Aladdin 2FA. Руководство пользователя

Инструкция по работе с мобильным приложением Aladdin 2FA

Версия продукта	1.3.0
Статус	Публичный
Дата	02.08.2023
Листов	51

Оглавление

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 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.

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.

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 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 на Рисунок 4. На нем отображаются зарегистрированные аутентификаторы, методы добавления аутентификаторов, кнопка вызова настроек приложения;

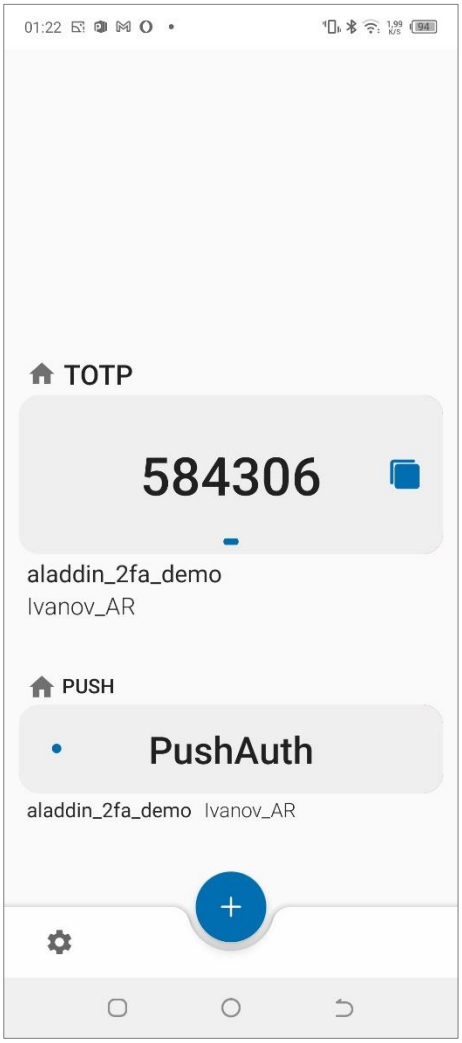

Рисунок 4 – Aladdin 2FA. Главный экран

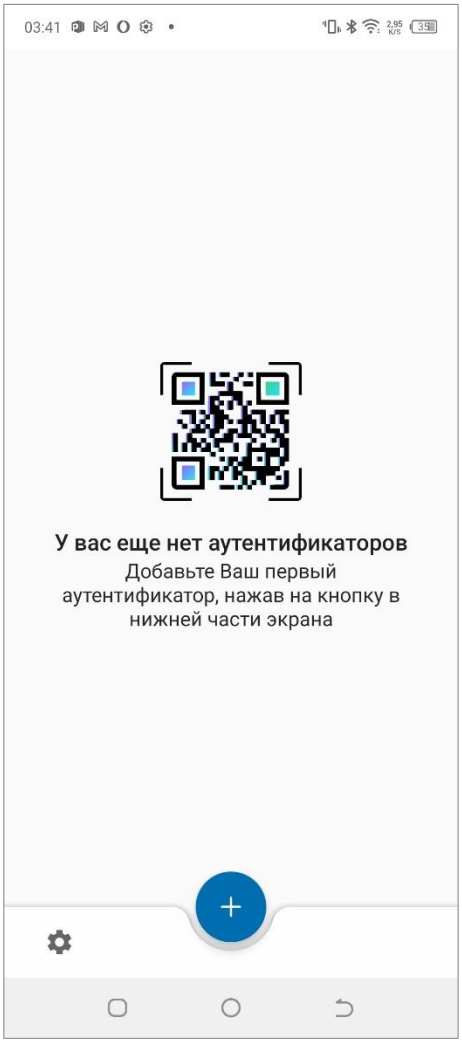

Рисунок 5 - Aladdin 2FA. Пустой экран

4. Пустой экран – приведен на Рисунок 5. На нем отображается информация о том, каким образом добавить аутентификатор. Пустой экран отображается при первом запуске приложения либо в случае, если все аутентификаторы были удалены.

2.2 Регистрация аутентификатора

Для регистрации аутентификатора можно воспользоваться следующими способами:

1. Отсканировать QR-код (см. подробнее п.3.2 шаг 2);
2. Воспользоваться ссылкой для регистрации (подробное описание см. ниже);

3. Добавить аутентификатор вручную (см. подробнее п.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 ниже (см. Рисунок 6, Рисунок 7, Рисунок 8).

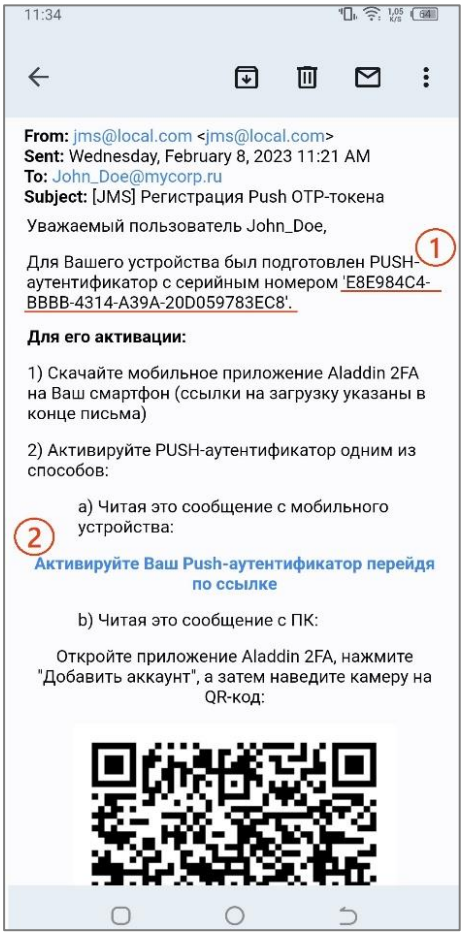

Рисунок 6 – Электронное письмо с вариантами регистрации в мобильном приложение Aladdin 2FA. Часть 1

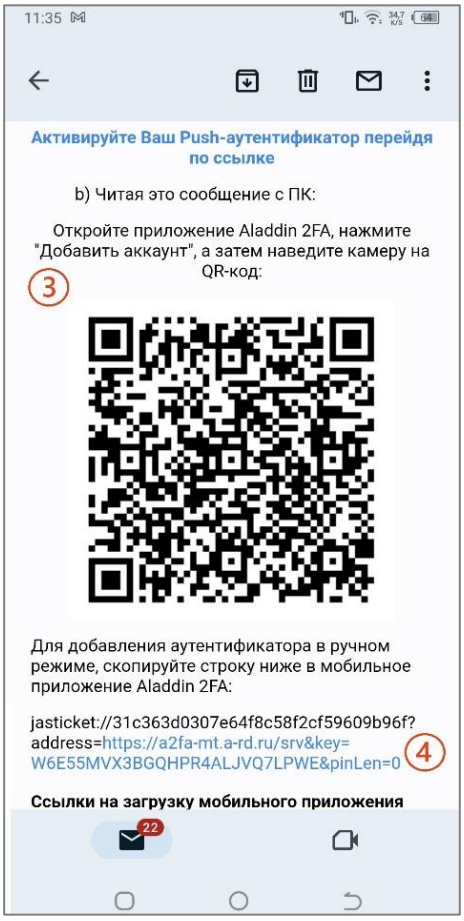

Рисунок 7 - Электронное письмо с вариантами регистрации в мобильном приложение Aladdin 2FA. Часть 2

Рисунок 8 - Электронное письмо с вариантами регистрации в мобильном приложение 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 приложение Aladdin 2FA. Описание настроек

Элемент управления	Описание
1	Серийный номер PUSH-аутентификатора. Серийный номер может понадобится 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
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.

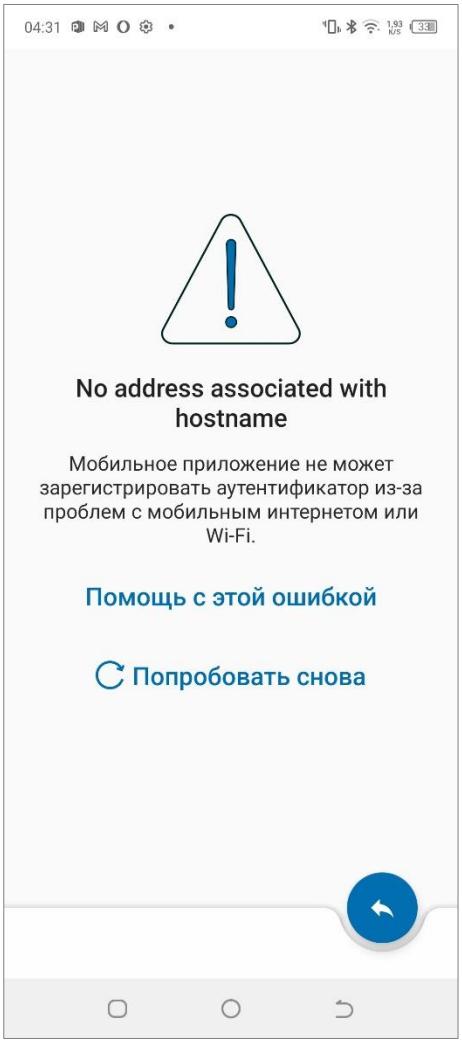

Рисунок 9 - Aladdin 2FA. Отображение окна с известной ошибкой

Рисунок 10 – Страница с описанием ошибки 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.

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 проблему.

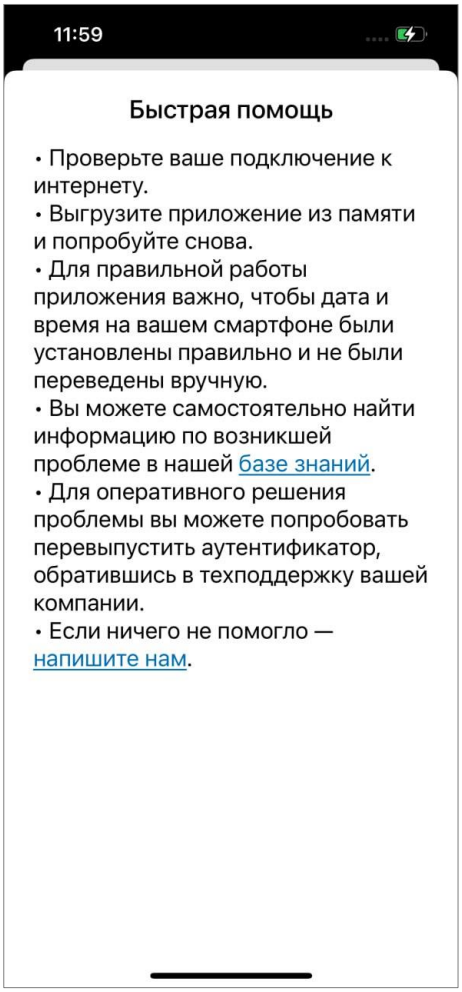

Рисунок 11 - Aladdin 2FA. Отображения окна [Быстрая помощь]

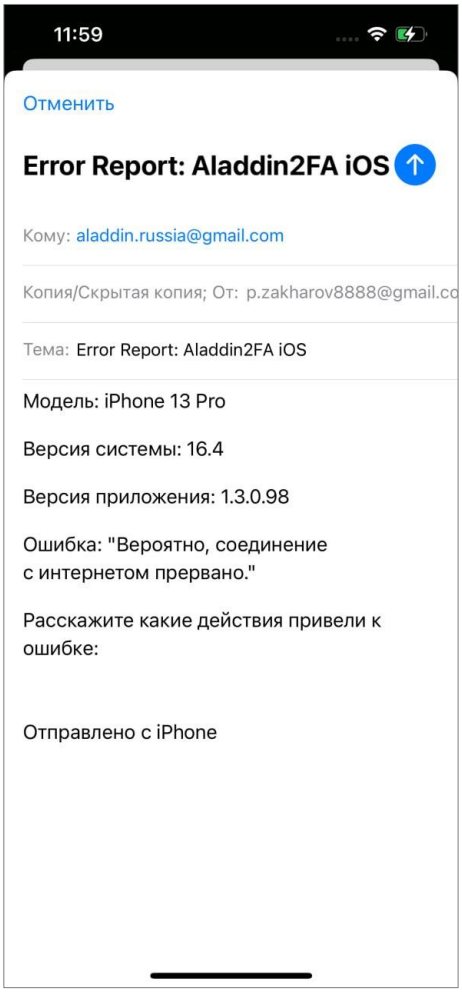

Рисунок 12 – Форма письма в техподдержку

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

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

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

3.1 Первый запуск приложения Aladdin 2FA

1. Нажмите на иконку приложения для его запуска -  ;
2. Будет открыто окно (см. Рисунок 13), где необходимо придумать пароль из четырех символов, с помощью которого будет осуществляться вход в приложение;
3. На следующем шаге ввести подтверждение пароля. После установки пароля, если на устройстве используется биометрия, будет предложено включить возможность входа, используя биометрию;

Рисунок 13 - Aladdin 2FA. Установка пароля

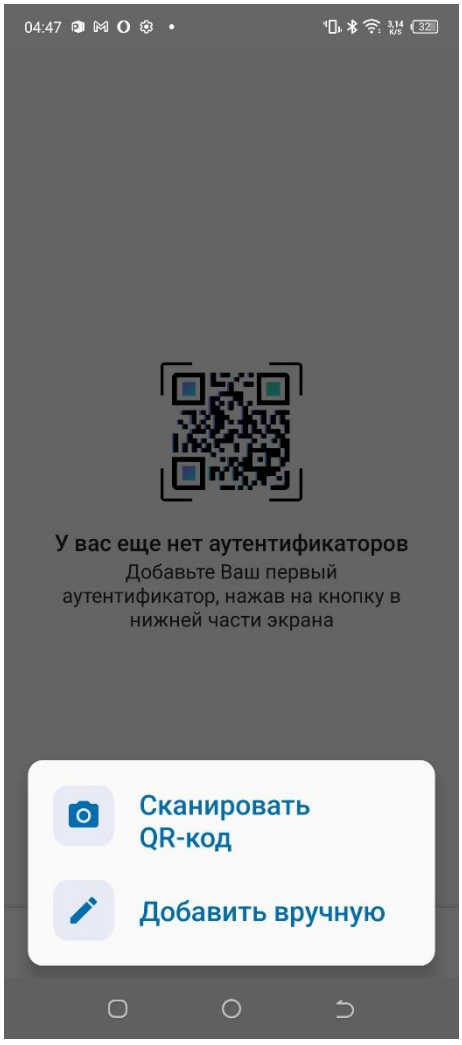

Рисунок 14 - Aladdin 2FA. Добавление аутентификатора

4. При первом входе в приложение на экране, приведенном выше (см. Рисунок 14), 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 15.

