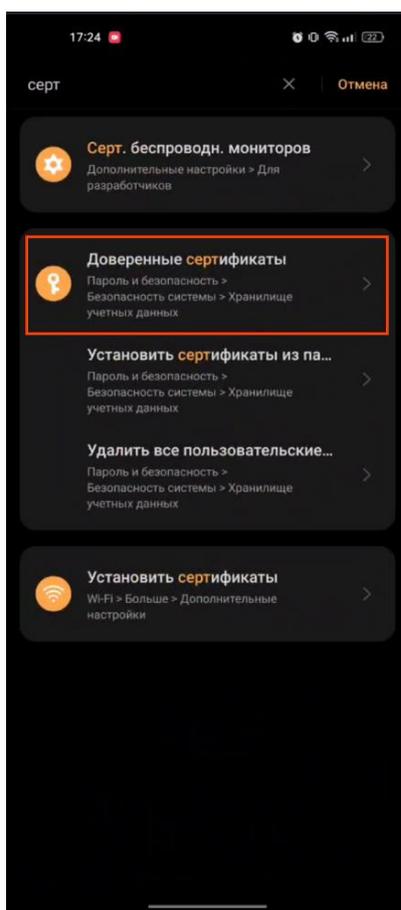


Рисунок 87 - Добавления сертификата в пользовательское хранилище. Доверенные сертификаты

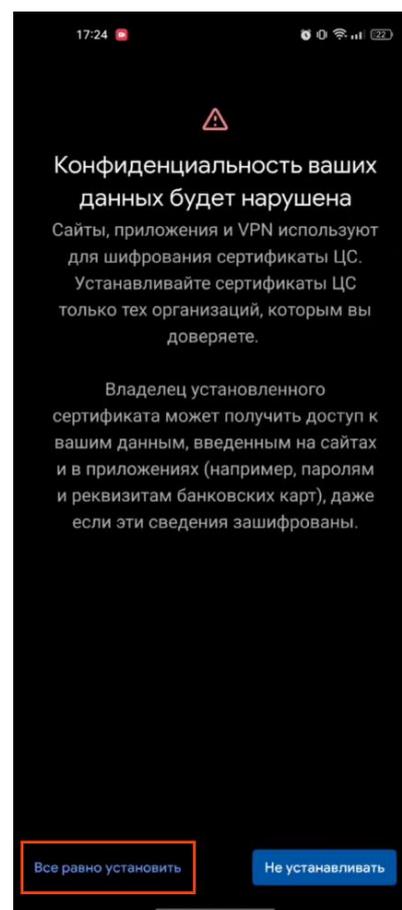


Рисунок 88 - Добавления сертификата в пользовательское хранилище. Экран с предупреждением о нарушении конфиденциальности

5. Появится всплывающее сообщение о том, что сертификат установлен (см. Рисунок 89);
6. Перейти в <Доверенные сертификаты> (см. Рисунок 89), выбрать вкладку [Пользователи], на ней будет отображаться добавленный сертификат (см. Рисунок 90);

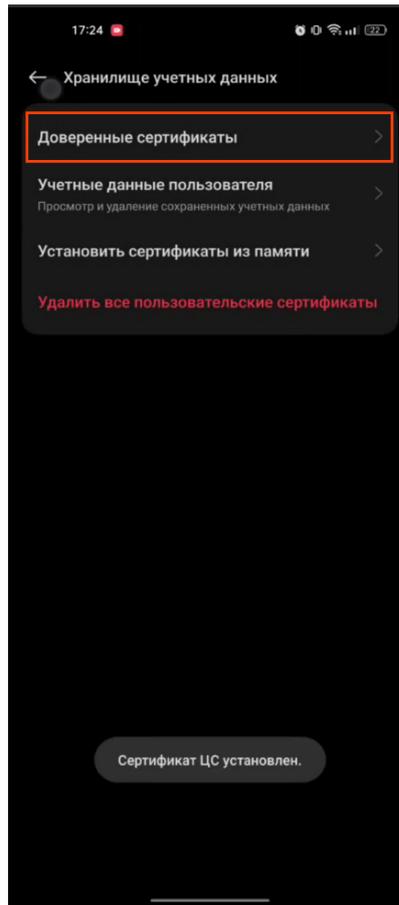


Рисунок 89 - Добавления сертификата в пользовательское хранилище. Всплывающее сообщение

