Aladdin 2FA Service. Руководство администратора для Windows

Настройка взаимодействия Aladdin 2FA Service и JMS

Версия продукта	1.3.5
Статус	Публичный
Дата	15.04.2026
Листов	62

Оглавление

1. О документе

1.1 Назначение документа

Настоящий документ представляет собой описание операций по установке и настройке серверного приложения Aladdin 2FA Service.

1.2 На кого ориентирован документ

Документ предназначен для администраторов, осуществляющих установку и настройку серверного приложения Aladdin 2FA Service.

1.3 Обозначения и сокращения

- Aladdin 2FA – мобильное приложение, представляющее собой генератор одноразовых паролей (OTP), используемых в качестве второго фактора аутентификации (2FA);
- Aladdin 2FA Service – серверное приложение, обрабатывающее запросы на выпуск OTP-токенов и генерацию одноразовых паролей;
- DMZ — сегмент сети, содержащий общедоступные сервисы (веб-сервис) и отделяющий их от частных (файловые серверы, рабочие станции). DMZ добавляет дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов;
- 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;
- MS SQL Server – СУБД для создания и работы с базами данных, необходимыми для работы приложений JAS, JMS и Aladdin 2FA Service;
- NGinx – веб-сервер и почтовый прокси-сервер, работающий под управлением операционных систем семейства Linux/Unix и Microsoft;
- NLB-кластер — это группа серверов, работающих вместе для обеспечения высокой доступности и масштабируемости приложений.
- OTP (One-Time Password) – одноразовый пароль, действительный только для одного сеанса аутентификации;
- PUSH-аутентификация – метод аутентификации с помощью push-уведомлений, используемый на мобильных устройствах;
- SQL Server Management Studio – программа для настройки и управления базами данных;
- Кластеризация – технология, объединения двух и более серверных узлов в логическую группу для обеспечения высокой доступности, работающих на них, сервисов.

2. Общие сведения

Aladdin 2FA Service – серверное приложение, предназначенное для автоматического выпуска программного аутентификатора и/или PUSH-токена и дальнейшего их использования с помощью мобильного приложения Aladdin 2FA во взаимодействии с системами JaCarta Management System (JMS) и JaCarta Authentication System (JAS).

Установка и настройка Aladdin 2FA Service осуществляется в два этапа. Для начала необходимо обеспечить наличие готовой инфраструктуры в виде заранее установленных серверов JMS и JAS в соответствии с документами «JaCarta Management System v.3.7. Руководство администратора. Часть 1. Установка и настройка» [2] и «JaCarta Management System v.3.7. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS)» [4].

> *Для стартовой конфигурации (для обеспечения работы самого сервиса Aladdin 2FA) достаточно установки только сервера JAS. Установка дополнительных компонентов JAS (JAS плагин для NPS, JAS-плагин для AD FS и др.) требуется для конкретных прикладных конфигураций, которые не рассматриваются в настоящем документе. Подробнее сложные конфигурации использования сервиса A2FA описаны в документе «JaCarta Authentication Server. Примеры интеграции с продуктами сторонних поставщиков».*

На втором этапе работы нужно установить и настроить программное обеспечение Aladdin 2FA Service. Для этого потребуются установка и настройка следующих компонентов: MS SQL Server, SQL Server Management Studio.

2.1 Назначение продукта

Aladdin 2FA – программная платформа, предназначенная для двухфакторной аутентификации, состоящая из мобильного приложения-аутентификатора Aladdin 2FA и серверного приложения Aladdin 2FA Service.

Основным инструментом для пользователя является мобильное приложение Aladdin 2FA, предназначенное для генерации одноразовых паролей, поддерживающее интерактивный способ входа - PUSH-аутентификацию. Подробное описание про установку и работу мобильного приложения Aladdin 2FA приведено в документе «Aladdin 2FA. Руководство пользователя» [1].

Серверное приложение Aladdin 2FA Service служит для связи мобильного приложение Aladdin 2FA и сервиса JAS. Подробно настройка Aladdin 2FA Service приведена в разделе 3. Установка.

2.2 Схема сетевого взаимодействия

Взаимодействие всех компонентов системы показано на рисунке (Рисунок 1): для обращения мобильного приложения Aladdin 2FA к серверу Aladdin 2FA Service необходим доступ извне. Рекомендуемым вариантом является доступ к Aladdin 2FA через любой прокси-сервер (в документе в качестве примера используется NGinx). Для корректной работы нужно обеспечить доступ до прокси-сервера из DMZ.

Опционально - Aladdin 2FA Service имеет режим работы без прокси-сервера.

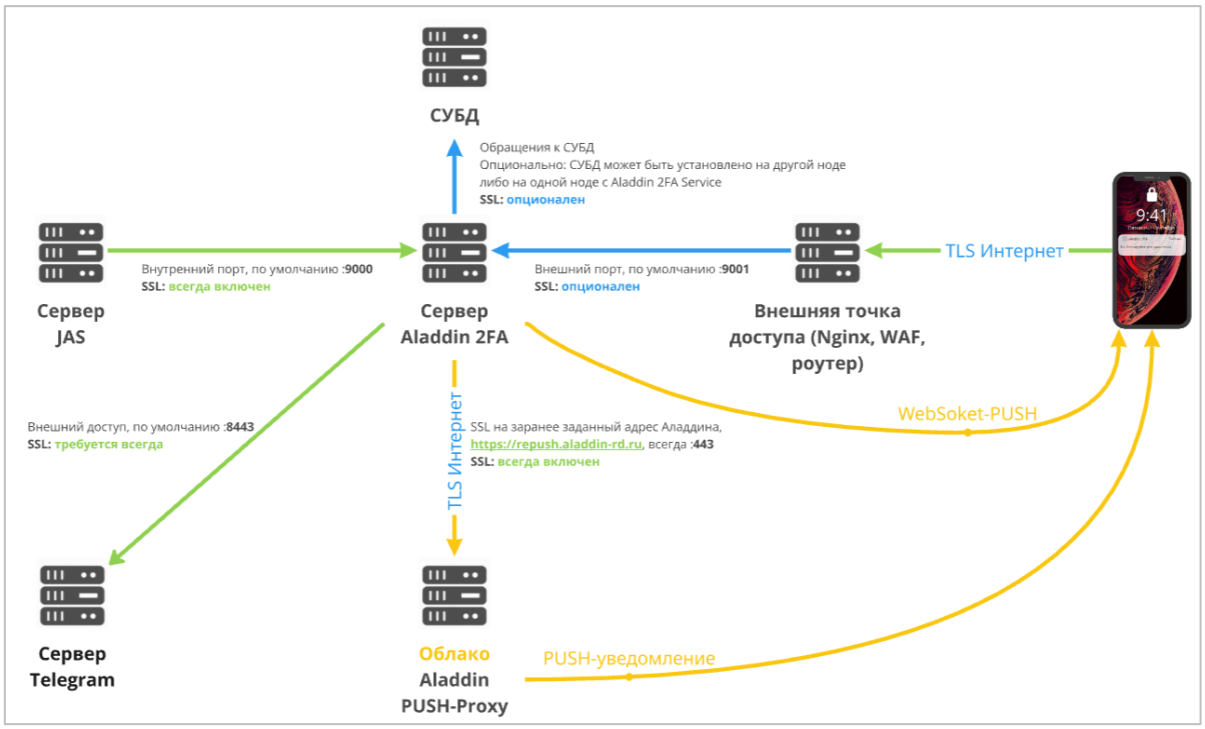

Рисунок 1 – Схема сетевого взаимодействия

2.3 Сценарии использования

Мобильное приложение Aladdin 2FA позволяет осуществлять двухфакторную аутентификацию посредством создания одноразового пароля, либо с помощью PUSH-аутентификации.

2.3.1 Генерация одноразового пароля

При выборе сценария работы с одноразовым паролем механизм аутентификации схематично будет выглядеть следующим образом (схема процесса приведена на ниже (см. Рисунок 2)):

1. Пользователь вводит в клиенте прикладной системы (например – в VPN-клиенте) личные данные и одноразовый пароль, сгенерированный в мобильном приложении Aladdin 2FA, для дальнейшей проверки на бэкенде прикладной системы;
2. Бэкенд прикладной системы отправляет запрос на сервер JAS с целью подтвердить проверку одноразового пароля;
3. На сервере JAS осуществляется проверка. Результат проверки отправляется обратно в бэкенд прикладной системы;
4. Бэкенд прикладной системы возвращает результат аутентификации в клиент целевой системы:

- В случае прохождения успешной проверки пользователь, используя аутентификационные данные своей учетной записи, получает доступ к ресурсу (личный кабинет, в VPN и т.д.);
- При отрицательном результате отображается сообщение об ошибке.

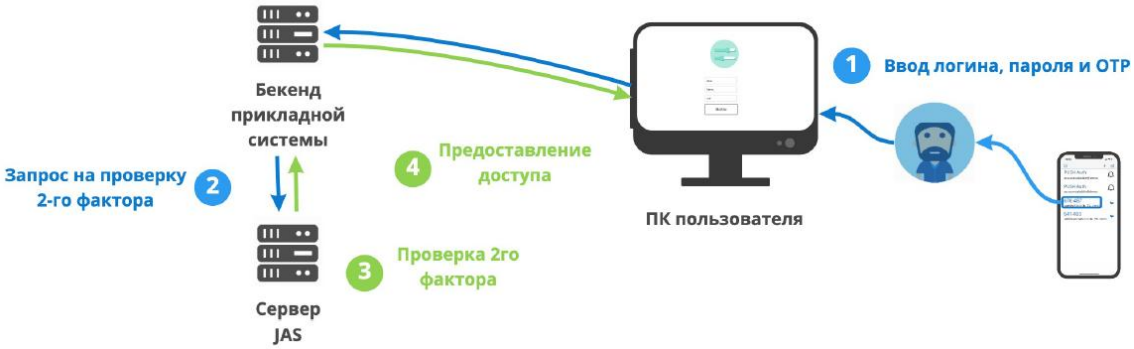

Рисунок 2 – Сценарий аутентификации с использованием одноразового пароля

2.3.2 PUSH–аутентификация

PUSH-аутентификация используется, если в приложении Aladdin 2FA пользователь имеет выпущенный по профилю JMS "Выпуск PUSH OTP-токенов" PUSH OTP-токен.

При попытке аутентификации в прикладной системе пользователь получает запрос на смартфон (PUSH-нотификацию). Для подтверждения входа в систему или отказа от него необходимо по PUSH-нотификации осуществить вход в мобильное приложение Aladdin 2FA, после чего подтвердить или отклонить вход.

При выборе сценария работы с PUSH-уведомлением механизм аутентификации схематично выглядит следующим образом (схема процесса приведена ниже, см. Рисунок 4):

1. В клиенте прикладной системы пользователь вводит личные данные для входа в учетную запись;
2. Сформированный запрос проходит цепочку серверов до сервера Aladdin 2FA, который отправляет запрос на сервер облачный сервер Aladdin PUSH-Proxy Proxy и параллельно по каналу WebSocket соединения, для доставки PUSH-уведомления на смартфон пользователя;
3. Пользователь получает PUSH-уведомление, нажав на которое входит в мобильное приложение, получая возможность принять/отклонить запрос на вход. С телефона пользователя запрос отправляется обратно на сервер Aladdin 2FA;
4. Сервер Aladdin 2FA инициирует проверку второго фактора в JAS;
5. В клиенте прикладной системы пользователь получит результат аутентификации:

- В случае успешной проверки пользователь получает доступ к ресурсу (личный кабинет, в VPN и т.д.);
- При отрицательном результате отображается сообщение об ошибке.

2.3.2.1 WebSocket соединение PUSH-нотификации

Между мобильным приложением и сервером Aladdin 2FA при регистрации первого аутентификатора устанавливается WebSocket соединение, позволяющее минимизировать риски задержек PUSH-уведомлений со стороны PUSH-провайдеров.
В момент формирования запроса на PUSH-уведомление, запрос параллельно отправляется через Aladdin PUSH-Proxy и WebSocket соединение. Отображение первого доставленного PUSH-уведомления и отсутствие дублирования одних и тех же PUSH-уведомлений, регулируется механизмами мобильного приложения. Стабильность WebSocket соединения и поддержание его в фоне, также управляется мобильным приложением.

> *Стабильность работы WebSocket соединения на ОС iOS в фоне ограничена, в связи с архитектурными особенностями этой ОС.*

2.3.2.2 Настройка прокси для использования WebSocket канала PUSH-нотификаций.

При использовании прокси-серера (например Nginx) для использования WebSocket соединения необходимо дополнительно настроить директиву (location) для проксирования пути WebSocket, перед основной директивой (location) для проксирования пути publicServer.

Пример, проксирование настроено с использованием пути /a2fa_public:

```
 server {
      listen       80;
      server_name  localhost;

      # проксирование на publicServer
      location /a2fa_public {
         proxy_pass http://localhost:9001/;
         proxy_set_header Host $host;
      }
 }
```

Добавление проксирования для WebSocket канала:

```
server {
      listen       80;
      server_name  localhost;

         # Добавляется проксирование на ws - добавляется перед основным
      location ^~ /a2fa_public/ws {
         proxy_pass http://localhost:9001/ws;
         proxy_set_header Host $host;

         # WS
         proxy_http_version 1.1;
         proxy_set_header Upgrade $http_upgrade;
         proxy_set_header Connection "Upgrade";
```

```
           # proxy_read_timeout должен быть в 3 раза больше интервала пинга WS - в
конфиге A2FA параметр publicServer.wsPingInterval (по умолчанию 10 минут)

           proxy_read_timeout 30m; # увеличение proxy_read_timeout до 30 минут

        }



        # проксирование на publicServer

        location /a2fa_public {

           proxy_pass http://localhost:9001/;

           proxy_set_header Host $host;

        }

    }
```

2.3.3 Телеграм-аутентификатор

При выборе сценария работы с телеграм-ботом механизм аутентификации схематично будет выглядеть следующим образом (схема процесса приведена ниже (см. Рисунок 3)):

1. Сервер JAS посылает запрос на создание задачи на регистрацию OTP-аутентификатора, посредством метода /createTGTicket.
2. В ответ Aladdin 2FA Service присылает гиперссылку на телеграм-бот;
3. Сервер JAS пересылает его пользователю;
4. Пользователь сканирует QR-код и переходит в телеграм-бот;
5. Пользователь нажимает кнопку «Старт», связывая свой телеграм профиль с профилем бота;
6. По нажатию кнопки в канале телеграм-бота, TG-бот через сервера TG, отправляет запрос на регистрацию OTP-аутентификатора
7. Aladdin 2FA Service связывает профиль TG с tokenUID. Отправляет ответ телеграмм с каким серийным номером аутентификатора профиль был связан. Через настроенный паблик порт.
8. Профиль телеграм-бота показывает его tokenUID для пользователя;
9. Сервер JAS пересылает в телеграм-бот пользователя значение OTP;
10. Пользователь получает значение OTP в свой телеграм-клиент.

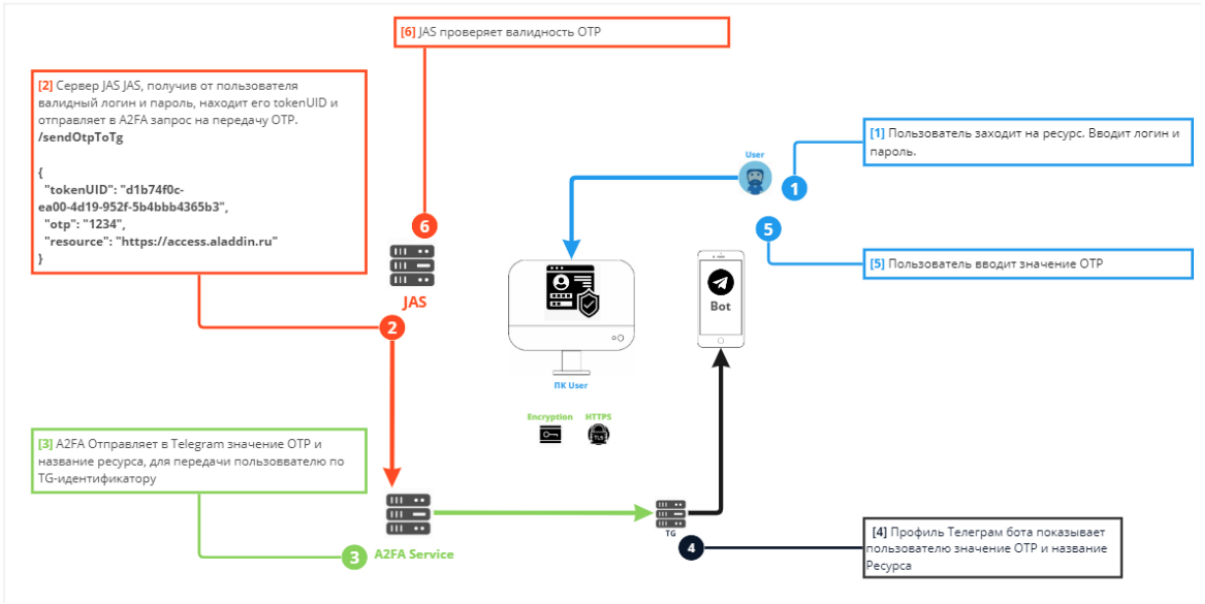

Рисунок 3 - Сценарий аутентификации с использованием телеграм-бота

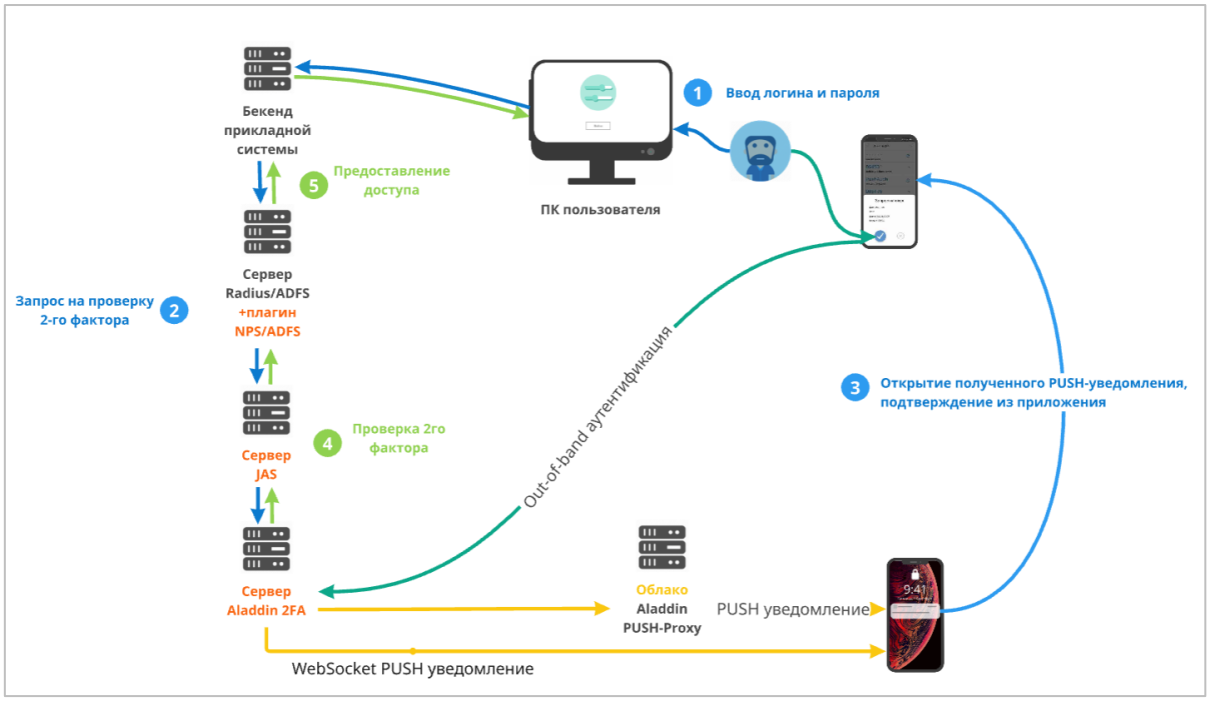

Рисунок 4 - Сценарий аутентификации с использованием PUSH-уведомления

2.4 Системные требования

Приложение Aladdin 2FA Service может быть установлено как одной машине с JAS, так и на отдельной машине.

Системные требования, необходимые для установки на отдельную машину, приведены ниже (см. Таблица 1).

Таблица 1 – Требования к среде функционирования

Параметр	Значение
Операционная система	• Microsoft Windows Server 2016; • Microsoft Windows Server 2019
Сервер СУБД	• Microsoft SQL Server 2016; • Microsoft SQL Server 2017; • Microsoft SQL Server 2019; • Microsoft SQL Server 2022
Дополнительное ПО	Microsoft .NET Framework 4.5 (или 4.6.2, 4.7, 4.8)
Процессор	4 ядра, частота от 3 ГГц
Оперативная память (не менее)	4 ГБ
Свободное место на жестком диске	Не менее 25 ГБ
Сетевой адаптер	100 Мб/с

2.5 Описание пакетов установки

Дистрибутив Aladdin 2FA Service включает следующие пакеты установки и обновления (см. Таблица 2):

Таблица 2 - Дистрибутив Aladdin 2FA Service

Файл	Описание
`Aladdin.2FA.Service-x.x.x.xx-x64.ru.msi`	Компонент для 64-битных систем, устанавливается на компьютер пользователя
`[Cert]`	Папка с самоподписанным сертификатом для быстрой настройки в качестве демонстрационных сертификатов. Содержит контейнер с расширением ".pfx"
`Aladdin 2FA Service. Руководство администратора под Windows.pdf`	Настоящее руководство администратора по настройке Aladdin 2FA Service
`Aladdin 2FA. Руководство пользователя.pdf`	Руководство пользователя по установке и работе с мобильным приложением Aladdin 2FA

Установка и настройка JMS Server и JAS Server осуществляется согласно следующей документации:

- «JaCarta Management System v3.7. Руководство администратора. Часть 1. Установка и настройка» [2];
- «JaCarta Management System v3.7. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS)» [4].

3. Установка

Перед установкой Aladdin 2FA Server необходимо убедиться в наличии заранее подготовленной инфраструктуры, в виде развернутых в сети серверов JMS, JAS, а также сервер СУБД.

Для доставки PUSH-уведомлений Aladdin 2FA Server использует облачный сервис доставки PUSH-уведомлений, доступный по адресу `repush.aladdin-rd.ru`. В ходе подготовки инфраструктуры необходимо проверить его доступность.

Так же для Aladdin 2FA Server необходимо настроить внешний доступ от мобильных приложений к серверу из интернета (см. Рисунок 1).

3.1 Настройка внешнего доступа

Во всех вариантах, рассмотренных в этом разделе, Aladdin 2FA Server разворачивается в сегменте сети DMZ.

> *Все имена домена (кроме `repush.aladdin-rd.ru`) из настоящего раздела являются демонстрационными и не предназначены для использования в реальной инфраструктуре*

3.1.1 С помощью Reverse-proxy

Вариант настройки через Reverse-proxy является приоритетным, так как лучше соответствует требованиям безопасности.

На рисунке (см. Рисунок 5) приведен пример типовой инфраструктуры для развертывания сервиса Aladdin 2FA Server.

