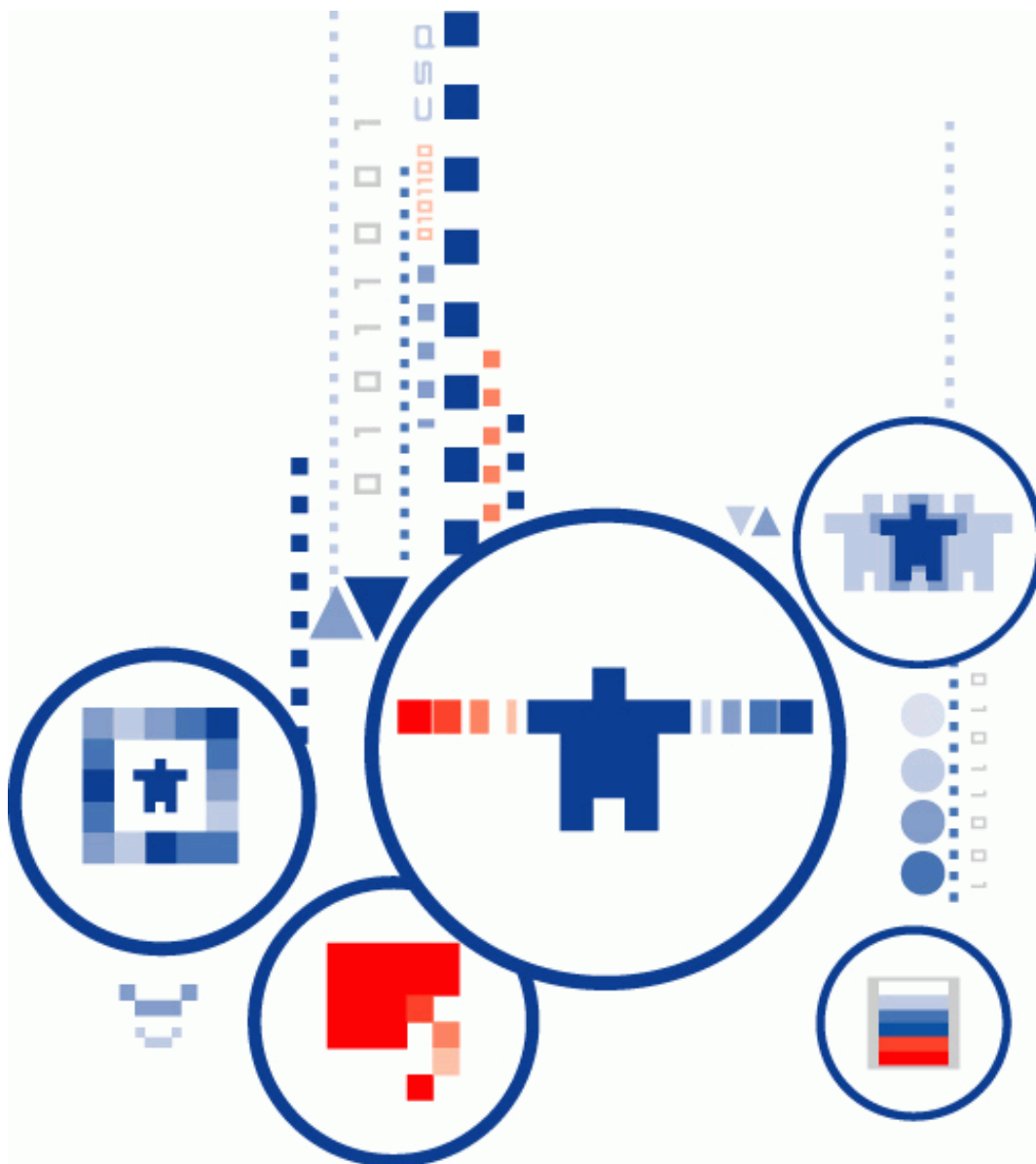




Программный комплекс

«КриптоПро Архив»

Руководство администратора Windows

ЖТЯИ.00117-01 92 03

Содержание

1 Общая информация	5
1.1 Архитектура	5
1.2 Системные требования	7
2 Установка	8
2.1 PostgreSQL	8
2.2 RabbitMQ	9
2.2.1 Erlang	10
2.2.2 RabbitMQ	10
2.2.3 Плагин Delayed Message	11
2.3 КriptoПро CSP	12
2.4 Microsoft Hosting Bundle	13
2.5 КriptoПро Архив	13
3 Настройка	15
3.1 Настройка RabbitMQ	15
3.2 Настройка PostgreSQL	19
3.2.1 Основная настройка	19
3.2.2 Сохранение подписанных документов (ранее Архив УЦ)	25
3.3 Настройка Oracle Database 12c Release 2	26
3.3.1 Основная настройка	26
3.3.2 Сохранение подписанных документов (ранее Архив УЦ)	27
3.4 Ввод лицензии	29
3.5 Настройка admin-api и client-api	31
3.5.1 Добавление серверного сертификата	31
3.5.2 Добавление приложения IIS	34
3.5.3 Настройка максимального размера запроса	38
3.5.4 Настройка брандмауэра	39
3.5.5 Установка сертификата суперпользователя	42

3.5.6 Конфигурационный файл	43
3.6 Настройка frontend	46
3.6.1 Добавление приложения IIS	46
3.6.2 Конфигурационный файл.....	48
3.7 Настройка signature-updater	49
3.7.1 Добавление службы	49
3.7.2 Конфигурационный файл.....	50
3.8 Настройка consumer.....	55
3.8.1 Добавление службы	55
3.8.2 Конфигурационный файл.....	55
4 Обновление.....	60
4.1 Обновление базы данных PostgreSQL	60
4.2 Обновление базы данных Oracle Database.....	61
5 Администрирование	63
5.1 Настройка хранилищ и информационных систем	63
5.1.1 Общее описание	63
5.1.2 Первичная настройка	64
5.1.3 Права и роли.....	67
5.2 Настройка дополнительных служб УЦ	69
5.3 Сохранение подписанных документов (ранее Архив УЦ)	72
5.4 Повторная обработка контейнеров.....	75
5.5 Управление суперпользователями.....	77

Используемые сокращения и обозначения

CAdES	Расширенная версия стандарта электронной подписи CMS (CMS Advanced Electronic Signatures).
OCSP	Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol).
TLS	Протокол защиты транспортного уровня.
БД	База данных.
ИС	Информационная система.
ОС	Операционная система.
ОЗУ	Оперативное запоминающее устройство.
ПО	Программное обеспечение.
СУБД	Система управления базами данных.
СХД	Система хранения данных.
ЭП	Электронная подпись.

1 Общая информация

В данном разделе содержатся архитектура решения и системные требования.

1.1 Архитектура

КriptoПро Архив (далее — Архив) состоит из следующих компонентов:

Компонент	Назначение
admin-api	Административный API для настройки Архива. Основные функции: регистрация хранилищ, информационных систем, мониторинг работы Архива.
client-api	API для использования информационными системами. Основные функции: создание, изменение и удаление контейнеров, скачивание усовершенствованных подписей.
signature-updater	Усовершенствование подписей до формата CAdES-A. Автоматическое повторное усовершенствование подписей перед истечением срока их действия.
frontend	Веб-интерфейс администратора.
consumer	Компонент предназначен для выполнения ряда опциональных действий: сохранение подписанных документов в СХД, отправка уведомлений о результате усовершенствования подписей, выполнение плагинов.
config	Централизованная настройка компонентов Архива на сервере.

Архив можно развернуть множеством способов. Ниже кратко описаны типовые: минимальная конфигурация на одном сервере (без использования очереди) и расширенная на одном сервере. Компоненты можно располагать на разных

серверах. Базу данных и очередь можно рассматривать как соответствующие кластеры.

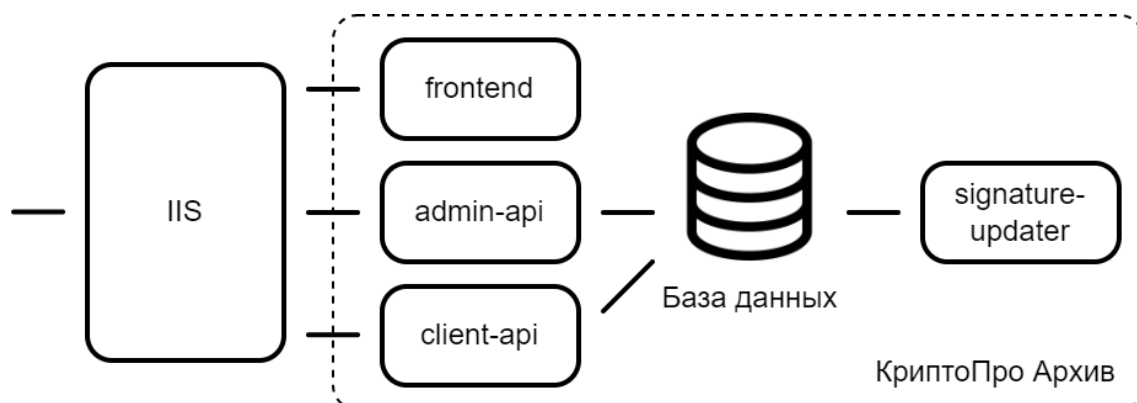


Рисунок 1. Минимальная конфигурация Архива на одном сервере. Линиями обозначены двусторонние взаимодействия компонентов.

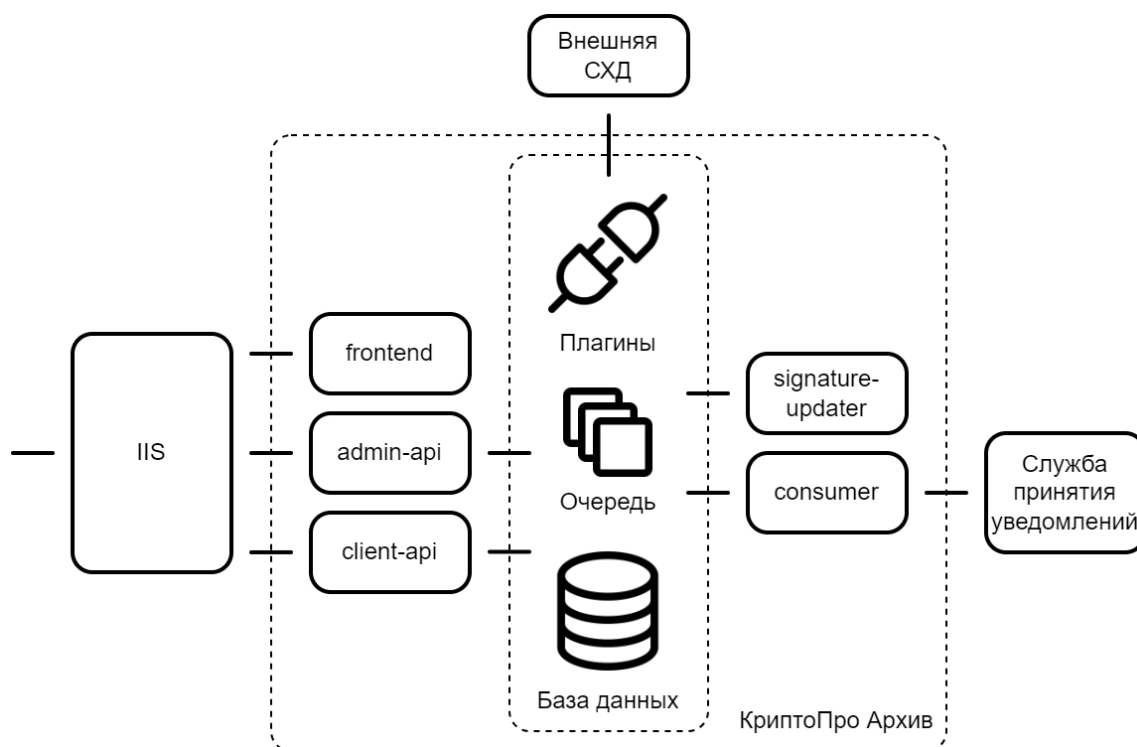


Рисунок 2. Расширенная конфигурация Архива на одном сервере. Линиями обозначены двусторонние взаимодействия компонентов. Для простоты очередь, база данных и плагины объединены в единый блок зависимостей, так как к ним могут обращаться все компоненты.

Основное отличие между конфигурациями — наличие очереди, к которой имеют доступ все компоненты, кроме frontend. Наличие очереди позволяет пользоваться дополнительной функциональностью: сохранение подписанных документов во внешнюю СХД, отправка HTTP-уведомлений с результатом усовершенствования, использование механизма плагинов. Взаимодействие с

ЖТЯИ.00117-01 92 03. КристоПро Архив. Руководство администратора Windows внешней СХД и HTTP-сервером для принятия уведомлений, а также выполнение плагинов осуществляет consumer.

1.2 Системные требования

Поддерживаемые ОС	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
Минимальный объём ОЗУ	8 ГБ
Поддерживаемые СУБД	• PostgreSQL 11 и выше • Oracle Database 12c Release 2
Поддерживаемые очереди (при использовании компонента consumer)	• RabbitMQ 3.8–3.13

2 Установка

В данном разделе описана полная установка КриптоПро Архив.