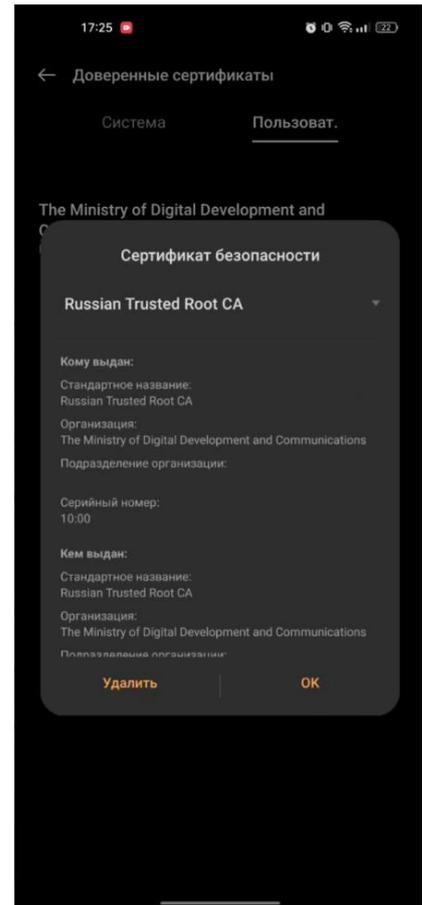


Рисунок 90 - Добавления сертификата в пользовательское хранилище. Добавленный сертификат

Для устройств с ОС iOS

Для добавления сертификата в пользовательское хранилище необходимо:

1. На устройстве зайти в [Файлы], выбрать сертификат, полученный от администратора (см. Рисунок 91);
2. Зайти в [Настройки], выбрать пункт <Основные>, далее <VPN и Управление устройством> в группе [Загруженный профиль] будет отображен сертификат (см. Рисунок 92);

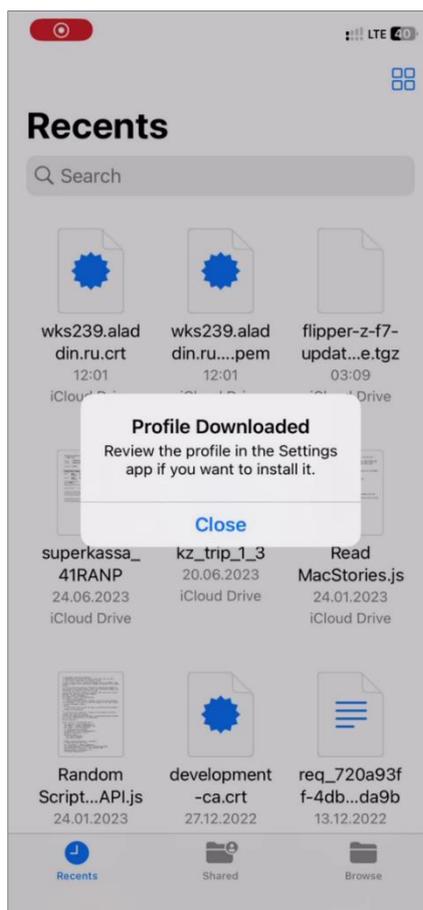


Рисунок 91 - Добавления сертификата в пользовательское хранилище. Загрузка профиля