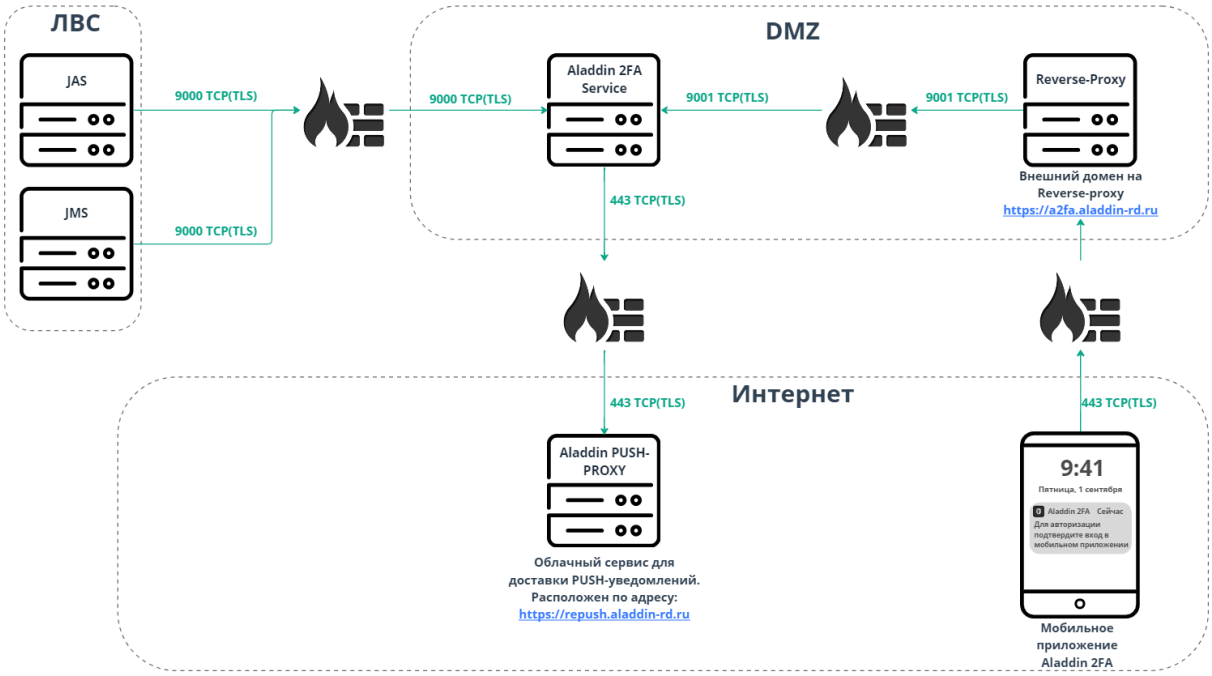

Рисунок 5 - Типовая инфраструктура с использованием Reverse-proxy

> *При обращении к серверу мобильные приложения осуществляют проверку доверия к сертификату TLS. Сертификат должен быть выдан общеизвестным УЦ, например, НУЦ минцифры или Let's Encrypt*

Для отправки PUSH-уведомлений сервису Aladdin 2FA Server необходим доступ к облачному сервису доставки PUSH-уведомлений, который находится по адресу `https://repush.aladdin-rd.ru`.

Подробная настройка сервиса Aladdin 2FA Server описана в подразделе 3.4 Установка Aladdin 2FA Service.

3.1.2 Проброс порта 9001 через опубликованный адрес для доступа из Интернета

На Рисунок 6 приведен пример типовой инфраструктуры для сервиса Aladdin 2FA без Reverse-Proxy. Это можно реализовать с помощью доступных технических средств, например, NAT на маршрутизаторе с access-листами или межсетевом экране, WAF.

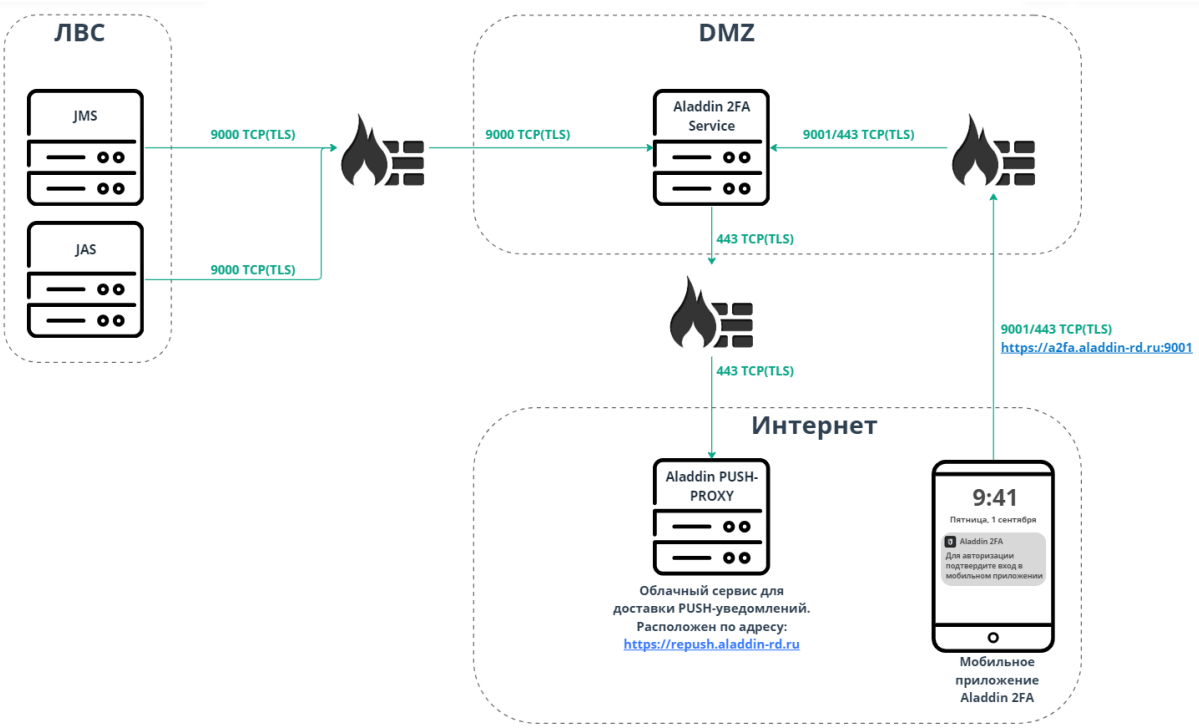

Рисунок 6 - Типовая инфраструктура с пробросом порта 9001 через опубликованный адрес для доступа из Интернета

> *При обращении к серверу мобильные приложения осуществляют проверку доверия к сертификату TLS. Сертификат должен быть выдан общеизвестным УЦ, например, НУЦ минцифры или Let's Encrypt*

Для отправки PUSH-уведомлений сервису Aladdin 2FA необходим доступ к облачному сервису доставки PUSH-уведомлений, который находится по адресу `https://repush.aladdin-rd.ru`.

Подробная настройка сервиса Aladdin 2FA Server описана в подразделе 3.4 Установка Aladdin 2FA Service.

3.1.3 С использованием NLB-кластера

Самые распространенные подходы для обеспечения отказоустойчивости Aladdin 2FA Service:

1. Active/Passive-кластер (например, Microsoft Failover Cluster). Подробная настройка Microsoft Failover Cluster описана в разделе 7;
2. Active/Active-кластер (например, NGINX в режиме реверс-прокси с NLB). Подробная информация о данной настройке предоставляется по запросу во время пилотного проекта.

Пример типовой схемы с использованием NLB-кластера приведен на рисунке (см. Рисунок 7).

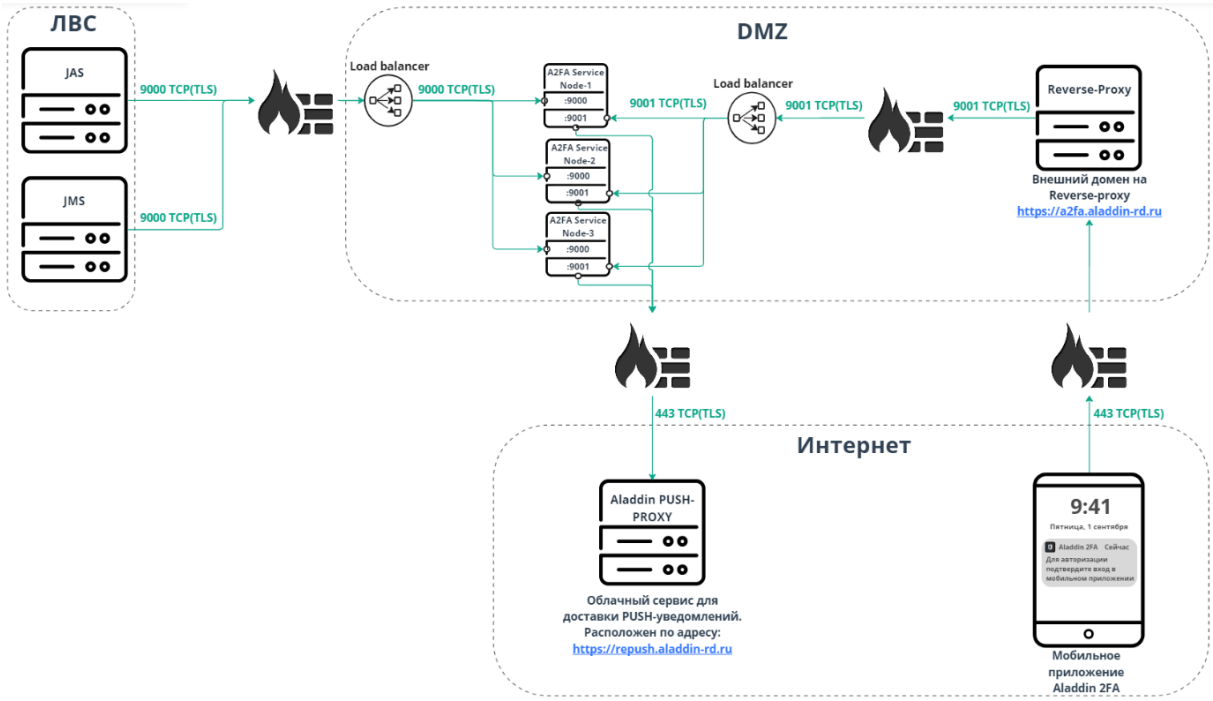

Рисунок 7 - Типовая инфраструктура с использованием NLB-кластера

> *При обращении к серверу мобильные приложения осуществляют проверку доверия к сертификату TLS. Сертификат должен быть выдан общеизвестным УЦ, например, НУЦ минцифры или Let's Encrypt*

Для отправки PUSH-уведомлений сервису Aladdin 2FA необходим доступ к облачному сервису доставки PUSH-уведомлений, который находится по адресу `https://repush.aladdin-rd.ru`.

Подробная настройка сервиса Aladdin 2FA Server описана в подразделе 3.4 Установка Aladdin 2FA Service.

3.2 Предварительная настройка СУБД

Для корректного запуска Aladdin 2FA Service необходимо предварительно сконфигурировать сервер СУБД. В настоящем руководстве будет рассмотрен вариант настройки MS SQL Server.

Сервер СУБД должен быть настроен следующим образом:

- Включен смешанный режим аутентификации;
- В протоколах СУБД должен быть включен протокол TCP/IP;
- Должен быть включен обозреватель MS SQL Server;
- Настроить необходимые правила для брандмауера.

Ниже приведен типовой вариант настройки MS SQL Server для работы с сервисом Aladdin 2FA.

3.2.1 Настройка смешанного режима аутентификации на сервере СУБД

Сервис Aladdin 2FA Service использует отдельную учетную запись для доступа к своей базе данных. Для ее работы необходим смешанный режим аутентификации на сервере MS SQL. Включить его можно при установке Сервера СУБД (см. Рисунок 8), либо при помощи SQL Server Management Studio (см. Рисунок 9).

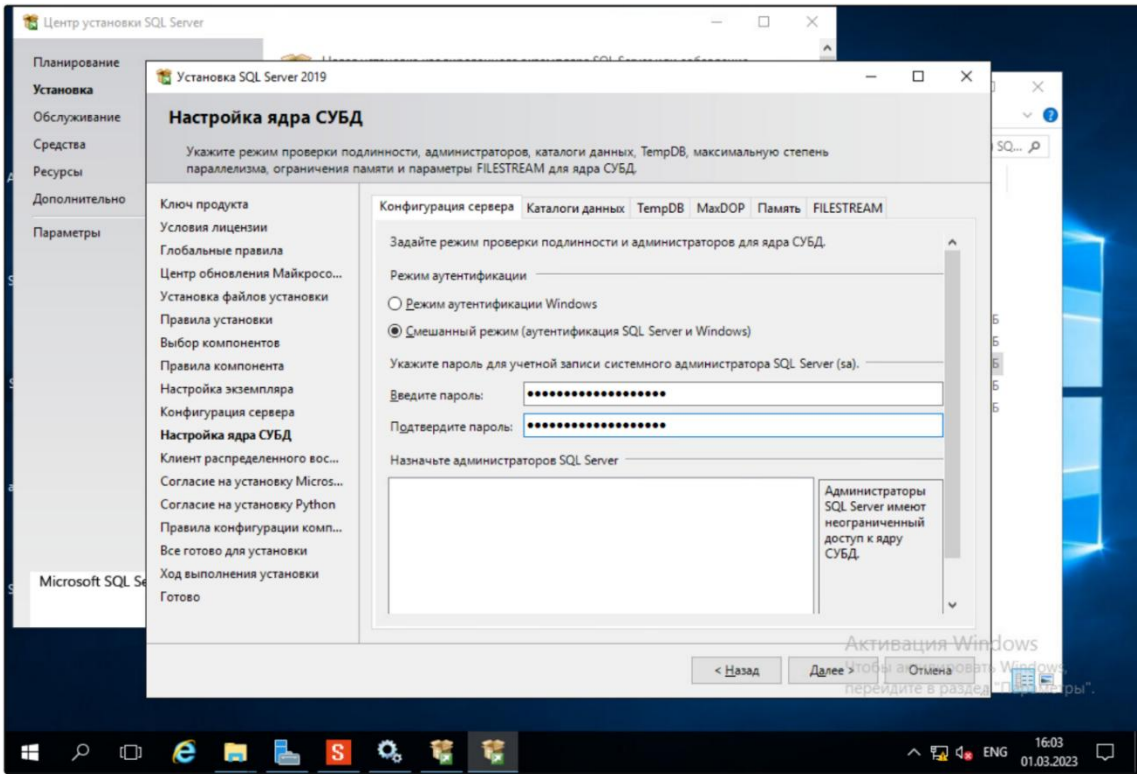

Рисунок 8 - Включение смешанного режима аутентификации при установке сервера СУБД

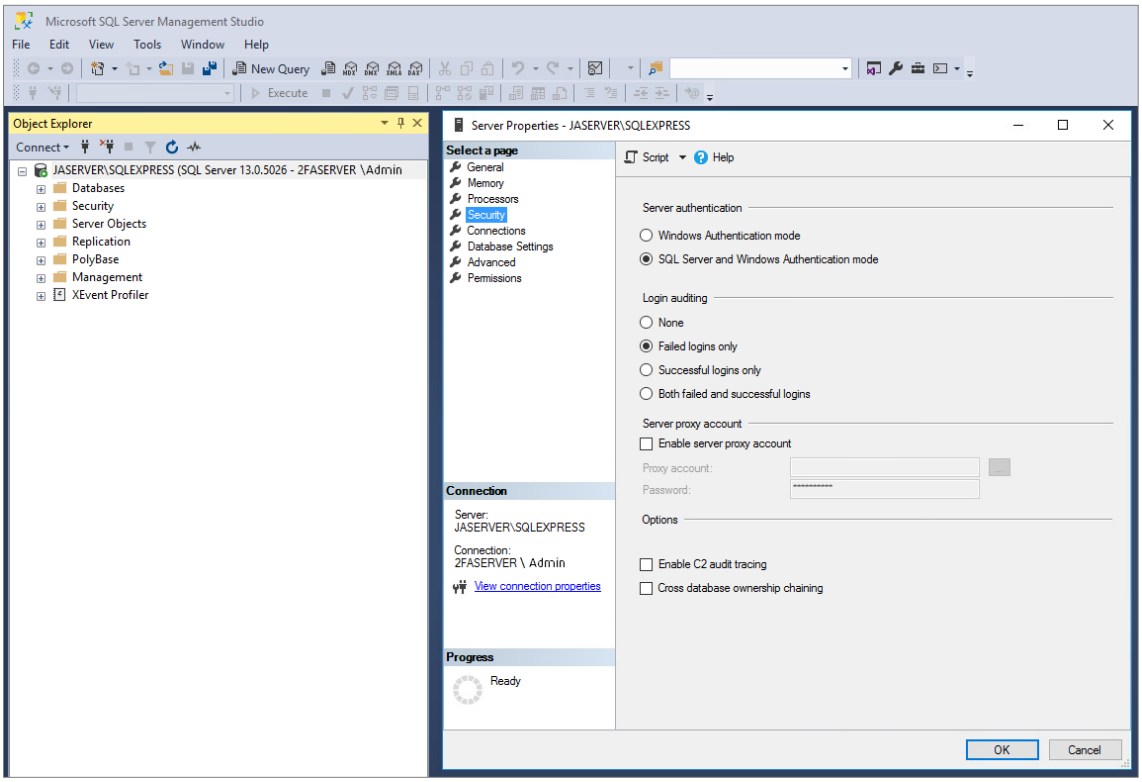

Рисунок 9 - Включение смешанного режима аутентификации в SQL Server Management Studio

> *Смешанный тип аутентификации предназначен для одновременного использования проверки подлинности Windows (встроенной Windows-аутентификации) и SQL-аутентификации (аутентификации с использованием учётных записей SQL-сервера)*

3.2.2 Включение протокола TCP/IP в SQL Server Configuration Manager

Сервис Aladdin 2FA Service для подключения к серверу СУБД использует протокол TCP/IP. Для того, чтобы его включить необходимо:

1. Открыть диспетчер конфигураций [SQL Server Configuration Manager] и раскрыть ветку <Сетевая конфигурация SQL Server>;
2. Для нужного экземпляра сервера – Instance - включить протокол TCP/IP (см. Рисунок 10, Рисунок 11).

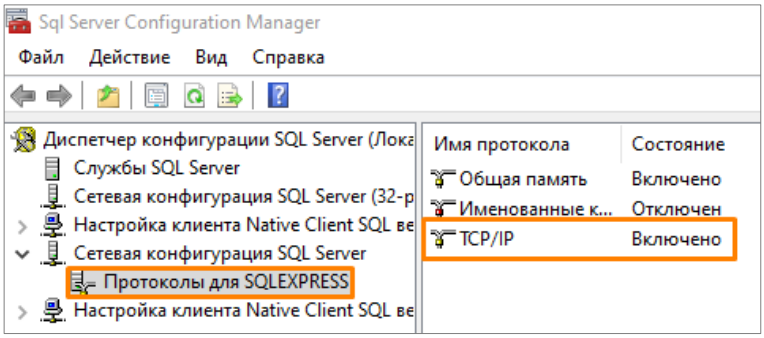

Рисунок 10 - Открыть свойства протокола TCP/IP

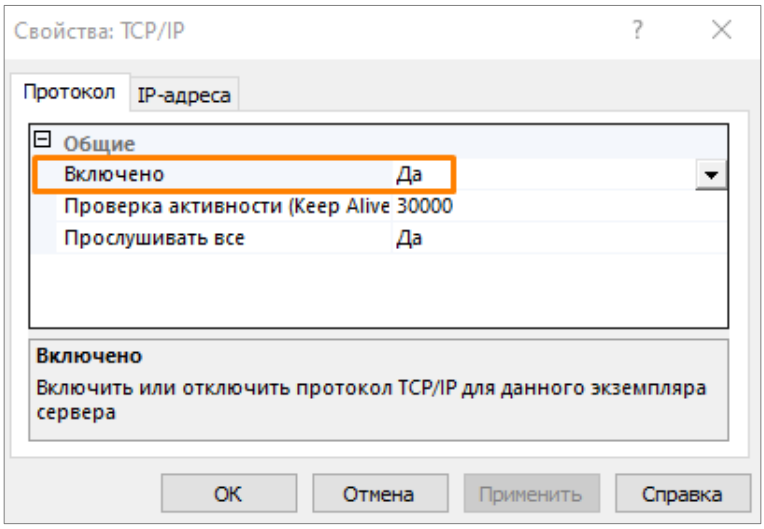

Рисунок 11 - Включить протокол TCP/IP

3.2.3 Включение обозревателя MS SQL Server

Для подключения к базе данных с внешнего компьютера необходимо включить службу [Обозреватель SQL Server].

Для подключения службы выполните следующие шаги:

1. В меню [Пуск] выбрать [Microsoft SQL Server] и открыть [Диспетчер конфигураций SQL Server];
2. В дереве [Диспетчер Конфигурации SQL Server] выбрать [Службы SQL Server]. В центральной части консоли в перечне выбрать службу [Обозреватель SQL Server] (см. Рисунок 12). Состояние этой службы должно быть <Работает>. Если это не так, перейти к следующему шагу;

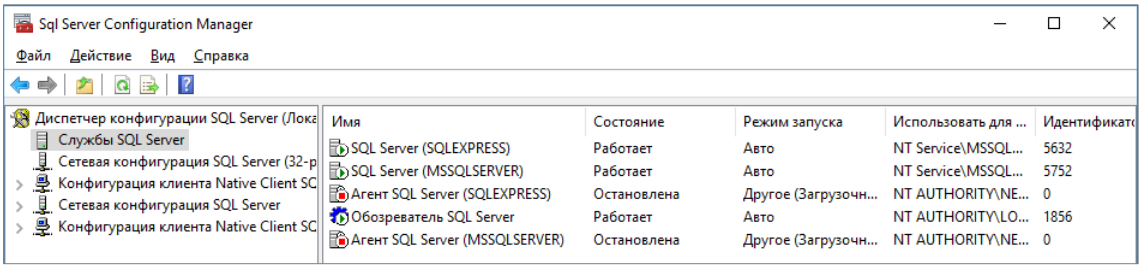

Рисунок 12 - Проверка работы обозревателя MS SQL

3. Открыть окно [Свойства] для службы [Обозреватель SQL Server] с помощью двойного нажатия левой кнопкой мыши по ней. На вкладке [Служба] для настройки [Режим запуска] задать значение <Авто> с помощью выпадающего списка (см. Рисунок 13);

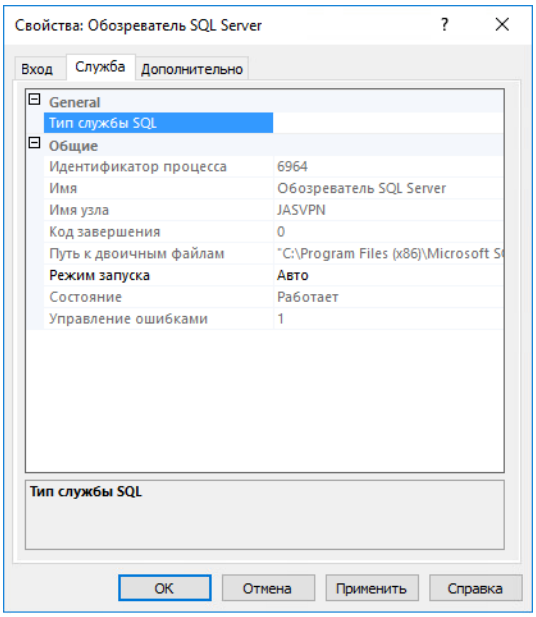

Рисунок 13 - SQL Server Configuration Management. Окно [Свойства Обозреватель SQL Server]. Вкладка [Служба]

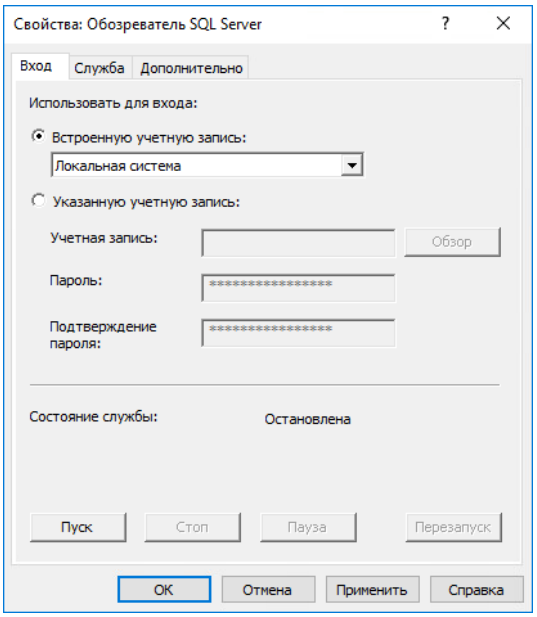

Рисунок 14 - SQL Server Configuration Management. Окно [Свойства Обозреватель SQL Server]. Вкладка [Вход]

4. Перейти на вкладку [Вход] и нажать кнопку <Пуск> для запуска службы (см. Рисунок 14).

3.3 Альтернативные варианты настройки сервера СУБД.