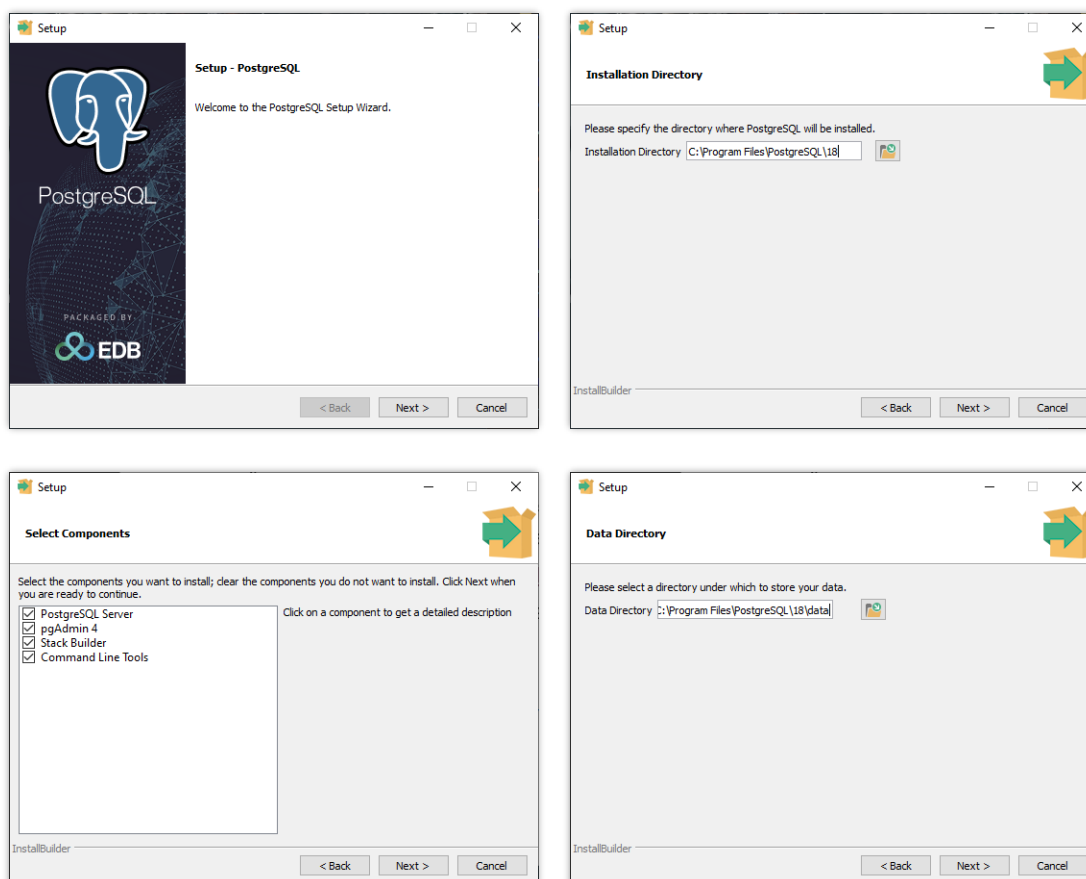
Предполагается, что на сервере уже установлены службы IIS.

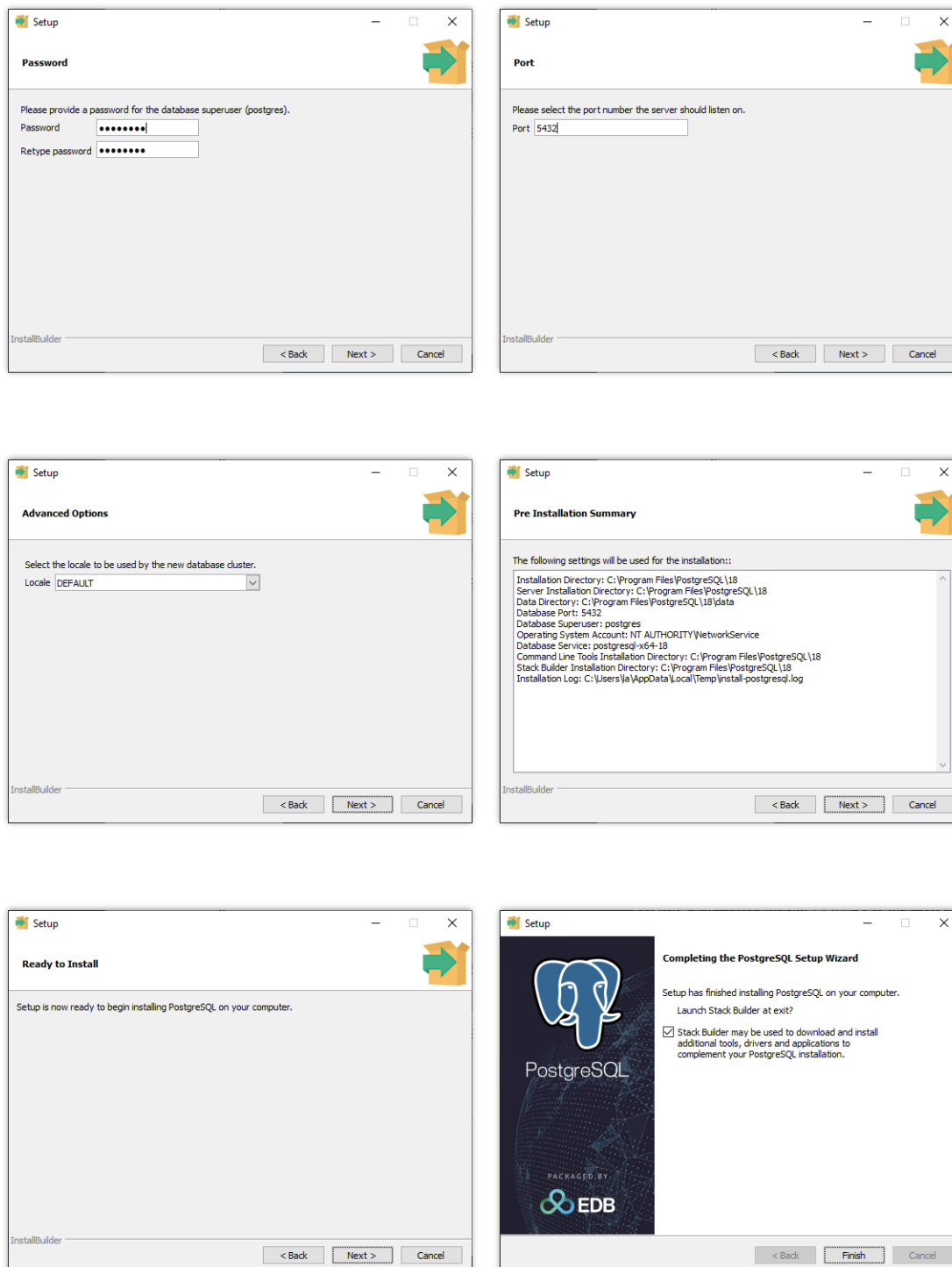
ВАЖНО

Не проводите установку от лица администратора сервера (пользователь Администратор). Создайте пользователя с правами администратора и выполните установку от его лица.

2.1 PostgreSQL

Если у Вас уже установлена одна из поддерживаемых СУБД, пропустите этот шаг. В дистрибутив Архива вложен PostgreSQL версии 18.3. От лица администратора запустите файл postgresql-18.3-2-windows-x64.exe из дистрибутива. В дистрибутив PostgreSQL включена графическая оболочка pgAdmin 4 и утилита Stack Builder. Необходимость этих компонентов за рамками данной инструкции и зависит от Ваших требований. Следуйте инструкциям. Ниже иллюстрация процесса установки.





Установка PostgreSQL завершена.

2.2 RabbitMQ

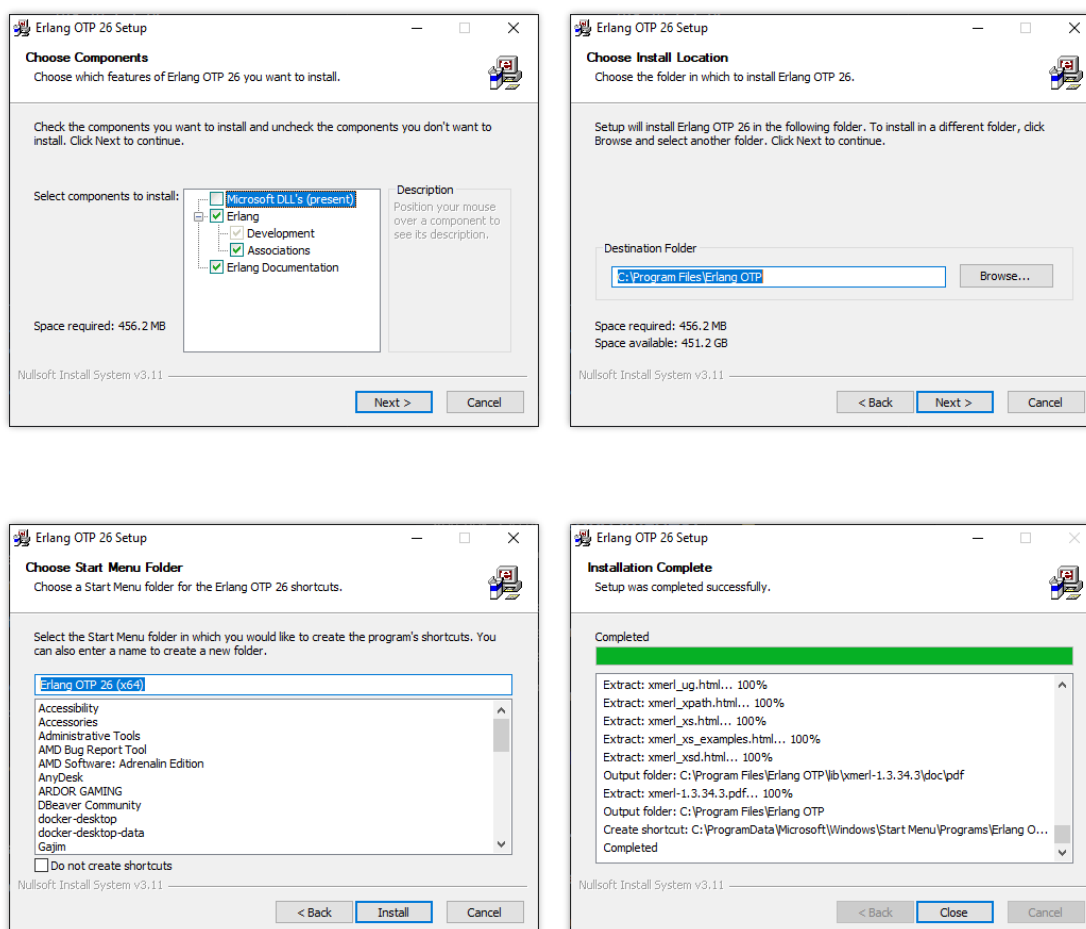
В дистрибутив Архива вложен RabbitMQ версии 3.13.7 со всеми зависимостями, необходимыми для работы Архива.

ВАЖНО

Если Вы не планируете использовать функциональность компонента consumer, RabbitMQ можно не устанавливать. В этом случае этот подраздел можно пропустить.

2.2.1 Erlang

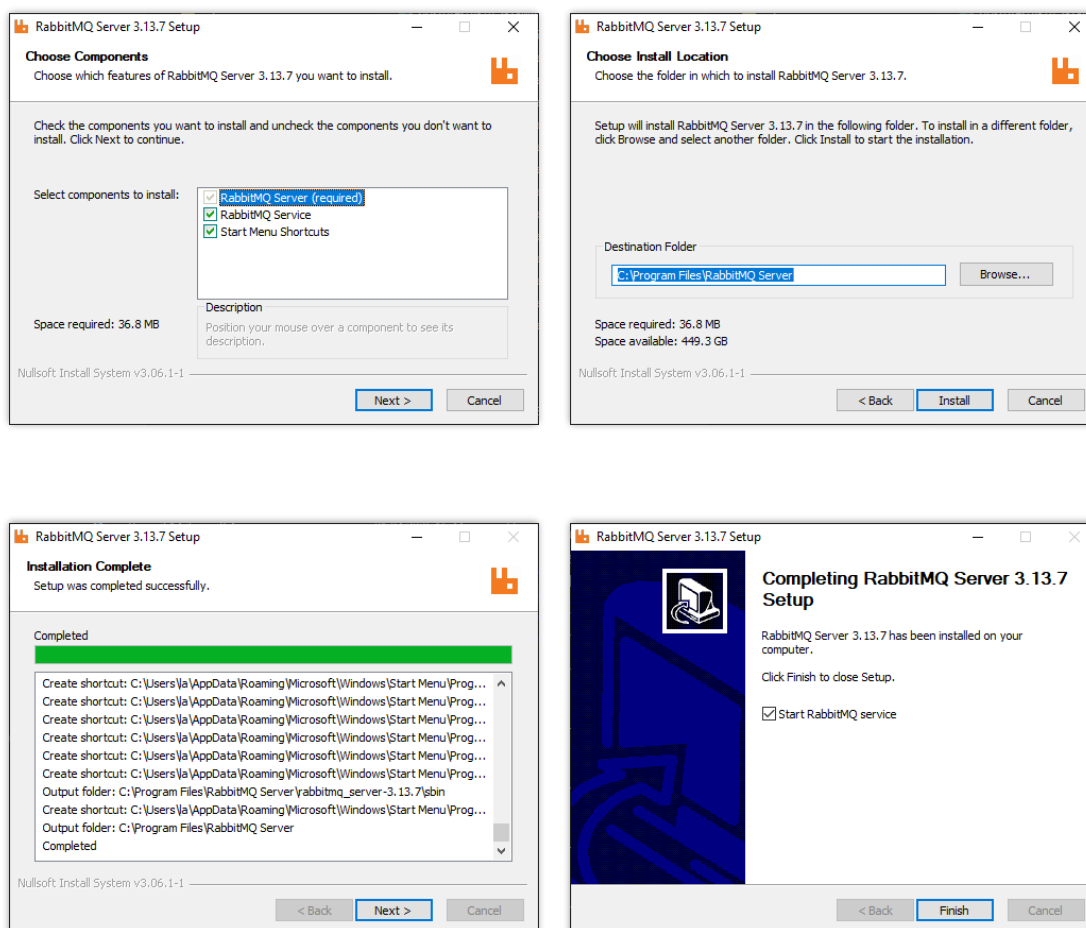
От лица администратора запустите файл `otp_win64_26.2.5.18.exe`. Следуйте инструкциям.



Erlang установлен.

2.2.2 RabbitMQ

От лица администратора запустите файл `rabbitmq-server-3.13.7.exe`. Следуйте инструкциям.



RabbitMQ установлен.