В зависимости от настроек смартфона может понадобится предоставить разрешение для 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;

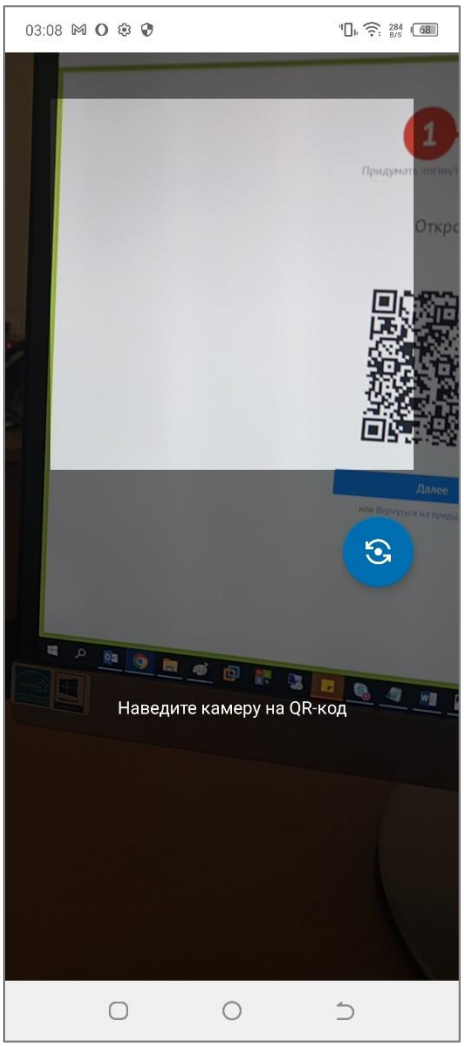

Рисунок 15 - Aladdin 2FA. Сканирование QR-кода

Рисунок 16 - Aladdin 2FA. Добавленный аутентификатор

6. После добавления аутентификатора главный экран приложения имеет вид, приведенный на Рисунок 16, 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

На главном экране мобильного приложения отображается перечень всех добавленных аутентификаторов (см. Рисунок 17).

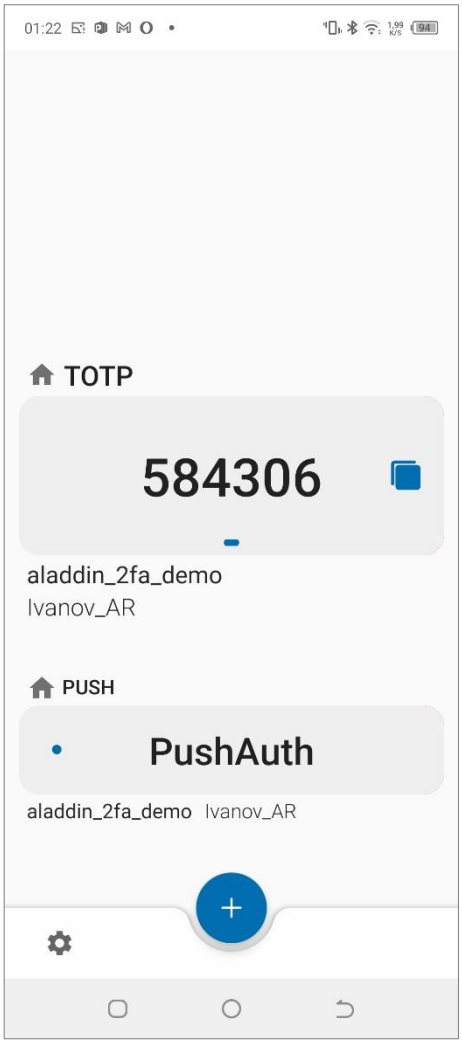

Рисунок 17 - Aladdin 2FA. Главный экран

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 15).

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 18) и нажать кнопку <Добавить аутентификатор>.

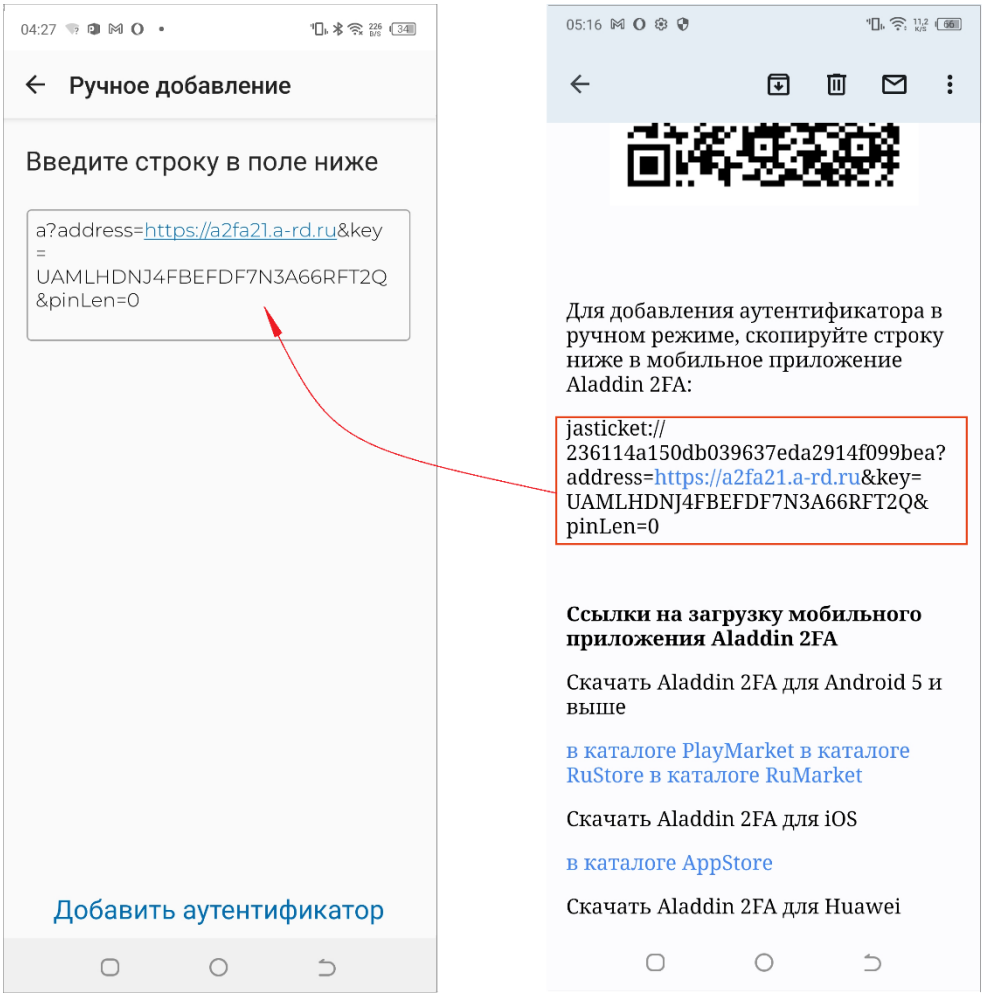

Рисунок 18 - Aladdin 2FA. Добавление аутентификатора вручную

В случае успешного добавления, аутентификатор появится в списке аутентификаторов на главном экране.
В случае, если при нажатии на кнопку <Добавить аутентификатор> на экране появилась ошибка (см. Рисунок 19), обратиться к администратору, выдавшему аутентификатор, и сообщить об ошибке (подробнее про возможные ошибки в приложении см. п. 2.3).

Рисунок 19 - Aladdin 2FA. Не удалось активировать аутентификатор вручную

3.3 Редактирование аутентификатора

При долгом нажатии на выбранном аутентификаторе становится доступен режим редактирования (см. Рисунок 20): можно удалить аутентификатор, переименовать его или, если аутентификаторов два и больше, изменить его местоположение.

Подробнее про каждую процедуру описано ниже.

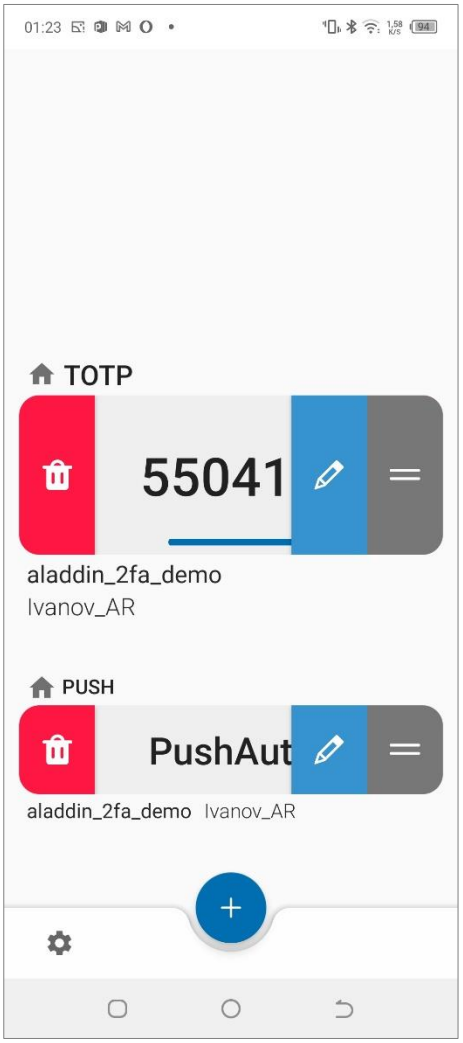

Рисунок 20 - Aladdin 2FA. Режим редактирования аутентификатора

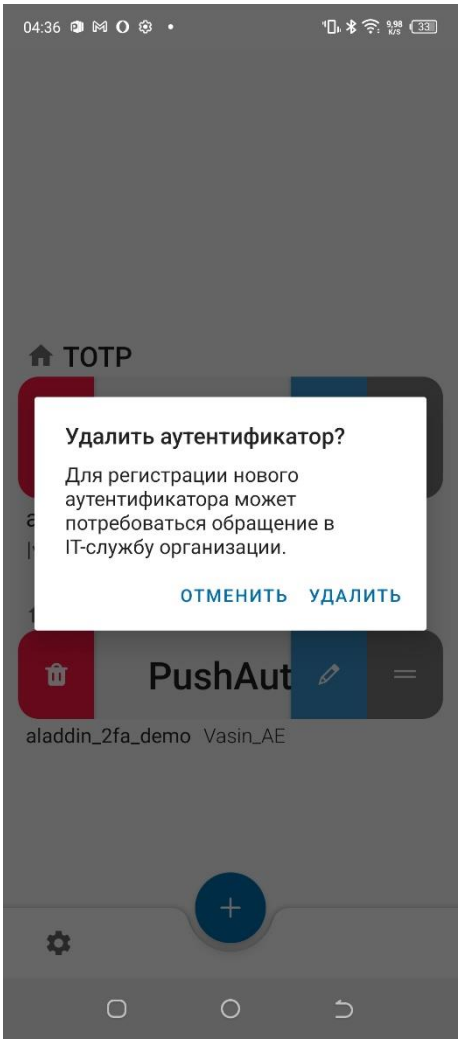

Рисунок 21 - Aladdin 2FA. Информационное сообщение при удаление аутентификатора

3.3.1 Удаление

1. Перейти в режим редактирования и нажать кнопку  . Появиться окно с информацией об удалении (см. Рисунок 21);
2. Подтвердить удаление записи с помощью кнопки <Удалить>.