3.3.1 Задание порта вручную

При необходимости можно уйти от динамического задания порта/портов, а зарезервировать его заранее. Для этого выполните следующие действия:

1. В меню [Пуск] выбрать [Microsoft SQL Server] и открыть [Диспетчер конфигураций SQL Server];
2. В дереве [Диспетчер Конфигурации SQL Server] выбрать и раскрыть <Сетевая конфигурация SQL Server>. Выбрать <Протоколы для «Название MSSQL сервера»> (см. Рисунок 10) (в примере имя экземпляра базы - <MSSQLSERVER>);
3. В центральном окне найти настройку [TCP/IP], кликнуть по ней два раза левой кнопкой мыши, будет открыто окно [Свойства TCP/IP];

4. *Для задания одного порта*. Перейти на вкладку [IP-адреса], в группе [IPAll] для настройки [TCP-порт] задать значение `1` (см. Рисунок 15). Перейти на вкладку [Протокол], для настройки [Прослушивать все] из выпадающего списка выбрать значение <Нет> (см. Рисунок 16). Нажать кнопку <OK> для сохранения;

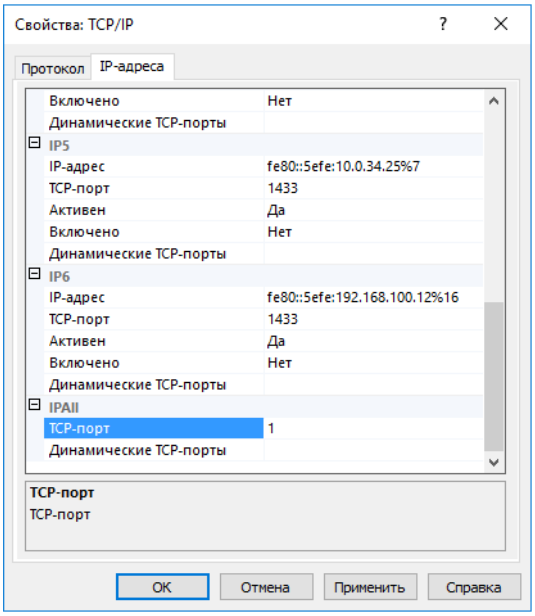

Рисунок 15 - SQL Server Configuration Management. Окно [Свойства TCP/IP]. Вкладка [IP-адреса]

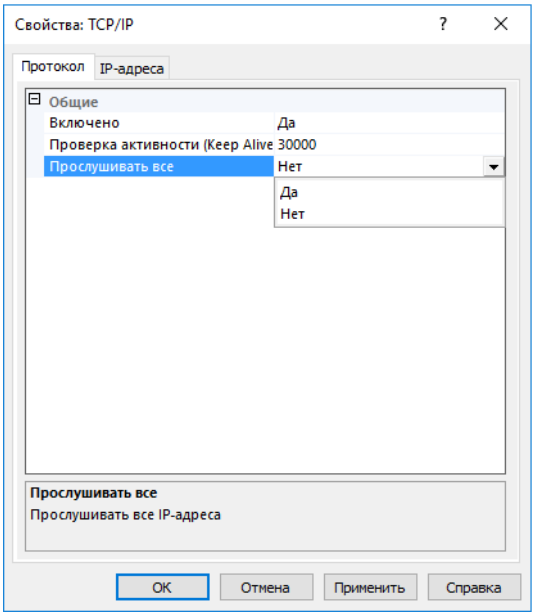

Рисунок 16 - SQL Server Configuration Management. Окно [Свойства TCP/IP]. Вкладка [Протокол]

5. *Для задания нескольких портов*. Перейти на вкладку [IP-адреса], в группе [IP3] для настройки [TCP-порт] задать значение `1`, для настройки [Включено] из выпадающего списка выбрать значение <Да> (см. Рисунок 17). В группе [IPAll] для настроек [TCP-порт] и [Динамические TCP-порты] удалить все значения (см. Рисунок 18). Нажать кнопку <OK> для сохранения;

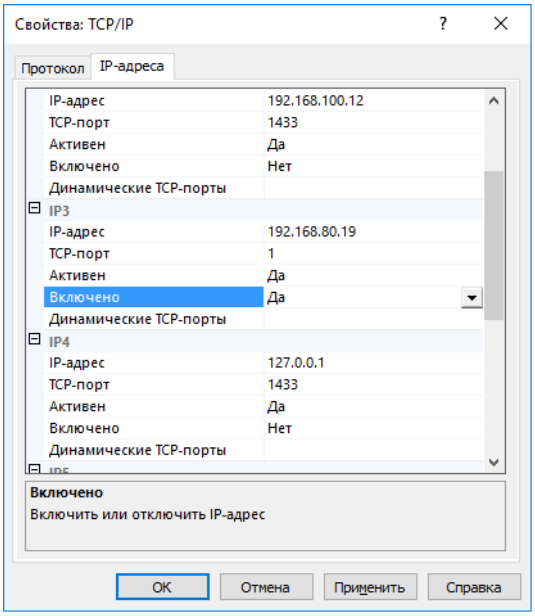

Рисунок 17 - SQL Server Configuration Management. Окно [Свойства TCP/IP]. Вкладка [IP-адреса]

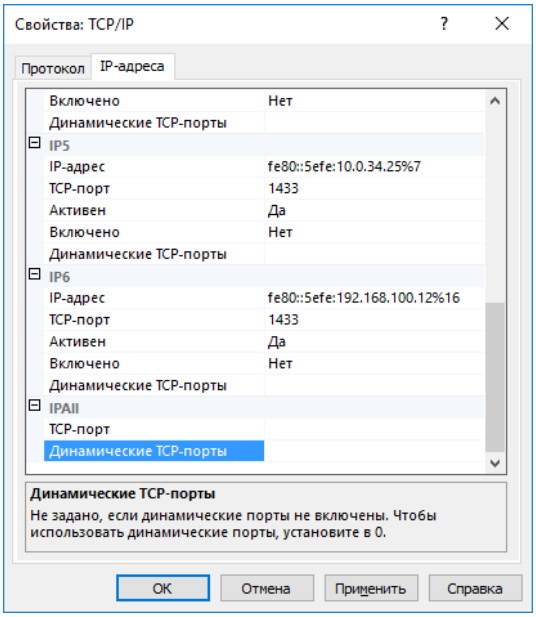

Рисунок 18 - SQL Server Configuration Management. Окно [Свойства TCP/IP]. Вкладка [Протокол]

> *Если параметр [Прослушивать все] на вкладке [Протокол] имеет значение <Да>, то будут использоваться только значения [TCP-порт] и [Динамический TCP-порт] в разделе [IPAll], а раздел [IP3] будет игнорироваться.*
>
> *Если параметр [Прослушивать все] имеет значение <Нет>, то параметры [TCP-порт] и [Динамический TCP-порт] в разделе [IPAll] будут игнорироваться, а использоваться будут параметры [TCP-порт], [Динамический TCP-порт] и [Включено] в разделе [IP3]*

3.3.2 Отключение брандмауэра Windows

Для отключения брандмауэра Windows необходимо выполнить следующие шаги:

1. Выбрать последовательно [Пуск], [Параметры], [Обновление и безопасность], [Безопасность Windows], [Брандмауэр и защита сети];
2. Выбрать профиль сети, для которого надо отключить брандмауэр: [Сеть домена], [Частная сеть] или [Общедоступная сеть] (см. Рисунок 19);

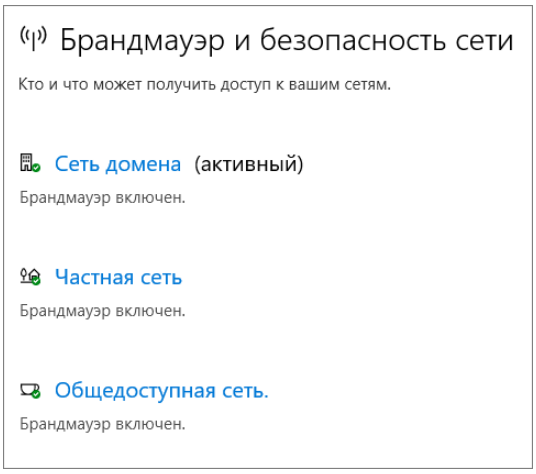

Рисунок 19 - [Брандмауэр и защита сети]. Профили сети

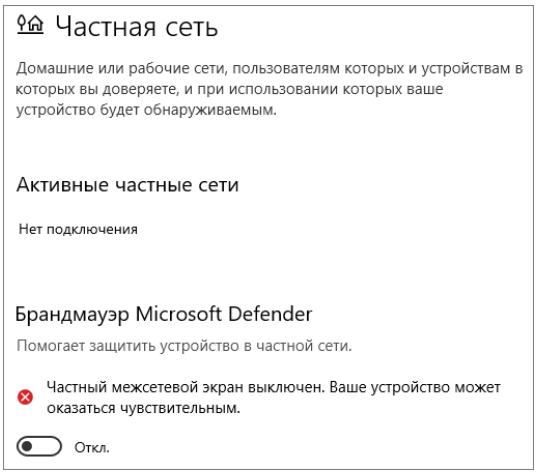

Рисунок 20 – [Частная сеть]. Отключение брандмауэра

3. В разделе [Брандмауэр Microsoft Defender] перевести параметр в значение <Откл.> (см. Рисунок 20).

3.3.3 Настройка Microsoft SQL Server для работы с TLS

Для настройки Microsoft SQL Server для работы с TLS необходимо выполнить следующие действия:

1. Создать сертификат на машине, где установлен Microsoft SQL Server, с помощью консоли хранилища сертификатов. Новый сертификат будет находиться в хранилище сертификатов компьютера (пример см. Рисунок 21);

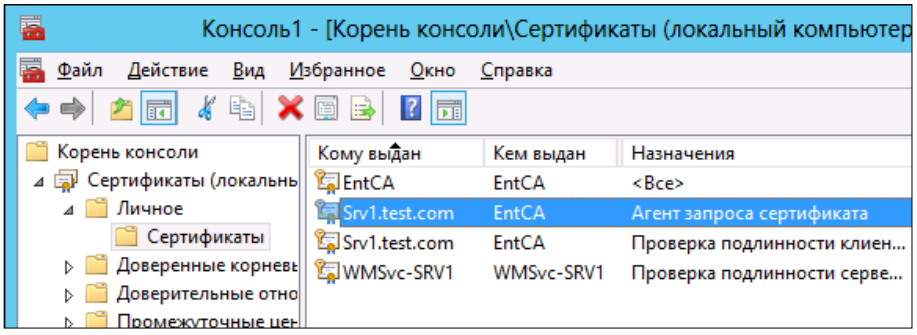

Рисунок 21 - Сертификат установлен в хранилище сертификатов компьютера

2. Запустить [Диспетчер конфигурации SQL Server]. В дереве развернуть узел <Сетевая конфигурация SQL Server>, выбрать пункт <Протоколы для ...>. После этого в верхнем меню выбрать <Действие>, <Свойства>;
3. Будет открыто окно [Свойства: Протоколы для SQLEXPRESS] (см. Рисунок 22). Необходимо изменить параметры подключения к инстансам. Для этого на вкладке [Флаги] у настройки [Принудительное шифрование] из выпадающего списка выбрать значение <Да>;

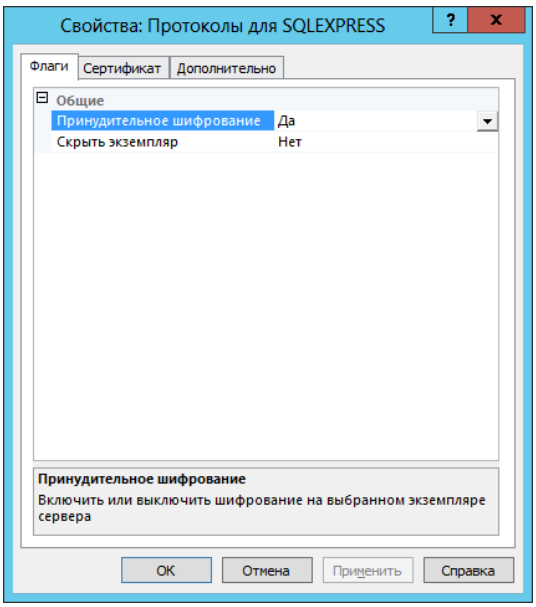

Рисунок 22 - [Свойства: Протоколы для SQLEXPRESS]. Вкладка [Флаги]

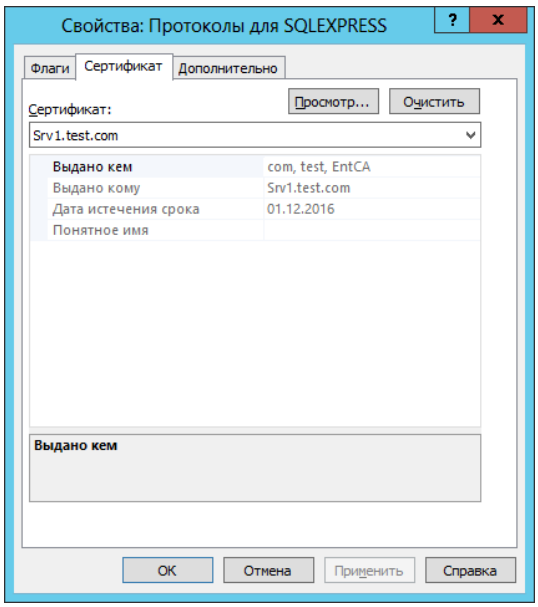

Рисунок 23 – [Свойства: Протоколы для SQLEXPRESS]. Вкладка [Сертификат]

4. Перейти на вкладку [Сертификат] (см. Рисунок 23), чтобы установить сертификат для создания защищенных соединений. Для этого в выпадающем списке <Сертификат> выберите сертификат для сервера SQL, установленный в хранилище локального компьютера на сервере SQL (сертификат, созданный на шаге 1);
5. Далее необходимо изменить параметры подключения клиентов. Для этого в окне консоли [Диспетчер конфигурации SQL Server] выбрать <Конфигурация клиента Native Client SQL>. После этого в верхнем меню выбрать <Действие>, <Свойства>. Будет открыто окно [Свойства: Конфигурация клиента Native Client SQL] (см. Рисунок 24). Для настройки [Force Protocol Encryption (Принудительное шифрование протокола)] задать из выпадающего списка значение <Да>. Нажать кнопку <OK> для закрытия окна свойств;

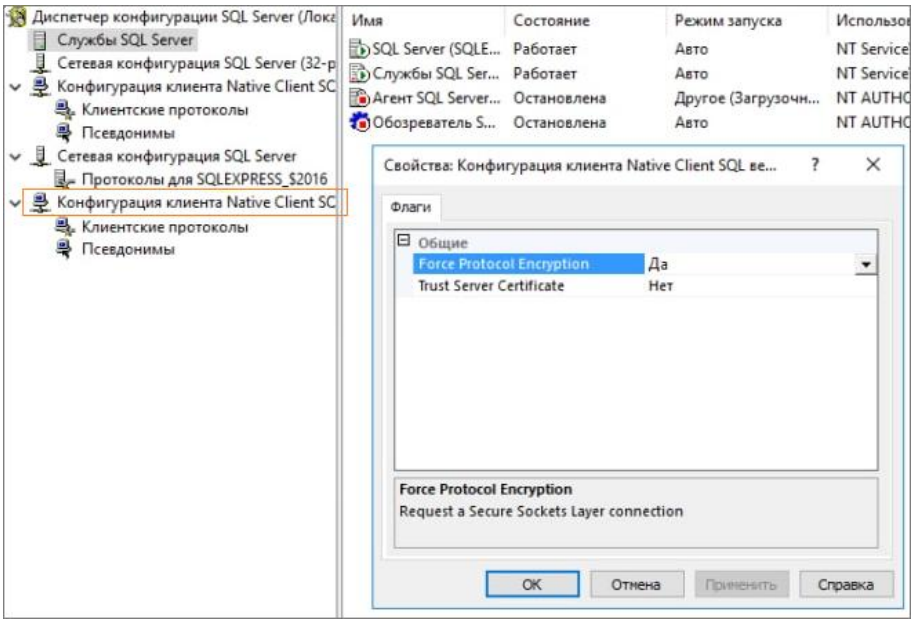

Рисунок 24 - [Диспетчер конфигурации SQL Server]. Окно [Свойства: Конфигурация клиента Native Client SQL]

6. Необходимо проверить, что в качестве встроенной учетной записи сервера SQL используется локальная система. Для этого необходимо у [SQL Server] вызвать контекстное меню и выбрать пункт <Свойства>. В окне [Свойства: SQL Server] в настройке [Использовать для входа] должно быть выбрано <Встроенную учетную запись> и в выпадающем списке - <Локальная система> (см. Рисунок 25);

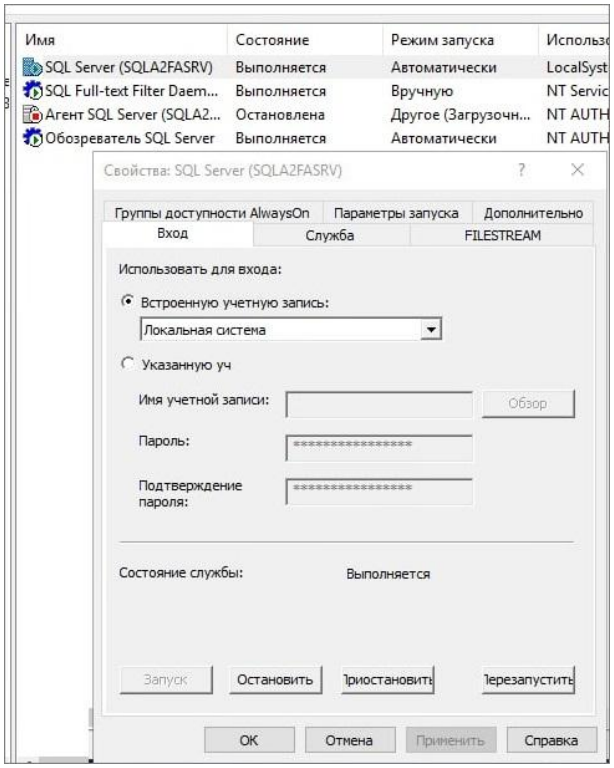

Рисунок 25 - [Диспетчер конфигурации SQL Server]. Окно [Свойства: SQL Server]

7. Перезапустить службу сервера SQL – [SQL Server] (на рисунке выше (Рисунок 24) –это первое наименование в перечне служб).

3.3.4 Скрипт для создания базы данных под MS SQL

Для создания новой базы данных с помощью скрипта необходимо выполнить следующие действия:

1. Открыть [Microsoft SQL Server Management Studio], подключится к серверу БД с правами администратора;
2. Среди элементов управления выбрать <Создать запрос> (см. Рисунок 26);

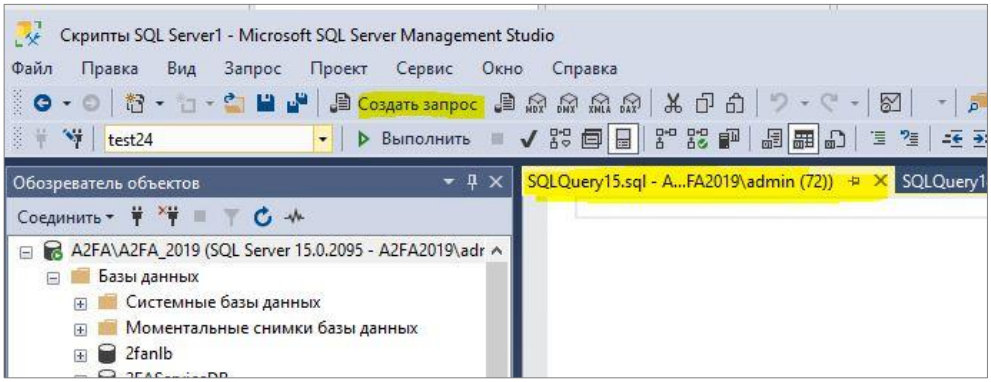

Рисунок 26 - Microsoft SQL Server Management Studio. Создание запроса

3. Переключиться в режим SQLCMD, если он не включен по умолчанию (см. Рисунок 27): вкладка [Запрос], <Режим SQLCMD>;

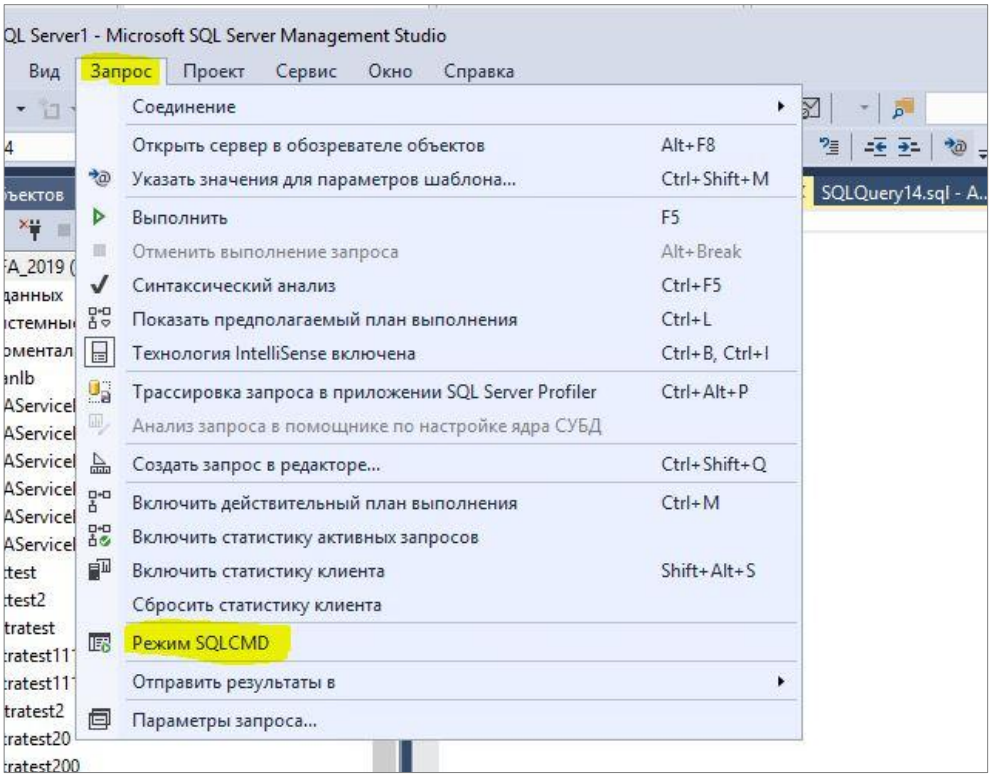

Рисунок 27 - Microsoft SQL Server Management Studio. Переключение в режим SQLCMD

4. В открывшимся окне ввести скрипт, приведенный ниже, выполнив подстановку параметров (имя БД, имя пользователя, пароль):

```
-- Укажите имя БД после DatabaseName

:setvar DatabaseName "2FAServiceDB"
```

```
-- Укажите имя пользователя БД после UserName

:setvar UserName "2FAServiceDB_USER"

-- Укажите пароль пользователя БД после UserPassword

:setvar UserPassword "ZXasqw12!@"


CREATE DATABASE [$(DatabaseName)]

GO

ALTER DATABASE [$(DatabaseName)]

SET READ_COMMITTED_SNAPSHOT ON;

GO

ALTER DATABASE [$(DatabaseName)]

SET ALLOW_SNAPSHOT_ISOLATION ON;

GO

USE [$(DatabaseName)]

IF NOT EXISTS (SELECT * FROM master.dbo.syslogins WHERE loginname =
'$(UserName)')

    BEGIN

        EXEC sp_addlogin [$(UserName)], [$(UserPassword)], [$(DatabaseName)],
N'us_english'

    END

IF NOT EXISTS (SELECT * FROM dbo.sysusers WHERE name = '$(UserName)' AND uid
< 16382)

    BEGIN

        EXEC sp_grantdbaccess [$(UserName)], [$(UserName)]

    END


EXEC sp_addrolemember N'db_datareader', [$(UserName)]

EXEC sp_addrolemember N'db_datawriter', [$(UserName)]

EXEC sp_addrolemember N'db_owner', [$(UserName)]
```

5. Выполнить скрипт: выбрать пункт меню <Выполнить> или нажать соответствующую кнопку на панели инструментов. Отобразиться сообщение о выполнении скрипта (см. Рисунок 28);

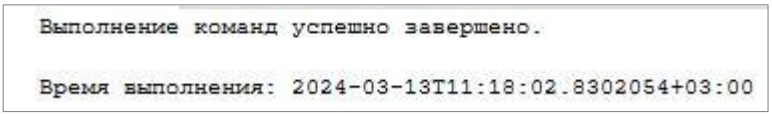

Рисунок 28 – Успешно выполненный скрипт

6. Перед запуском Aladdin 2FA Service необходимо добавить пользователя и пароль от БД в конфигурационный файл `config.yaml`, расположенный по пути: `C:\Program Files\Aladdin2FAService\config.yaml`,чтобы сервис зашифровал его:

```
database:

  type: mssql

user: 2FAServiceDB_USER

password: ZXasqw12!@
```

3.4 Установка Aladdin 2FA Service

> *Для корректной работы серверных компонентов Aladdin 2FA Service, в операционной системе предварительно необходимо настроить синхронизацию времени.*
>
> *Например - синхронизация времени может быть настроена с помощью доменного NTP-сервера, внешнего или с помощью специальных служб, работающих по протоколу NTP (chronyd, timesyncd и т.д.).*

Установка и настройка Aladdin 2FA Service осуществляется с помощью Мастера установки.