2.2.3 Плагин Delayed Message

Переместите файл `rabbitmq_delayed_message_exchange-3.13.0.ez` в папку `C:\Program Files\RabbitMQ Server\rabbitmq_server-3.13.7\plugins`. От лица администратора выполните три команды в PowerShell:

```
cd 'C:\Program Files\RabbitMQ Server\rabbitmq_server-3.13.7\sbin\'
.\rabbitmq-plugins.bat enable rabbitmq_delayed_message_exchange
.\rabbitmq-plugins.bat enable rabbitmq_management
```

Успешный вывод двух последних команд выглядит примерно так:

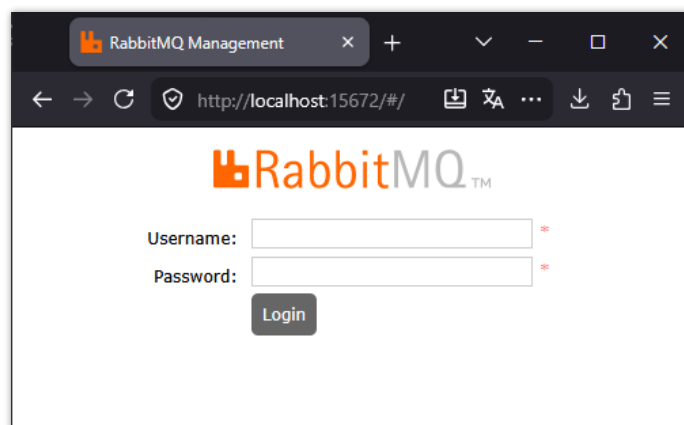
```
Enabling plugins on node rabbit@server_name:
rabbitmq_management
The following plugins have been configured:
  rabbitmq_delayed_message_exchange
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_web_dispatch
Applying plugin configuration to rabbit@server_name...
The following plugins have been enabled:
```

```
rabbitmq_management  
rabbitmq_management_agent  
rabbitmq_web_dispatch
```

set 4 plugins.

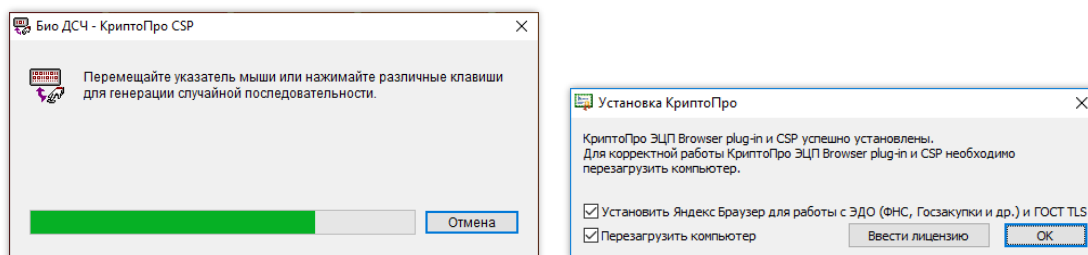
Offline change; changes will take effect at broker restart.

Перезапустите RabbitMQ Server через программу «Службы» от лица администратора. Для проверки работоспособности можно перейти на сайт <http://localhost:15672>. В случае успеха откроется панель управления RabbitMQ:



2.3 КриптоПро CSP

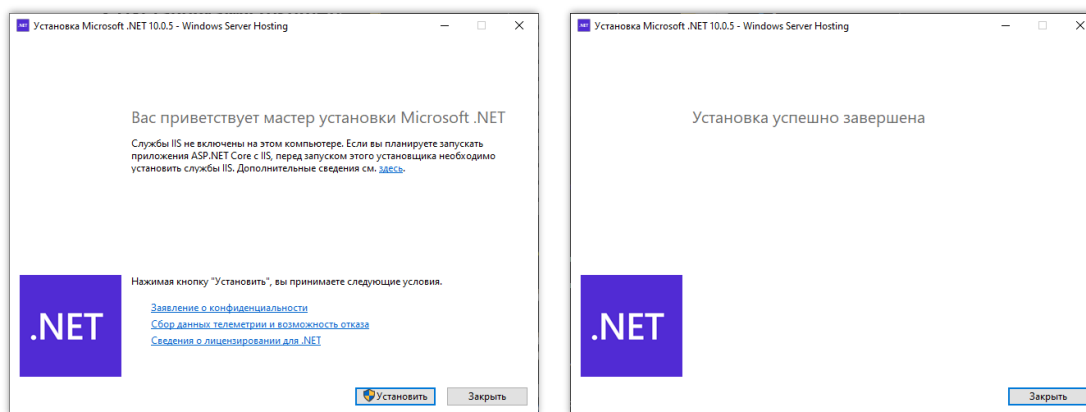
Скачайте актуальную версию КриптоПро CSP с официального сайта <https://cryptopro.ru/products/csp>. Запустите скачанный установочный файл от имени администратора. Следуйте инструкциям по установке.



Установка КриптоПро CSP завершена.

2.4 Microsoft Hosting Bundle

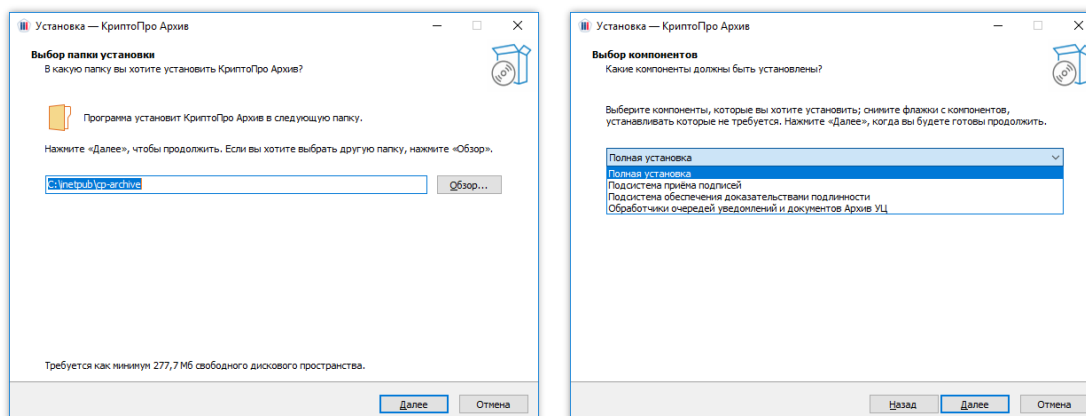
Для работы Архива через веб-сервер IIS необходимо установить Microsoft Hosting Bundle. Запустите файл `dotnet-hosting-10.0.5-win.exe` из дистрибутива. Следуйте инструкциям по установке.



Установка Microsoft Hosting Bundle завершена.

2.5 КристоПро Архив

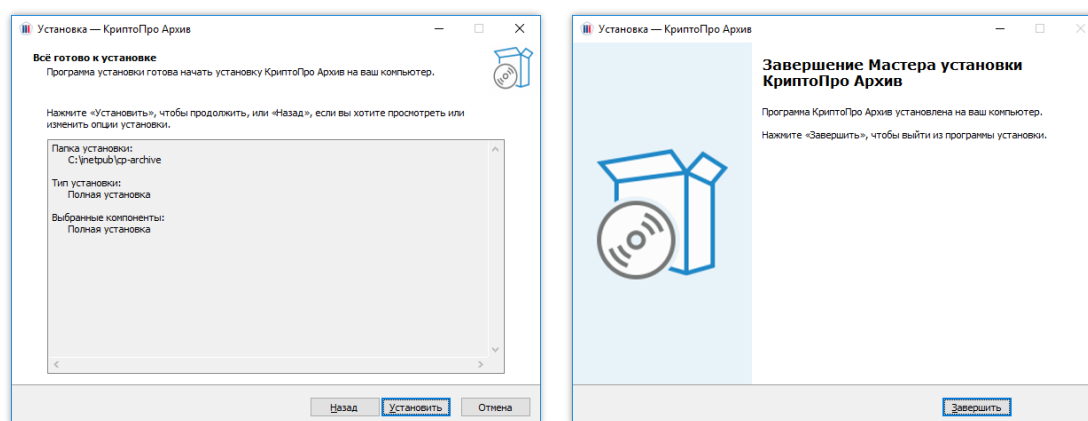
Запустите файл `cp-archive_<version>_win-x64.exe` из дистрибутива, где `<version>` — версия дистрибутива. Появится окно:



Возможен выбор компонентов для установки. Соответствие между названиями вариантов установки и набором устанавливаемых компонентов приведено в таблице (программа `config` будет установлена во всех сценариях):

Вариант	Набор компонентов
Полная установка	Все доступные компоненты
Подсистема приёма подписей	• admin-api • client-api • frontend
Подсистема обеспечения доказательств подлинности	• signature-updater
Обработчики очередей	• consumer

Выберите подходящий вариант и нажмите «Далее».



Установка Архива завершена.

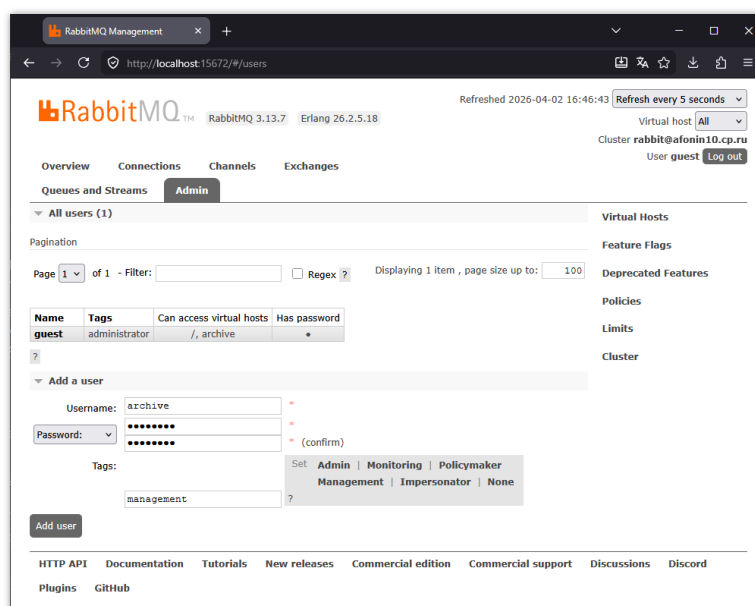
3 Настройка

3.1 Настройка RabbitMQ

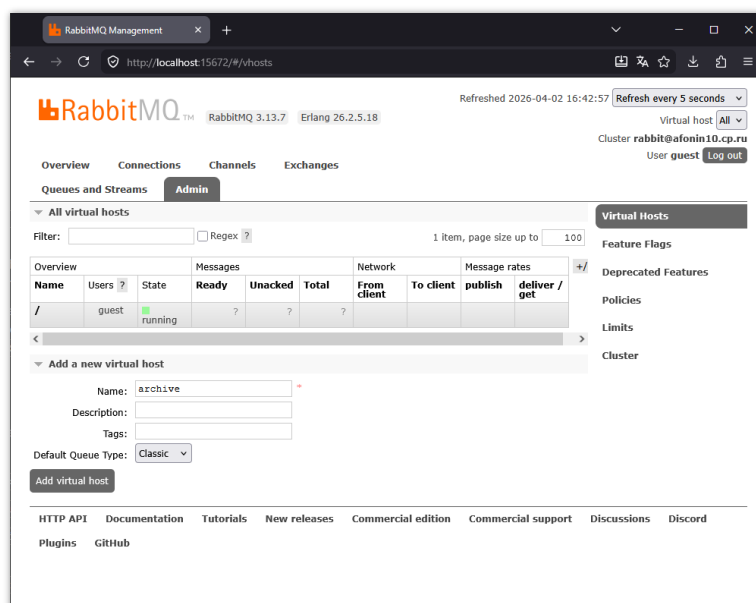
Настройка RabbitMQ заключается в создании пользователя, от лица которого Архив будет подключаться к RabbitMQ, и необходимых очередей и обменников.

Откройте панель управления RabbitMQ по адресу <http://localhost:15672>. Зайдите с учётными данными пользователя guest, пароль «guest». Перейдите в раздел «Admin».

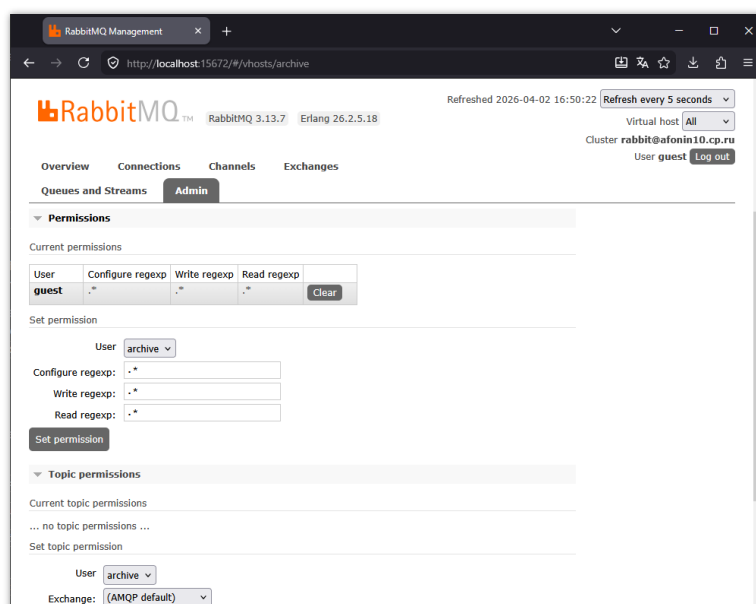
Добавьте пользователя archive, от лица которого Архив будет подключаться к RabbitMQ. Опционально установите для этого пользователя тэг «management», чтобы Архив мог просматривать состояния очередей. Нажмите «Add user».



Перейдите в раздел «Virtual Hosts». Создайте виртуальный хост «archive», к которому будет подключаться Архив.