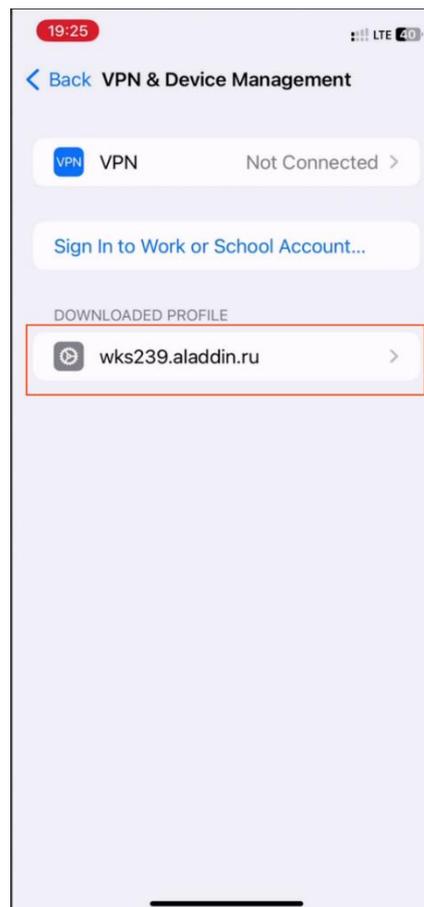


Рисунок 92 - Добавления сертификата в пользовательское хранилище. Загруженный сертификат

3. Подтвердить действие паролем от устройства;
4. Будет открыто окно [Предупреждение] (см. Рисунок 93). Нажать кнопку <Установить>;
5. Вернуться в [Настройки], <Основные>, <Профиль> - там будет отображаться загруженный сертификат (см. Рисунок 94);
6. Перейти в [Настройки], <Основные>, <Об этом устройстве>, <Доверие сертификатам> и активировать сертификат с помощью переключателя (см. Рисунок 94).

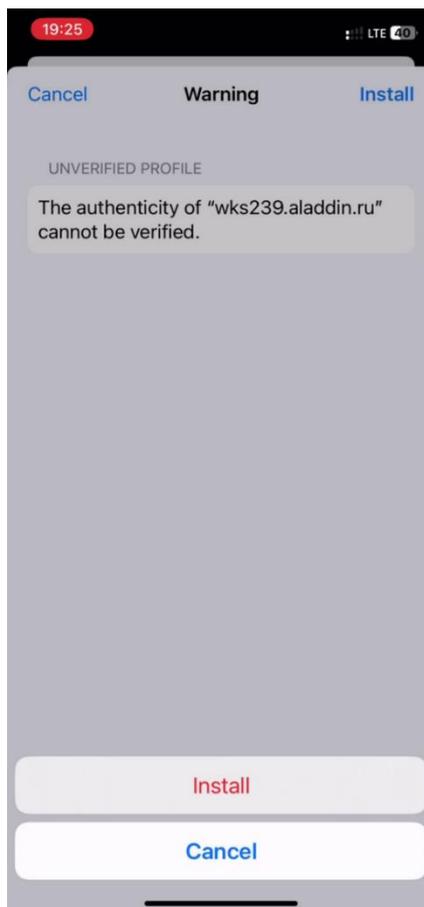


Рисунок 93 - Добавления сертификата в пользовательское хранилище. Установка сертификата

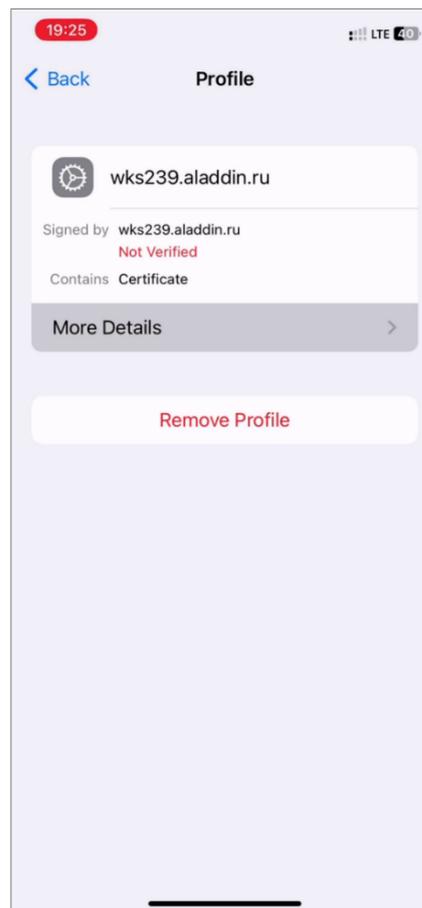


Рисунок 94 - Добавления сертификата в пользовательское хранилище. Загруженный сертификат в настройке [Профиль]

Приложение Б. Запуск телеграм-бота

Для устройств с ОС Android

Для запуска телеграм-бота необходимо:

1. Запросить QR-код у администратора A2FA;
2. На устройстве перейти в <Камеру>;
3. Отсканировать QR-код и перейти по ссылке;
4. Будет открыто приложение «Telegram» со страницей телеграм-бота;
5. Нажать кнопку «Старт» (см. Рисунок 95);
6. Бот отправит сообщение об успешной регистрации пользователя (см. Рисунок 96).