Перед установкой необходимо убедиться, что на машине установлены следующие компоненты:

- Microsoft SQL Server;
- SQL Server Management Studio.

> *Перед началом установки рекомендуется отключить брандмауэр Windows (см. п. 3.3.2 Отключение брандмауэра Windows)*

Перед началом установки необходимо разархивировать предварительно загруженный дистрибутив Aladdin 2FA Service.

Для установки Aladdin 2FA Service необходимо выполнить следующие действия:

1. Запустить файл `Aladdin.2FA.Service-x.x.x.xx-x64.ru.msi`, будет открыто окно Мастера установки – [Программа установки Aladdin 2FA Service];
2. В окне приветствия нажать кнопку <Далее> (см. Рисунок 29);
3. На шаге [Лицензионное соглашение] выбрать опцию <Я принимаю лицензионное соглашение> и нажать кнопку <Далее> (см. Рисунок 30);

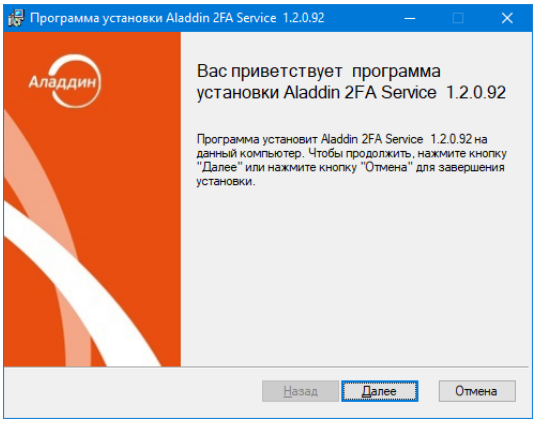

Рисунок 29 - Программа установки Aladdin 2FA Service

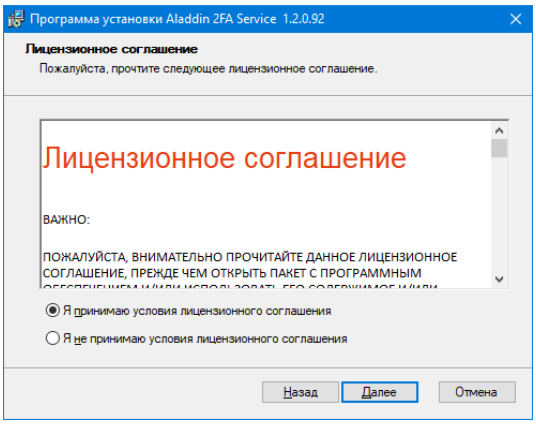

Рисунок 30 - Программа установки Aladdin 2FA Service. Шаг [Лицензионное соглашение]

4. На шаге [Папка назначения] указать путь для установки сервиса и нажать кнопку <Далее> (см. Рисунок 31);
5. На следующем шаге нажать кнопку <Установить> и дождаться окончания установки;
6. Будет отображено окно завершения установки сервиса. Нажать кнопку <Готово> для закрытия Мастера установки (см. Рисунок 32);

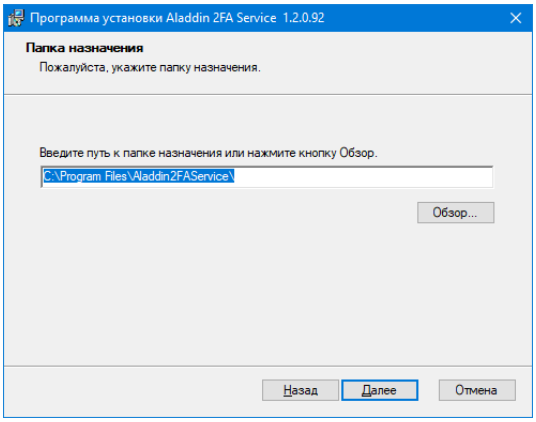

Рисунок 31 - Программа установки Aladdin 2FA Service. Шаг [Папка назначения]

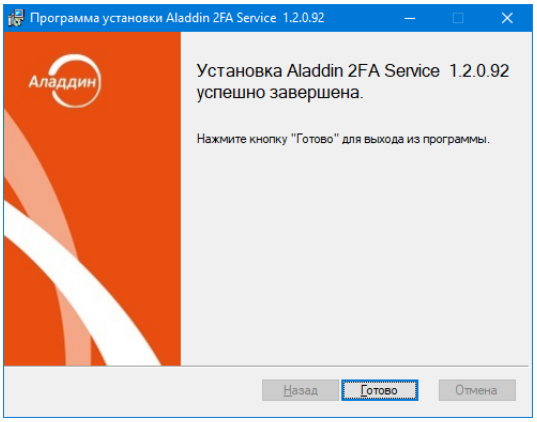

Рисунок 32 - Программа установки Aladdin 2FA Service. Окончание установки

7. Сразу после завершения установки будет открыто приветственное окно Мастера настройки службы Aladdin 2FA Service (далее - Мастер настройки). Нажать кнопку <Далее> (см. Рисунок 33);
8. На шаге [Настройка учётной записи] оставьте выбранной опцию <Системная учётная запись> и нажать кнопку <Далее> (см. Рисунок 34);

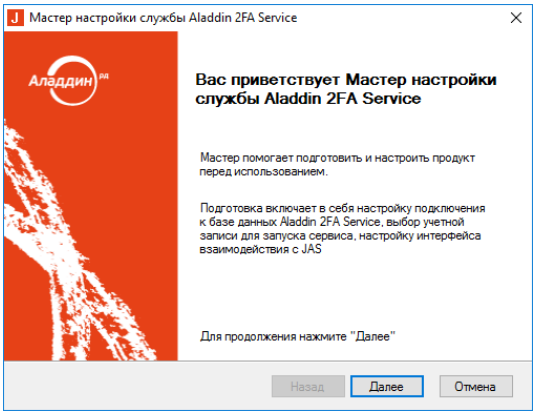

Рисунок 33 - Мастер настройки службы Aladdin 2FA Service

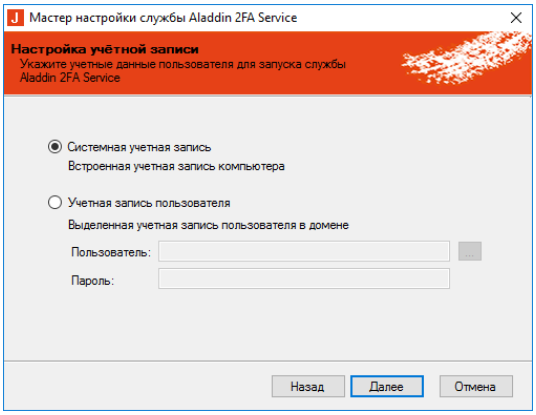

Рисунок 34 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка учётной записи]

9. На шаге [Подключение к серверу БД] (см. Рисунок 35) выполните следующие настройки (см. Таблица 3):

Таблица 3 - Мастер настройки службы Aladdin 2FA Service. Шаг [Подключение к серверу БД]. Настройки

Параметр	Значение
[Укажите сервер БД Aladdin 2FA Service]	Дождаться проверки существующих экземпляров MS SQL Server (значок будет двигаться) и выбрать из выпадающего списка имя сервера, который будет использован для работы с приложением. В списке серверов могут отображаться не все доступные удаленно экземпляры служб MS SQL Server. Если нужный экземпляр MS SQL Server

	не отображается в списке, полное имя этого экземпляра следует ввести вручную
<Использовать TLS>	Установить галочку, если для подключения к выбранному серверу необходимо использовать защищенное соединение
<Указать порт>	Установить галочку, если SQL-сервер настроен на определённый порт. Тогда необходимо указать этот порт, чтобы Aladdin 2FA Service обращался к нему при такой схеме работы. По умолчанию порт не указывать
[Логин]	Имя учетной записи для подключения к серверу Microsoft SQL
[Пароль]	Пароль учетной записи для подключения к серверу Microsoft SQL
<Аутентификация Windows>	Установить галочку для подключения к базе данных с использованием проверки подлинности Windows *При выборе пункта убедиться, что пользователю, от имени которого выполняется мастер настройки, предоставлены права на администрирование SQL-сервера*

Чтобы проверить корректность настроек, нажмите <Тест соединения>. Если соединение настроено верно, отобразится соответствующее сообщение (см. Рисунок 36). В случае некорректного соединения с базой данной, появится окно с ошибкой. Переход к следующему шагу будет недоступен до тех пор, пока не установлено соединение;

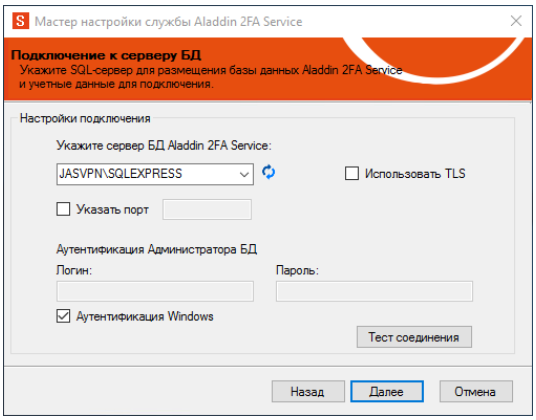

Рисунок 35 - Мастер настройки службы Aladdin 2FA Service. Шаг [Подключение к серверу БД]

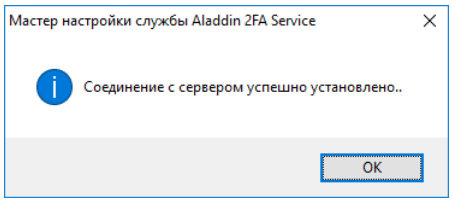

Рисунок 36 - Мастер настройки службы Aladdin 2FA Service. Сообщение об успешном соединении с сервером

10. На шаге [База данных] выбрать настройку <Создание новой базы данных> и нажать кнопку <Далее> (см. Рисунок 37);
11. На шаге [Параметры базы данных] (см. Рисунок 38) задайте следующие параметры (см. Таблица 4):

Таблица 4 - Мастер настройки службы Aladdin 2FA Service. Шаг [Параметры базы данных]. Настройки

Параметр	**Значение**
[Укажите имя БД]	При необходимости изменить или оставить по умолчанию предложенное имя БД
<Использовать TLS>	Установить галочку, если для подключения к выбранному серверу необходимо использовать защищенное соединение

<Создать новый логин>	Не проставлять галочку, если есть необходимость использовать уже имеющуюся пару логин—пароль
[Логин]	При необходимости логин по умолчанию отредактировать или оставить без изменения
[Пароль] [Подтверждение пароля]	Указать пароль и его подтверждение, если создается новая пара логин—пароль. Если используется ранее созданный логин, просто ввести пароль

Нажать кнопку <Далее> для перехода к следующему шагу;

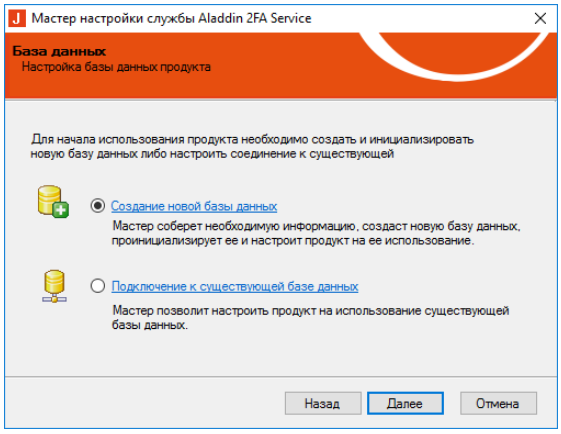

Рисунок 37 - Мастер настройки службы Aladdin 2FA Service. Шаг [База данных]

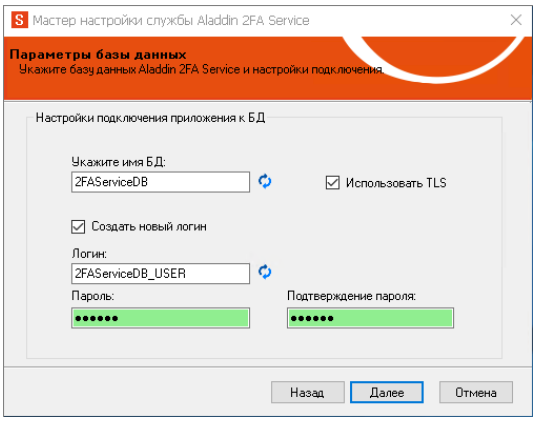

Рисунок 38 - Мастер настройки службы Aladdin 2FA Service. Шаг [Параметры базы данных]

12. На шаге [Настройки подключения JAS] (см. Рисунок 39) задаются настройки подключения к серверу JAS. Задайте параметры подключения в соответствии с описанными настройками ниже (см. Таблица 5):

Таблица 5 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройки подключения JAS]. Настройки

Параметр	**Значение**
<JAS расположен на одном компьютере со службой 2FA Service>	Поставить галочку сервис JAS находится на одном сервере с устанавливаемым A2FA (см. Рисунок 39)
<Сетевой интерфейс>	Поле доступно, если не выбран пункт <JAS расположен на одном компьютере со службой 2FA Service>. В раскрывающемся списке выберите сетевой интерфейс для подключения к серверу JAS или введите его значение вручную, если в списке оно отсутствует (см. Рисунок 40)
[Порт подключения]	Указать порт для подключения 9000

Тип соединения подрзумевается только по протоколу HTTPS

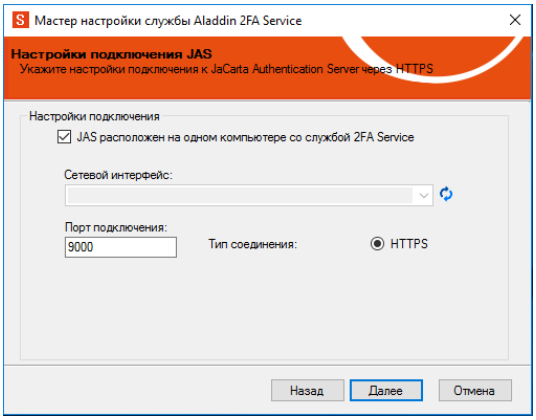

Рисунок 39 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройки подключения JAS]

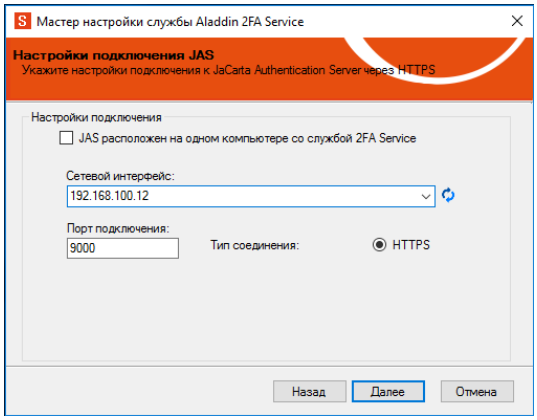

Рисунок 40 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройки подключения JAS]. Выбор сетевого интерфейса

13. На шаге [Расположение сертификата JAS] необходимо выбрать хранилище сертификата, где расположен сертификат для установки защищенного соединения между сервисами JAS и Aladdin 2FA Service.

    13.1. При выборе значения <Хранилище сертификатов Windows> и нажатии кнопки <Далее> (см. Рисунок 41) будет осуществлён переход на шаг [Настройка интерфейса JAS] (см. Рисунок 42).

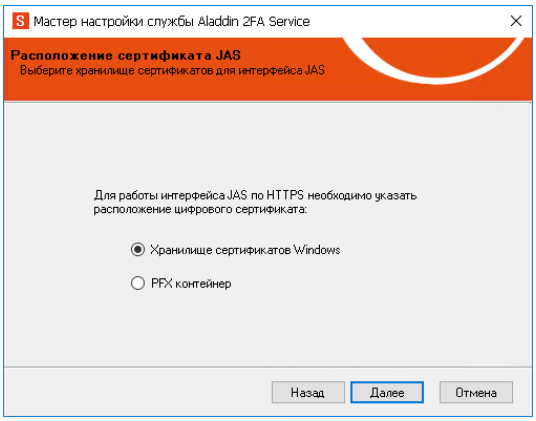

Рисунок 41 - Мастер настройки службы Aladdin 2FA Service. Шаг [Расположение сертификата JAS]. Выбор настройки <Хранилище сертификатов Windows>

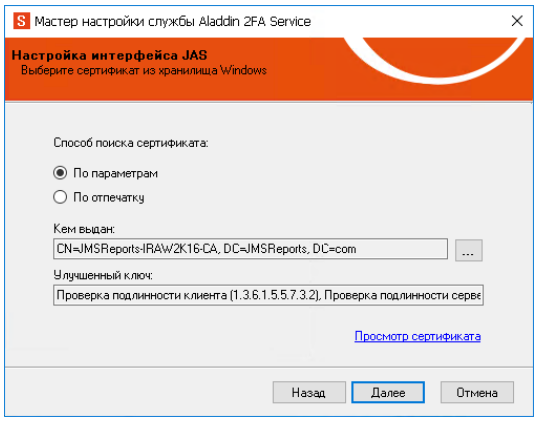

Рисунок 42 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка интерфейса JAS]. Поиск сертификата <По параметрам>

13.2. Далее необходимо выбрать сертификат с помощью кнопки  (см. Рисунок 42). Будет выбран сертификат по умолчанию. Если необходимо указать другой сертификат, то весь перечень сертификатов можно раскрыть с помощью кнопки <Больше вариантов> (см. Рисунок 43).
После чего поля [Кем выдан] и [Улучшенный ключ] автоматически заполнятся валидными значениями выбранного сертификата (см. Рисунок 42). При нажатии на кнопку <Просмотр сертификата> будет открыто окно с подробной информацией о выбранном сертификате (см. Рисунок 46);

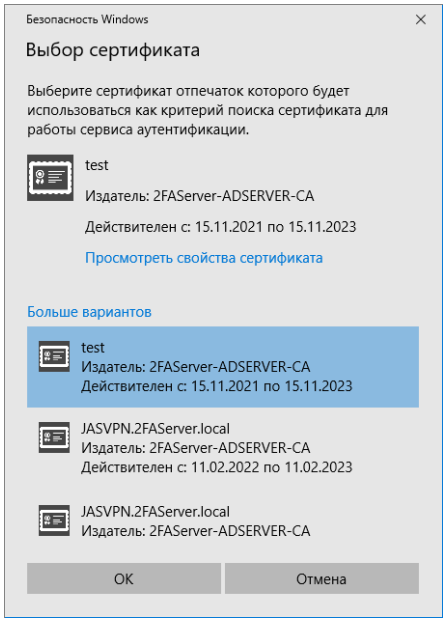

Рисунок 43 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка интерфейса JAS]. Выбор сертификата

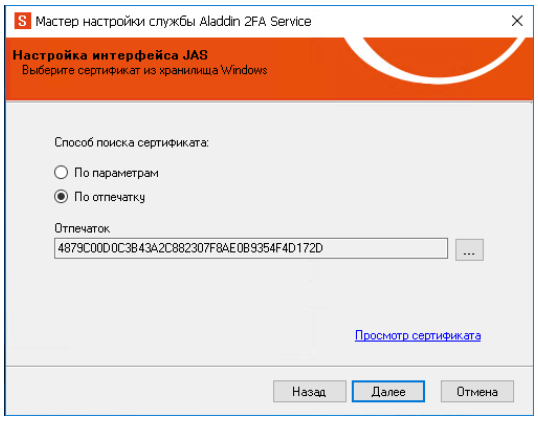

Рисунок 44 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка интерфейса JAS]. Поиск сертификата <По отпечатку>

13.3. Если выбрать значение <По отпечатку> и указать сертификат с помощью кнопки ... (см. Рисунок 44), то в поле [Отпечаток] будет отображен хэш выбранного сертификата (см. Рисунок 45). При нажатии на кнопку <Просмотр сертификата> будет открыто окно с подробной информацией о выбранном сертификате (см. Рисунок 46);

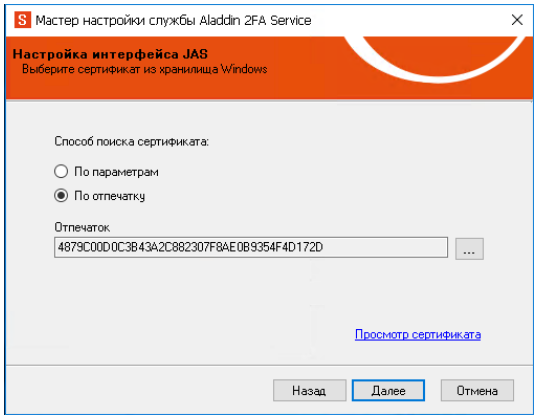

Рисунок 45 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка интерфейса JAS]. Выбор сертификата

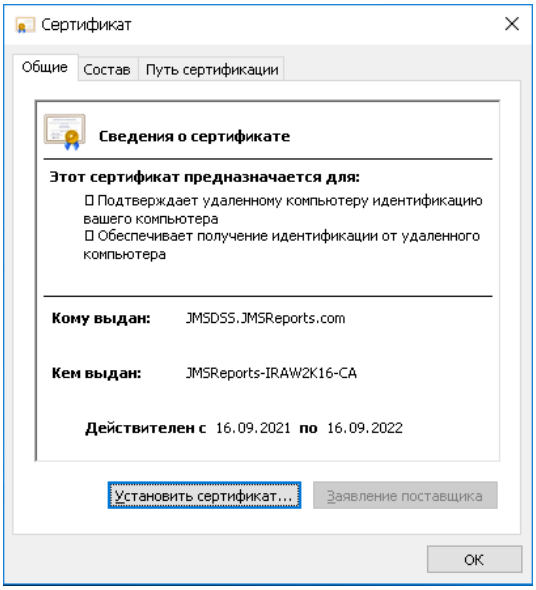

Рисунок 46 – Данные сертификата

13.4. Если на шаге [Расположение сертификата JAS] выбрать значение <PFX контейнер> (см. Рисунок 41) и нажать кнопку <Далее>, будет осуществлен переход на шаг [Настройка подключения JAS], где с помощью кнопки ... надо указать либо pfx контейнер, либо сертификат. При выборе контейнера (файл вида `*.pfx`), необходимо в поле [Пароль контейнера] указать пароль (см. Рисунок 47). Если выбран сертификат, то в поле [Путь к файлу закрытого ключа] указать директорию файла ключа (см. Рисунок 48). Нажать кнопку <Далее> для перехода к следующему шагу;

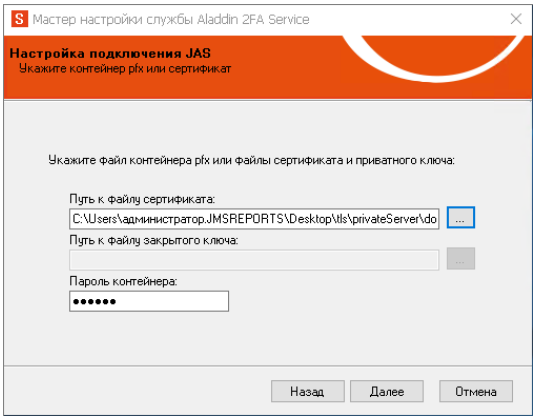

Рисунок 47 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка подключения JAS]. Выбор pfx контейнера

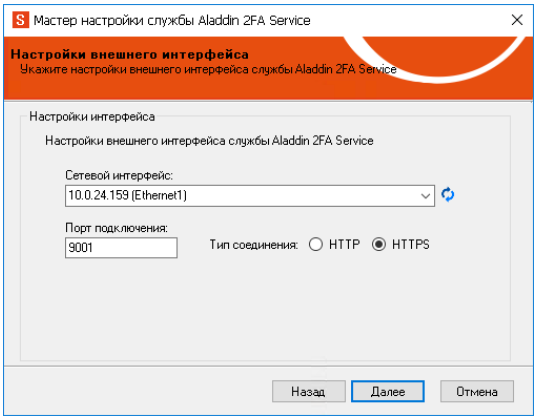

Рисунок 48 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка подключения JAS]. Выбор сертификата

14. На шаге [Настройки внешнего интерфейса] осуществляются настройки внешнего интерфейса Aladdin 2FA Service (см. Рисунок 49). Соединение может осуществляться, как по протоколу HTTPS, так и по HTTP.

- При выборе типа соединения по HTTP и нажатии на кнопку <Далее> будет осуществлен переход на шаг 15;
- При выборе типа соединения по HTTPS и нажатии на кнопку <Далее> будет осуществлен переход на шаг [Расположение сертификатов внешнего интерфейса] (см. Рисунок 50).