В случае, если операция удаления применяется к единственному аутентификатору, то после удаления будет отображен пустой экран.

3.3.2 Переименование

1. Перейти в режим редактирования и нажать кнопку  ;
2. Будет открыто окно [Лейбл аутентификатора] (см. Рисунок 22), в котором можно поменять название аутентификатора, заданное по умолчанию, на другое имя. Еще можно поменять иконку отображения аутентификатора;

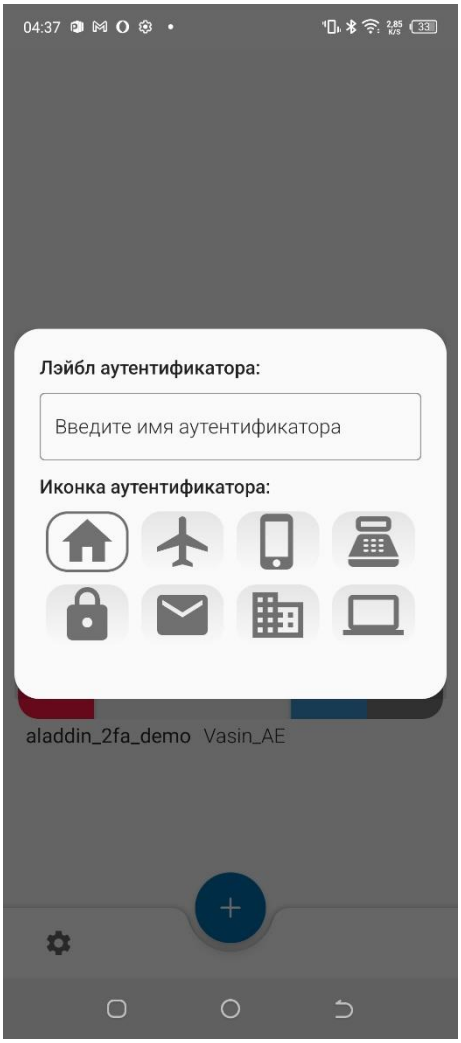

Рисунок 22 - Aladdin 2FA. Задание нового имени для аутентификатора

3. В поле [Введите имя аутентификатора] ввести новое имя и выбрать иконку. Изменения сохраняются автоматически после каждого нажатия по экрану.

3.3.3 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 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 23).

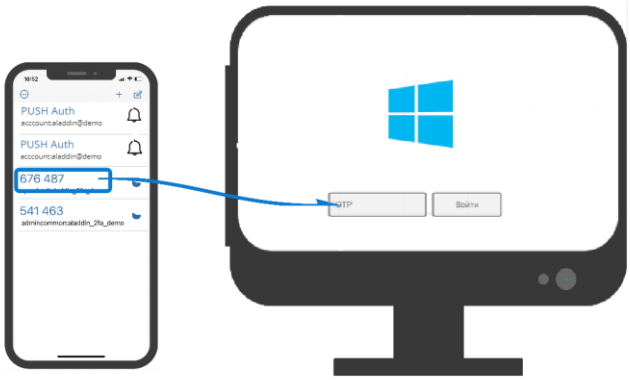

Рисунок 23 – Ввод сгенерированного одноразового кода в соответствующее поле

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 аутентифкатора, зарегистрированного с помощью PUSH-аутентификации, отображается идикатор 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.

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 24);

   Для пользователей Android версии 11 и ниже доступна функция раскрыть уведомление с помощью кнопки  *. Будут доступны кнопки <Принять> и <Отклонить*

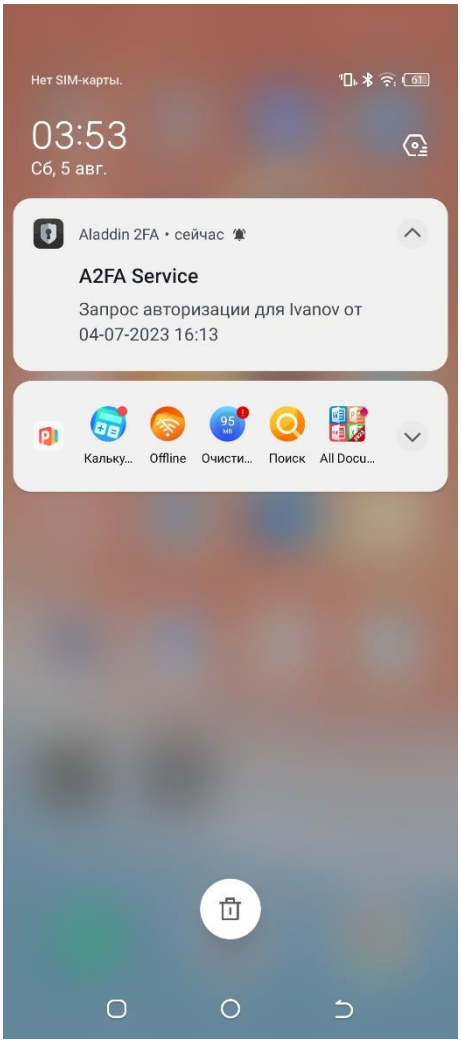

Рисунок 24 - Aladdin 2FA. Уведомление с запросом на авторизацию

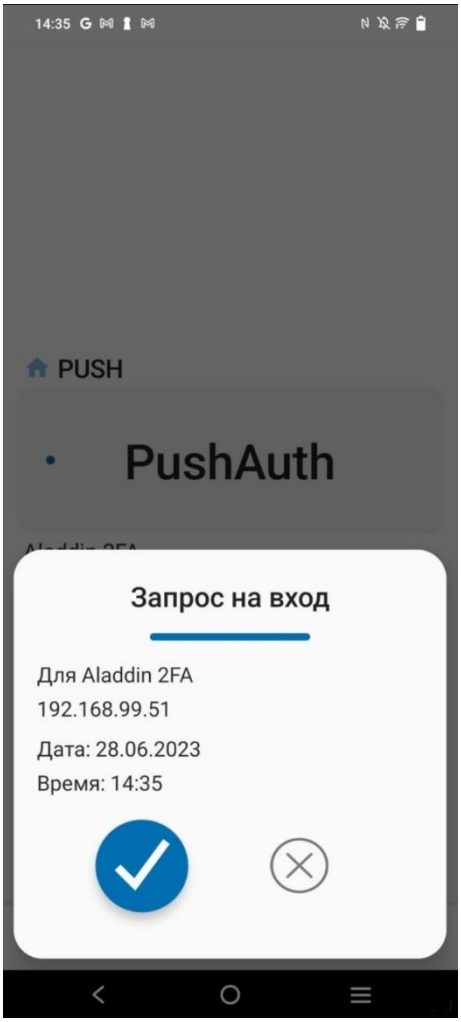

Рисунок 25 - Aladdin 2FA. Запрос на авторизацию в приложении

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. Будет открыто окно [Запрос на вход] с информацией и кнопками  - <Принять> и  - <Отклонить> (см. Рисунок 25);
5. После нажатия на любую из кнопок будет отображать окно [Проверка] (см. Рисунок 26), пока происходит процесс подтверждения/отклонения авторизации;
6. При нажатии на кнопку <Принять> авторизация будет подтверждена (см. Рисунок 27). Окно с подтверждением закроется автоматически;

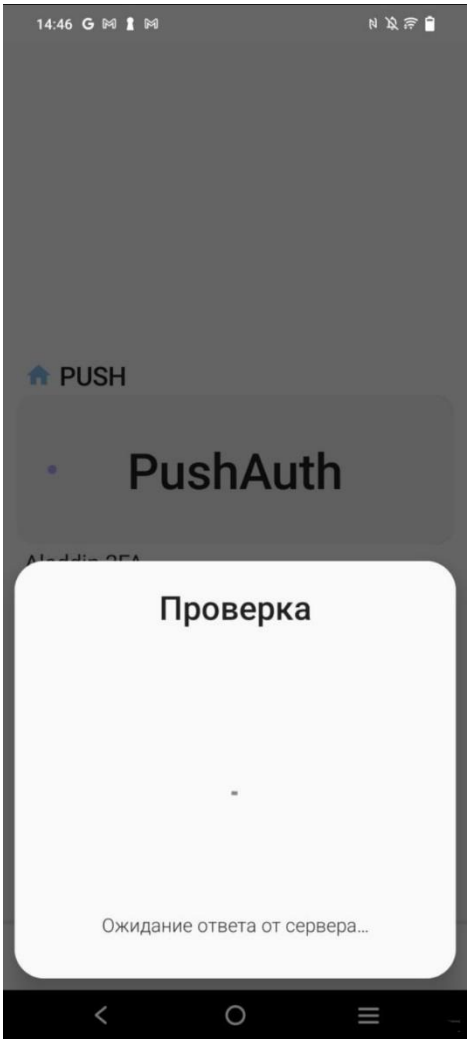

Рисунок 26 - Aladdin 2FA. Поверка ответа на запрос авторизации

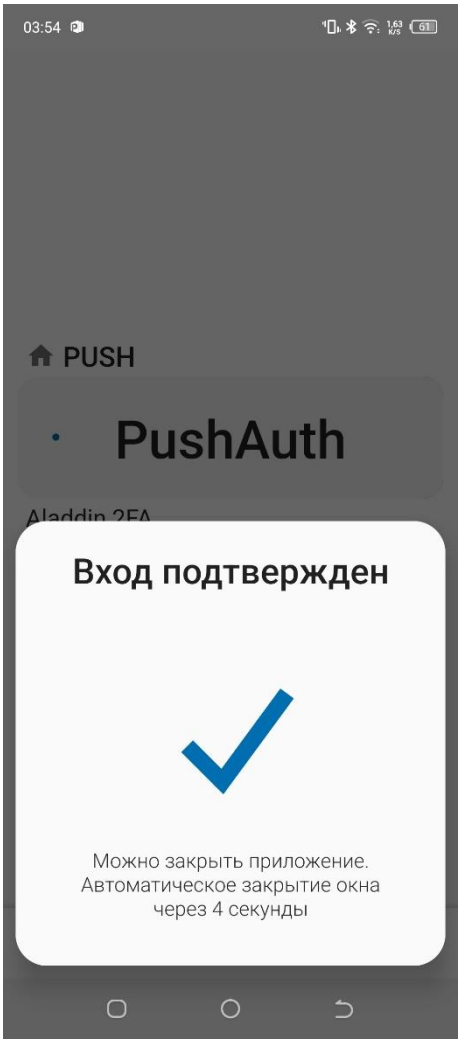

Рисунок 27 - Aladdin 2FA. Запрос на авторизацию подтвержден

7. При нажатии на кнопку <Отклонить> авторизация будет отклонена (см. Рисунок 28). Окно [Вход отклонен] закроется автоматически.

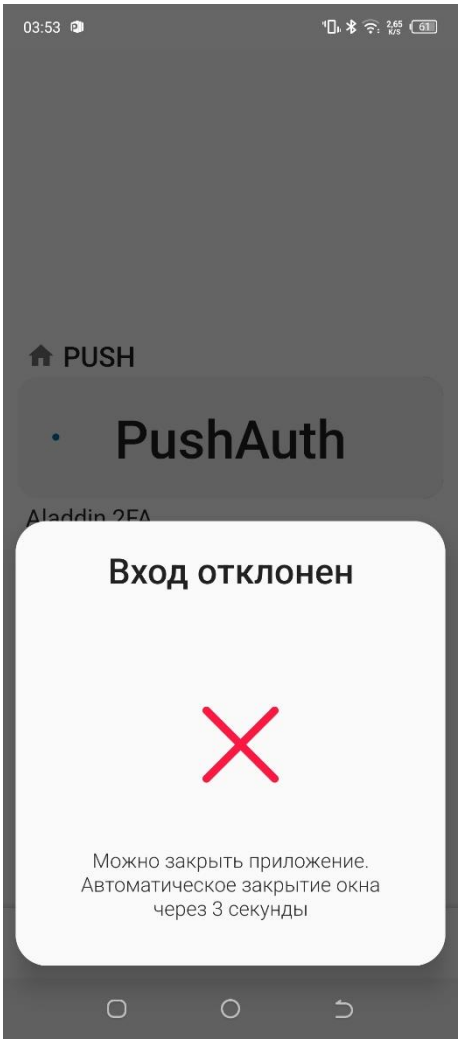

Рисунок 28 - Aladdin 2FA. Запрос на авторизацию отклонен

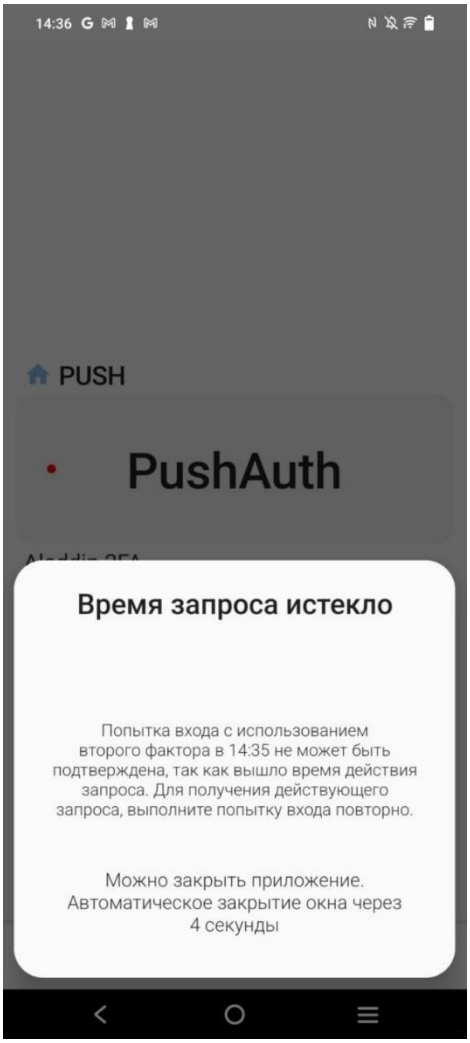

Рисунок 29 - Aladdin 2FA. Запрос на авторизацию отклонен

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 отобразиться окно [Время запроса истекло] (см. Рисунок 29). Рекомендуется осуществить повторный вход в приложение Aladdin 2FA.