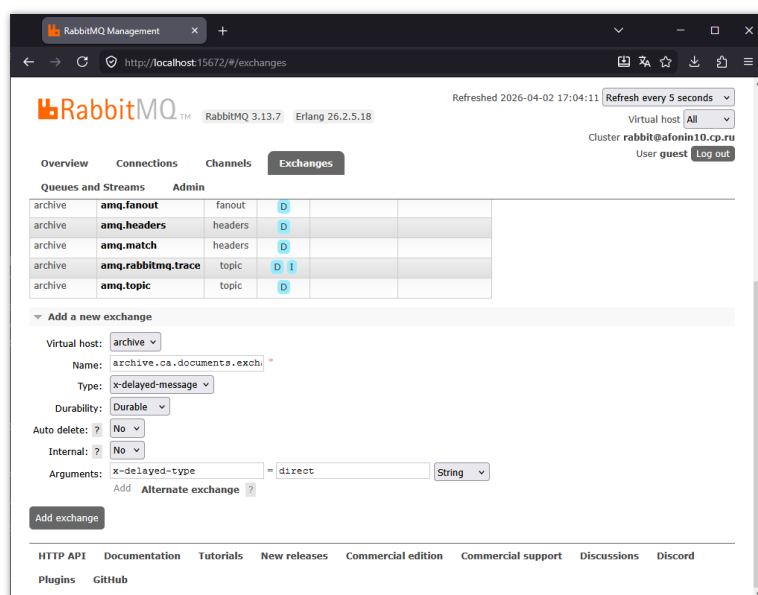


Нажмите на имя созданного виртуального хоста. Прокрутите до раздела «Permissions». В выпадающем меню «User» выберите пользователя «archive» и нажмите «Set permission»:



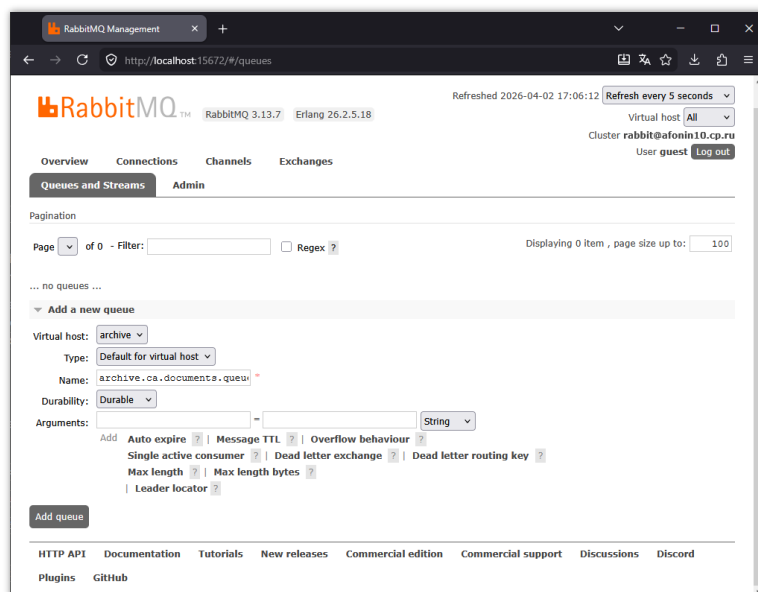
На этом создание пользователя завершено. Перейдите в раздел «Exchanges», прокрутите до «Add a new exchange». Далее создайте 4 обменника:

Имя поля	Значение
Name	- archive.ca.documents.exchange - archive.notifications.exchange - archive.signatures.exchange - archive.reports.requests.exchange (необходимо создать все 4 обменника)
Virtual host	archive
Type	x-delayed-message
Durability	Durable
Auto delete	No
Internal	No
Arguments	x-delayed-type=direct



Перейдите в раздел «Queues and Streams» и создайте 4 очереди:

Имя поля	Значение
Virtual host	archive
Type	Default for virtual host
Name	- archive.ca.documents.queue - archive.notifications.queue - archive.signatures.queue - archive.reports.requests.queue (необходимо создать все 4 очереди)
Durability	Durable
Arguments	



Настройка RabbitMQ завершена.

3.2 Настройка PostgreSQL

3.2.1 Основная настройка

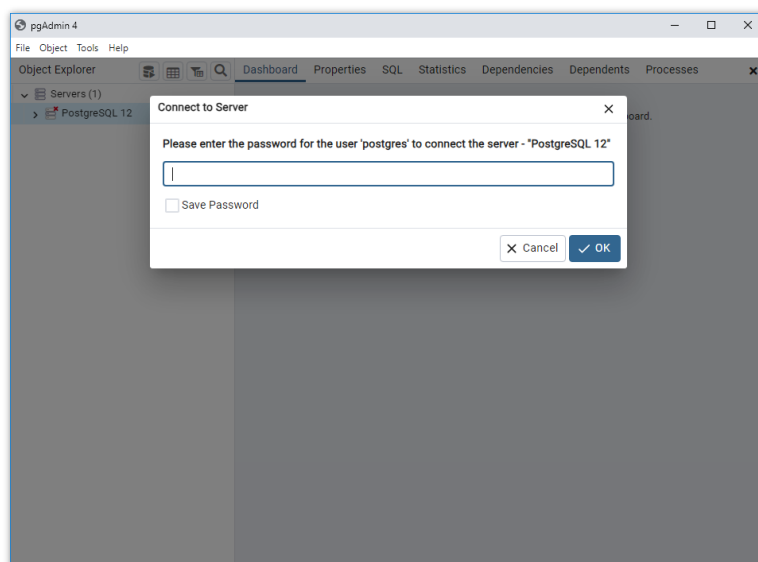
Настройка PostgreSQL заключается в создании пользователя, от лица которого Архив будет подключаться к БД, и самой БД. Предполагается, что программы установлены по стандартным путям, как указано в инструкциях по установке. В противном случае в примерах ниже заменить эти пути на соответствующие. Проводить настройку можно с использованием любого клиента PostgreSQL. Ниже используется pgAdmin 4.

Замечание: ниже описано создание пользователя и базы данных, владельцем которой является созданный пользователь. Если такого ограничения недостаточно с точки зрения безопасности, пользователя можно не делать владельцем базы данных. В таком случае минимальные права, требуемые пользователю базы данных для работы с КристоПро Архив:

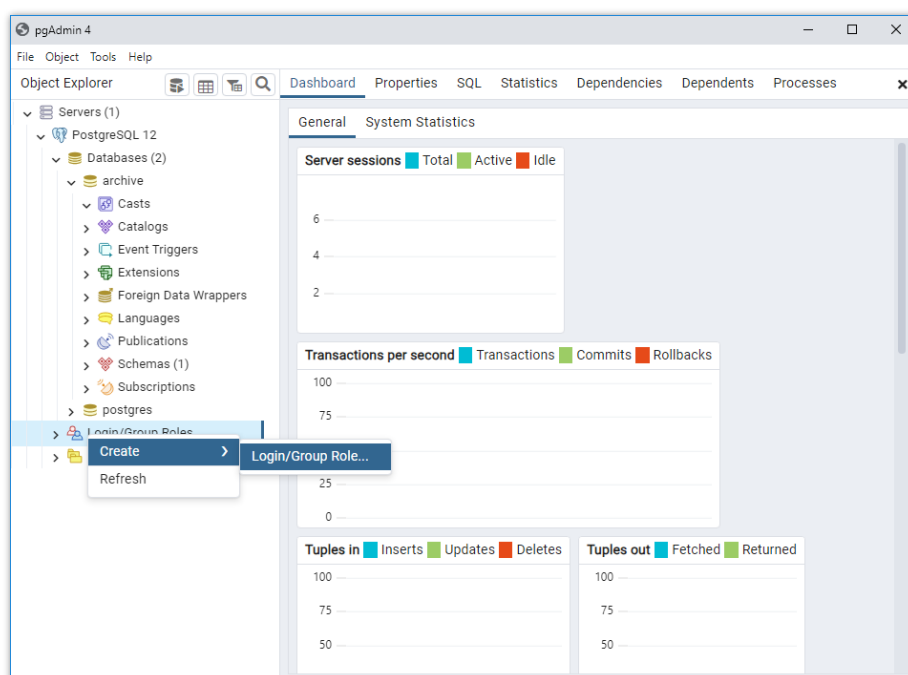
- На каждую таблицу права INSERT, SELECT, UPDATE, DELETE.
- На хранимые функции право EXECUTE.

Замечание: настоятельно рекомендуется производить резервное копирование всех создаваемых баз данных.

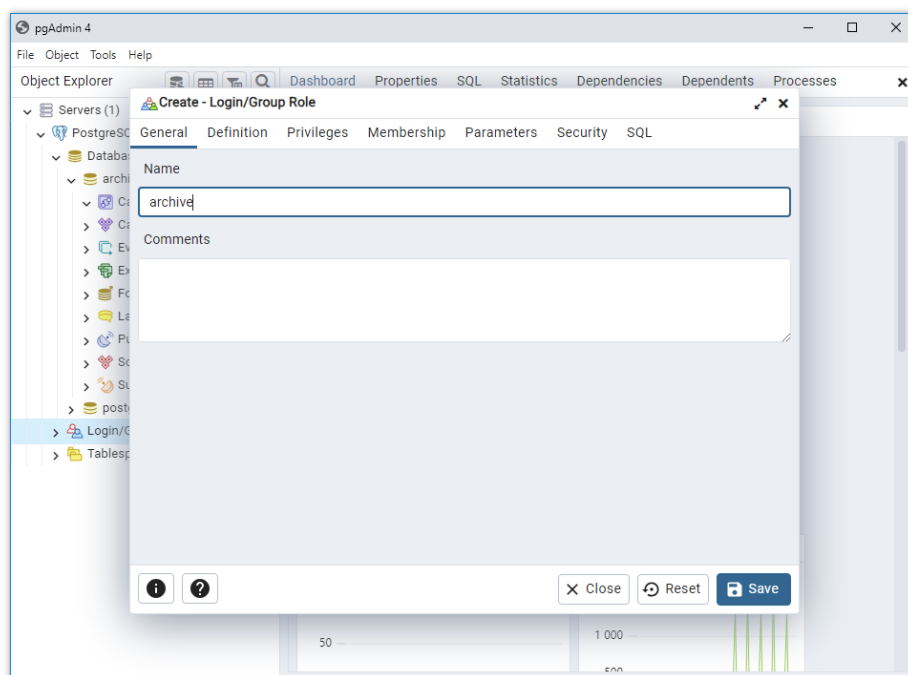
Для создания базы данных PostgreSQL, совместимой с КристоПро Архив, создайте пользователя, от лица которого будет происходить подключение к базе данных со стороны Архива. Для этого откройте pgAdmin4, разверните вкладку «Servers» и введите пароль пользователя postgres:



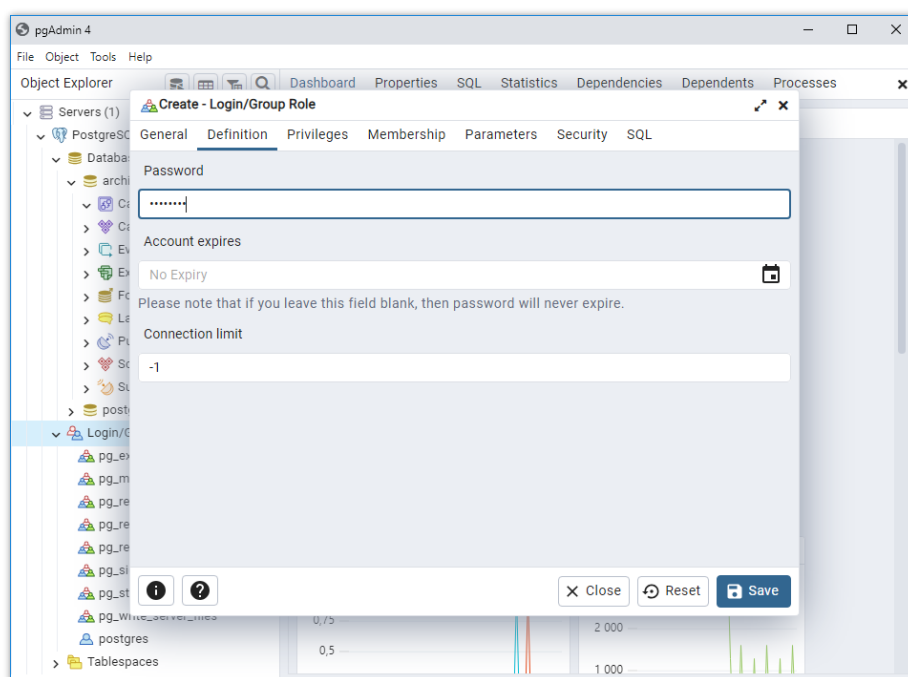
Создайте пользователя. Для этого откройте Login/Group Roles > Create > Login/Group Role...:



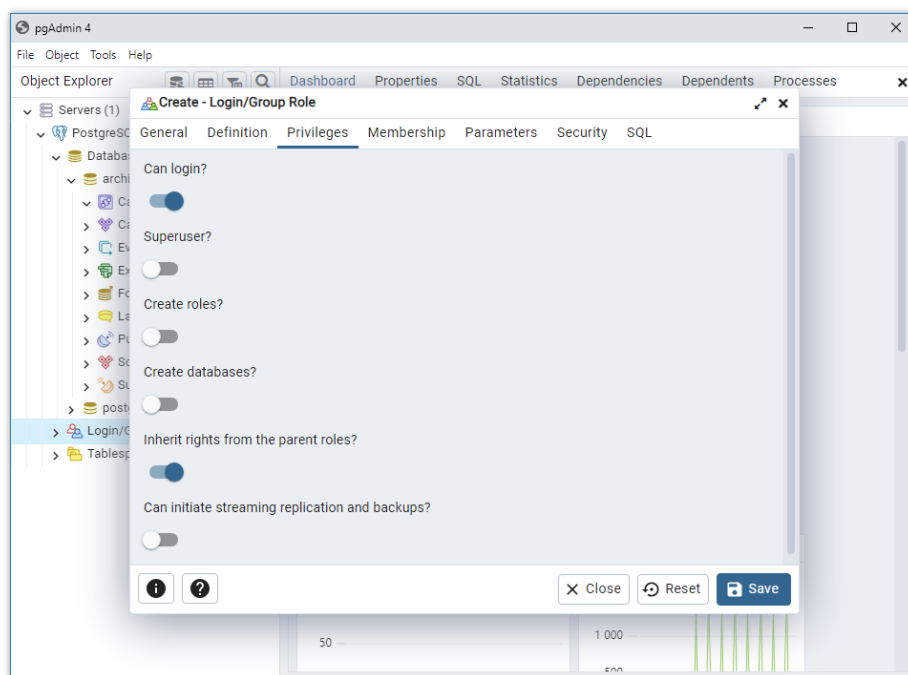
В открывшемся окне на вкладке «General» введите имя пользователя. В примере ниже используется archive. Это значение рекомендуется изменить:



Придумайте пароль создаваемого пользователя и введите его во вкладке «Definition»:

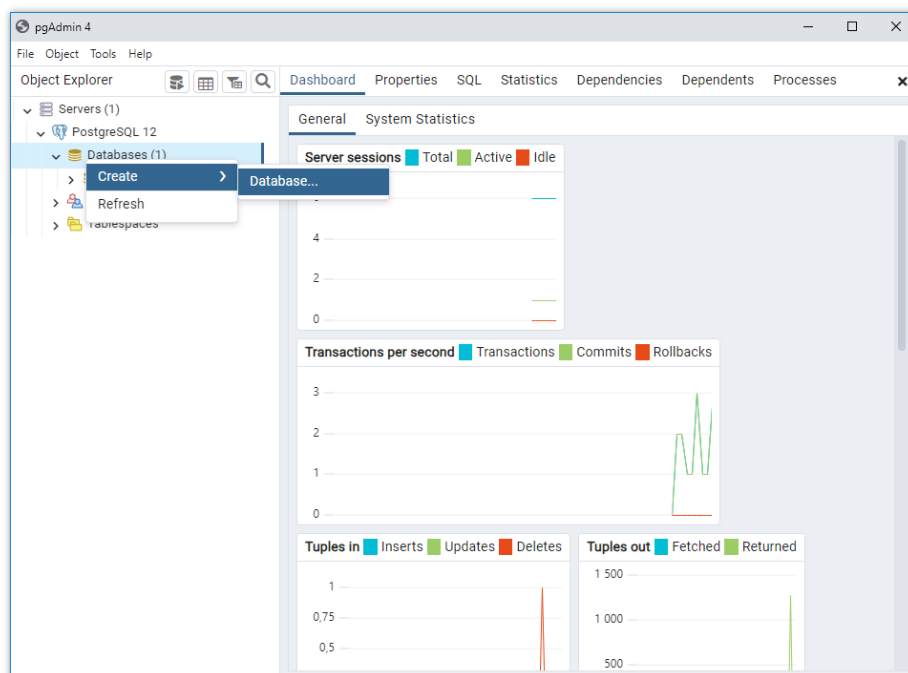


Откройте вкладку «Privileges» и отметьте пункт «Can login?»:

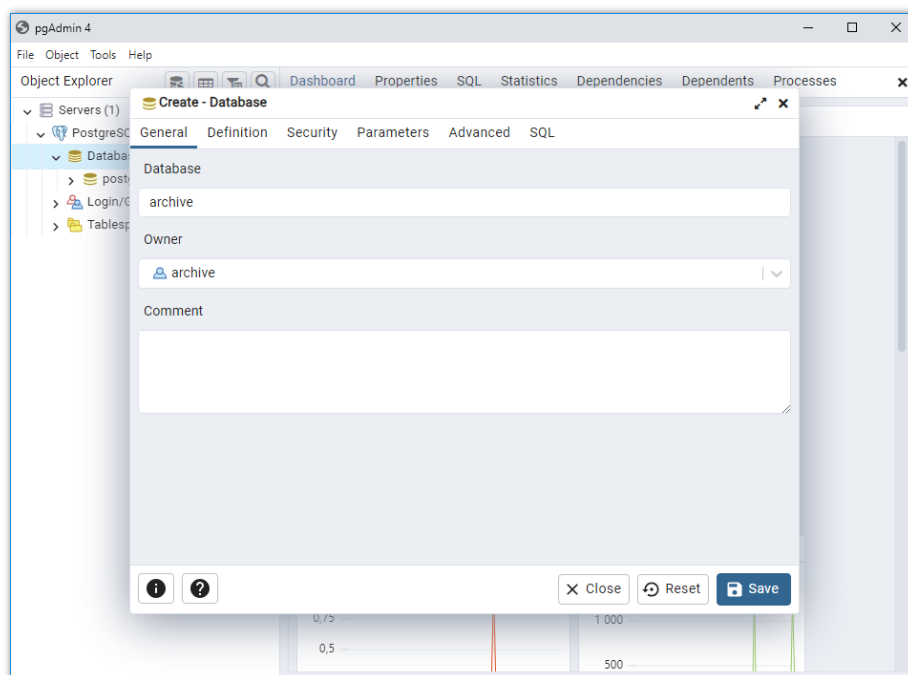


Нажмите «Save». Пользователь создан. Теперь он будет отображаться в списке «Login/Group Roles».

Создайте базу данных, которая будет использоваться Архивом. Для этого нажмите Databases > Create > Database...:



Введите имя базы данных. В примере ниже — archive. Его рекомендуется изменить. В качестве владельца (поле «Owner») укажите созданного пользователя.



Нажмите «Save». Пустая база данных создана.

Для заполнения созданной базы данных выполните следующую команду в PowerShell от лица администратора, заменив поля <username>, <password>, <host> и <database> на имя, пароль созданного пользователя, адрес сервера PostgreSQL и имя созданной базы данных соответственно:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
  --database `
  --mode use `
  --database-provider PostgreSQL `
  --connection-string "username = <username>; password = <password>; host =
  <host>; database = <database>"
```

Описание параметров программы приведены в таблице ниже.

Имя параметра	Описание
<code>--database</code>	Указание на то, что требуется выполнить миграцию базы данных.
<code>--mode</code>	Режим миграции. Определяет, нужно ли создать новую базу данных (значение create), заполнить существующую (use) или обновить существующую заполненную до новой версии (upgrade).
<code>--database-provider</code>	Имя провайдера баз данных. Должно быть указано PostgreSQL.
<code>--connection-string</code>	Строка подключения к базе данных. Обратите внимание на то, что подключение должно производиться к существующей базе данных.

Программа заполнит созданную базу данных необходимыми для работы объектами. После успешного выполнения на экране будет написано Миграция успешно выполнена.

Для того, чтобы созданная база данных была указана в настройках всех компонентов КристоПро Архив, выполните следующие команды, заменив <username> на имя созданного пользователя, <password> на пароль созданного пользователя, <host> на адрес сервера с PostgreSQL и <database> на имя созданной базы данных:

```
C:\inetpub\cp-archive\config\Archive.Config set `
    --database-provider PostgreSQL

C:\inetpub\cp-archive\config\Archive.Config set `
    --connection-string "username = <username>; password = <password>; host =
    <host>; database = <database>"
```

Получить значение установленной строки подключения, настроенной для всех установленных компонент, можно командой

```
C:\inetpub\cp-archive\config\Archive.Config get --connection-string
```

Пример вывода:

```
admin-api: username = <username>; password = <password>; host = <host>;
database = <database>
```

```
client-api: username = <username>; password = <password>; host = <host>;  
database = <database>  
consumer: username = <username>; password = <password>; host = <host>; database  
= <database>  
signature-updater: username = <username>; password = <password>; host = <host>;  
database = <database>
```

Настройка базы данных PostgreSQL завершена.

3.2.2 Сохранение подписанных документов (ранее Архив УЦ)

Создайте БД таким же образом, как и при основной настройке, но назовите её иначе. Выполните миграцию каталога БД. Для этого от лица администратора выполните

```
C:\inetpub\cp-archive\config\Archive.Config migrate `  
  --database `  
  --mode use `  
  --database-provider PostgreSQL `  
  --connection-string "username = <username>; password = <password>; host =  
<host>; database = <database>" `  
  --ca `  
  --type catalogue
```

Дополнительно создайте БД, в которой будут храниться подробные данные о сохранённых документах и опционально сами документы. Выполните миграцию:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `  
  --database `  
  --mode use `  
  --database-provider PostgreSQL `  
  --connection-string "username = <username>; password = <password>; host =  
<host>; database = <database>" `  
  --ca `  
  --type storage
```

3.3 Настройка Oracle Database 12c Release 2

3.3.1 Основная настройка

Замечание: настоятельно рекомендуется производить резервное копирование всех создаваемых баз данных.

Для быстрого автоматического создания пользователя и схемы, достаточных для работы с КристоПро Архив, выполните следующую команду, указав пароль администратора базы данных <password>, источник данных <data_source> и имя создаваемого пользователя <username>:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
--database `
--mode create `
--database-provider Oracle `
--connection-string "User ID = SYS; DBA Privilege = SYSDBA; Password =
<password>; Data Source = <data_source>" `
--target "<username>"
```

Описание параметров программы приведены в таблице ниже.

Имя параметра	Описание
<code>--database</code>	Указание на то, что требуется выполнить миграцию базы данных.
<code>--mode</code>	Режим миграции. Определяет, нужно ли создать новую базу данных (значение create), заполнить существующую (use) или обновить существующую заполненную до новой версии (upgrade).
<code>--database-provider</code>	Имя провайдера баз данных. Должно быть указано Oracle.
<code>--connection-string</code>	Строка подключения к базе данных. Обратите внимание на то, что подключение должно производиться к существующему пользователю/схеме.
<code>--target</code>	Имя создаваемого пользователя (схемы).

Эта команда от лица администратора базы данных создаст пользователя с именем <username> и заполнит его схему необходимыми для работы объектами. После успешного выполнения на экране будет написано Миграция успешно выполнена. Для того, чтобы пользователь стал активным, необходимо сменить его пароль. Пароль по умолчанию: «cryptopro». Таким образом, команда для смены пароля:

```
ALTER USER <username> IDENTIFIED BY <password> REPLACE cryptopro;
```

Для того, чтобы созданная база данных была указана в настройках всех компонентов КриптоПро Архив, выполните следующие команды в PowerShell от имени администратора, заменив <password> на пароль пользователя <username> и <data_source> на адрес сервера с Oracle:

```
C:\inetpub\cp-archive\config\Archive.Config set `
  --database-provider Oracle

C:\inetpub\cp-archive\config\Archive.Config set `
  --connection-string "User ID = <username>; Password = <password>; Data
  Source = <data_source>"
```

Получить значение установленной строки подключения, настроенной для всех установленных компонент, можно командой

```
C:\inetpub\cp-archive\config\Archive.Config get --connection-string
```

Пример вывода:

```
admin-api: User ID = <username>; Password = <password>; Data Source =
<data_source>
client-api: User ID = <username>; Password = <password>; Data Source =
<data_source>
consumer: User ID = <username>; Password = <password>; Data Source =
<data_source>
signature-updater: User ID = <username>; Password = <password>; Data Source =
<data_source>
```

Основная настройка базы данных Oracle Database завершена.

3.3.2 Сохранение подписанных документов (ранее Архив УЦ)

Выполните следующую команду для создания и миграции каталога БД:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
  --database `
  --mode create `
  --database-provider Oracle `
  --connection-string "User ID = SYS; DBA Privilege = SYSDBA; Password =
  <password>; Data Source = <data_source>" `
```

```
--target "<catalogue_username>" `
--ca `
--type catalogue
```

Выполните следующую команду для создания БД, в которой будут храниться подробные данные о сохранённых документах и опционально сами документы:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
--database `
--mode create `
--database-provider Oracle `
--connection-string "User ID = SYS; DBA Privilege = SYSDBA; Password =
<password>; Data Source = <data_source>" `
--target "<storage_username>" `
--ca `
--type storage
```

3.4 Ввод лицензии

Для ввода лицензии в PowerShell выполните от имени администратора

```
C:\inetpub\cp-archive\config\Archive.Config set `
  --license `
  --serial '<serial>' `
  --org '<org>'
```

Где вместо <serial> укажите серийный номер лицензии с бланка лицензии, а вместо <org> — имя организации, как оно указано в балке с лицензией.

Обратите внимание, что кавычки необходимо экранировать символом обратной косой черты (\). Например,

```
C:\inetpub\cp-archive\config\Archive.Config set `
  --license `
  --serial '01234-56789-01234-56789-01234' `
  --org '000 \"КРИПТО-ПРО\"'
```

В результате выполнения на экран будут выведены сведения об активированной лицензии. Пример вывода:

```
Серийный номер: <серийный номер>
Наименование организации: <имя организации>
Срок действия лицензии: <срок действия лицензии>
Версия продукта: 1.0
Описание: <описание лицензии>

Лицензия установлена на следующие программы:
admin-api
client-api
consumer
signature-updater
```

При возникновении ошибок проверьте написание имени организации, а также обратите внимание на поле «Причина» вывода.

Для ввода нескольких лицензий повторить указанные выше шаги для каждой лицензии. Полученные лицензии будут автоматически установлены для тех компонентов, для которых они предназначены.

Для просмотра установленных лицензий выполнить команду

```
C:\inetpub\cp-archive\config\Archive.Config get --license
```

Пример вывода:

```
--- admin-api:
Серийный номер: <серийный номер>
Наименование организации: <имя организации>
Срок действия лицензии: <срок действия лицензии>
```

Версия продукта: 1.0

Описание: <описание лицензии>

--- admin-api (Архив УЦ):

Пробная лицензия до 01.01.2024 14:05:30.

--- client-api:

Серийный номер: <серийный номер>

Наименование организации: <имя организации>

Срок действия лицензии: <срок действия лицензии>

Версия продукта: 1.0

Описание: <описание лицензии>

--- client-api (Архив УЦ):

Пробная лицензия до 01.01.2024 14:05:30.

3.5 Настройка admin-api и client-api

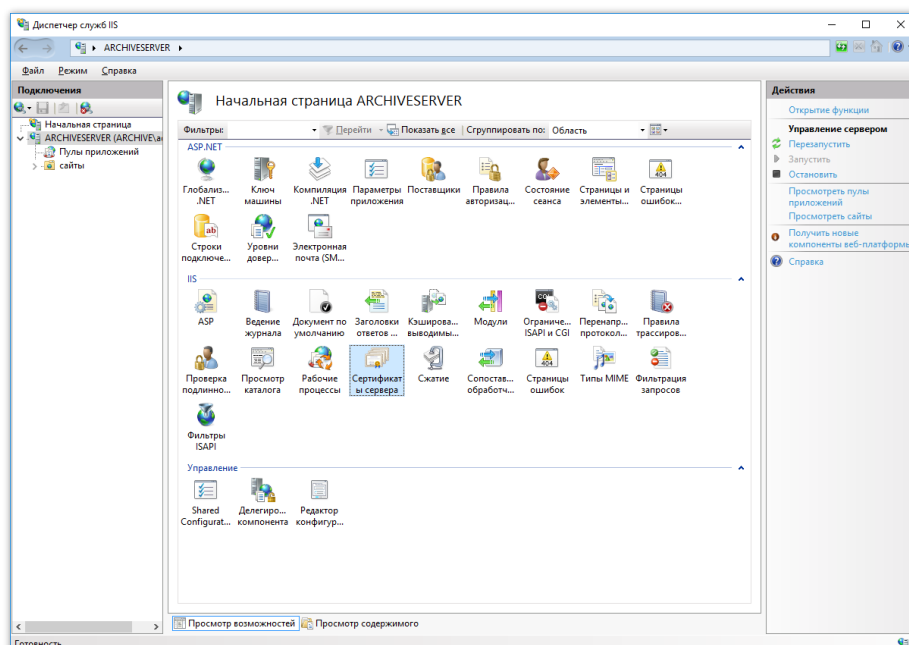
В данном разделе описана настройка admin-api и client-api — служб КриптоПро Архив для обработки пользовательских запросов, таких как создание контейнеров, получение логов, получение истории контейнера, отправка подписей на повторную обработку, управление пользователями и так далее. Для настройки потребуется установленный на сервере КриптоПро Архив в конфигурации «Полная установка» (установлены все компоненты) или «Подсистема приёма подписей» (установлены только admin-api и client-api). Также потребуются

- Сертификат проверки подлинности сервера КриптоПро Архив в формате PFX для обеспечения соединения с программой по протоколу mTLS.
- Сертификат суперпользователя КриптоПро Архив в формате PFX.

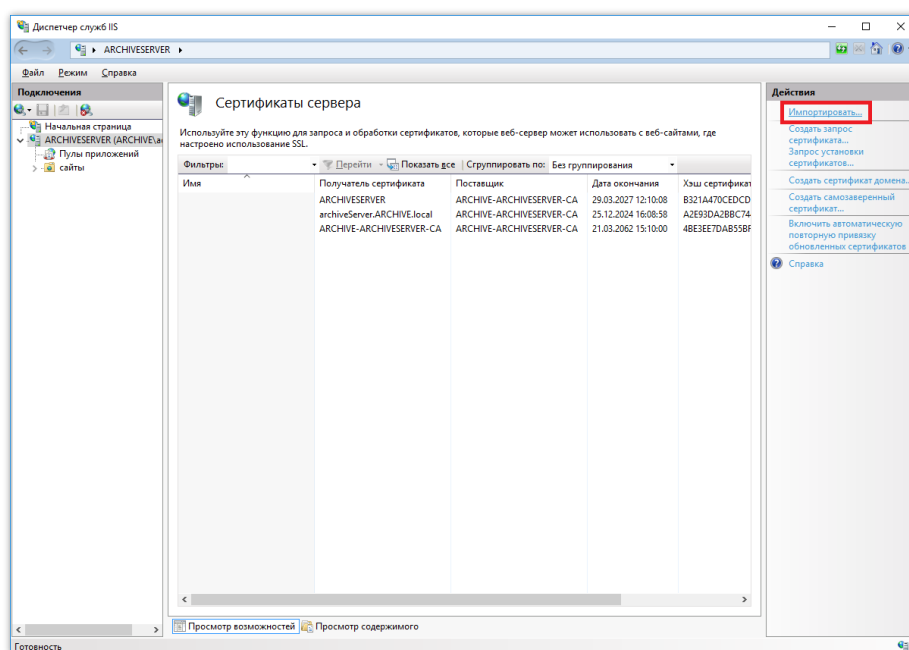
Ниже описана настройка admin-api. Настройка client-api производится в точности тем же образом, за исключением значения порта и названия приложения. В инструкции ниже указаны различия в местах, где они есть.

3.5.1 Добавление серверного сертификата

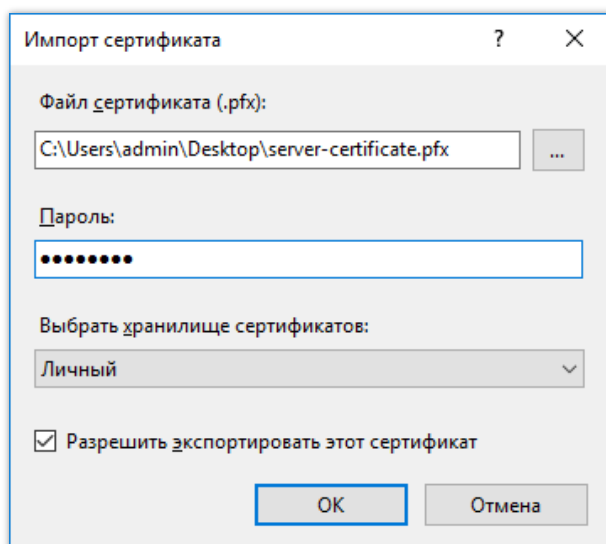
Добавьте сертификат проверки подлинности сервера в IIS. Если он уже был добавлен, повторно этого делать не нужно — используйте добавленный. Для добавления откройте IIS, выберите слева вкладку с именем сервера и дважды нажмите на «Сертификаты сервера»:



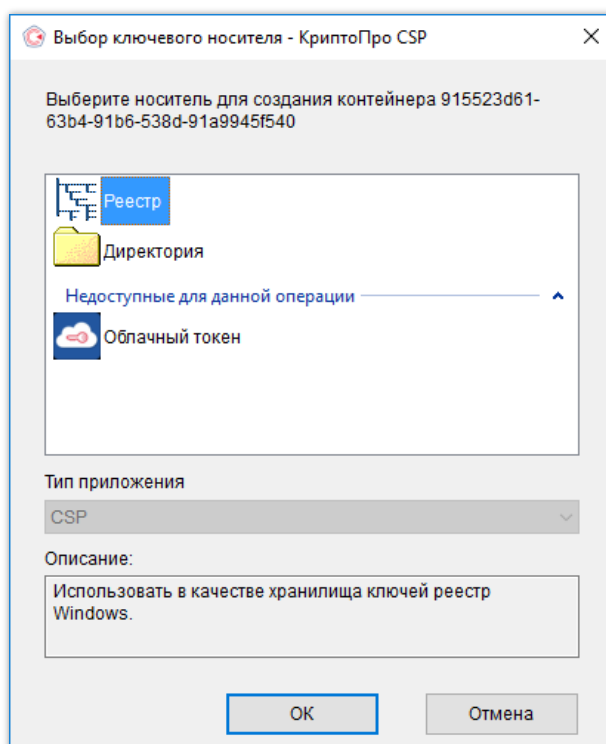
В меню справа выберите «Импортировать»:



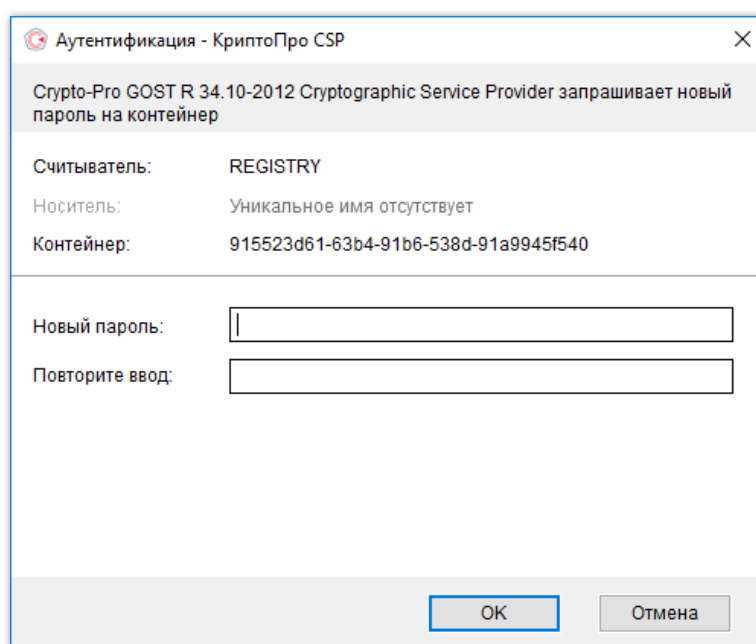
В появившемся окне укажите путь к сертификату и введите пароль:



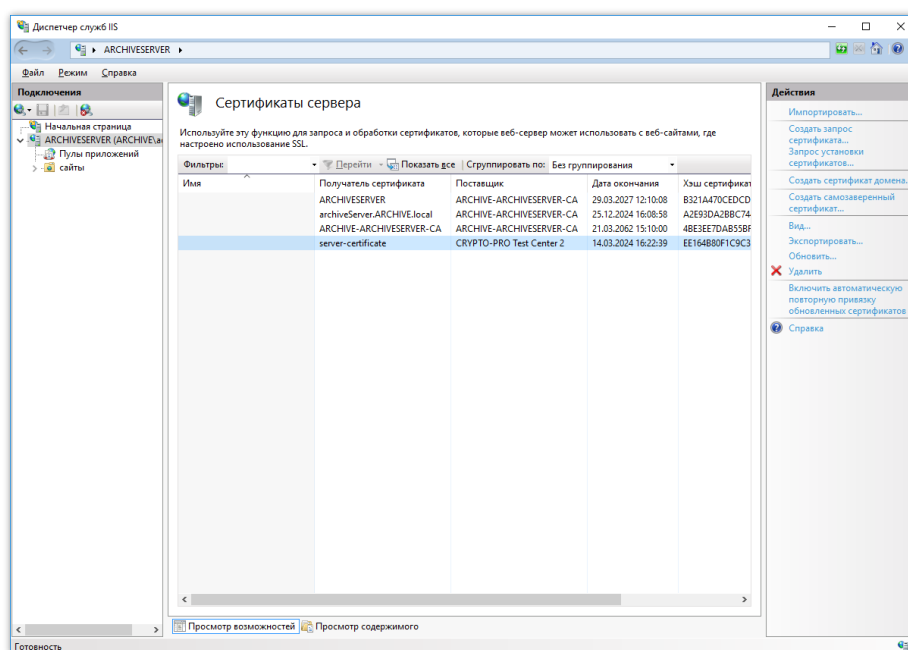
Нажмите «OK». В качестве носителя выберите «Реестр»:



Нажмите «OK». В открывшемся окне не вводите пароль. Нажмите «OK»:



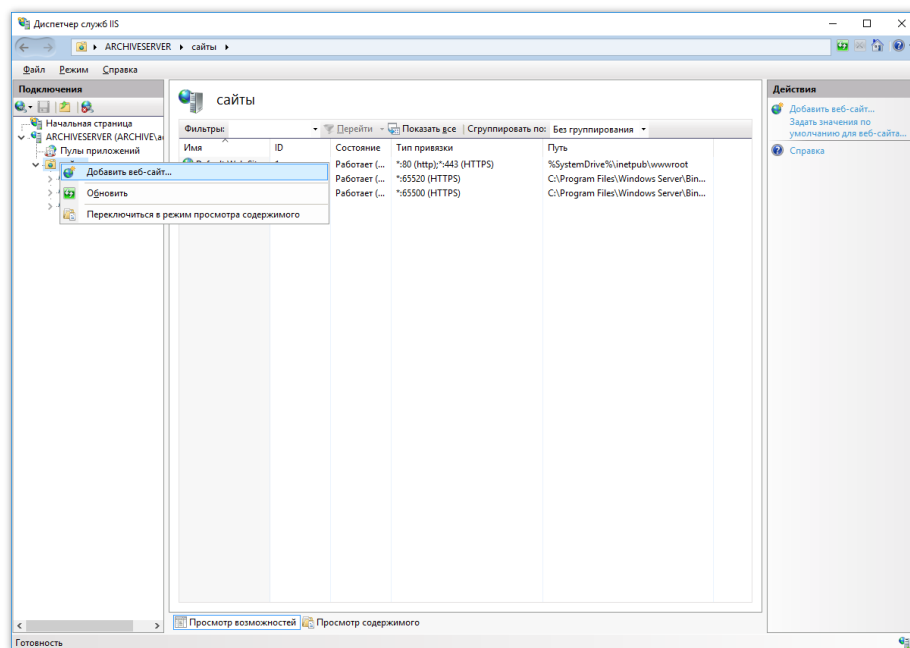
Сертификат появится среди добавленных:



Добавление серверного сертификата завершено.

3.5.2 Добавление приложения IIS

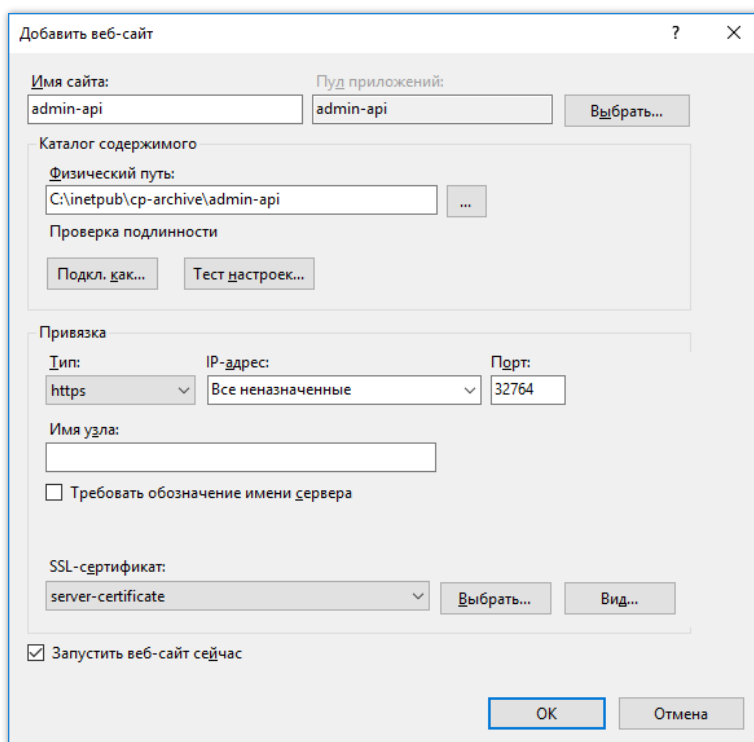
Служба admin-api (client-api) работает через IIS. Для добавления admin-api (client-api) как приложения IIS правой кнопкой мыши нажмите «сайты», затем «Добавить веб-сайт...»:



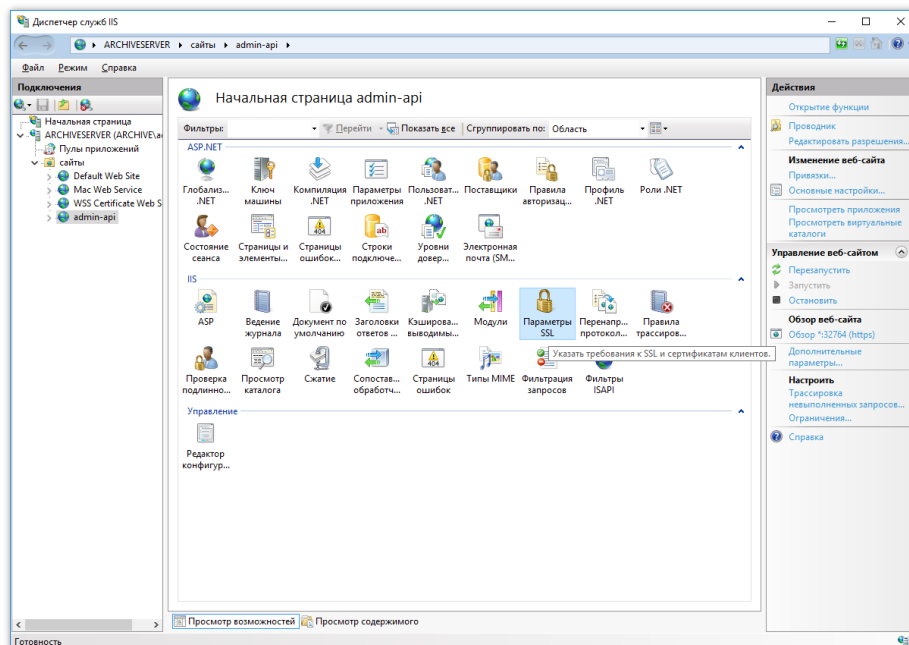
Параметры, которые необходимо заполнить, приведены в таблице ниже.

Имя параметра	Значение