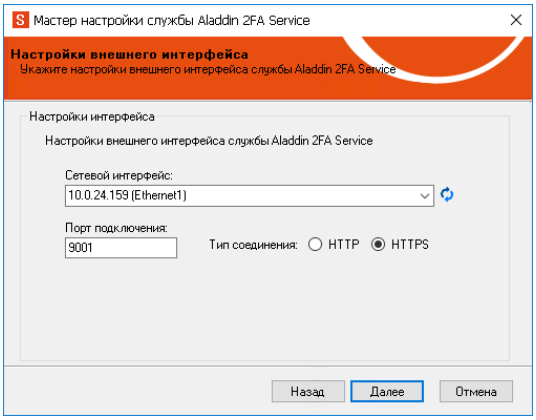

Рисунок 49 - Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка внешнего интерфейса]. Выбор pfx контейнера

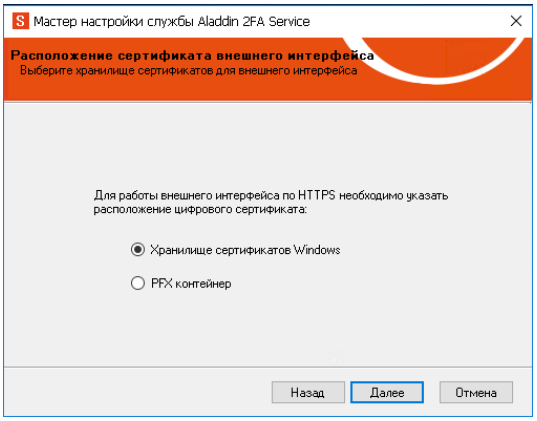

Рисунок 50 - Мастер настройки службы Aladdin 2FA Service. Шаг [Внешний адрес сервиса]

Настройки по добавлению внешнего сертификата аналогичны настройкам по добавлению сертификата между сервисами JAS и Aladdin 2FA Service на предыдущем шаге (см. шаг 13);

15. На шаге [Внешний адрес сервиса] (см. Рисунок 51) в поле [Домен] указать внешний адрес, обратившись по которому мобильные приложения пользователей смогут обмениваться данными с сервером A2FA (подробнее схема взаимодействия приведена на Рисунок 1). Этот домен – точка обращений мобильных устройств для запроса безопасной передачи секрета. Для данного домена обязательно должен быть валидный доменный сертификат, который должен быть установлен либо на прокси-сервере, либо на самом Aladdin 2FA Service. Нажать кнопку <Далее>;

> *В конце домена публикации (FQDN) не должно быть «/»! Пример: https://domain.com/a2fa*

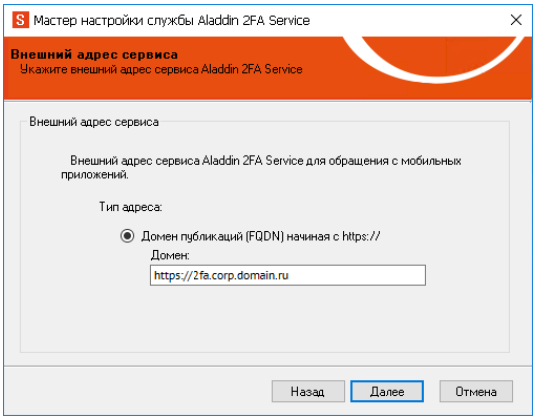

Рисунок 51 - Мастер настройки службы Aladdin 2FA Service. Шаг [Внешний адрес сервиса]

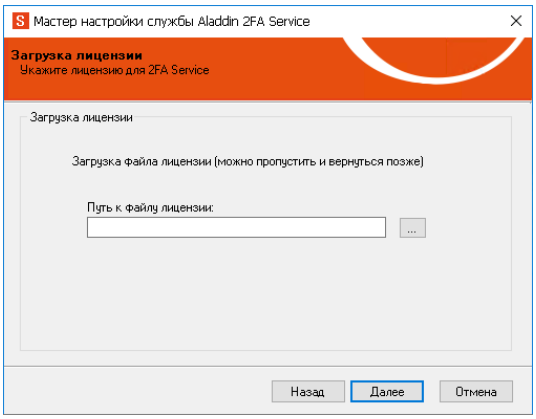

Рисунок 52 - Мастер настройки службы Aladdin 2FA Service. Шаг [Загрузка лицензии]

16. На следующем шаге [Загрузка лицензии] нужно указать директорию файла с лицензией (файл вида `*.lic`) (см. Рисунок 52). Данный шаг можно пропустить, перейдя к следующему с помощью кнопки <Далее>;

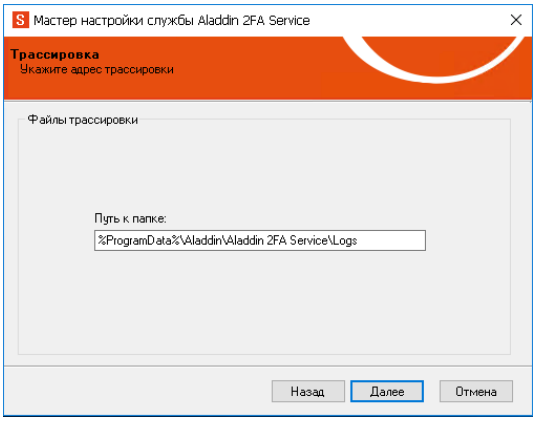

Рисунок 53 - Мастер настройки службы Aladdin 2FA Service. Шаг [Трассировка]

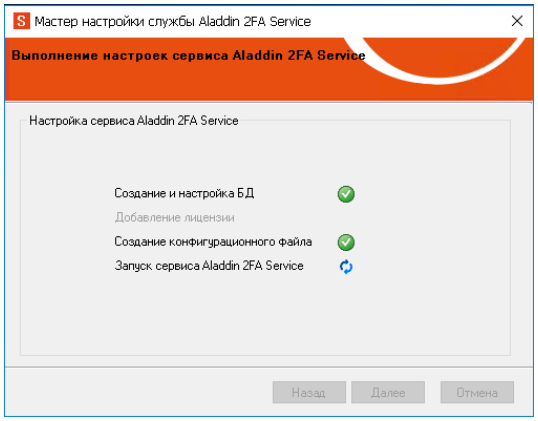

Рисунок 54 - Мастер настройки службы Aladdin 2FA Service. Выполнение настройки

17. На шаге [Трассировка] в поле [Путь к папке] указать путь к папке хранения логов службы и нажать кнопку <Далее> (см. Рисунок 53);
18. Начнет выполняться настройка сервиса Aladdin 2FA Service. Дождаться завершения настройки сервиса и нажать кнопку <Далее> (см. Рисунок 54);

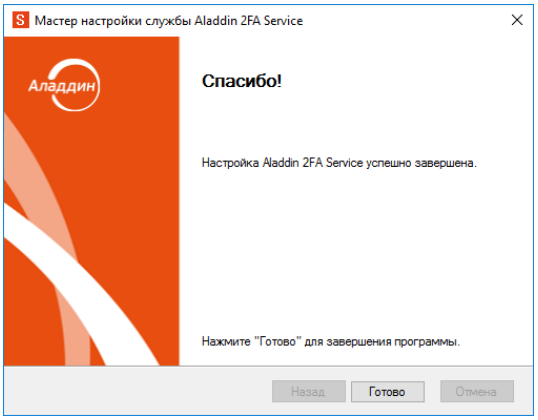

Рисунок 55 - Мастер настройки службы Aladdin 2FA Service. Завершение настройки

19. Будет выведено сообщение об успешной установке сервиса. Нажать кнопку <Готово> (см. Рисунок 55).

3.4.1 Проверка запуска сервиса после работы Мастера настройки

Для того чтобы проверить, что служба запустилась, необходимо:

1. Раскрыть список служб (см. Рисунок 56);

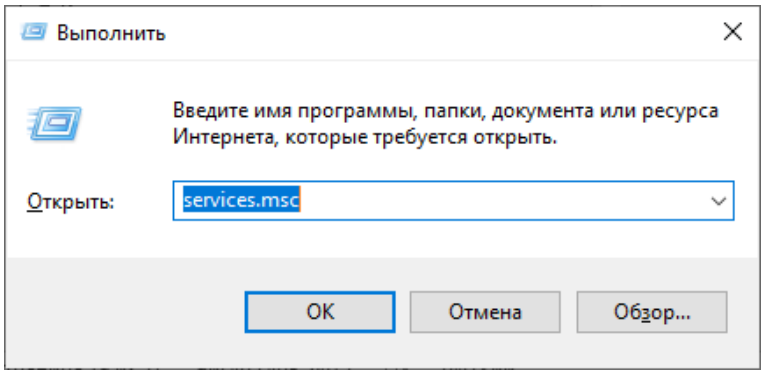

Рисунок 56 – Окно [Выполнить]

2. В перечне служб найти службу"aladdin-2fa-service" и убедиться, что она находится в состояние [Выполняется] и тип запуска [Автоматически] (см. Рисунок 57);

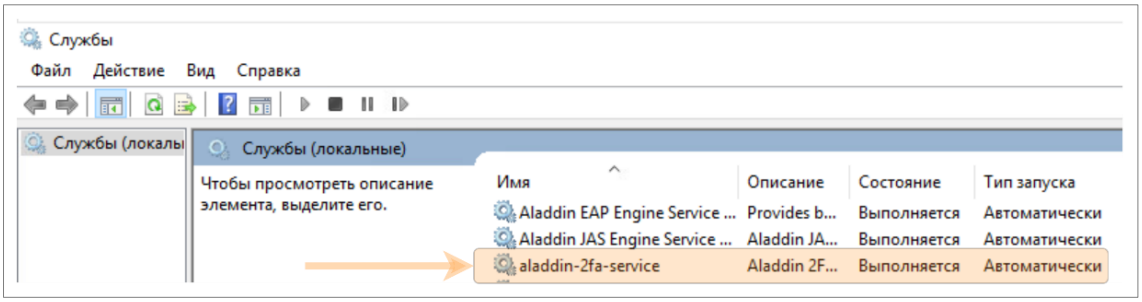

Рисунок 57 – Служба aladdin-2fa-service в перечне служб

3. Спустя 5 секунд обновить информацию: нажать кнопку <Обновление> (см. Рисунок 58). Служба "aladdin-2fa-service" по-прежнему должна иметь состояние [Выполняется] и тип запуска [Автоматически].

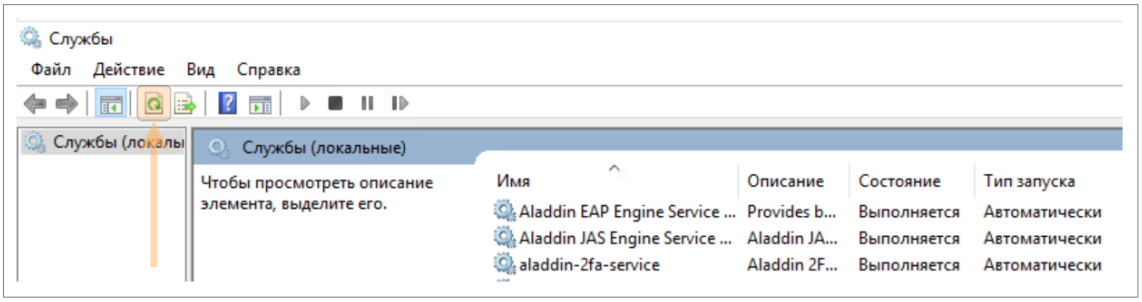

Рисунок 58 – Обновление состояния службы

3.4.2 Добавление pfx-сертификата в хранилище Windows. Типовой вариант настройки

Чтобы добавить pfx-сертифкат в хранилище локального компьютера на Aladdin 2FA Service, выполните следующие действия:

1. По выбранному файлу нажать правой кнопкой мыши, вызвать контекстное меню и выбрать пункт <Установить PFX> (см. Рисунок 59);

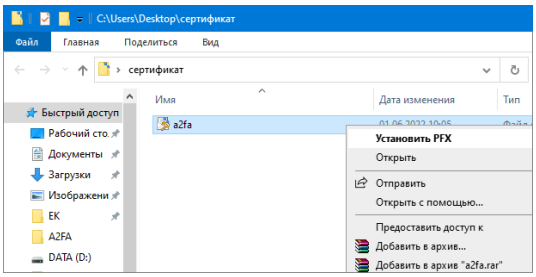

Рисунок 59 – Вызов контекстного меню у pfx-сертифката

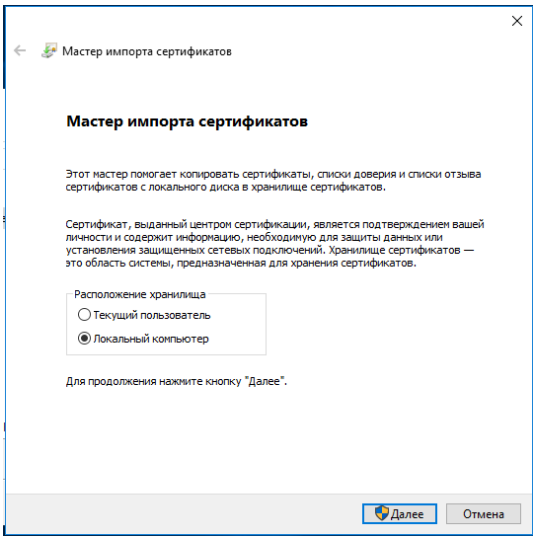

Рисунок 60 – Мастер импорта сертификатов. Выбор хранилища

2. Будет открыт Мастер импорта сертификатов (см. Рисунок 60). В настройке [Расположение хранилища] выбрать <Локальный компьютер>, нажать кнопку <Далее> для перехода на следующий шаг;
3. На шаге [Импортируемый файл] убедиться, что указан верный файл для импорта (см. Рисунок 61). В противном случае с помощью кнопки <Обзор> выбрать другой сертификат. Нажать кнопку <Далее> для перехода на следующий шаг;
4. На шаге [Защита с помощью закрытого ключа] ввести пароль в одноименном поле (см. Рисунок 62). Нажать <Далее>;

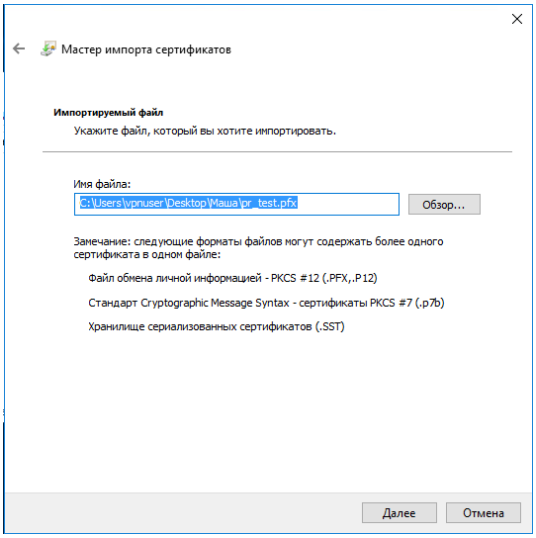

Рисунок 61 – Мастер импорта сертификатов. [Импортируемый файл]

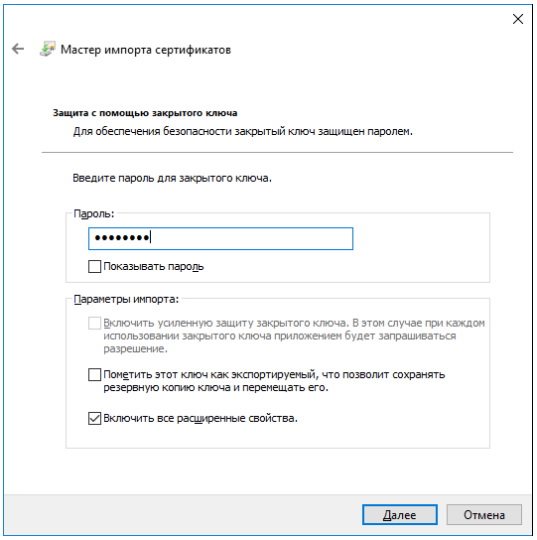

Рисунок 62 – Мастер импорта сертификатов. [Защита с помощью закрытого ключа]

5. На шаге [Завершение мастера импорта сертификатов] проверить корректность данных импортируемого сертификата и, если все верно, нажать кнопку <Готово> (см. Рисунок 63). После будет отображено информационное сообщение (см. Рисунок 64);

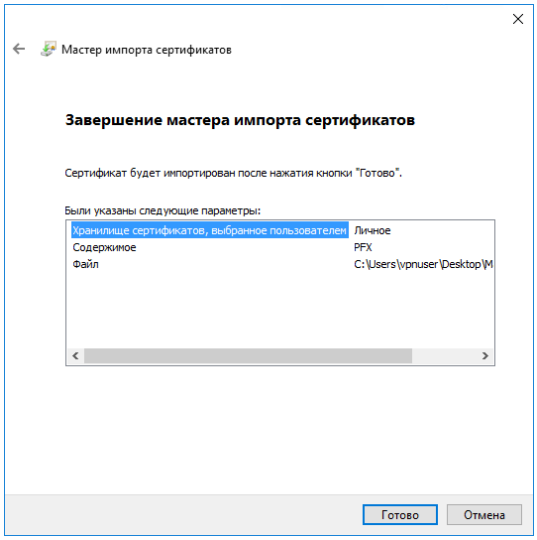

Рисунок 63 – Мастер импорта сертификатов. [Завершение мастера импорта сертификатов]

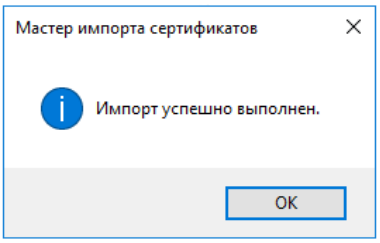

Рисунок 64 – Мастер импорта сертификатов. [Защита с помощью закрытого ключа]

6. Убедиться, что pfx-сертификат импортирован можно, например, с помощью Просмотра сертификатов в оснастке MMC (из командной строки выполните команду `certmgr.msc`) (см. Рисунок 65).

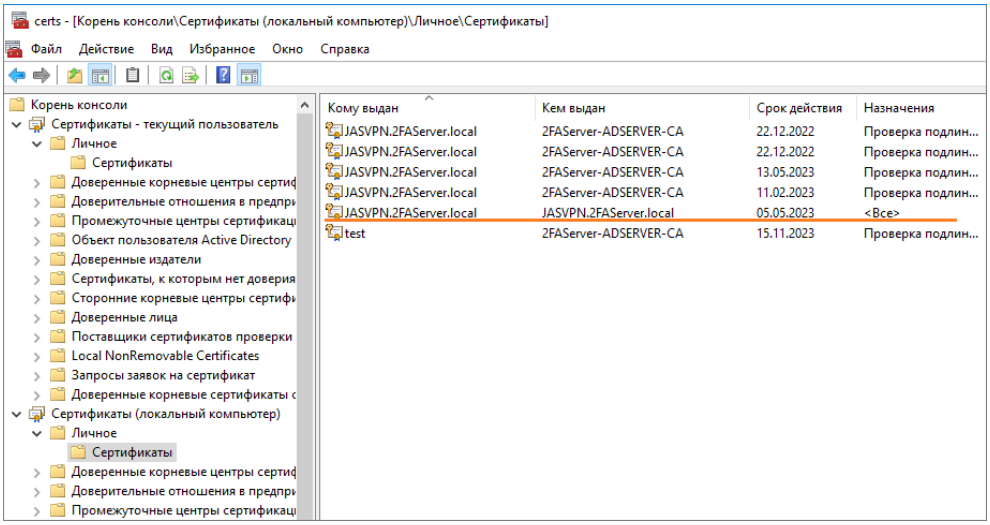

Рисунок 65 - Сертификат установлен в хранилище сертификатов компьютера

4. Управление из сервиса JAS

4.1 Подключение к JAS

Для подключения к серверу JAS выполните настройки, описанные в руководстве по установке и настройке JMS [2], в разделе «Настройки подключения к JAS» в части настроек секции «Веб-сервис безопасной передачи OTP-секрета».

4.2 Настройка выпуска OTP- и PUSH-токенов на базе платформы Aladdin 2FA

Порядок выполнения всех настроек, связанных с обеспечением возможности выпуска пользователями OTP- и PUSH-токенов, используемых в рамках платформы Aladdin 2FA, описан в руководстве по функциям управления JMS [3], в разделе «Порядок настройки самостоятельного выпуска пользователями OTP-аутентификатора».

4.3 Портал самообслуживания

Портал самообслуживания — web-портал в составе продукта JMS, который позволяет пользователю управлять своими электронными ключами, OTP- и PUSH-токенами самостоятельно с помощью web-клиента JMS.

В рамках совместной работы Aladdin 2FA и JMS с помощью Портала самообслуживания пользователь может самостоятельно, например, аутентифицироваться на нем с помощью одноразового пароля, выпустить OTP-токен (см. Рисунок 66), активировать PUSH OTP-токен (см. Рисунок 67), управлять OTP-токеном из личного кабинета.

Порядок выпуска, активации и осуществление других функций управления описан в руководстве пользователя JMS [5].

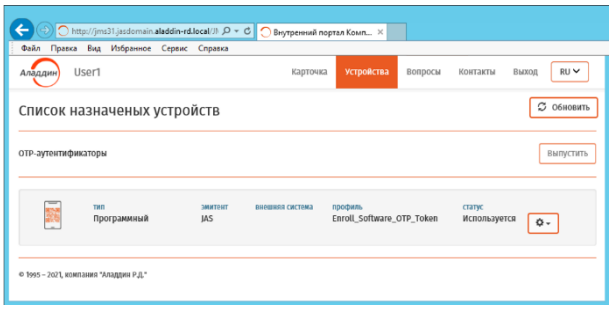

Рисунок 66 – Портал самообслуживания. Выпущенный OTP-токен

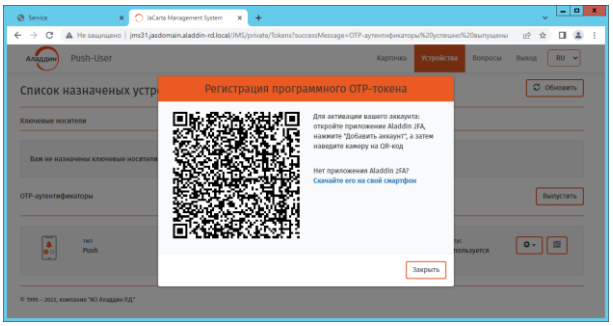

Рисунок 67 - Портал самообслуживания. Окно с QR-кодом для активации OTP-токена

4.4 План обслуживания

План обслуживания – процедура, предназначенная для выполнения регулярных операций массового обслуживания над объектами JMS: учетные записи пользователей, электронные ключи, сертификаты, рабочие станции и др.

С помощью консоли JMS администратор запускает план обслуживания по умолчанию и план обслуживания жизненного цикла OTP-токенов. При успешном выполнении плана обслуживания жизненного цикла OTP-токенов на почтовые ящики пользователей придут письма с вариантами регистрации аутентификаторов в мобильном приложении Aladdin 2FA. Пример такого письма приведен ниже (см. Рисунок 68, Рисунок 69).

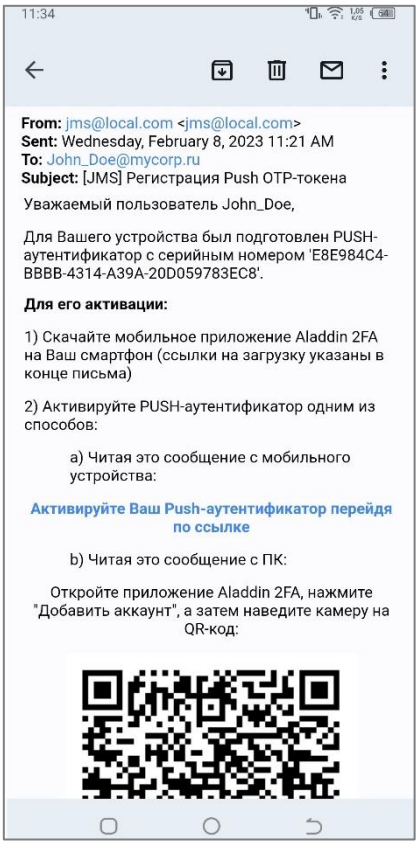

Рисунок 68 – Письмо для пользователя с вариантами регистрации в мобильном приложение Aladdin 2FA. Часть 1

Рисунок 69 - Письмо для пользователя с вариантами регистрации в мобильном приложение Aladdin 2FA. Часть 2

Подробно процесс регистрации аутентификатора в мобильном приложении описан в документе «Aladdin 2FA. Руководство пользователя» [1], в пункте «Регистрация аутентификатора».

Подробно про задачи, входящие в каждый план обслуживания, и их настройку приведено в руководстве по функциям управления JMS [3], в разделе «Планы обслуживания» (в частности в пунктах «План обслуживания жизненного цикла OTP-токенов», «План обслуживания по умолчанию»).