3.5.2 PUSH-аутентификация в открытом приложении

Если был осуществлен вход в приложение Aladdin 2FA, то запрос на авторизацию появится автоматически (см. Рисунок 25). 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 опциями (см. Рисунок 30).

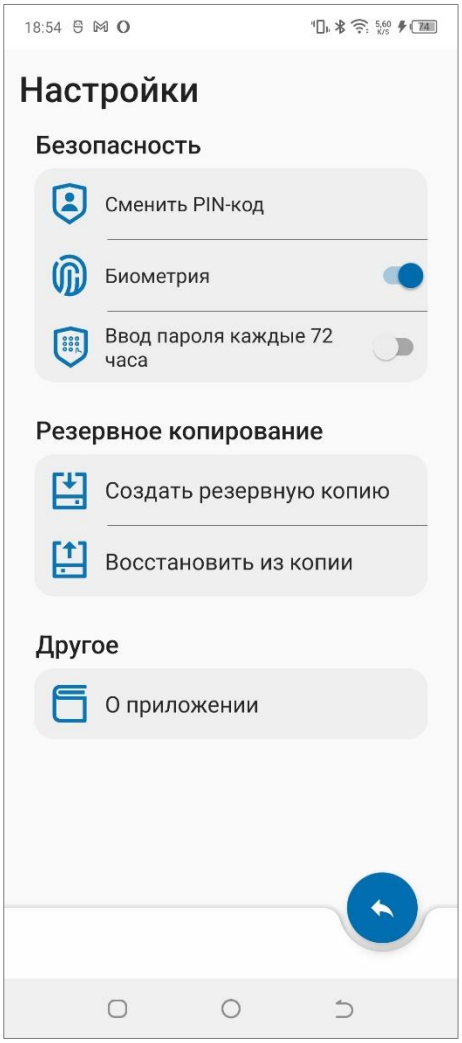

Рисунок 30 - Aladdin 2FA. Настройки приложения

Рисунок 31 - Aladdin 2FA. О приложении

	<Сменить PIN-код> - при нажатии на кнопку будет открыто окно для смены PIN-кода (см. Рисунок 13). Нужно ввести новый PIN-код и его подтверждение
	<Биометрия> - кнопка для переключения режима входа в приложение с помощью отпечатка пальца. *Если смартфон не поддерживает биометрию, данной кнопки в меню опций не будет*
	<Создать резервную копию> - кнопка для перехода к операции создания бэкапа данных приложения. Подробнее см. п. 3.7.1
	<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 31)

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 меню 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 32). Войти в приложение можно будет только по заданному паролю

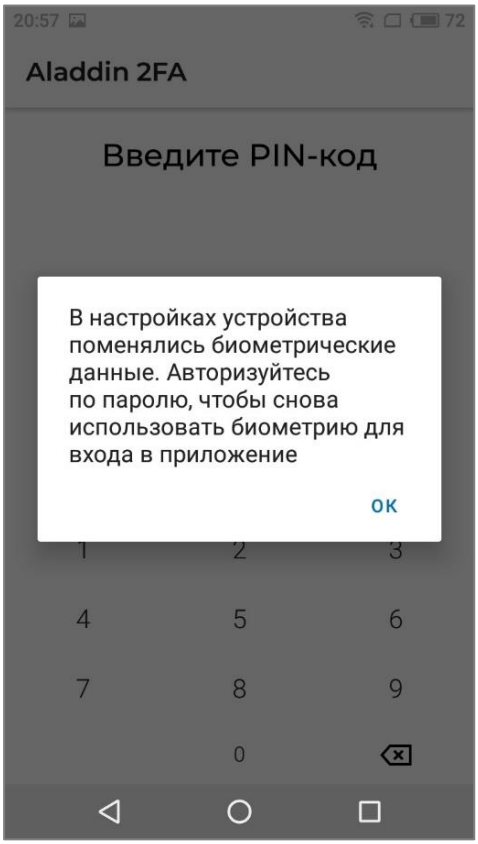

Рисунок 32 - Aladdin 2FA. Настройки приложения

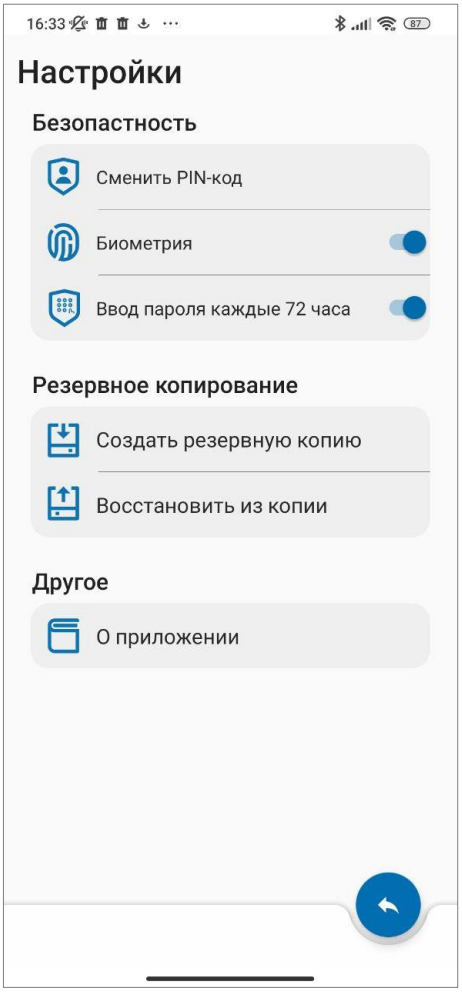

Рисунок 33 - Aladdin 2FA. Отключение регулярного ввода PIN-кода

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 33), которая по умолчанию включена. При выключении тумблера <Напоминать пароль> 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*

При нажатии на кнопку <Резервное копирование> откроется экран резервного копирования с информацией и полями для пароля восстановления.

В поле [Пароль восстановления] будет отображать автоматически сгенерированный 16-значный код, который надо будет повторить в поле [Повторите пароль восстановления] (см. Рисунок 34).

> ***Данный пароль необходимо запомнить, так как восстановить его нельзя, но он понадобиться на этапе воостановления бэкапа***

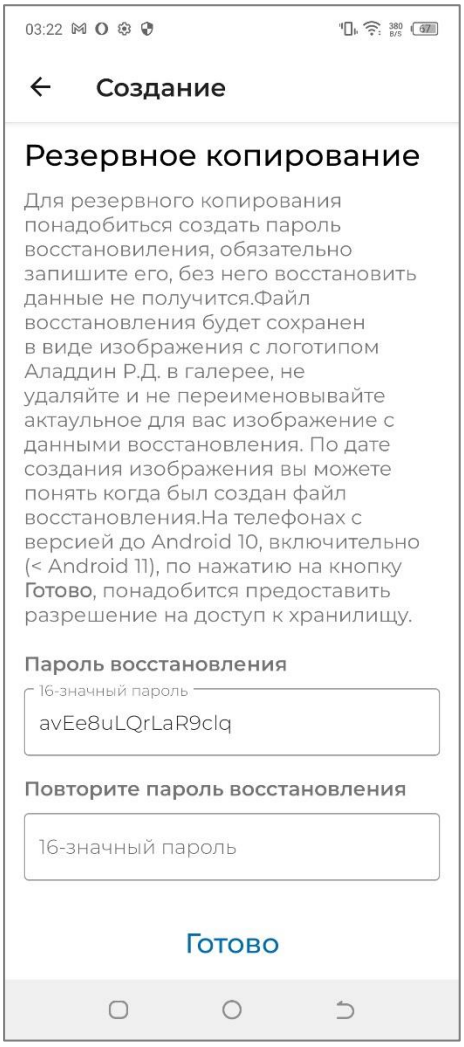

Рисунок 34 - Aladdin 2FA. Создание резервной копии

Рисунок 35 - Файл резервной копии в виде логотипа

Резервная копия хранится на устройстве в виде изображения с логотипом компании Аладдин Р.Д. в галерее устройства (см. Рисунок 35). Изображение нельзя удалять и переименовывать.

3.9 Восстановление из копии

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

При нажатии на кнопку <Восстановление из копии> будет открыт экран [Восстановление], где необходимо ввести 16-значный код, сохраненный при резервном копировании (см. Рисунок 36). Нажать кнопку <Восстановить>.

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

Если был введен неправильный пароль или изображение с бэкапом было создано на другом устройстве, после нажатия на кнопку <Восстановить>, будет отображаться ошибка (см. Рисунок 37).

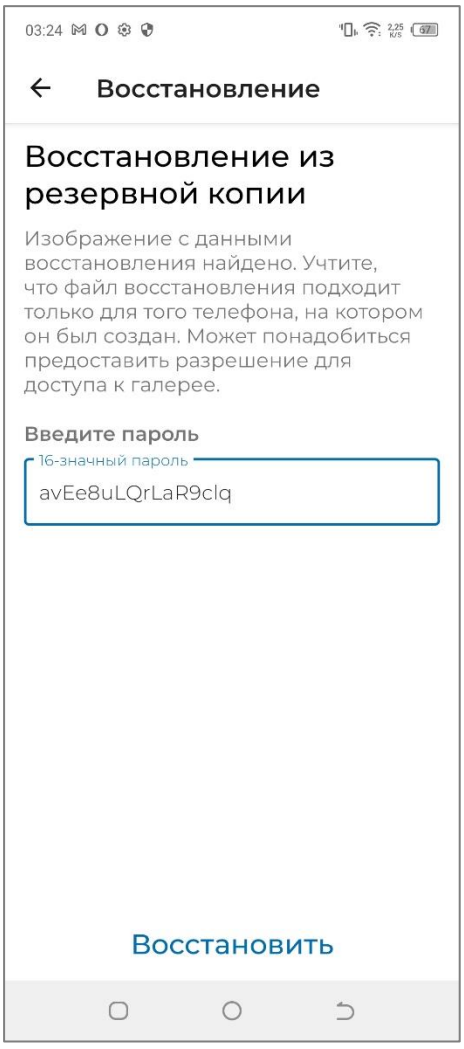

Рисунок 36 - Aladdin 2FA. Восстановление из резервной копии

Рисунок 37 - 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 бэкапа (см. Рисунок 38). Данная процедура возможна если все операции производились на одном устройстве.