Имя сайта	admin-api (client-api)
Физический путь	C:\inetpub\cp-archive\admin-api (C:\inetpub\cp-archive\client-api для client-api)
Привязка. Тип	https
Привязка. Порт	32764 (32767 для client-api)
SSL-сертификат	Добавленный ранее сертификат (в примере — server-certificate).

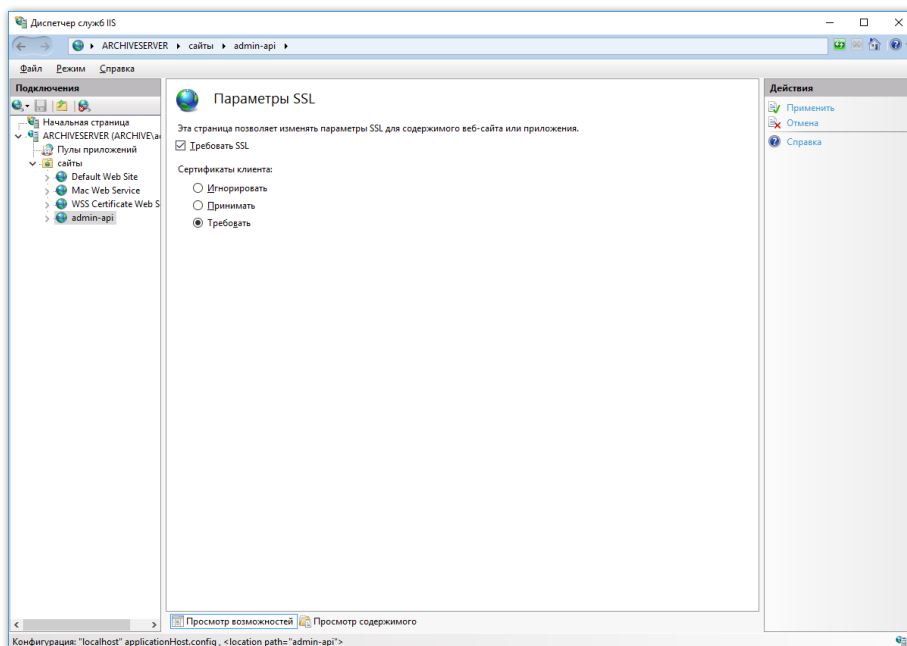
Пример заполнения страницы:



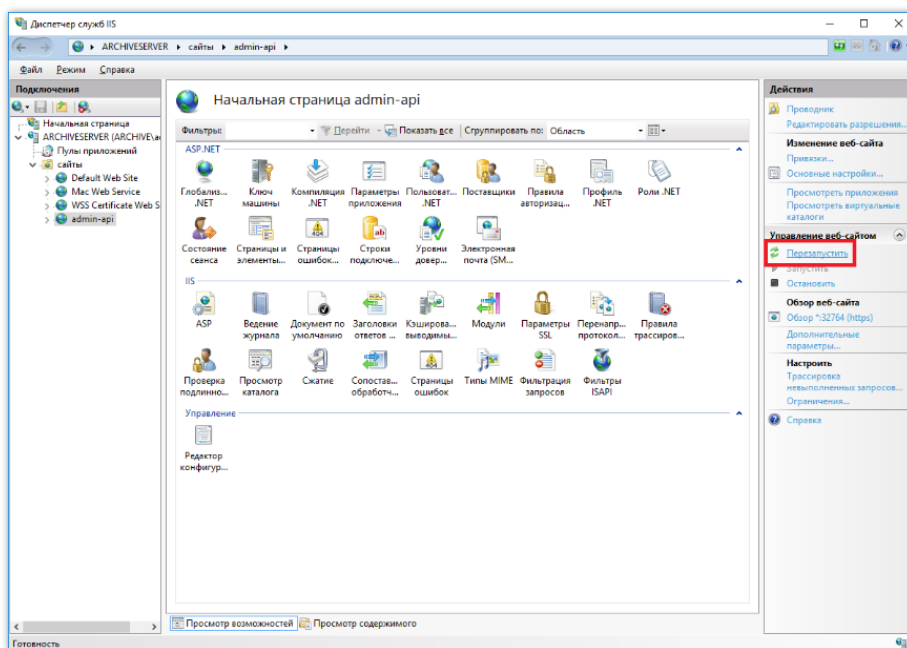
Нажмите «ОК». Откройте в IIS страницу созданного приложения и дважды нажмите «Параметры SSL»:



Отметьте пункт «Требовать SSL» и выберите пункт «Требовать»:



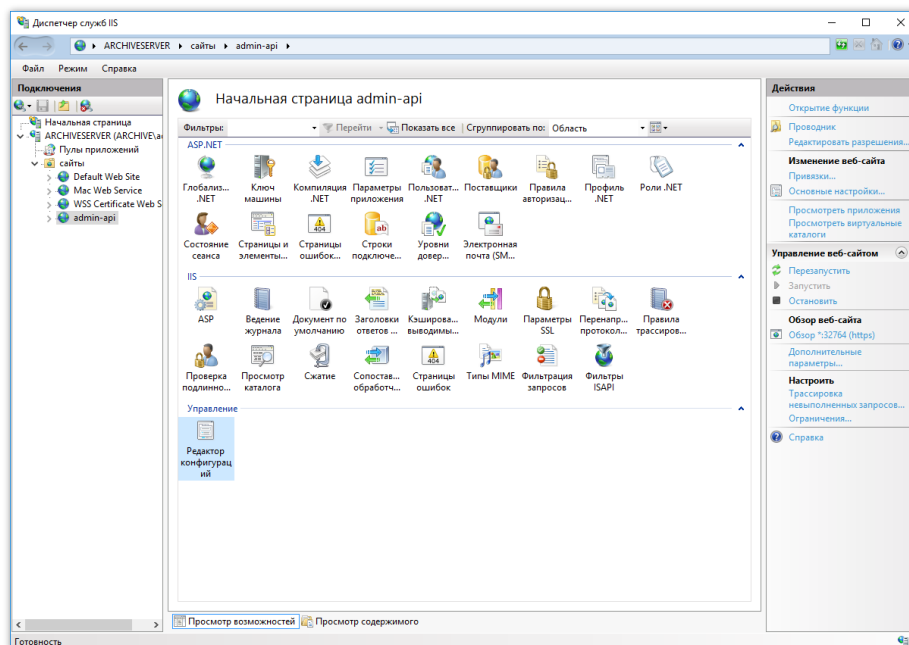
Нажмите «Применить» (справа). Вернитесь на страницу приложения и нажмите «Перезапустить»:



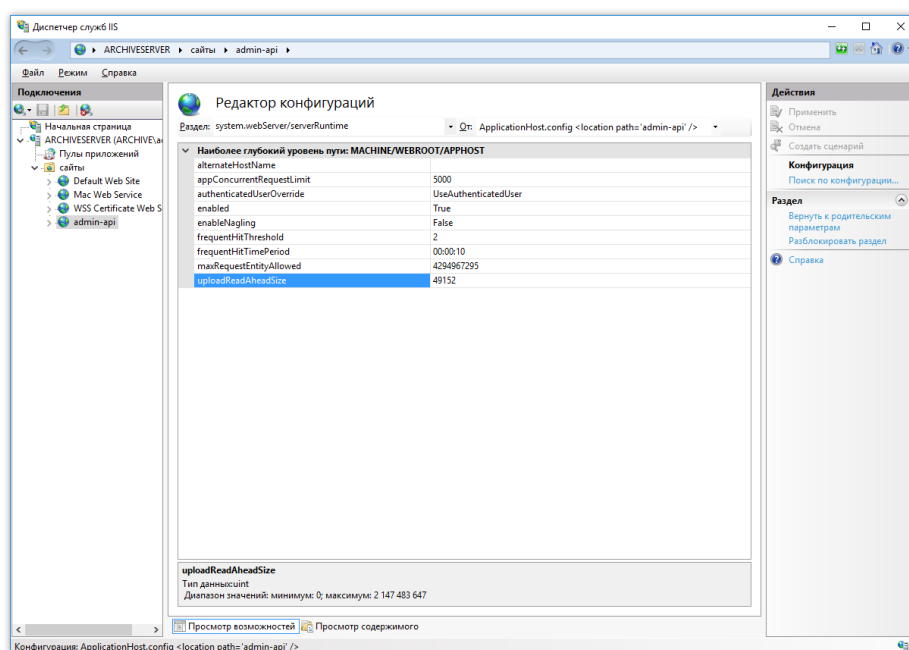
Настройка приложения IIS завершена. Далее необходимо настроить саму службу. После изменения настроек необходимо перезапускать приложение тем же образом, что описан выше.

3.5.3 Настройка максимального размера запроса

По умолчанию IIS не позволяет загружать на сервер файлы размером более 30 МБ. Для того, чтобы это изменить, откройте IIS, выберите сайт admin-api (client-api) и дважды нажмите на «Редактор конфигураций»:



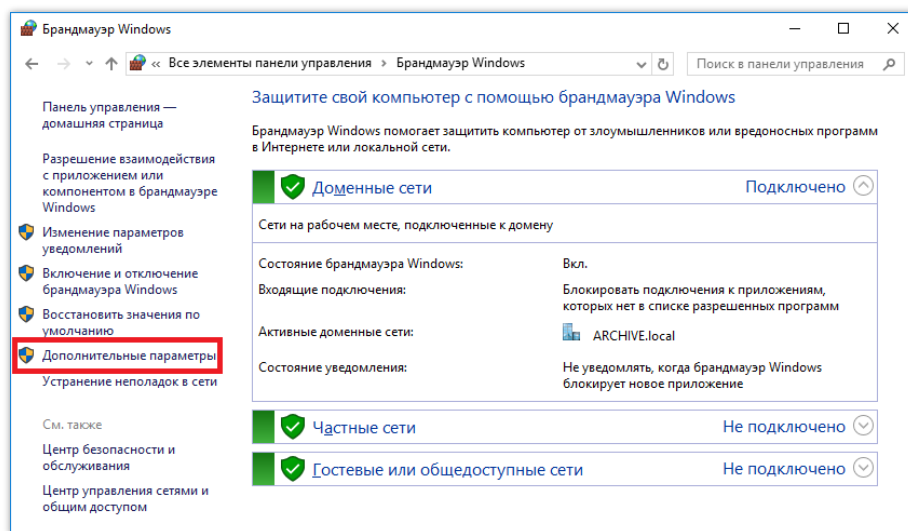
В поле «Раздел» введите «system.webServer/serverRuntime» и нажмите «Enter»:



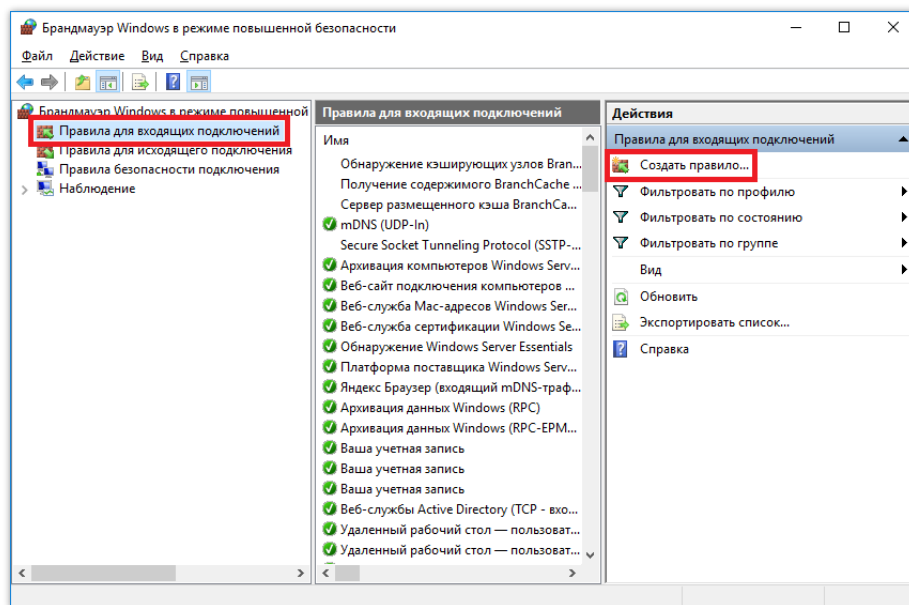
Необходимо изменить значение поля «uploadReadAheadSize» на требуемое значение. В этом поле указывается количество байт, определяющее размер буфера для чтения пользовательского запроса. Максимальное значение: 2147483647. Более подробно с этим и другими параметрами можно ознакомиться в [официальной онлайн-документации](#).

3.5.4 Настройка брандмауэра

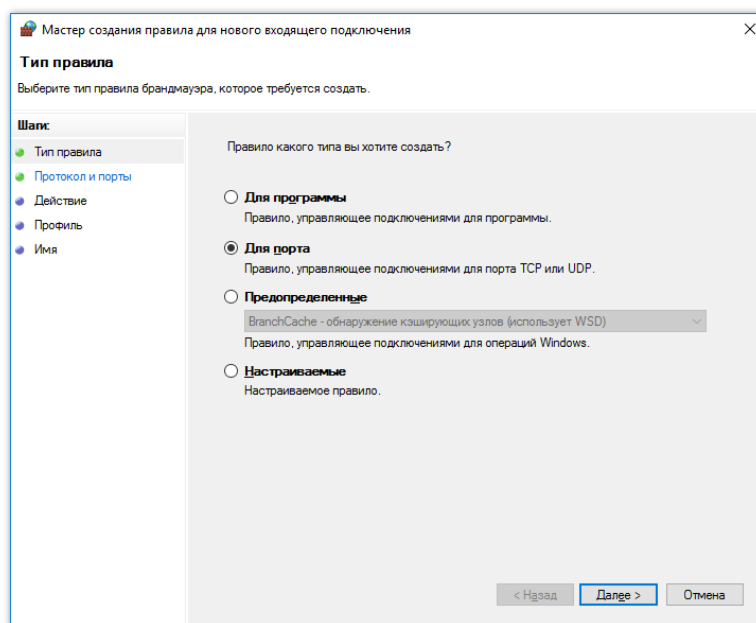
Для того, чтобы открыть порты служб admin-api и client-api, запустите программу «Брандмауэр Windows» и выберите «Дополнительные параметры» слева:



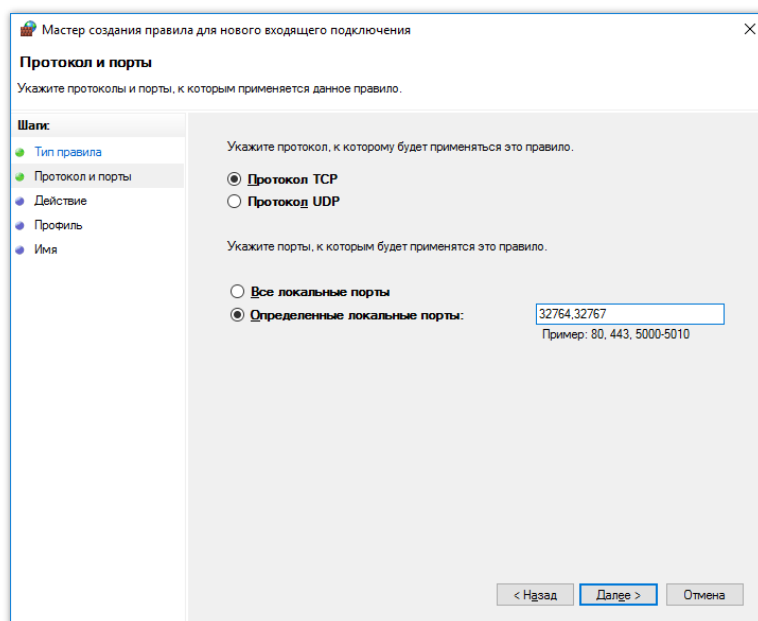
Выберите вкладку «Правила для входящих подключений» слева и нажмите «Создать правило...» справа:



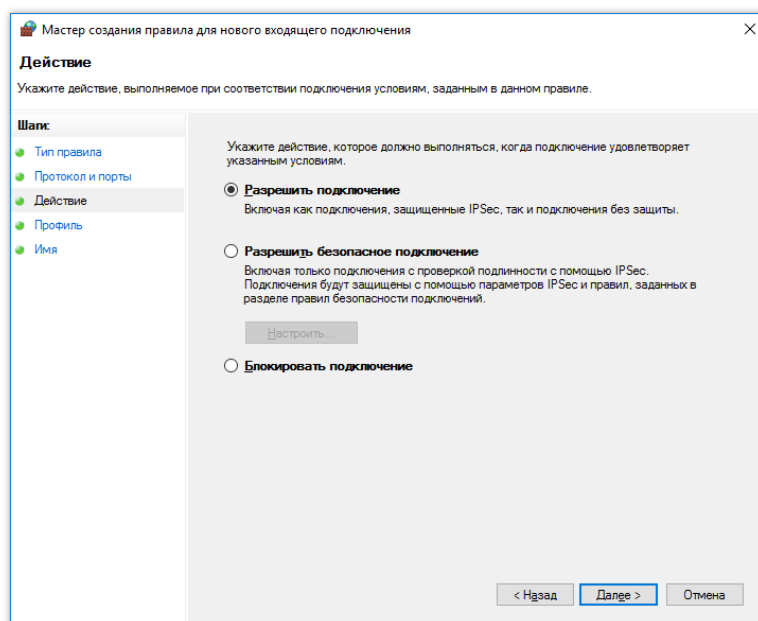
В появившемся окне отметьте пункт «Для порта» и нажмите «Далее»:



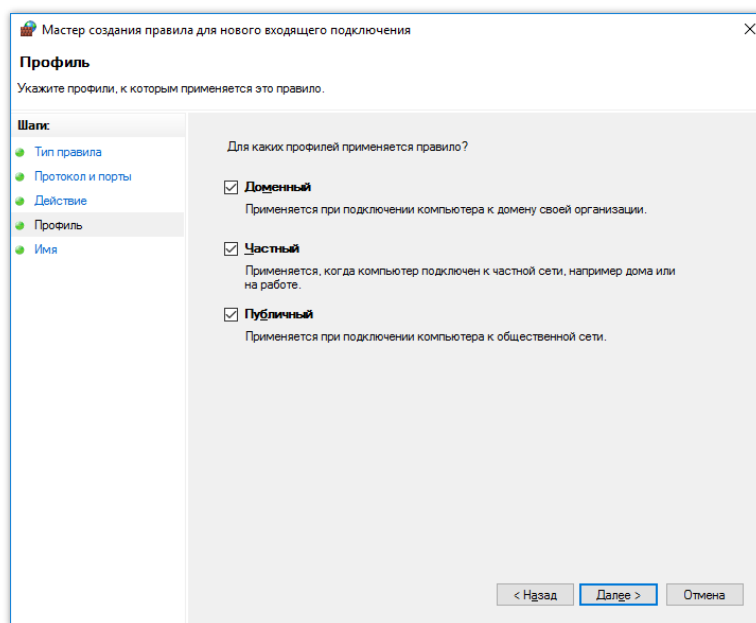
Выберите пункты «Протокол TCP», «Определенные локальные порты», укажите значения 32764,32767 и нажмите «Далее»:



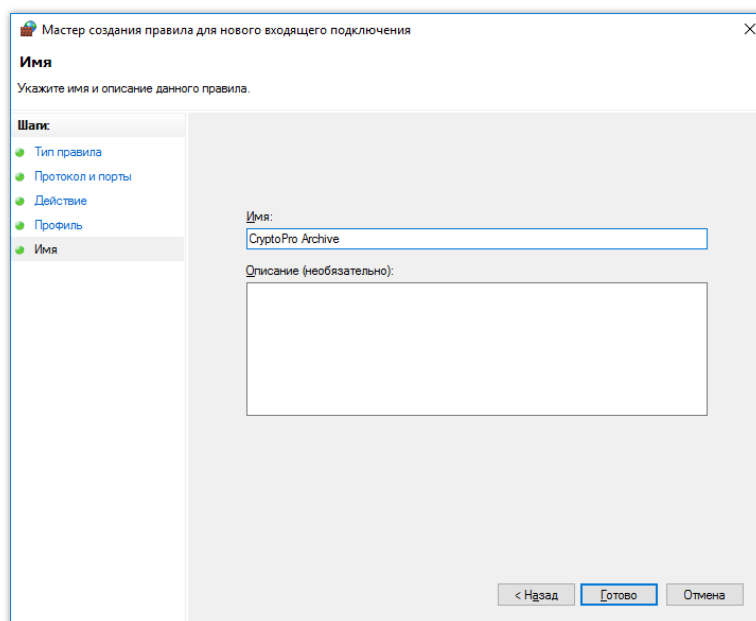
Выберите пункт «Разрешать подключение» и нажмите «Далее»:



Отметьте все пункты и нажмите «Далее»:



Введите имя правила (в примере ниже CryptoPro Archive) и нажмите «Готово»:



Настройка правила Брандмауэра Windows завершена.

3.5.5 Установка сертификата суперпользователя

Установите отпечаток суперпользователя. Для этого выполните следующую команду, заменив <thumbprint> на SHA-1 отпечаток сертификата суперпользователя и <provider> — на используемого провайдера баз данных (PostgreSQL или Oracle):