5. Повторная настройка

Режим повторной настройки применяется для изменения или обновления параметров, которые были пропущены на этапе установки или уже неактуальны: добавить или обновить лицензию, обновить устаревшие сертификаты, перенастроить базу данных на работу с TLS, запустить службу A2FA от другой учетной записи.

> *В случае повторной настройки, Мастер настройки позволяет воспользоваться установленной на этапе настойки конфигурацией: поля будут заполненны введенными ранее значениями. Пример повторной настройки сервиса расписан в подразделе 5.2.*

5.1 Добавление или обновление лицензии

1. Для повторной настройки необходимо запустить Мастер настройки. Выбрать на шаге [Режим работы] <Загрузка лицензии> (см. Рисунок 70). На шаге [Загрузка лицензии] указать файл сертификата в поле [Путь к файлу лицензии] (см. Рисунок 71).

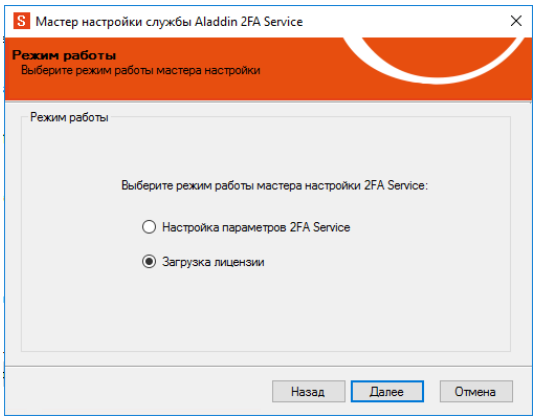

Рисунок 70 - Мастер настройки службы Aladdin 2FA Service. Шаг [Режим работы]

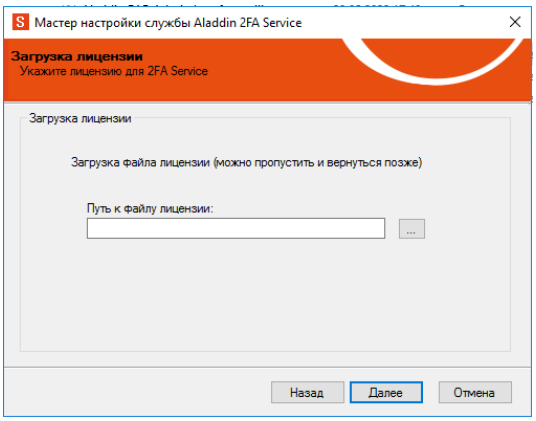

Рисунок 71 - Мастер настройки службы Aladdin 2FA Service. Шаг [Загрузка лицензии]

2. При загрузке лицензии будет отображено информационное сообщение об активации лицензии (см. Рисунок 72) или ее некорректности (см. Рисунок 73).

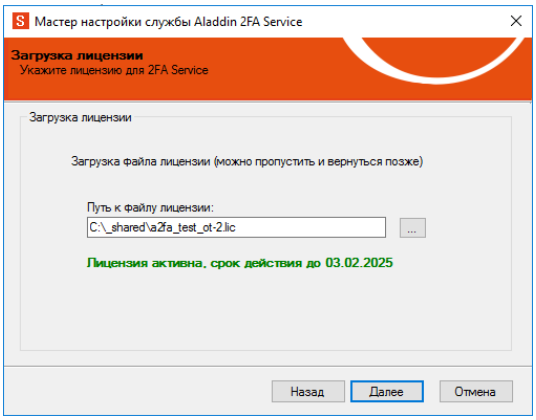

Рисунок 72 - Мастер настройки службы Aladdin 2FA Service. Шаг [Режим работы]

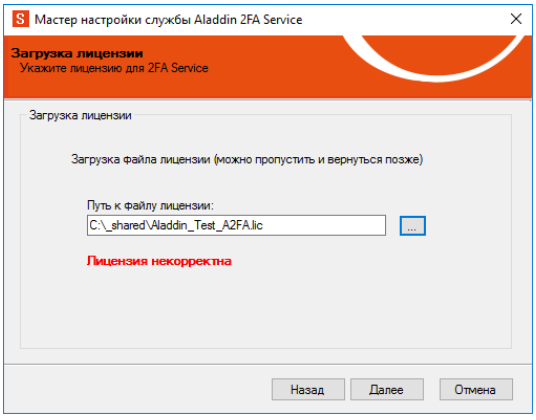

Рисунок 73 - Мастер настройки службы Aladdin 2FA Service. Шаг [Загрузка лицензии]

5.2 Обновление сертификата на внутреннем интерфейсе.

Для обновления TLS-сертификата на внутреннем интерфейсе необходимо:

1. Необходимо запустить Мастер настройки. Выбрать на шаге [Режим работы] <Настройка параметров 2FA Service > (см. Рисунок 74);
2. На шаге [База данных] выбрать <Использовать последние настройки подключения> (см. Рисунок 75);

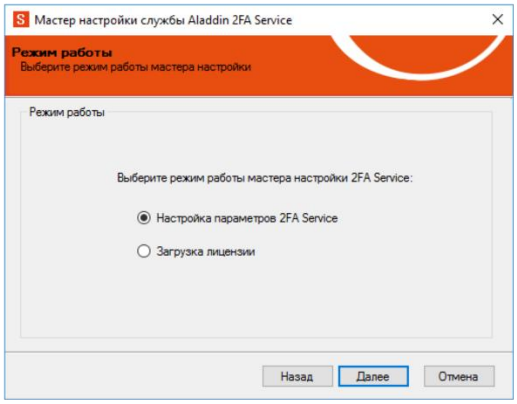

Рисунок 74 – Мастер настройки службы Aladdin 2FA Service. Шаг [Режим работы]

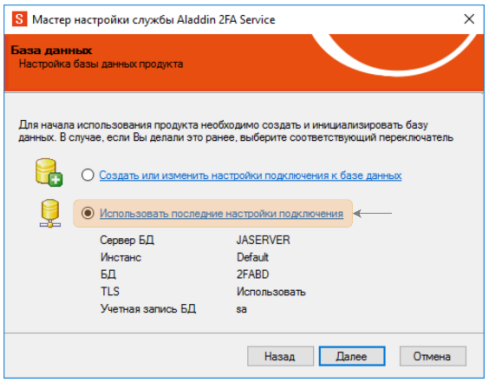

Рисунок 75– Мастер настройки службы Aladdin 2FA Service. Шаг [База данных]

3. Пройти шаги Мастера настройки до шага [Настройка интерфейса JAS]. Раскрыть список доступных сертификатов: в настройке [Способ поиска сертификата] выбрать <По отпечатку> и нажать кнопку ... (см. Рисунок 76);

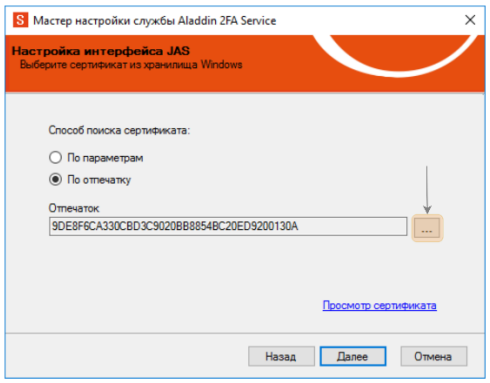

Рисунок 76– Мастер настройки службы Aladdin 2FA Service. Шаг [Настройка интерфейса JAS

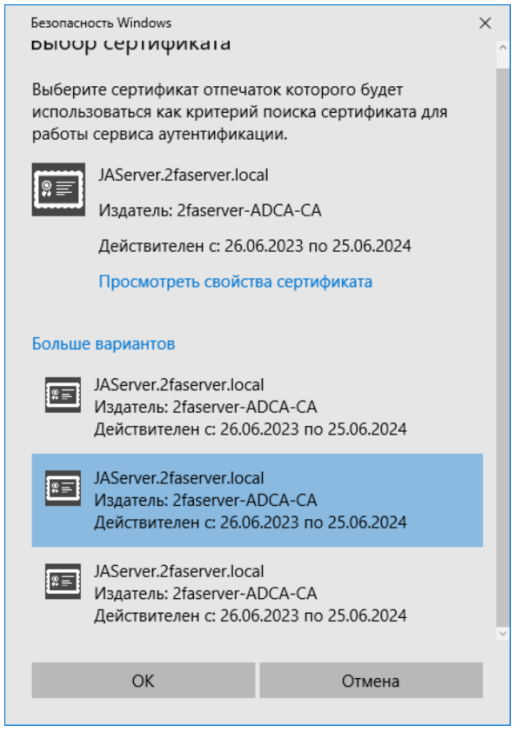

Рисунок 77– Мастер настройки службы Aladdin 2FA Service. Выбор сертификата

4. В окне [Выбор сертификата] выбрать нужный сертификат из хранилища и нажать <OK> (см. Рисунок 77);
5. Пройти все остальные шаги Мастера настройки без изменений;

6. После прохождения Мастера Настройки убедиться, что сервис запустился (см. раздел 3.4.1).

5.3 Перенастройка базы данных на работу с TLS

Для активации поддержки режима TLS при взаимодействии с Microsoft SQL Server необходимо отредактировать конфигурационный файл, расположенный по пути: `C:\Program Files\Aladdin2FAService\config.yaml`.Если открыть файл прямо из директории, его, возможно, не удастся изменить или сохранить. Рекомендуется скопировать файл конфигурации в пользовательскую директорию и сохранить изменения там. Для внесения изменений потребуется заменить исходный конфигурационный файл в директории `C:\Program Files\Aladdin2FAService` на измененный. После этого необходимо перезапустить службу Aladdin 2FA. Для этого с помощью сочетания клавиш `Win+R` и команды `services.msc` открыть окно [Службы]. В нем найти службу [aladdin-2fa-service] и нажать кнопку  - <Перезапуск службы> (см. Рисунок 78).

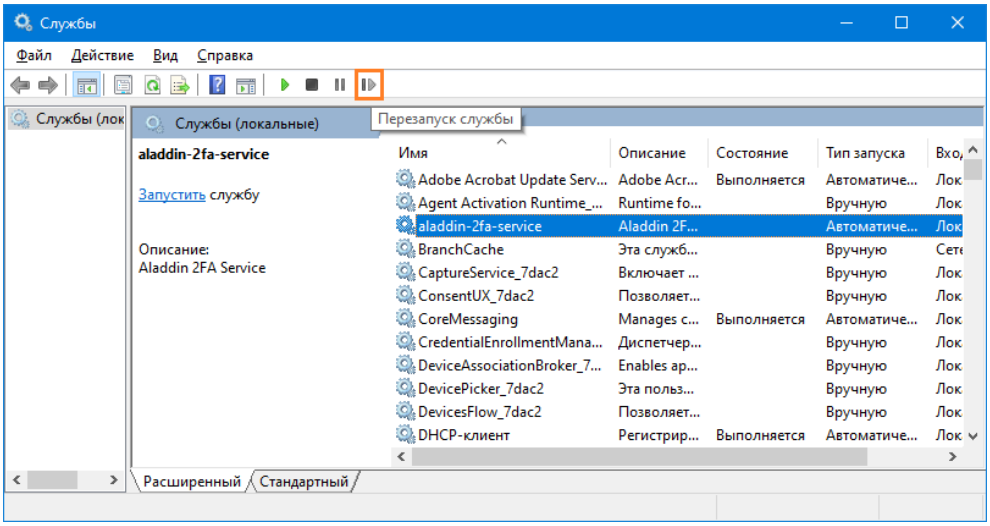

Рисунок 78 – [Службы]. Перезапуск службы [aladdin-2fa-service]

Включить режим TLS можно с помощью редактирования конфигурационного файла одним из следующих способов:

1. В строке подключения к базе данных в конце добавить `TrustServerCertificate=true`. Пример:

```
database:
  # Тип БД
  type: mssql
  # Подключаемая БД
  path:
sqlserver://2FAServiceDB%5FUSER:P%40ssw0rd%21@JMS37?database=2FAServiceDB&con
nection+timeout=30&TrustServerCertificate=true
```

2. С принудительной проверкой доменного имени из сертификата. Для этого в строке подключения добавить `TrustServerCertificate=false&hostNamelnCertificate=wks10.domain.ru`. Пример:

```
database:
  # Тип БД
  type: mssql
  # Подключаемая БД
```

```
  path:
sqlserver://2FAServiceDB%5FUSER:P%40ssw0rd%21@JMS37?database=2FAServiceDB&con
nection+timeout=30&TrustServerCertificate=false&hostNamelnCertificate=wks10.d
omain.ru
```

5.4 Запуск службу A2FA от другой учетной записи

В случае, если необходимо поменять учетную запись для запуска сервиса (например, вместо локальной системы запустить под доменным пользователем), выполните следующие действия:

1. Поменять учетную запись. Для этого помощью сочетания клавиш `Win+R` и команды `services.msc` открыть окно [Службы]. В нем найти службу [aladdin-2fa-service], вызвать контекстное меню и выбрать пункт <Свойства>. В открывшимся окне перейти на вкладку [Вход в систему] (см. Рисунок 79). Выбрать пункт <С учетной записью>, нажать кнопку <Обзор>, чтобы указать имя служебной учетной записи. В полях [Пароль] и [Подтверждение] соответственно ввести пароль и подтверждение пароля служебной учетной записи. Нажмите <OK>, чтобы закрыть окно и сохранить изменения;

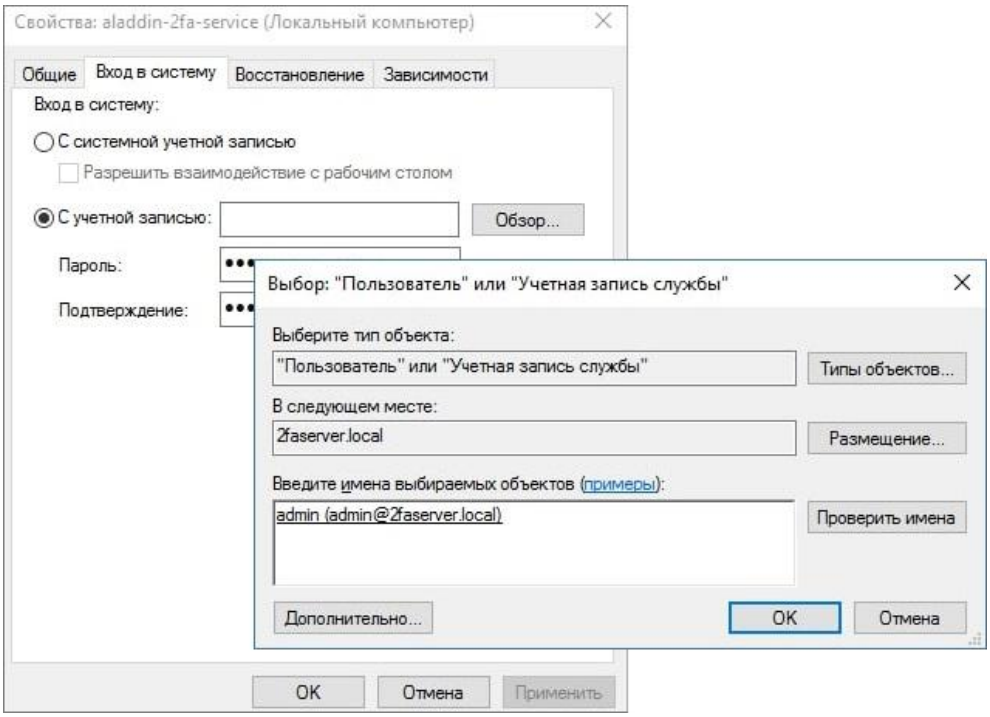

Рисунок 79 - [Службы]. Смена учетной записи для службы [aladdin-2fa-service]

2. Перезапустить службу. Для этого выбрать в перечне служб [aladdin-2fa-service] и нажать кнопку  - <Перезапуск службы> (см. Рисунок 78);
3. Запустить Мастер настройки. На шаге [Режим работы] выбрать <Настройка параметров 2FA Service>, с помощью кнопки <Далее> пройти шаги, обновляя все пароли (например, от pfx-контейнеров или сертификатов и учетных записей SQL);

> *Обновление всех паролей является обязательным условием*

4. В окне [Службы] проверить, что служба [aladdin-2fa-service] запущена.

6. Обновление версии продукта

Для обновления Aladdin 2FA Service на новую версию сначала удалите все установленные компоненты Aladdin 2FA, после чего выполните установку новой версии и первоначальную настройку конфигурации, описанную в п. 3.3.3 Настройка Microsoft SQL Server для работы с TLS.

> *Перед обновлением убедитесь, что создана актуальная резервная копия БД*

7. Кластеризация

В Aladdin 2FA Service реализована поддержка службы кластеров Microsoft Failover Cluster, что позволяет гарантировать бесперебойность процессов аутентификации.

7.1 Подготовка кластера к развертыванию роли General Service

Перед настройкой роли General Service необходимо выполнить следующие действия:

1. Для Aladdin 2FA Service при настройке кластерной роли нужно делегировать учетной записи самого FC-кластера право на создание учетных записей типа "Компьютер" в том контейнере AD, в котором находится учетная запись данного кластера. В противном случае настройка завершается ошибкой:

```
Event ID 1069.
Cluster resource 'ald-2fa' of type 'Network Name' in clustered role 'ald-2fa' failed.
The error code was '0x5' ('Access is denied.');
```

2. После делегирования, в результате работы мастера, создается учетная запись для роли и в DNS регистрируется DNS-имя;
3. После того, как была создана роль, делегирование можно отозвать.

7.2 Настройка роли General Service со службой A2FA в отказоустойчивом кластере

> *Настройка кластера в данном разделе приведена на примере платформы Windows Server 2016*

На каждом из узлов кластера необходимо установить и сконфигурировать Aladdin 2FA Service.

1. Запустить [Диспетчер отказоустойчивости кластеров]. Для этого на сервере запустить [Диспетчер сервера], затем в меню [Сервис] выбрать <Диспетчер отказоустойчивости кластеров>;
2. В окне [Диспетчер отказоустойчивого кластера], раскрыть дерево кластера, вызвать контекстное меню у объекта [Роли] и выбрать пункт <Настроить роль> (см. Рисунок 80);

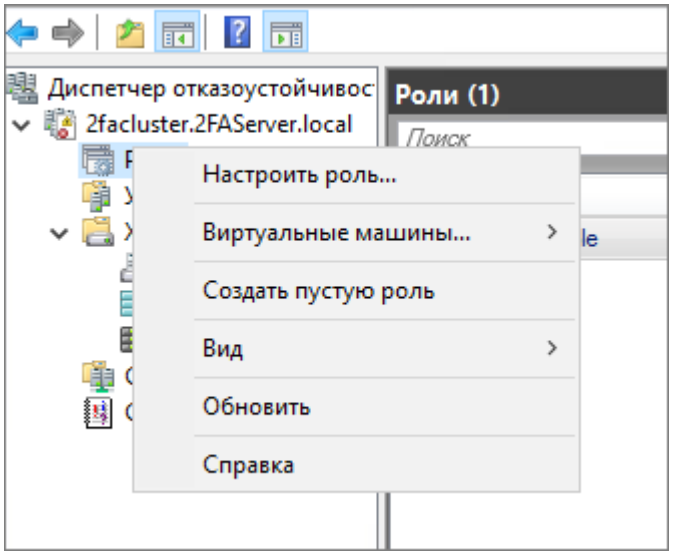

Рисунок 80 - [Диспетчер отказоустойчивого кластера]. Выбор пункта <Настроить роль>

3. Будет запущен [Мастер высокой доступности]. На шаге выбора роли выбрать <Универсальная служба> (см. Рисунок 81) и нажать кнопку <Далее>;

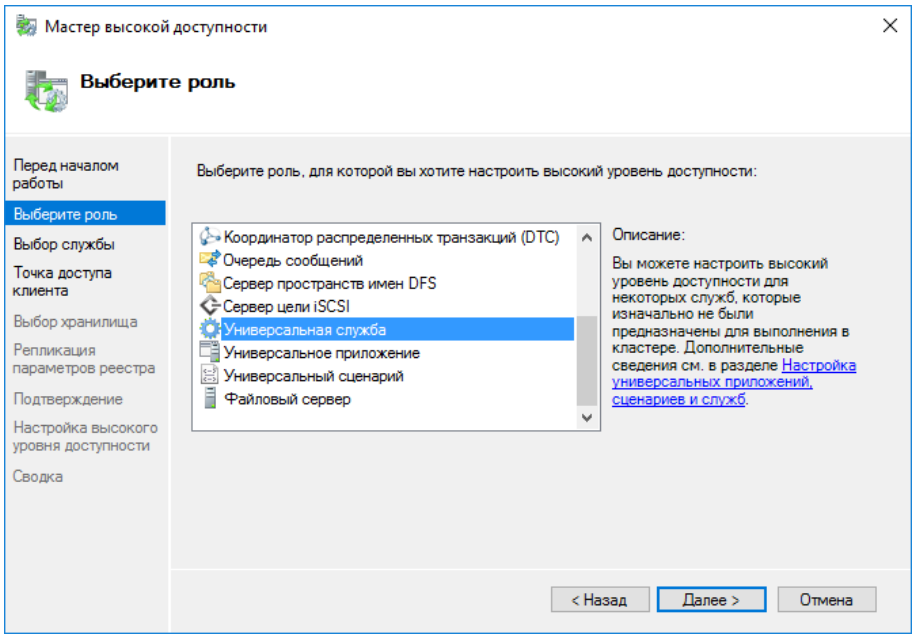

Рисунок 81 - [Мастер высокой доступности]. Шаг [Выберите роль]

4. На шаге [Выбор службы] выбрать в перечне служб службу <aladdin-2fa-service> (см. Рисунок 82). Нажать кнопку <Далее> для перехода к следующему шагу;

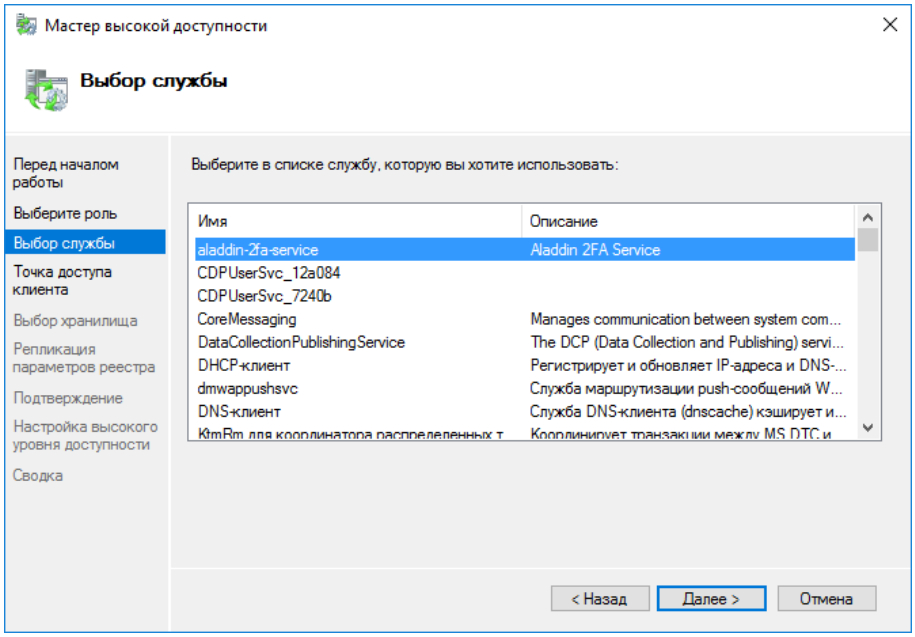

Рисунок 82 - [Мастер высокой доступности]. Шаг [Выбор службы]

5. На шаге [Точка доступа клиента] задать следующие настройки (см. Рисунок 83):

- [Имя] – задать уникальное NetBIOS-имя, которое может содержать буквы, цифры, дефисы и знаки подчеркивания. Учитывается регистр. Максимальная длина составляет 15 символов;
- В таблице ниже задать адаптер и IP-адрес, который будет выделен для всех узлов кластера службы A2FA Service;