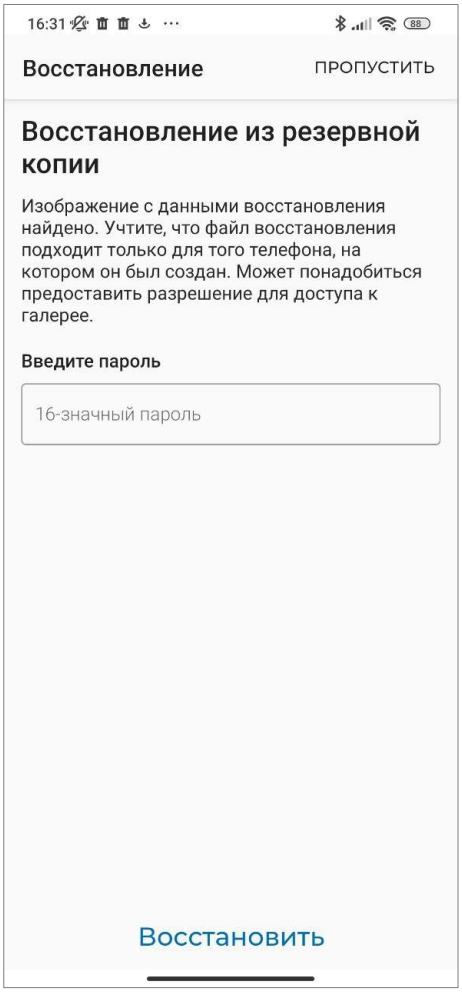

Рисунок 38 - Aladdin 2FA. Восстановление из резервной копии при переустановке приложения

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 (см. Рисунок 39), где необходимо придумать пароль из четырех символов, с помощью которого будет осуществляться вход в приложение;
3. На следующем шаге ввести подтверждение пароля. После установки пароля, если на устройстве используется биометрия, будет предложено включить возможность входа, используя биометрию;

Рисунок 39 - Aladdin 2FA. Установка пароля

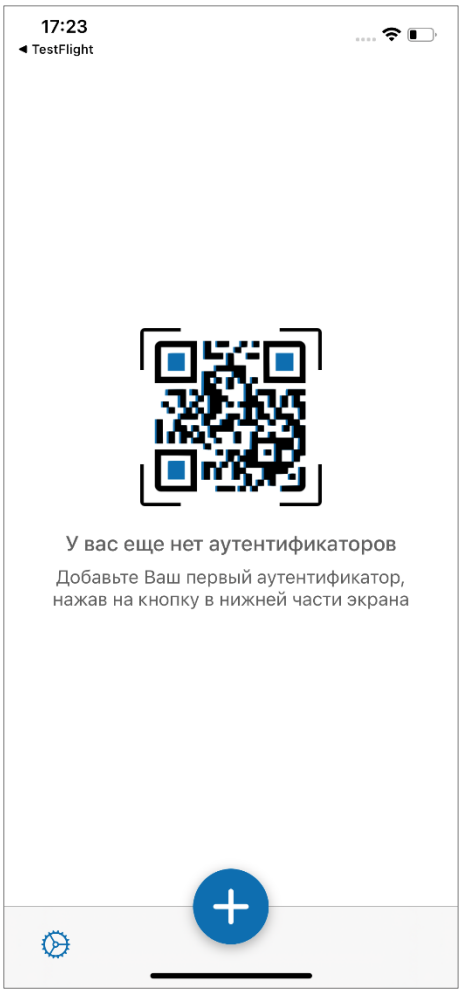

Рисунок 40 - Aladdin 2FA. Добавление аутентификатора

4. При первом входе в приложение на экране, приведенном выше (см. Рисунок 40), добавить аутентификатор с помощью кнопки  ;

> *В зависимости от настроек смартфона может понадобится предоставить разрешение для камеры*

5. На следующем экране (см. Рисунок 41) 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 41):
   1) – кнопка переключения между камерами устройства. Позволяет считать QR-код с помощью фронтальной камеры;
   2) – <Ввести код вручную> - подробнее про функцию добавления в п. 4.2;

Рисунок 41 - Aladdin 2FA. Сканирование QR-кода

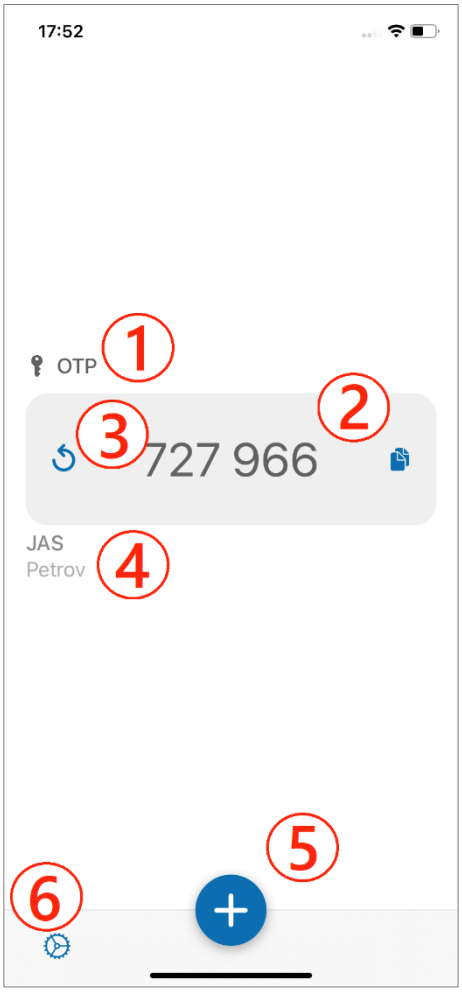

Рисунок 42 - Aladdin 2FA. Добавленный аккаунт

6. Будет добавлен аккаунт (см. Рисунок 42), 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  ;
   3) – элемент управления для обновления сгенерированного одноразового пароля;
   4) – учетные данные пользователя;
   5) – кнопка добавления аккаунта (см. п. 4.2);
   6) – переход к меню с настройками приложения (см. п. 4.6).

4.2 Добавление аутентификатора

На главном экране мобильного приложения отображается перечень всех добавленных аутентификаторов (см. Рисунок 44).

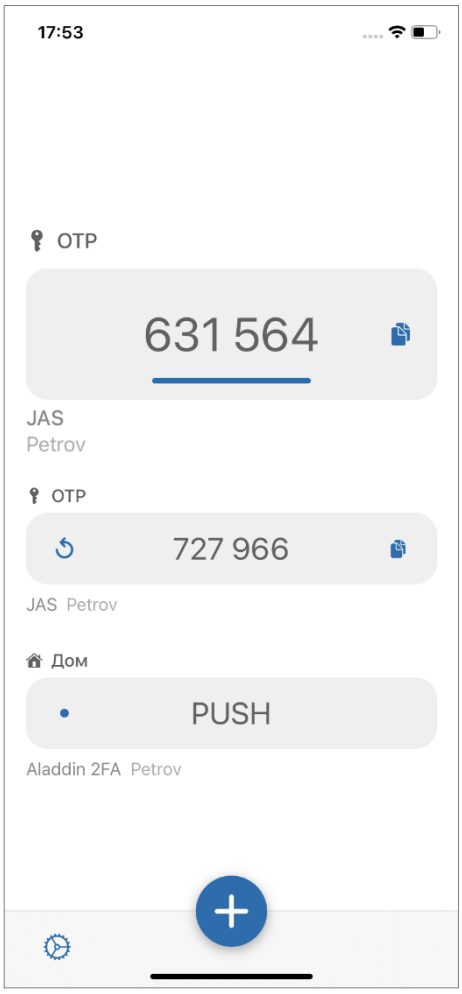

Рисунок 43 - Aladdin 2FA. Главный экран

1. Нажать кнопку  внизу главного экрана;
2. Будет открыта камера для сканирования QR-кода (см. Рисунок 41), 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 аккаунтов*

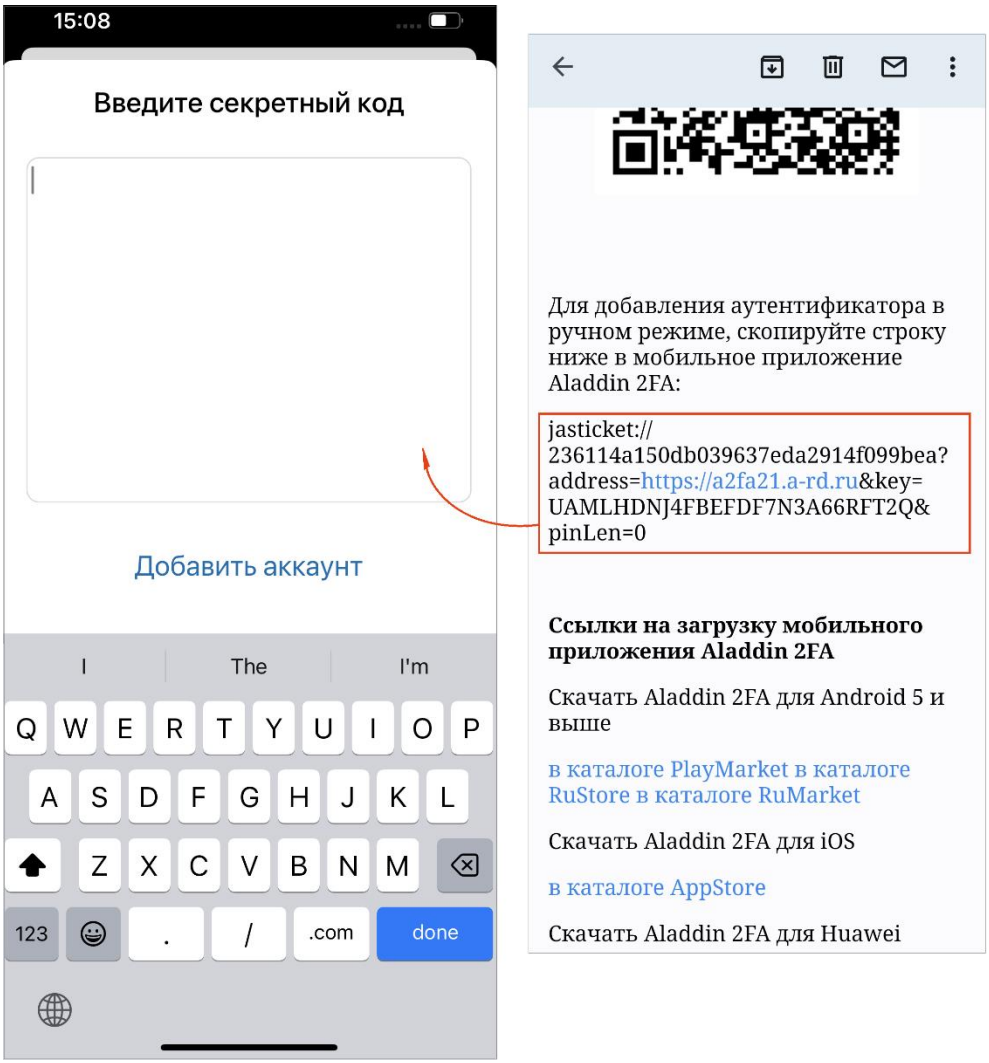

Рисунок 44 - Aladdin 2FA. Добавление аутентифкатора вручную

4.3 Редактирование аутентификатора

При долгом нажатии на выбранном аутентификаторе становится доступен режим редактирования (см. Рисунок 45): можно удалить аутентификатор, переименовать его или, если аутентификаторов два и больше, изменить его местоположение.

Подробнее про каждую процедуру описано ниже.

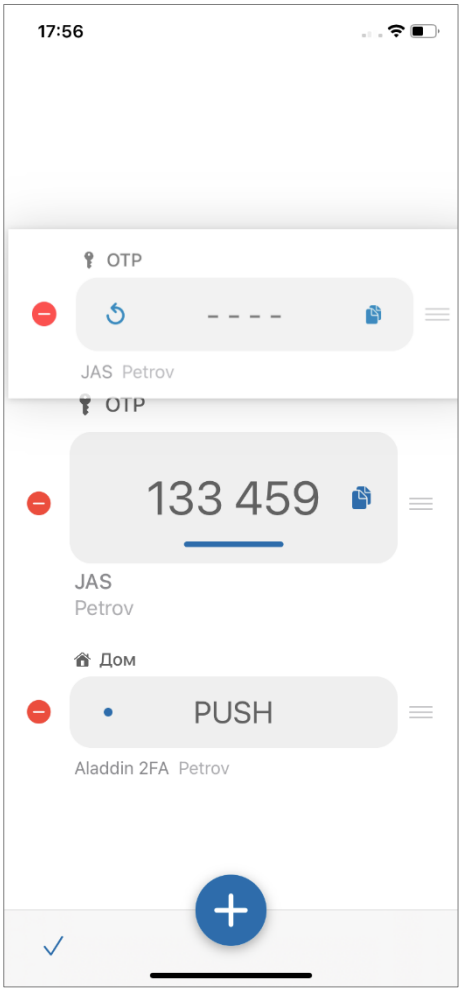

Рисунок 45 - Aladdin 2FA. Режим редактирования аутентификатора

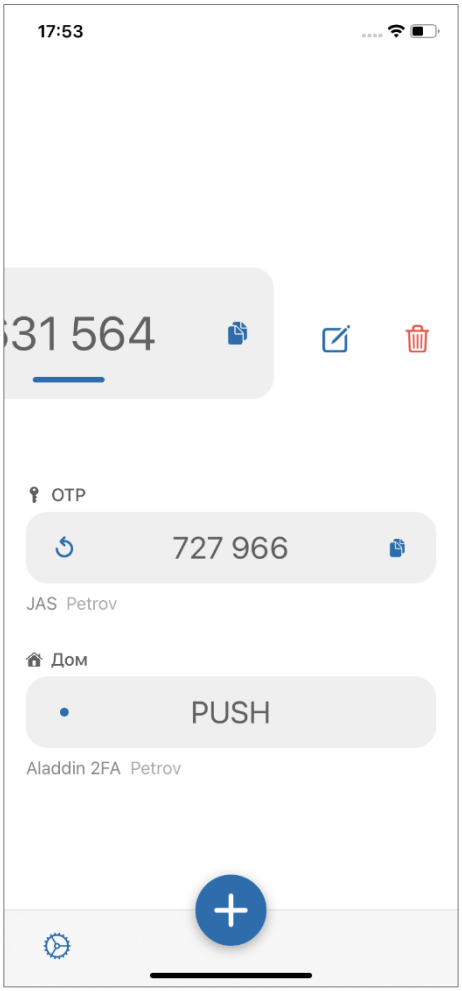

Рисунок 46 - Aladdin 2FA. Удаление аутентификатора

4.3.1 Удаление

Для удаления аутентификатора необходимо выполнить следующие действия:

1. Перейти в режим редактирования и нажать кнопку  (см. Рисунок 45). Также можно свайпнуть аутентификатор влево, тогда справа отобразиться кнопка  - <Удалить> (см. Рисунок 46);

1. Нажать на кнопку  или  . Появится информационное сообщение (пример сообщения приведен на Рисунок 21 для ОС Android);
2. Подтвердить удаление аутентификатора.