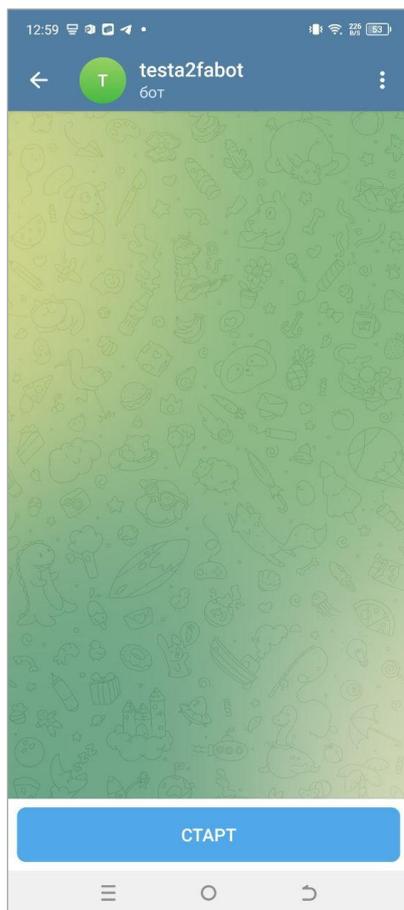


Рисунок 95 – Запуск телеграм-бота



Рисунок 96 – Успешная регистрация пользователя

При использовании телеграм-бота для входа на свой ресурс (личный кабинет, почту и т.д.) необходимо ввести код (вставить, если он был скопирован) в нужное поле в качестве второго фактора аутентификации (см. Рисунок 97).



Рисунок 97 – Код для авторизации на ресурсе

Для устройств с ОС iOS

Для запуска телеграм-бота необходимо:

1. Запросить QR-код у администратора A2FA;
2. На устройстве перейти в <Камеру>;
3. Отсканировать QR-код и перейти по ссылке;
4. Будет открыто приложение «Telegram» со страницей телеграм-бота;
5. Нажать кнопку «Старт» (см. Рисунок 98);
6. Бот отправит сообщение об успешной регистрации пользователя (см. Рисунок 99).