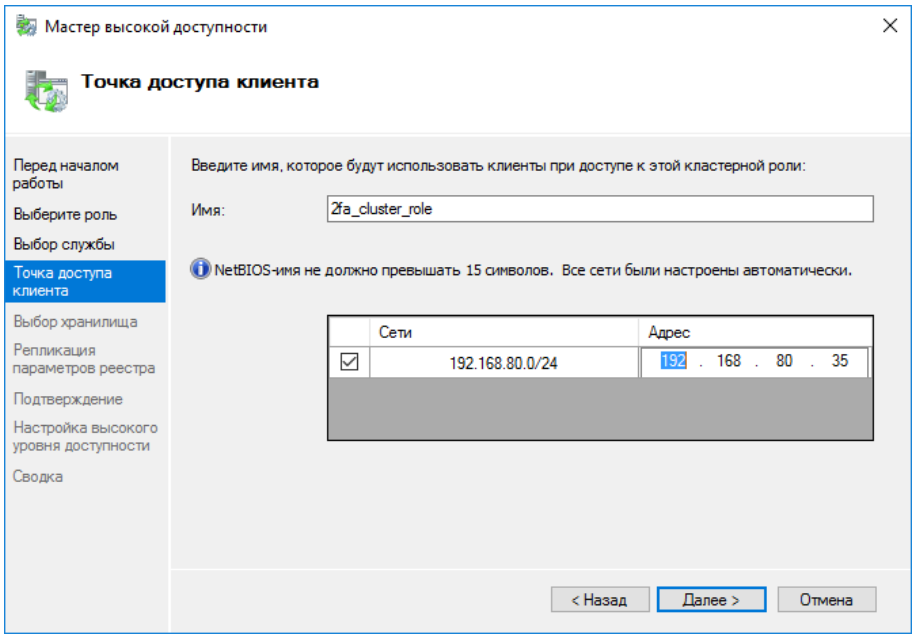

Рисунок 83 – [Мастер высокой доступности]. Шаг [Точка доступа клиента]

6. На шаге [Выбор хранилища] для данной кластерной роли хранилище не требуется, поэтому с помощью кнопки <Далее> для перейти к следующему шагу (см. Рисунок 84);

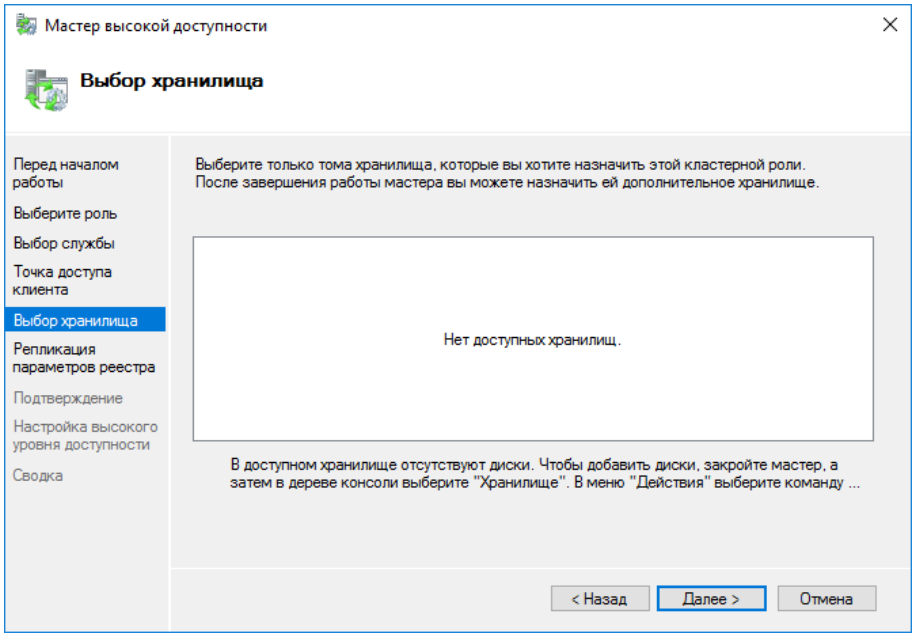

Рисунок 84 - [Мастер высокой доступности]. Шаг [Выбор хранилища]

7. На шаге [Репликация параметров реестра] указать с помощью кнопки <Добавить> общий раздел под службу A2FA Service для всех узлов кластера (см. Рисунок 85). Нажать кнопку <Далее> для перехода к следующему шагу;

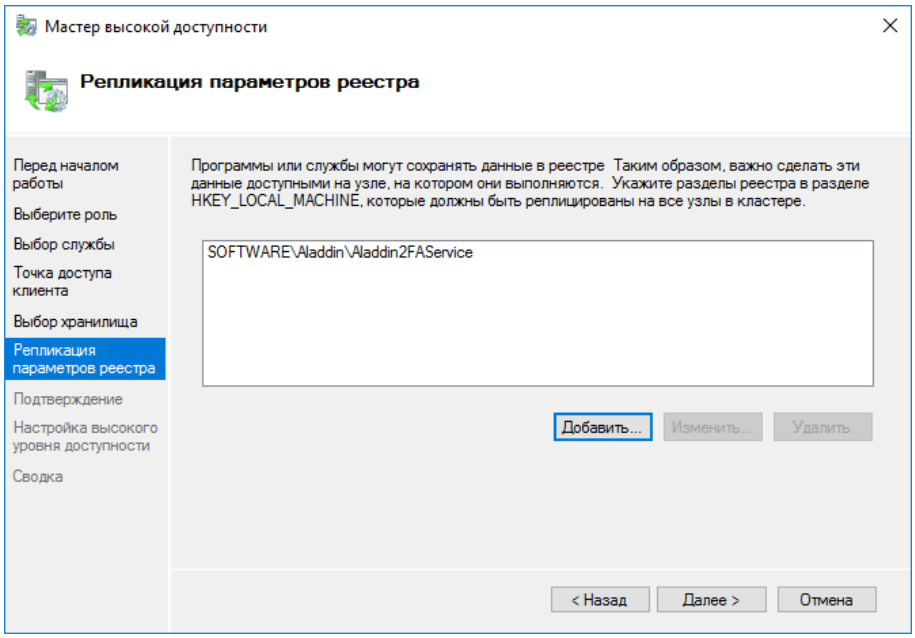

Рисунок 85 - [Мастер высокой доступности]. Шаг [Репликация параметров реестра]

8. На шаге [Подтверждение] проверить заданные ранее настройки и нажать кнопку <Далее> (см. Рисунок 86);

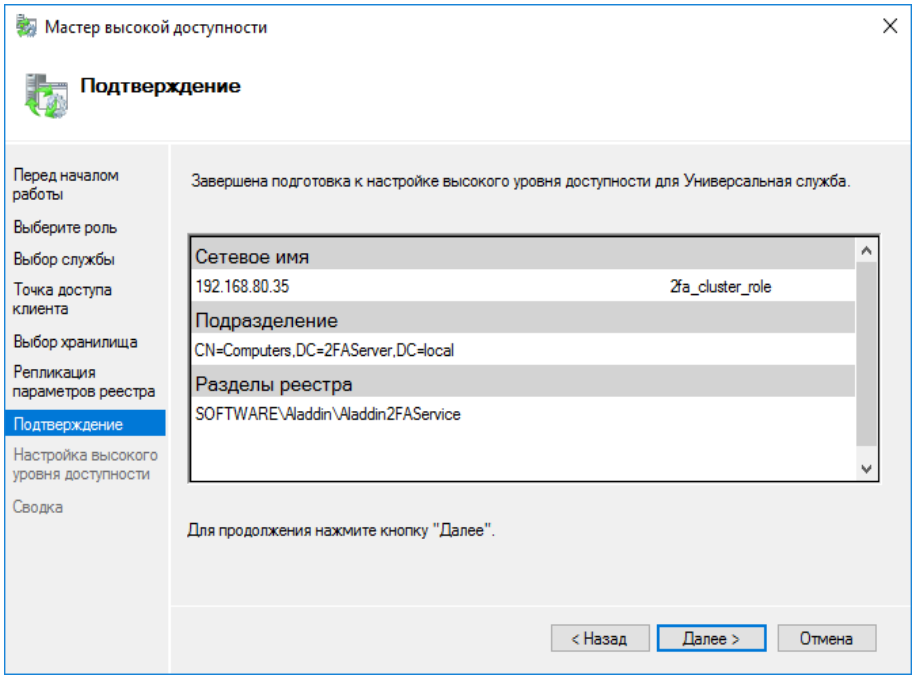

Рисунок 86 - [Мастер высокой доступности]. Шаг [Подтверждение]

9. На шаге [Сводка] представлены настроенные ранее параметры для роли (см. Рисунок 87). Можно сформировать отчет и ознакомиться с ним, для этого нажать кнопку <Просмотреть отчет>. Для закрытия окна установщика нажать кнопку <Готово>.

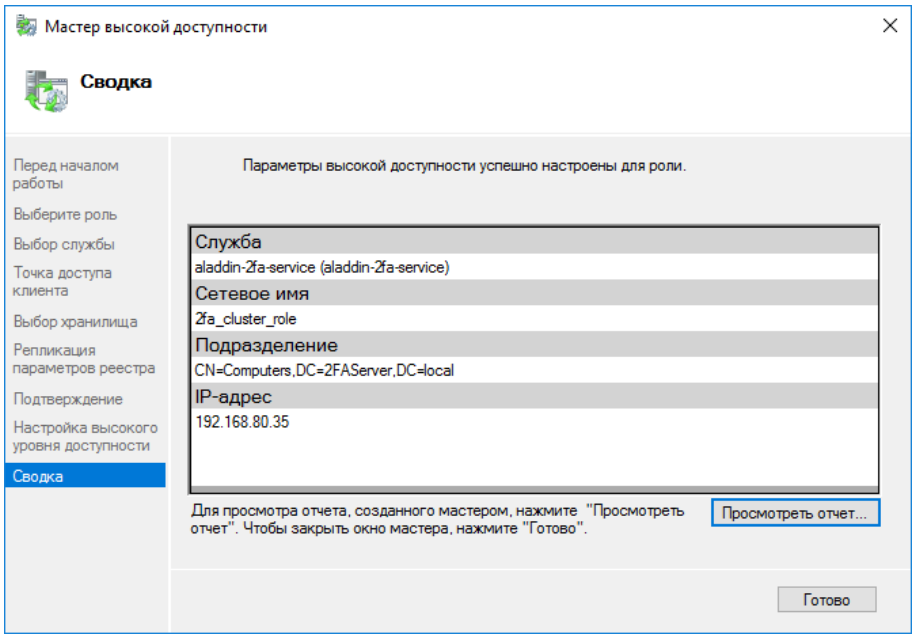

Рисунок 87 - [Мастер высокой доступности]. Шаг [Сводка]

7.3 Проверка работы настроенной роли

Проверить, что роль «General Service» для кластера настроена корректно можно следующим образом:

1. В окне консоли [Диспетчер отказоустойчивого кластера] раскрыть дерево кластера, выбрать объект [Роли]. В центральной части панели выбрать созданную на прошлом шаге роль. В примере - `2fa_claster_role` (см. Рисунок 88). Будут отображены опции выбранной роли.

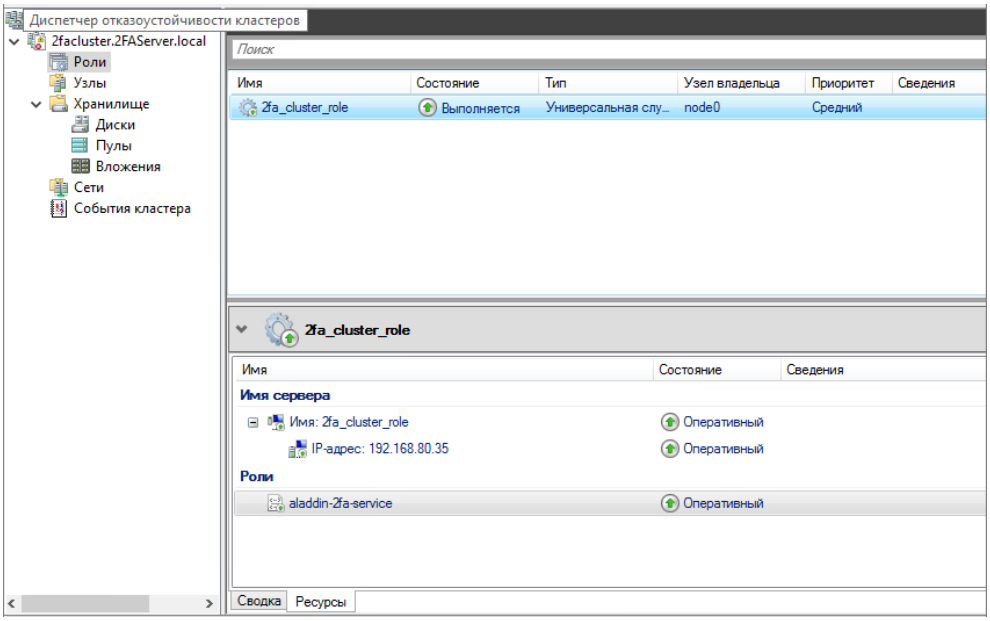

Рисунок 88 - [Диспетчер отказоустойчивого кластера]. Выбор настроенной роли

Если на вкладке [Ресурсы] в столбце [Состояние] напротив каждого объекта будет значение <Оперативный>, значит настройка роли была проведена успешно.

2. Для проверки можно переключить узел владельца на другой.

Для этого в окне консоли [Диспетчер отказоустойчивого кластера] в центральной части панели выбрать созданную ранее роль, вызвать у нее контекстное меню с помощью правой кнопки мыши и последовательно выбрать <Переместить>, <Выбрать узел> (см. Рисунок 89);

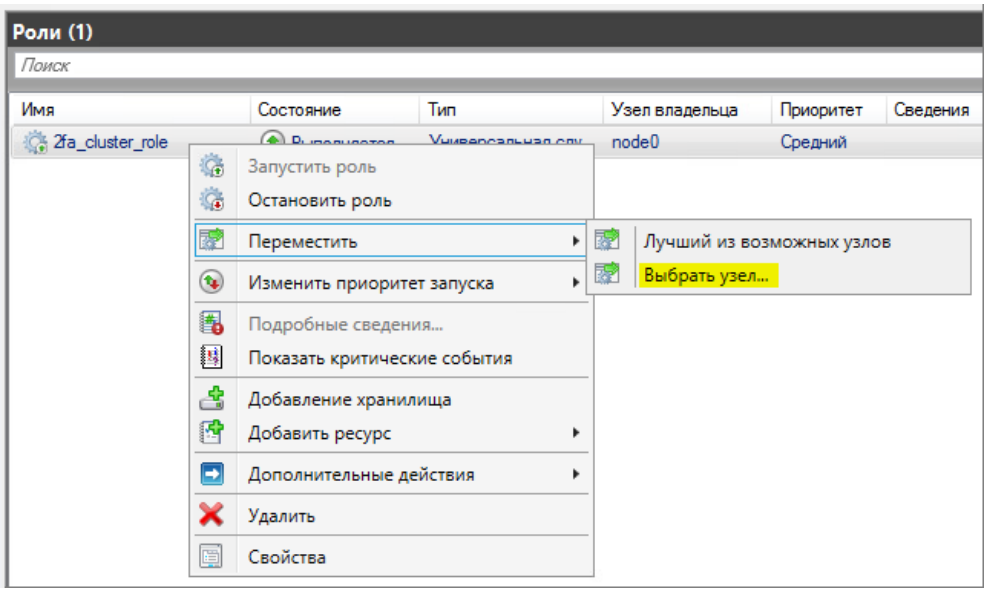

Рисунок 89 - [Диспетчер отказоустойчивого кластера]. Выбор нового узла владельца

Будет открыто окно [Переместить кластерную роль] (см. Рисунок 90). Выберите нужный узел кластера и нажмите кнопку <OK>.

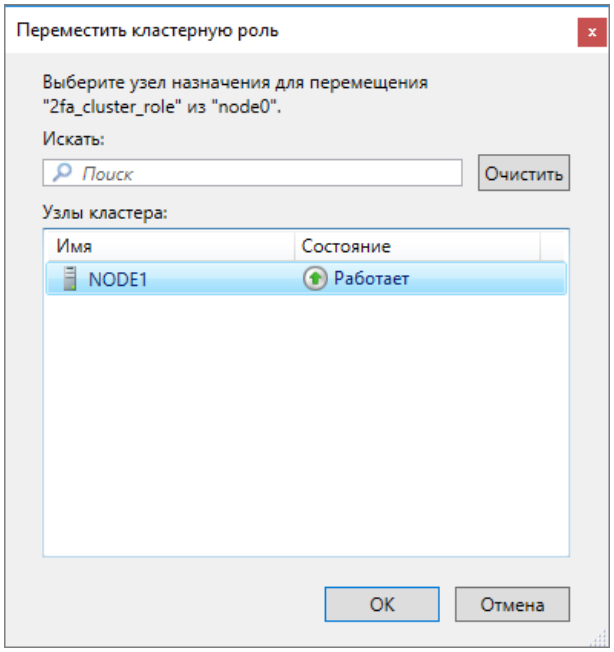

Рисунок 90 – Окно [Переместить кластерную роль]

В случае успешного переключения в окне консоли [Диспетчер отказоустойчивого кластера] в центральной части панели сменится узел владельца - в примере название узла поменялось с `NODE 0` на `NODE 1` (см. Рисунок 91). Ресурсы роли при этом также должны иметь состояние <Оперативный>.

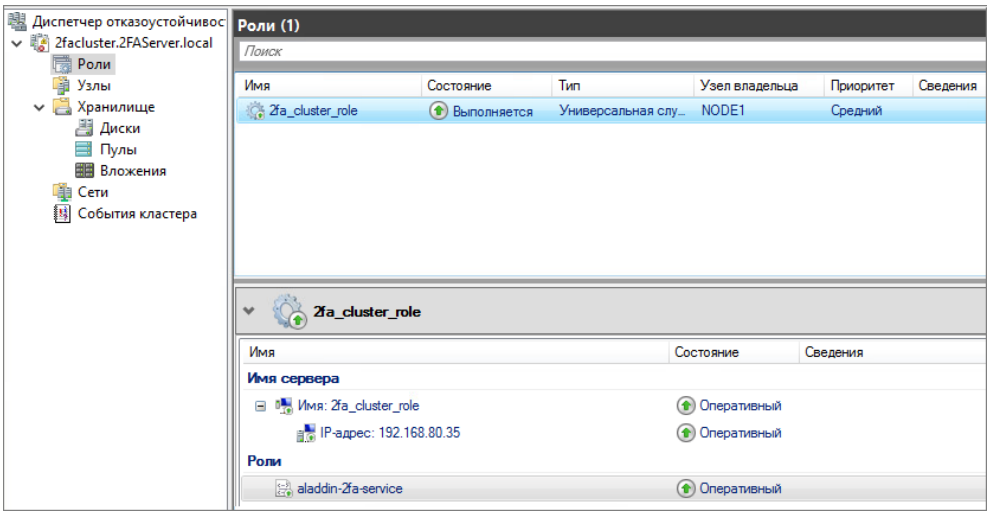

Рисунок 91 - [Диспетчер отказоустойчивого кластера]. Смена узла

3. Так же необходимо проверить работу службы на узле владельца. В случае успешной настройки у службы будет состояние <Выполняется> (см. Рисунок 92).

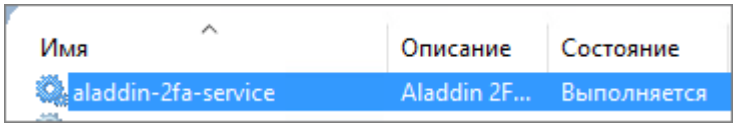

Рисунок 92 – Служба в состояние <Выполняется>

8. Сбор логов

Для сбора логов скопируйте из директории `C:\ProgramData\Aladdin\Aladdin 2FA Service\Logs\aladdin-2fa-service` следующие файлы:

- `main.log`;
- `privateServer.log`;
- `publicServer.log`.

Затем поместите эти файлы в архив и отправьте в техподдержку компании Аладдин.

9. Настройки сервиса для использования Telegram, для передачи второго фактора

9.1 Введение

Сервис Aladdin 2FA поддерживает двухфакторную аутентификацию через сервер Telegram.

Сервер Telegram использует технологию webhook для работы с сервисом Aladdin 2FA.

Webhook – это механизм, который позволяет внешним сервисам принимать уведомления от Telegram и отправлять запросы к нему. Когда пользователь отправляет сообщение в канал или группу, подключенную к определенному вебхуку, сервер Telegram отправляет запрос на этот вебхук. Таким образом можно получать сообщения из Telegram и обрабатывать их в реальном времени.

Техническое окружение:

- установленный дистрибутивом A2FA Service на ОС Windows;
- установленная и настроенная БД (PostgreSQL или MSSQL);
- установленное приложение Telegram на мобильном устройстве.

Для установки и настройки необходимы:

- включенная в лицензию опция телеграм-бота;
- сертификаты для Private Server и сервера телеграм-бота.

Для подключения к Telegram нужны сертификаты, выпущенные либо доверенным УЦ (например - let's encrypt), либо самоподписанным УЦ (например, доменным - MS CA).

Сетевое окружение

Для корректной работы необходимо:

1. Использовать протокол IPv4;
2. Разрешить входящий трафик на сетевом оборудовании из подсетей 149.154.160.0/20 и 91.108.4.0/22 на один из портов (443, 80, 88, 8443), который будет использоваться в сервисе Aladdin 2FA;
3. Зарегистрировать доменное имя для Webhook;
4. Использовать доменный или самоподписанный сертификат;
5. В сертификате должно быть указано зарегистрированное доменное имя в параметре «Common Name»;
6. В сертификате должны быть указаны промежуточные сертификаты для проверки цепочки сертификатов.

9.2 Конфигурация Telegram-бота для сервера A2FA

9.2.1 Регистрация бота в Telegram

Для регистрации бота в Telegram необходимо выполнить следующие действия:

1. Открыть приложение Telegram и найти аккаунт «@BotFather»;
2. Запустить диалог с BotFather, нажав на кнопку «Start»;
3. Ввести команду `/newbot`, чтобы начать процесс создания нового бота;
4. Придумать уникальное имя для бота, которое должно заканчиваться на «_bot»;

5. Выбрать «username» для бота, который будет использоваться как ссылка для доступа к нему. Необходимо убедиться, что оно уникальное и нажать кнопку «Отправить»;
6. После этого в диалоге с BotFather отображается «токен» созданного бота;

> *«Токен» это набор символов, чисел и специальных символов*

7. Добавить описание бота, указав его назначение и основные функции;
8. Добавьте логотип для бота.
9. Выбрать тип бота «приватный». Для изменения типа необходимо:
   - ввести команду `/mybots`;
   - выбрать созданного бота;
   - нажать на кнопку «Bot Settings» -> «Group Privacy» -> «Turn on». Текст параметра должен измениться на «Privacy mod is [enadled](https://core.telegram.org/bots/features#privacy-mode) for ...»;

> *Данная настройка позволяет обращаться к боту только по ссылке*

10. Запретить добавление бота в группы. Для этого необходимо:
    - ввести команду `/mybots`;
    - выбрать созданного бота;
    - нажать кнопку «Allow Groups?». Текст параметра должен измениться на «Groups are currently **disabled** for ...»;
11. Сохранить «токен» бота, который будет использоваться для его аутентификации при взаимодействии сервиса Aladdin 2FA с API Telegram.

> ***Важно!*** *Полученный токен нужно хранить в секрете. Не передавать его 3-м лицам и не хранить в открытом виде*

9.2.2 Настройка параметров сервера A2FA

Настройка параметров Aladdin 2FA сервиса для взаимодействия с серверами Telegram.

Для включения телеграм-бота Aladdin 2FA в конфигурационном файле необходимо добавить следующий блок параметров:

```
tgBotServer:

  externalAddress: https://somednsname.ru #Указывается зарегистрированное доменное имя для Webhook.

address: 192.168.1.10:8443 # Указывается адрес сетевого интерфейса, на котором установлен сервис Aladdin 2FA и порт (443, 80, 88, или 8443) из перечисленных. Если сервис находится за пограничным устройством (сетевым экраном, сетевым балансировщиком и т.д.), допускается указание любого порта, но на пограничном устройстве обязательно должен быть открыт любой из перечисленных портов т.к. сервера Telegram работают только с этими номерами портов.

Tls # Указывается сертификат или контейнер сертификата, который выпускался для зарегистрированного доменного имени. Если сервис Aladdin 2FA находится за пограничным сетевым устройством и это устройство поддерживает создание TLS(TLS v1.2), данный пункт можно не включать, а вся настройка TLS проводится на пограничном устройстве.

pfx:

  pfxContainer: tls/tgBot/localhost_8443.pfx

  pwdContainer: 1234567890

token: 6279835370:TAGMd6JuC8Ts5FAJcB55vNifIbJdxQMEdd4 # Указывается токен, который сгенерировал **BotFather**. осле запуска сервиса данное поле будет заменено полем encryptedToken с зашифрованным токеном.
```

```
timeout: 60

debug: true # Отладочный режим Telegram-бота. При включенном режиме отладки(--verbose) будет записываться отладочная информация бота
```

Для подключения без использования NGINX указать `externalAddress` в разделе `tgBotServer` с портами (test.ru:8443). Порт допустимо указывать в одном из следующих форматах:

- `externalAddress: https://test.ru:8443`;
- `address: 1.1.1.1:8443`.