4.3.2 Переименование

1. Перейти в режим редактирования и нажать кнопку  ;
2. Будет открыто окно (см. Рисунок 47), в котором можно поменять название аутентификатора, заданное по умолчанию, на другое имя. Еще можно поменять иконку отображения аутентификатора;

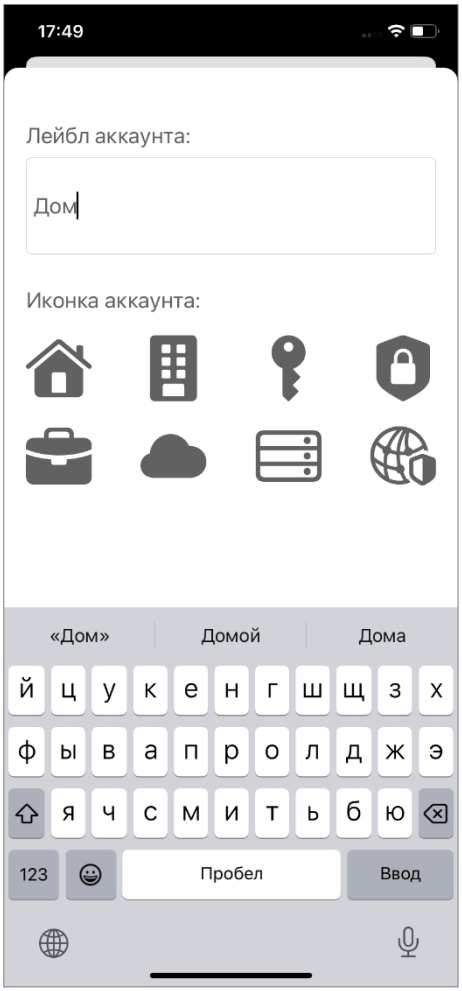

Рисунок 47 - Aladdin 2FA. Задание нового имени для аутентификатора

3. 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

4.4 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 48).

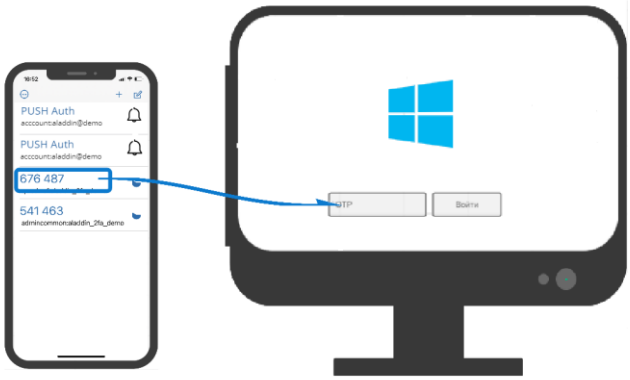

Рисунок 48 – Ввод сгенерированного одноразового кода в соответствующее поле

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 аутентифкатора, зарегистрированного с помощью PUSH-аутентификации, отображается идикатор 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 49);
2. Нажать на полученное уведомление. Будет осуществлен переход в приложение Aladdin 2FA;

Рисунок 49 - Aladdin 2FA. Уведомление с запросом на авторизацию

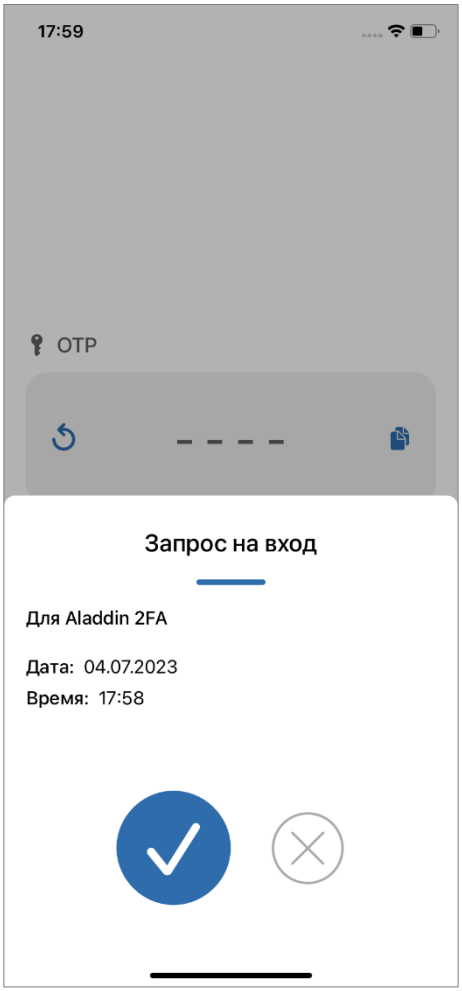

Рисунок 50 - Aladdin 2FA. Запрос на авторизацию в приложении

3. Ввести пароль или осуществить вход с помощью биометрии;
4. В приложении будет отображено окно [Запрос на вход] с информацией и кнопками  - <Принять> и  - <Отклонить> (см. Рисунок 50);
5. При нажатии на кнопку <Принять> авторизация будет подтверждена (см. Рисунок 51). Окно с подтверждением закроется автоматически;

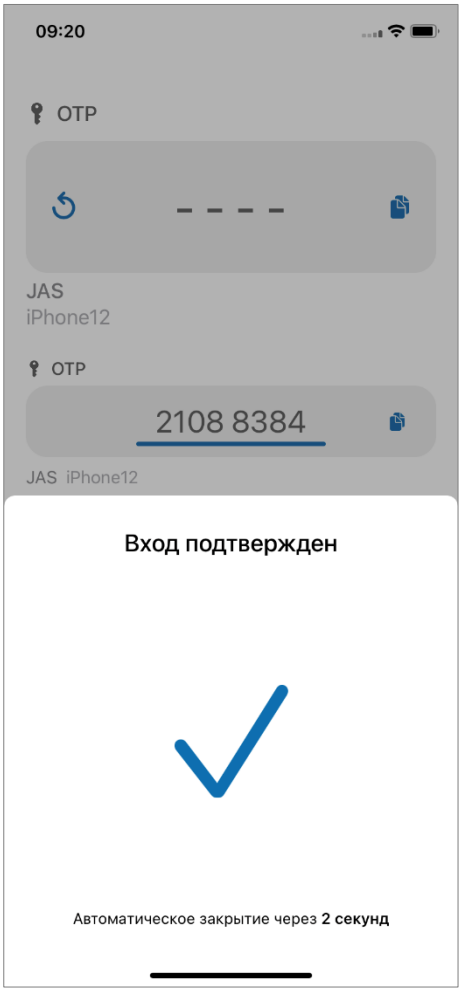

Рисунок 51 - Aladdin 2FA. Подтверждение входа

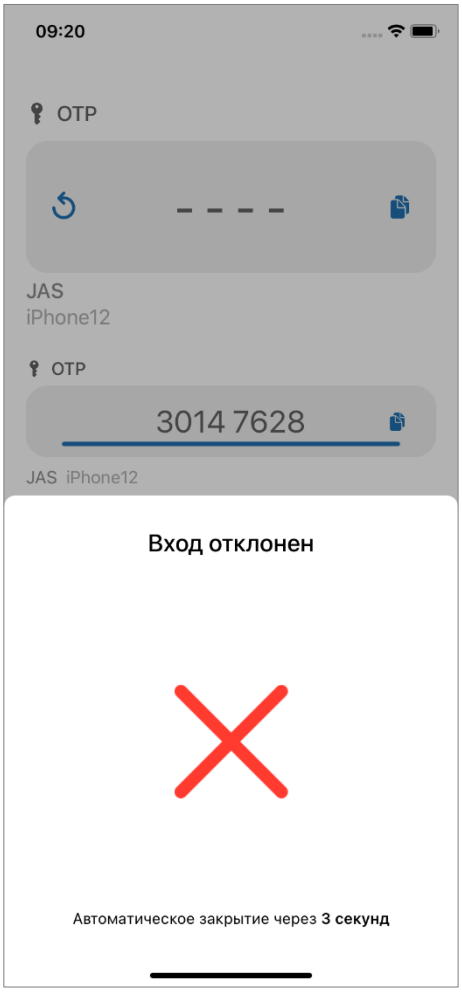

Рисунок 52 - Aladdin 2FA. Запрос на авторизацию отклонен

6. При нажатии на кнопку <Отклонить> авторизация будет отклонена (см. Рисунок 52). Окно [Вход отклонен] закроется автоматически.

4.5.2 PUSH-аутентификация в открытом приложении

Если был осуществлен вход в приложение Aladdin 2FA, то запрос на авторизацию появится автоматически (см. Рисунок 50). 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 53):

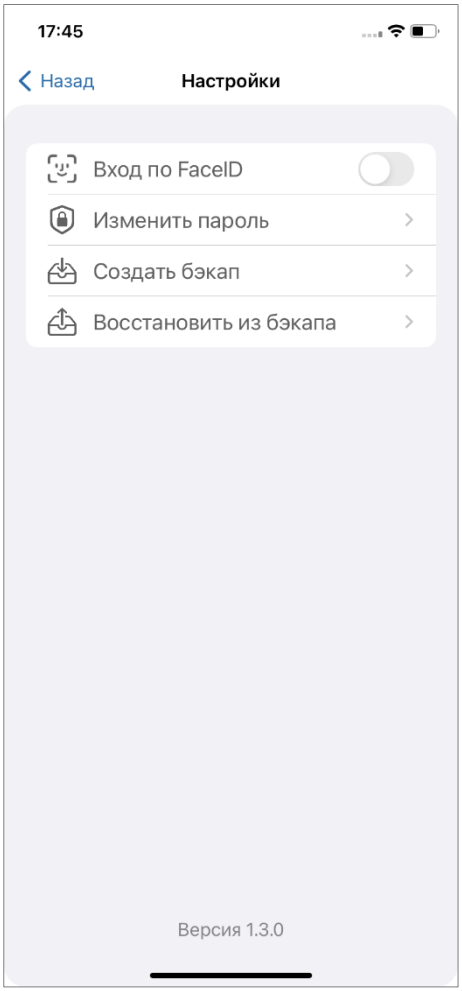

Рисунок 53 - Aladdin 2FA. Настройки приложения

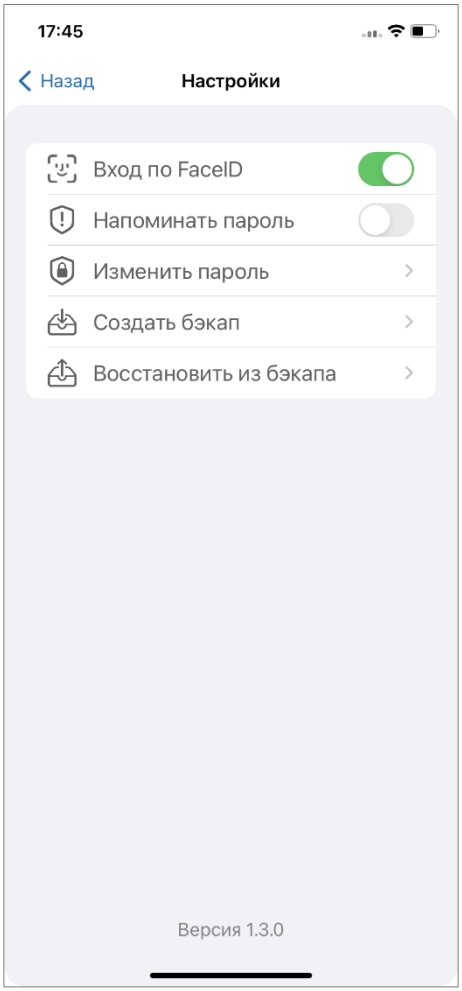

Рисунок 54 - Aladdin 2FA. Отключение регулярного ввода пароля

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

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 меню 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 54), которая по умолчанию включена. При выключении тумблера <Напоминать пароль> приложение перестает запрашивать ввод пароля раз в 72 часа. В таком случае ответственность за запоминание пароля остается за пользователем, так как восстановить его не получиться.

4.8 Создание бэкапа

> *Для безопасности данных рекомендуется производить процедуру создания бэкапа после каждого добавленного аутентификатора*

Для создания резервной копии необходимо:

1. Нажать кнопку <Создать бэкап>, ввести пароль для создания резервной копии (см. Рисунок 57);
2. На экране [Создать бэкап] приведена справочная информация о процессе создания резервной копии (см. Рисунок 58).