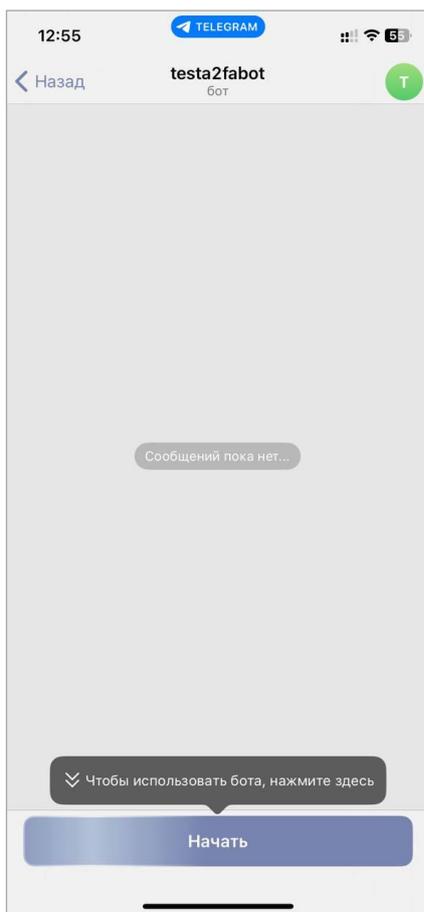


Рисунок 98 – Запуск телеграм-бота

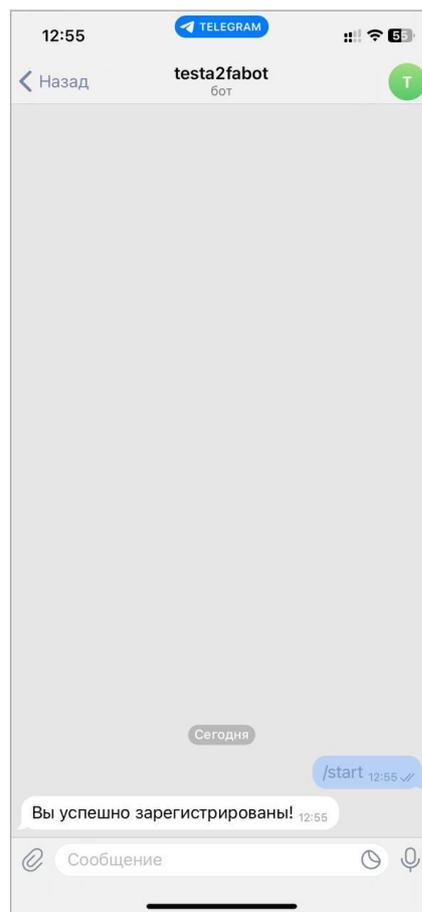


Рисунок 99 – Успешная регистрация пользователя

При использовании телеграм-бота для входа на свой ресурс (личный кабинет, почту и т.д.) необходимо ввести код (вставить, если он был скопирован) в нужное поле в качестве второго фактора аутентификации (см. Рисунок 100).

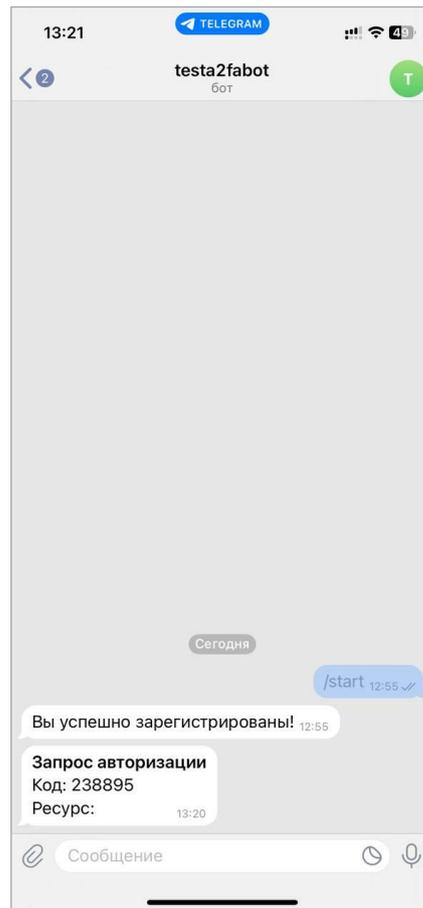


Рисунок 100 – Код для авторизации на ресурсе

Контакты

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания "Аладдин Р.Д."

Телефон: +7 (495) 223-00-01 (секретарь)

E-mail: aladdin@aladdin.ru (общий)

Web: <https://www.aladdin.ru>

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техническая поддержка

Контакты службы техподдержки:

Телефон: +7 (499) 702-39-68

Web: www.aladdin.ru/support/

Список литературы

- 1 Aladdin 2FA Service. Руководство администратора под Windows
 - 2 JaCarta Management System v3.7. Руководство пользователя
JaCarta Management System 4LX. Руководство пользователя
-

Регистрация изменений

Версия документа	Изменения
1.3	В связи с выходом релиза мобильного приложения Aladdin 2FA версии 1.3.0 обновлены скриншоты, переработана структура разделов. Добавлены разделы: п.2.1 Обозначения экранов .., п.2.3 Добавление сертификата .., п.2.4 Что делать в случае возникновения ошибки, п.3.3 Редактирование аккаунта, п.4.3 Редактирование аккаунта, п.4.8 Создание бэкапа, п.4.9 Восстановление из бэкапа
1.2	Добавлены разделы п.3.8 Резервное копирование, п.3.9 Восстановление из копии
1.2	Обновлено описание п. 3.2: добавление аккаунта вручную
1.2	Обновление скриншотов к выходу релиза
1.1	Обновление описания п.2.1 Регистрация аутентификатора
1.1	Приведение документа к корпоративному шаблону. Обновление скриншотов
1.0	Исходная версия документа по работе с мобильным приложением Aladdin 2FA версии 1.0.0