> *В поле `address` допустимо указывать параметр в виде `address: :8443`*

9.3 Варианты использования TLS для подключения к телеграм-боту

Для подключения к телеграм-боту с использованием TLS доступны следующие варианты настройки:

- с использованием реверс-прокси (см. п. 9.3.1);
- без использования реверс-прокси (см. п. 9.3.2);

9.3.1 Настройка телеграм-бота с реверс-прокси (на примере NGINX)

В случае подключения через NGINX, для защиты соединения будет использован tls сертификат, используемый NGINX. В этом случае, в конфигурационном файле в разделе `tgBotServer` указывать сертификат не нужно.

На рисунке (см. Рисунок 93) приведен пример подключения с имеющимися локациями, необходимо указать не занятые порты и открыть их в системе.

Локация (location) в Nginx — структура в конфигурационном файле, определяющая, какие правила будут применяться к URL и запросам.

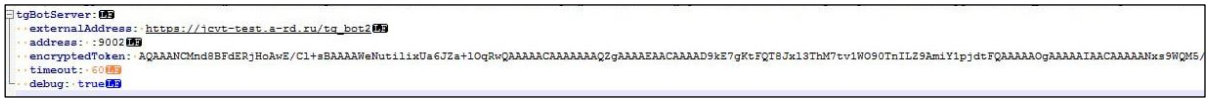

Рисунок 93 – Пример конфигурационного файла с использованием локаций NGINX

9.3.2 Настройка телеграм-бота без реверс-прокси (без NGINX)

В случае подключения без реверс-прокси, для защиты соединения будет использован tls сертификат, указанный в разделе `tgBotServer`. Имеется два способа указания сертификатов:

- с помощью параметра cert: в этом случае, указать путь до сертификата (certificate) и ключа (privateKey) (см. Рисунок 94);
- с помощью pfx: в этом случае, указать путь до pfx-контейнера (pfxContainer) и пароль от него (pwdContainer) (см. Рисунок 95).

> *Доменное имя должно быть зарегистрированным*

Для корректной работы телеграм-бота с использованием самоподписанных сертификатов или выпущенных доверенным УЦ необходимо в конфигурационный файл добавить параметр `externalRootCertificate` с указанием пути до сертификата, который является корневым для сертификата, указанного в параметрах TLS блока tgBotServer.

Рисунок 94 – Пример использования сертификата TLS

Рисунок 95 – Пример использования pfx-контейнера

9.3.3 Создание самоподписанного сертификата

Для создания самоподписанного сертификата необходимо выполнить следующие действия:

1. Открыть консоль управления;
2. Перейти в раздел "Сертификаты (локальный компьютер)" – "Сертификаты";
3. Открыть контекстное меню и нажать на кнопку "Все задачи" – "Запросить новый сертификат" (см. Рисунок 96);

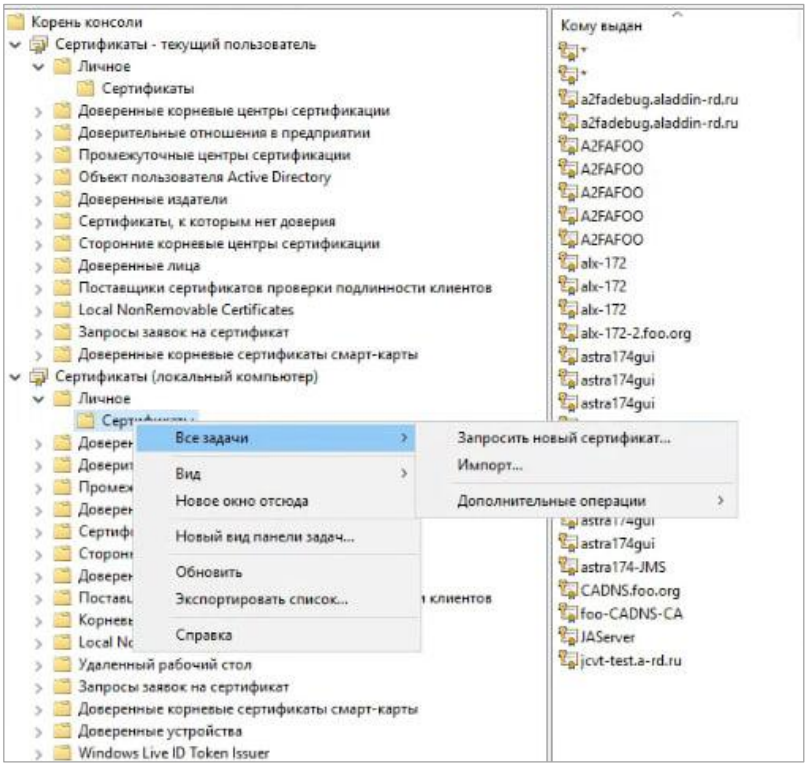

Рисунок 96 – Консоль управления

4. В открывшемся окне нажать кнопку "Далее" (см. Рисунок 97);

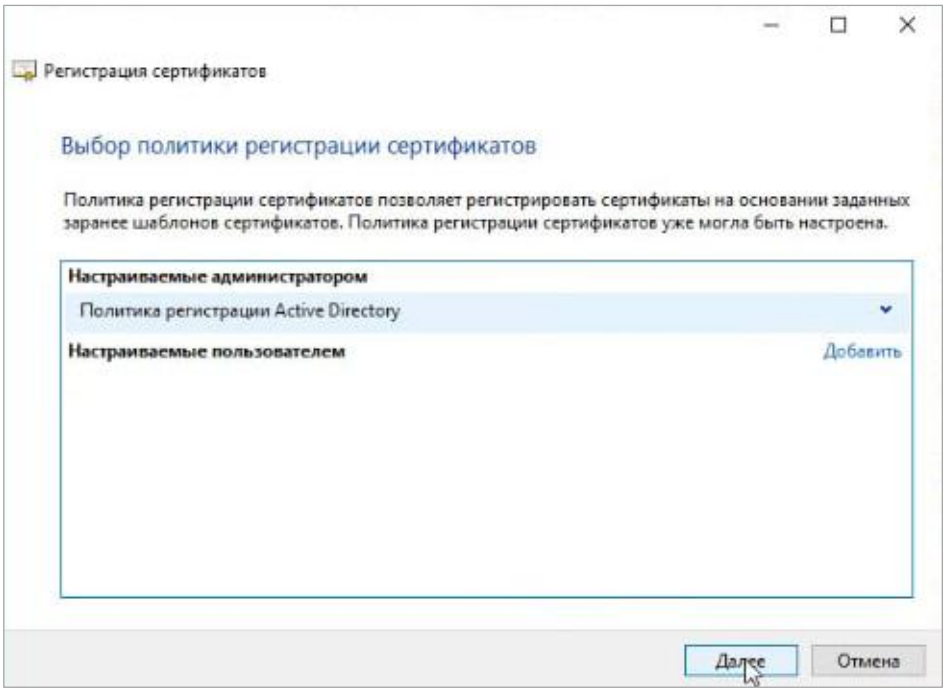

Рисунок 97 – Окно «Регистрация сертификатов»

5. Далее в окне с шаблонами сертификатов выбрать нужный сертификат и нажать на предупреждение, необходимо задать тип и общее имя (см. Рисунок 98);
6. Нажать кнопку "Добавить";

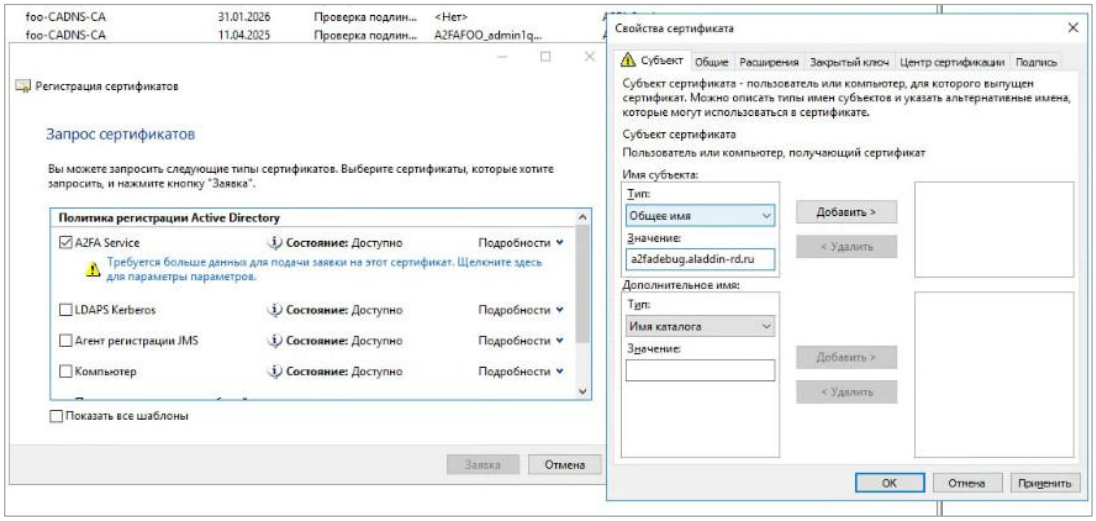

Рисунок 98 – Окно «Свойства сертификата»

7. Перейти во вкладку "Общее" и указать имя для контейнера (см. Рисунок 99);
8. Нажать кнопку "ОК";

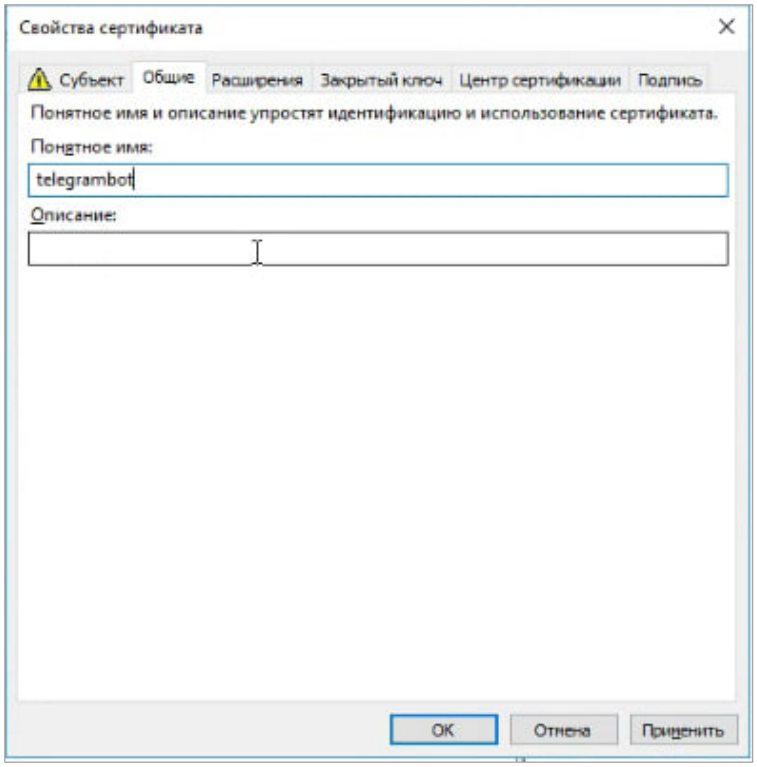

Рисунок 99 – Окно «Свойства сертификата»

9. После выполненных действий сертификат отображается в списке сертификатов (см. Рисунок 100);

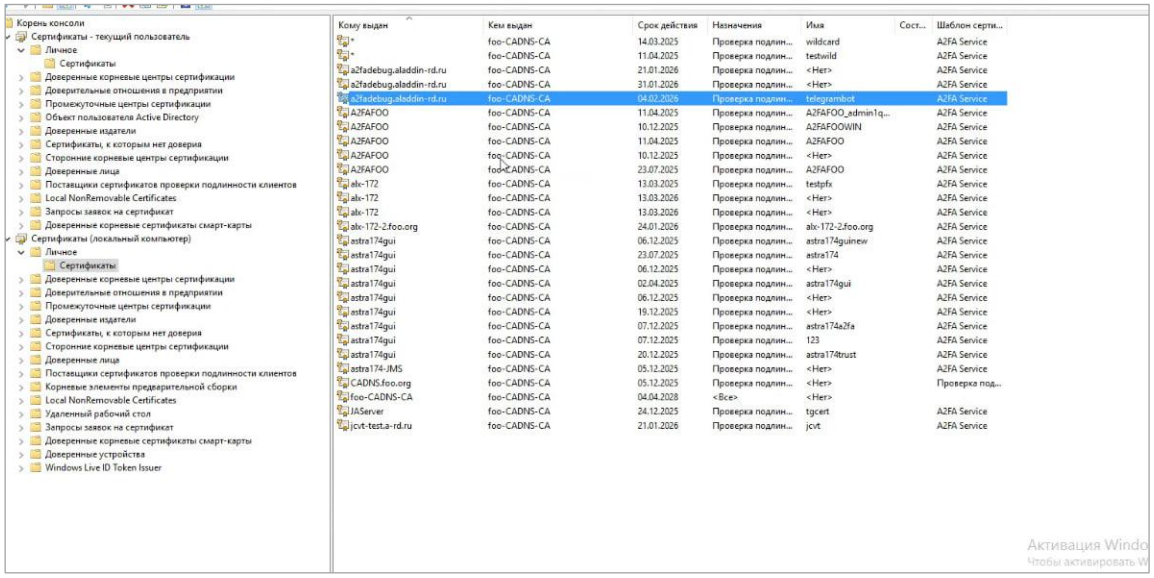

Рисунок 100– Отображение зарегистрированного сертификата в списке сертификатов

10. У добавленного сертификата открыть контекстное меню и нажать кнопку "Экспорт";
11. Нажать "Да, экспортировать закрытый ключ" (см. Рисунок 101);

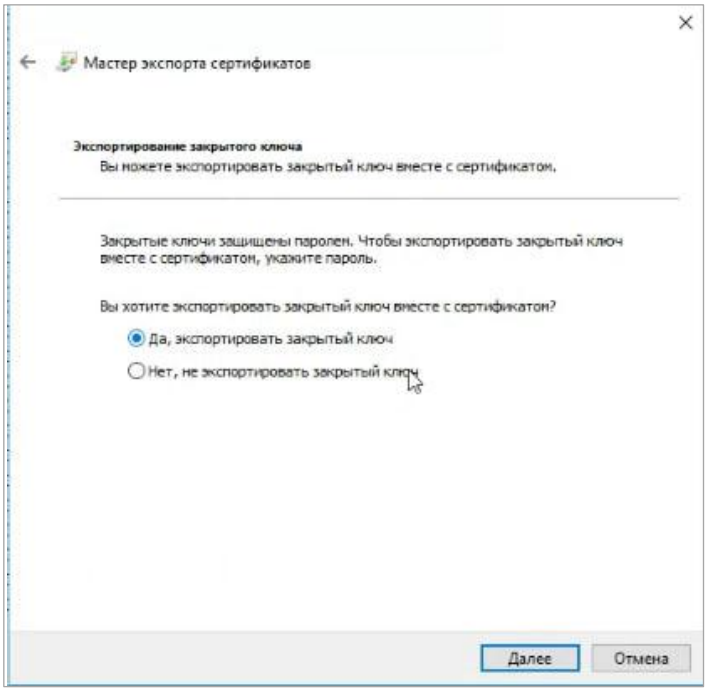

Рисунок 101– Окно «Мастер экспорта сертификатов»

12. Выбрать формат экспортируемого файла;
13. Задать пароль и его подтверждение;
14. Указать имя файла;
15. Нажать кнопку "Готово" (см. Рисунок 102);

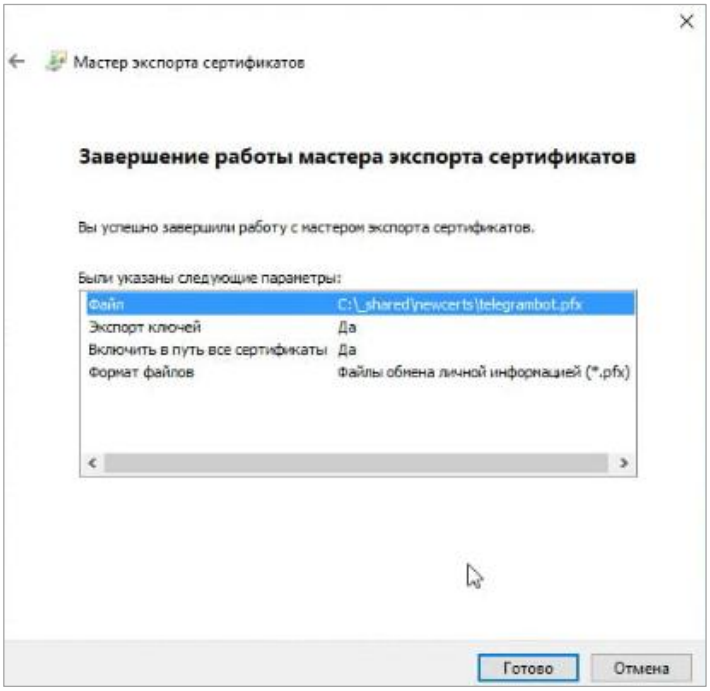

Рисунок 102– Окно «Свойства сертификата»

16. Нажать кнопку "ОК" для закрытия уведомления об успешном импорте (см. Рисунок 103).

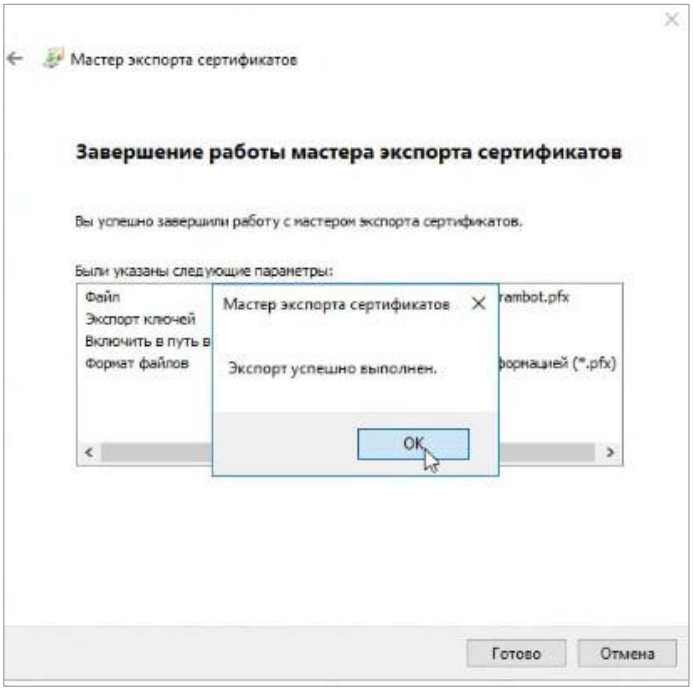

Рисунок 103– Уведомление об успешном импорте сертификата

Также необходим корневой сертификат, которым был подписан сертификат для телеграм-бота.

Для того, чтобы телеграм-бот работал необходимо в external указать корневой сертификат и перенести оба сертификата на ВМ, на которой установлен сервер Aladdin 2FA Service и телеграм-бот.

Далее необходимо добавить в конфигурационный файл в раздел настройки телеграм-бота следующие параметры:

```
tgBotServer:
  externalAddress: https://a2fadebug.aladdin-rd.ru:8443
  address: :8443
  token: klkmhhmkhmfgk;mhtk;rklty5i6j54khr065
  externalRootCertificate: /home/test/tgcert.crt
  tls:
    cert:
      certificate: /home/test/tgcert.crt
      privateKey: /home/test/tgkey.key
  timeout: 60
  debug: true
```

9.3.4 Вариант с использованием PFX

Для того, чтобы пользоваться pfx-контейнером необходимо в конфигурационном файле в разделе настройки телеграм-бота указать корневой сертификат:

```
tgBotServer:
  externalAddress: https://a2fadebug.aladdin-rd.ru:8443
  address: :8443
  token: klkmhhmkhmfgk;mhtk;rklty5i6j54khr065
  externalRootCertificate: /home/test/tgcert.crt
  tls:
    pfx:
      pfxContainer: /home/test/tgpfx.pfx
      pwdContainer: admin1q2W
  timeout: 60
  debug: true
```

9.4 Диагностика

Корректность настроек можно проверить способами, описанными ниже.

9.4.1 Проверка соединения

При возникновении ряда ошибок необходимо выполнить диагностику телеграм-бота для этого необходимо:

1. Перейти на тестовую страницу с помощью ссылки, которая указана в разделе `tgBotServer` в параметре `externalAddress`, к которой добавляется /test;
2. В результате могут быть отражены следующие ошибки:
   - "Не удается получить доступ к сайту" – при отсутствии соединения, неправильных настройках сети и т.д.;
   - "200, OK" – соединение установлено корректно;
   - "404, not found" – неверно указана ссылка на сервис телеграм-бота;
   - "Предупреждение: Вероятная угроза безопасности" – при использовании самоподписанного или недоверенного сертификата правильно ли указан путь до этого сертификата. При подтверждении перехода должен вернуться ответ "OK";
   - "525 – SSL Handshake Failed" – при использовании невалидного tls-сертификата.

Для корректной работы телеграм-бота с использованием самоподписанных сертификатов или выпущенных доверенным УЦ необходимо в конфигурационный файл добавить параметр `externalRootCertificate` с указанием пути до сертификата, который является корневым для сертификата, указанного в параметрах TLS блока tgBotServer.

9.4.2 Проверка настройки TLS

Для того что бы проверить что настройки TLS Telegram-бота необходимо выполнить следующие шаги:

1. Включить в настройках «tgBotServer» параметр «debug: true»;
2. Запустить сервис с параметром –verbose в консоли и убедиться, что сервис успешно запущен;
3. В консоли найти строчку:

```
Endpoint: setWebhook, params: map[allowed_updates:null
url:https://somednsname.ru/1c48863afe7f7c6ea22724f23c5f5a0fed2aa86ec3459189af962a1faca
45b63]`
```

где `https://somednsname.ru/1c48863afe7f7c6ea22724f23c5f5a0fed2aa86ec3459189af962a1faca45b6` адрес Webhook.

4. Скопировать адрес Webhook
5. Открыть бот разработчиков Telegram, расположенный по адресу: https://t.me/CanOfWormsBot;
6. Ввести команду `/start` и следовать инструкциям (бот проверит ваш сертифкат).

Подробное описание запуска бота в мобильном приложении Telegram приведено в документе «Aladdin 2FA. Руководство пользователя» [1], которое доступно для загрузки на официальном сайте компания «Аладдин Р. Д.».

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. Руководство пользователя

2 JaCarta Management System v3.7. Руководство администратора. Часть 1. Установка и настройка,
JaCarta Management System 4LX. Руководство администратора. Часть 1. Установка и настройка

3 JaCarta Management System v3.7. Руководство администратора. Часть 2. Функции управления,
JaCarta Management System 4LX. Руководство администратора. Часть 2. Функции управления

4 JaCarta Management System v3.7. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS),
JaCarta Management System 4LX. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS),

5 JaCarta Management System v3.7. Руководство пользователя,
JaCarta Management System 4LX. Руководство пользователя

Регистрация изменений

Версия документа	Изменения
1.3.5	Добавлены: • Пункт 2.3.2.1 WebSocket соединение PUSH-уведомления; Изменено: • Схема сетевого взаимодействия – добавлен WebSocket и TG-сервис; • Описание сценария PUSH-уведомление, в связи с добавлением WebSocket соединения;
1.3.1	Добавлен п. 8 Сбор логов
1.3.1	Обновлены разделы 3.1, 5.2
1.3.0	Добавлен п. 3.2.5 Скрипт для создания базы данных под MS SQL
1.3.0	Добавлен п. 4.4 План обслуживания
1.2.0	Добавлен п. 7.1 Подготовка кластера к развертыванию роли General Service
1.2.0	Обновлено описание раздела 4. Управление из сервиса JAS; добавлен раздел 1. О документе
1.2.0	Добавлен п. 4.2 Обновление сертификата; п. 4.3 Перенастройка базы данных на работу с TLS
1.2.0	Добавлен п. 3.3.3 Настройка Microsoft SQL Server для работы с TLS
1.2.0	Добавлены п. 7.2 Настройка роли General Service со службой A2FA в отказоустойчивом кластере; п. 7.3 Проверка работы настроенной роли
1.2.0	Обновление версии документа в связи с релизом новой версии 1.2.0 Aladdin 2FA
1.0	Исходная версия документа для Aladdin 2FA версии 1.0.0