Рисунок 55 - Aladdin 2FA. Создание резервной копии

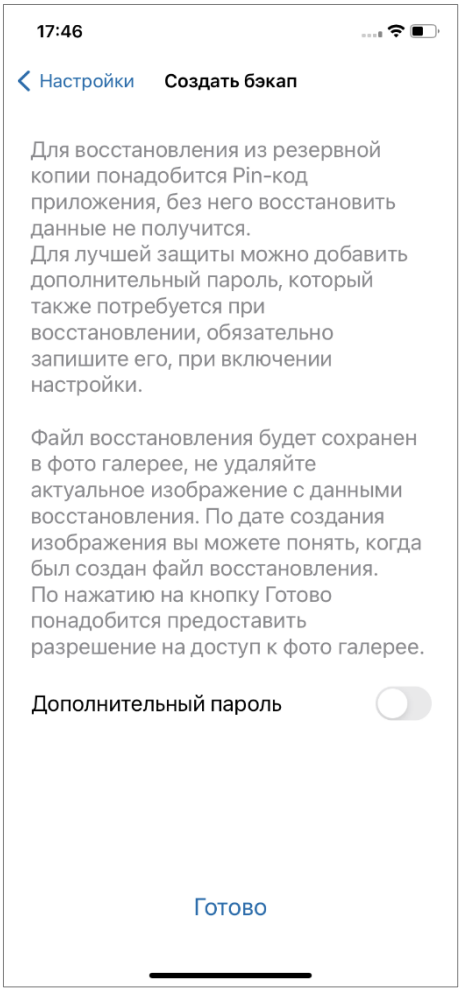

Рисунок 56 - Aladdin 2FA. Файл резервной копии в виде логотипа

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 57);

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 58). После нажатия на кнопку <Готово> будет создана резервная копия (см. Рисунок 59).

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

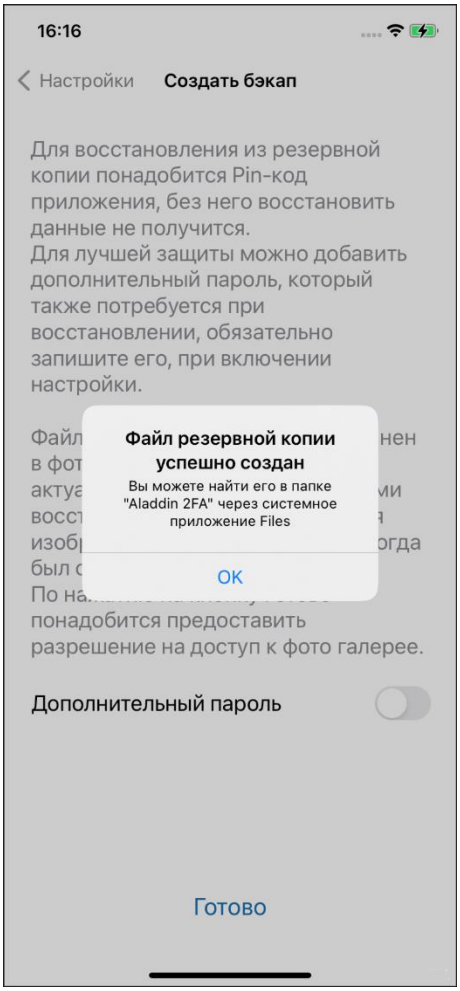

Рисунок 57 - Aladdin 2FA. Информационное сообщение о созданном бэкапе

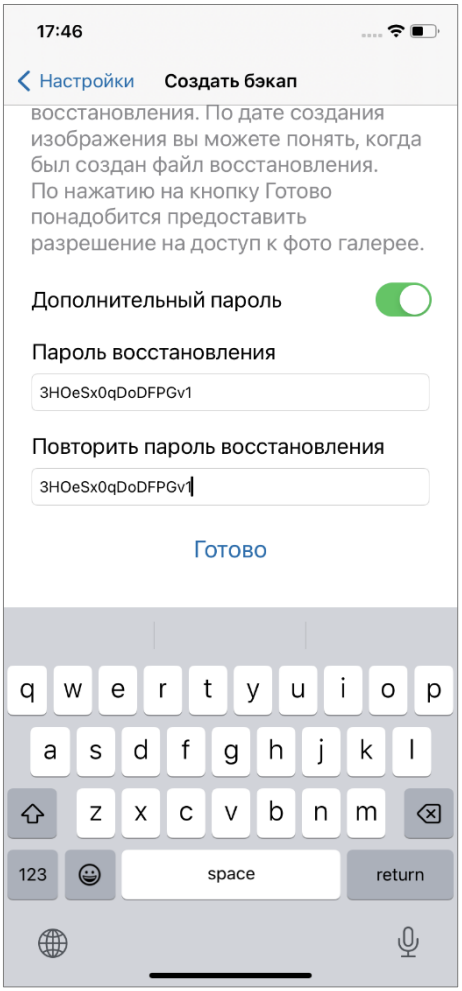

Рисунок 58 - Aladdin 2FA. Дополнительный пароль при создании резервной копии

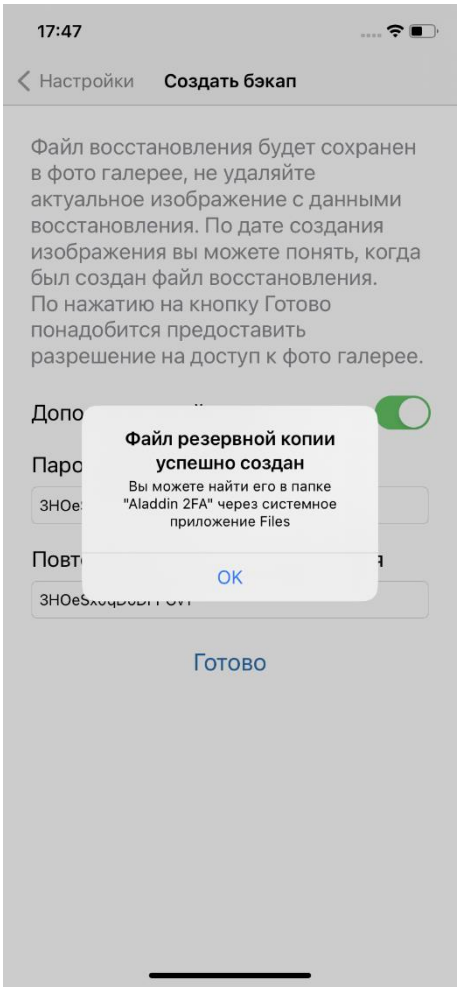

Рисунок 59 - Aladdin 2FA. Информационное сообщение о созданном бэкапе

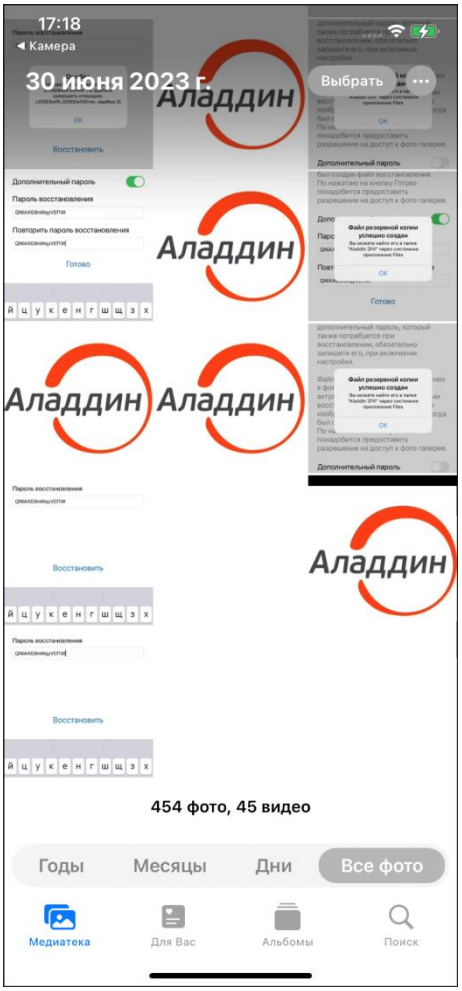

Рисунок 60 - Файл резервной копии в виде логотипа

Резервная копия хранится на устройстве в виде изображения с логотипом компании Аладдин Р.Д. в галерее устройства (см. Рисунок 60). 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 61). Необходимо нажать кнопку <Выбрать файл восстановления> и указать файл, содержащий бэкап (см. Рисунок 62).

Рисунок 61 - Aladdin 2FA. Восстановление из резервной копии

Рисунок 62 – Выбор изображения, представляющего собой бэкап

Если резервная копия создавалась с использованием дополнительного пароля, то появится поле [Пароль восстановления], в котором необходимо ввести 16-значный код, указанный при создании резервной копии (см. Рисунок 63). Нажать кнопку <Восстановить>.

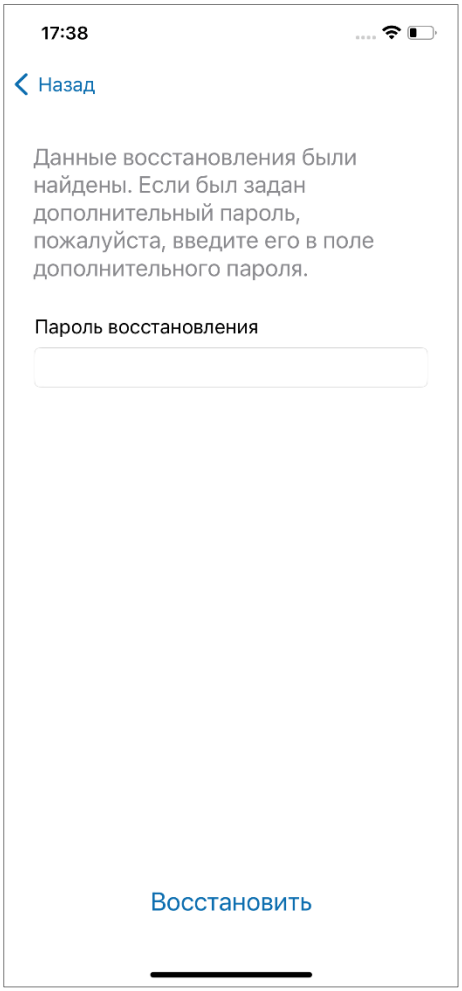

Рисунок 63 - Aladdin 2FA. Восстановление из резервной копии. Ввод дополнительного пароля

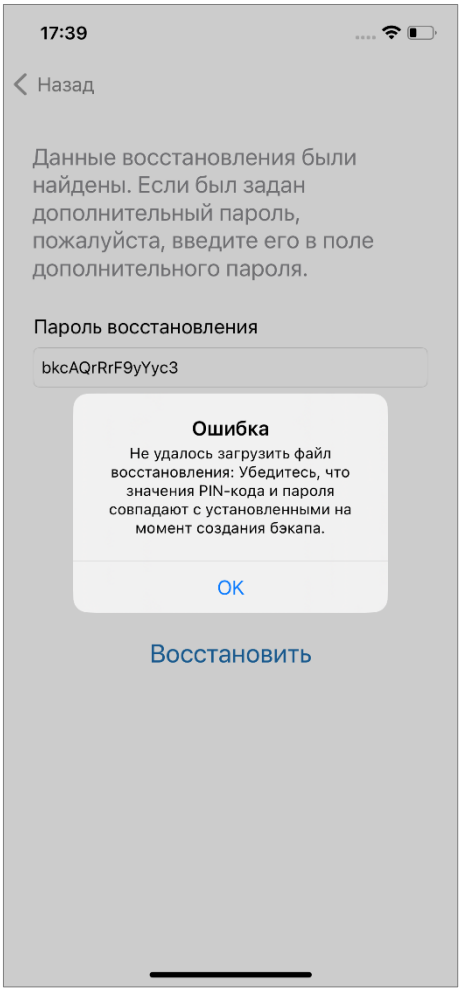

Рисунок 64 – Aladdin 2FA. Ошибка при восстановлении бэкапа

> *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 64).

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. На устройстве перейти в <Настройки>
2. <Установить сертификаты из памяти>, далее <Сертификат центра сертификации>
3. Будет открыт экран [Конфиденциальность ваших данных будет нарушена] с информационной информацией, нажать кнопку <Все равно установить> (см. Рисунок 66). Подтвердить действие PIN-кодом или предъявлением биометрии;

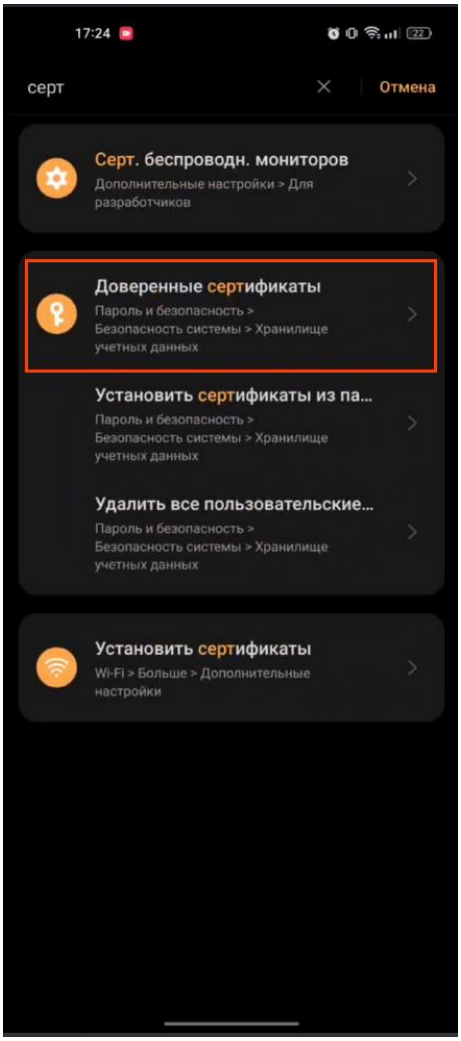

Рисунок 65 - Добавления сертификата в пользовательское хранилище. Доверенные сертификаты

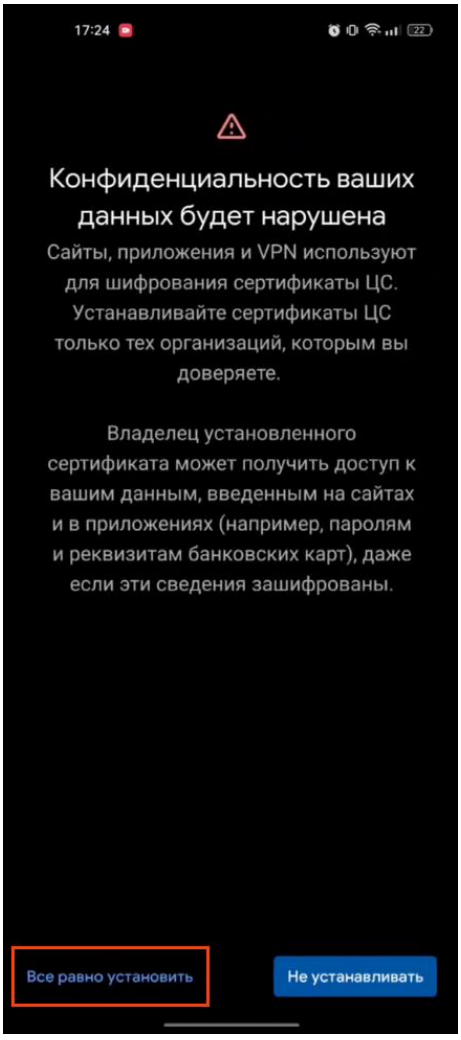

Рисунок 66 - Добавления сертификата в пользовательское хранилище. Экран с предупреждением о нарушении конфиденциальности

4. Появится всплывающее сообщение о том, что сертификат установлен (см. Рисунок 67);
5. Перейти в <Доверенные сертификаты> (см. Рисунок 67), выбрать вкладку [Пользователи], на ней будет отображаться добавленный сертификат (см. Рисунок 68);

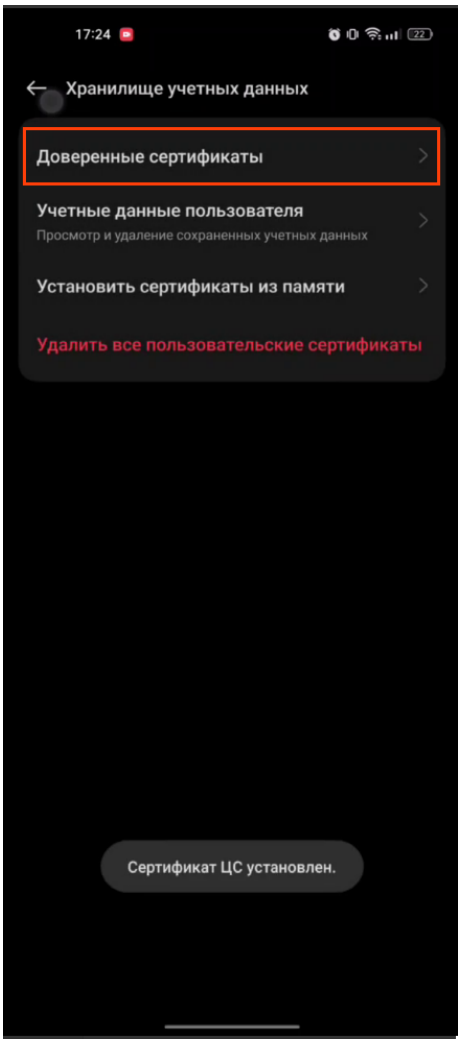

Рисунок 67 - Добавления сертификата в пользовательское хранилище. Всплывающее сообщение

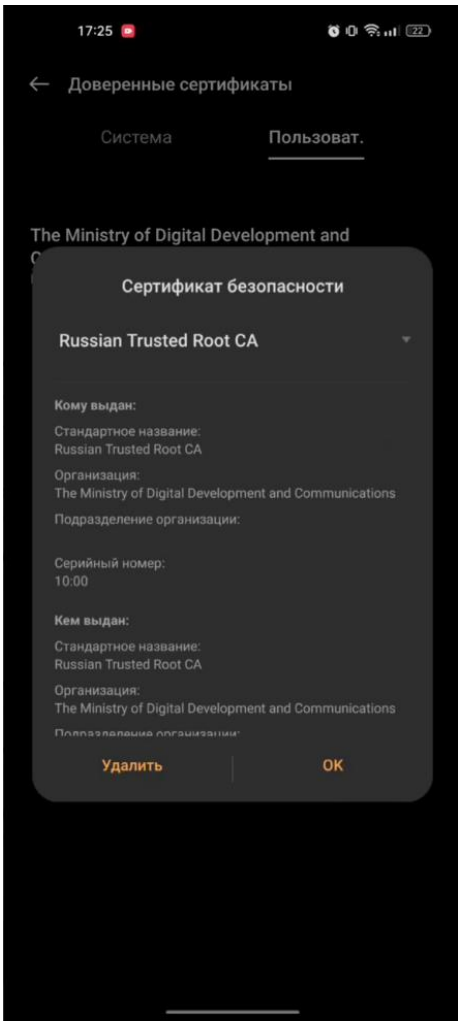

Рисунок 68 - Добавления сертификата в пользовательское хранилище. Добавленный сертификат

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 69);
2. Зайти в [Настройки], выбрать пункт <Основные>, далее <VPN и Управление устройством> в группе [Загруженный профиль] будет отображен сертификат (см. Рисунок 70);

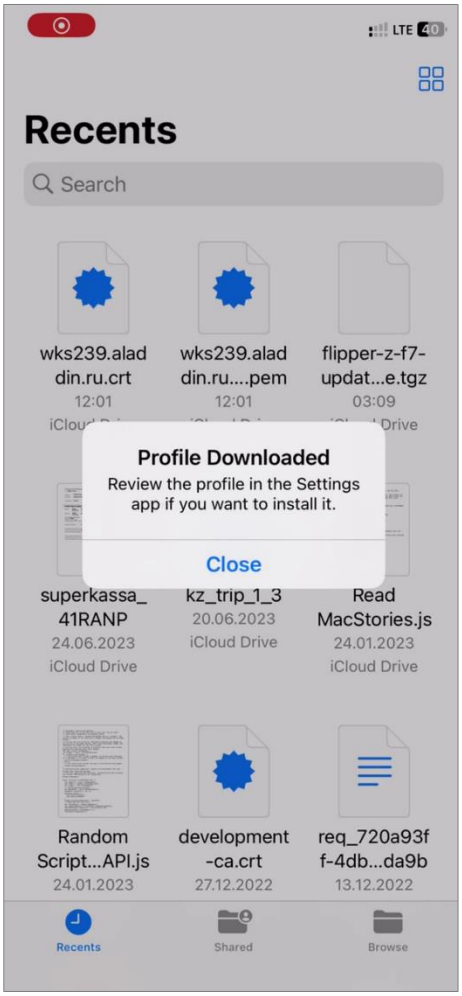

Рисунок 69 - Добавления сертификата в пользовательское хранилище. Загрузка профиля

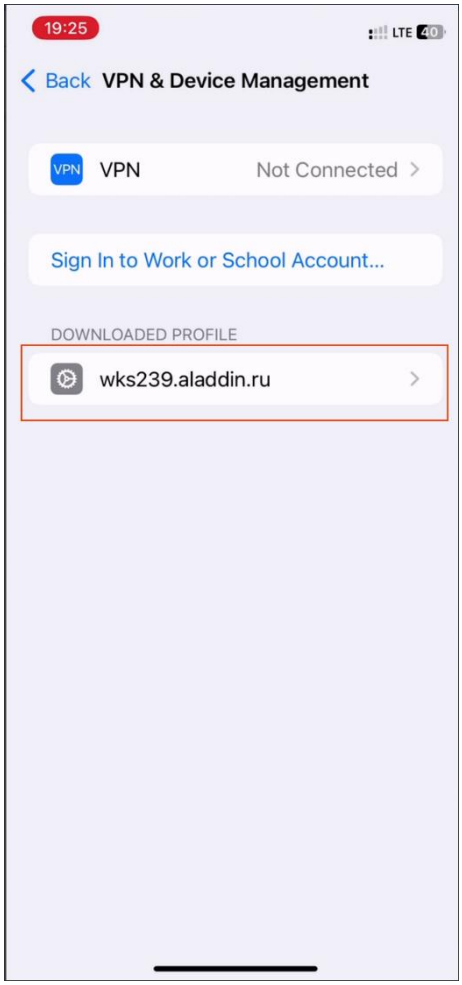

Рисунок 70 - Добавления сертификата в пользовательское хранилище. Загруженный сертификат

3. Подтвердить действие паролем от устройства;
4. Будет открыто окно [Предупреждение] (см. Рисунок 71). Нажать кнопку <Установить>;
5. Вернуться в [Настройки], <Основные>, <Профиль> - там будет отображаться загруженный сертификат (см. Рисунок 72);
6. Перейти в [Настройки], <Основные>, <Об этом устройстве>, <Доверие сертификатам> и активировать сертификат с помощью переключателя (см. Рисунок 73).

Рисунок 71 - Добавления сертификата в пользовательское хранилище. Установка сертификата

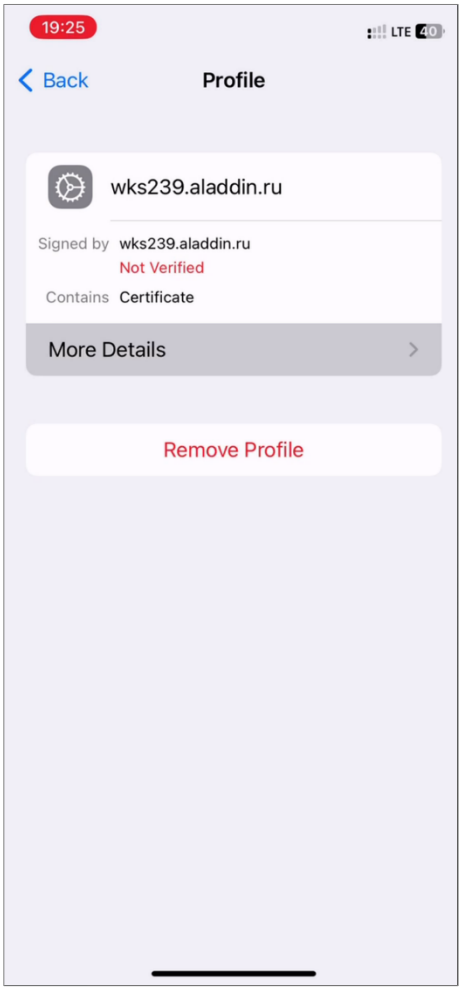

Рисунок 72 - Добавления сертификата в пользовательское хранилище. Загруженный сертификат в настройке [Профиль]

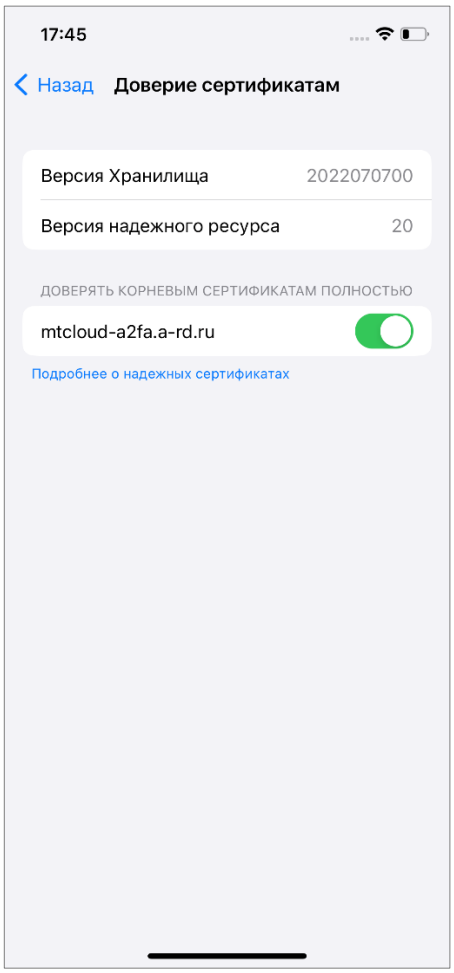

Рисунок 73 - Добавления сертификата в пользовательское хранилище. Активация загруженного сертификата

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

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