```
C:\inetpub\cp-archive\config\Archive.Config set `
--superuser `
--thumbprint <thumbprint> `
--database-provider <provider>
```

После успешного выполнения на экран будет выведено сообщение «Значение успешно изменено». Убедитесь, что на сервере в Локальном хранилище установлены корневые сертификаты сертификатов всех подключающихся пользователей, включая суперпользователя.

3.5.6 Конфигурационный файл

Конфигурационный файл admin-api (client-api) расположен по пути

C:\inetpub\cp-archive\admin-api\appsettings.json (для client-api:

C:\inetpub\cp-archive\client-api\appsettings.json). Этот JSON-файл

поддерживает комментарии: строки, начинающиеся с «//», не учитываются.

После изменения конфигурации перезапустите соответствующую службу в IIS.

```
{
  // Данная секция неактивна на Windows.
  "Kestrel": {
    "Endpoints": {
      "Http": {
        "Url": "http://localhost:5000"
      }
    }
  },

  "Serilog": {
    "Using": [
      "Serilog.Sinks.Console",
      "Serilog.Sinks.File",
      "Serilog.Sinks.Elasticsearch",
      "Serilog.Sinks.ManticoreSearch"
    ],
    "MinimumLevel": {
      // Общий уровень логирования.
      "Default": "Debug",

      // Переопределение уровней логирования для компонентов.
      "Override": {
        "Microsoft.EntityFrameworkCore": "Warning",
        "Microsoft.EntityFrameworkCore.Query": "Warning",
        "Microsoft.AspNetCore": "Warning"
      }
    }
  },

  // Перечисление мест, куда писать логи.
  "WriteTo": [
    {
      // Пример настройки логирования в файл.
      // Рекомендуется использовать именно логирование в файл.
    }
  ]
}
```

```

    "Name": "File",
    "Args": {
        // Путь к файлу, в который будут записаны логи.
        // Путь должен быть доступен для записи сервисом.
        "path": "<path>",

        // Как часто менять файл логов.
        "rollingInterval": "Day",

        // Менять файл логов при превышении размера текущего файла.
        "rollOnFileSizeLimit": true,

        // Сколько файлов оставлять. Будут сохранены только последние файлы.
        "retainedFileCountLimit": 31,

        // (опционально) JSON-формат логов. Удалите или закомментируйте это
        // поле для записи логов в обычном формате.
        "outputTemplate": "[{Timestamp:HH:mm:ss} {Level:u3}] {Message:lj}
{Properties:j}{NewLine}{Exception}"
    }
},
{
    // Пример настройки логирования в Elasticsearch.
    // Удалите эту секцию, если не используете Elasticsearch.
    "Name": "Elasticsearch",
    "Args": {
        // Адрес Elasticsearch.
        "nodeUri": "http://localhost:9200",

        // Имя индекса Elasticsearch.
        "indexFormat": "archive.web-{0:yyyy.MM.dd}",

        // Поля, необходимые для совместимости.
        "autoRegisterTemplateVersion": "ESv7",
        "autoRegisterTemplate": true
    }
},
{
    // Пример настройки логирования в ManticoreSearch.
    // Удалите эту секцию, если не используете ManticoreSearch.
    "Name": "ManticoreSearch",
    "Args": {
        // Адрес ManticoreSearch.
        "basePath": "http://127.0.0.1:9308",

        // Имя индекса ManticoreSearch.
        "indexName": "archive_logs",

        // Имя кластера в случае использования кластера.
        "clusterName": null
    }
}
]
},

"ConnectionStrings": {
    // Строка подключения к БД.
    "DefaultConnection": "<main_connection_string>"
},

// Настройка сохранения подписанных документов.
"ArchiveCa": {

```

```

// Активна ли функциональность.
// Если false, остальные значения в этой секции не имеют значения.
// Для работы необходим RabbitMQ и программа consumer.
"UseArchiveCa": false,

"ConnectionStrings": {
  // Строка подключения к каталогу БД.
  // СУБД должна быть та же, что указана в секции General.
  "DatabaseCatalogue": "<catalogue_connection_string>"
},
},

"General": {
  // СУБД. Возможные значения: PostgreSQL, Oracle.
  "DatabaseProvider": "PostgreSQL"
},

"RabbitMq": {
  // Виртуальный хост RabbitMQ.
  "VirtualHost": "archive",

  // Имя пользователя RabbitMQ.
  "Username": "archive",

  // Пароль пользователя RabbitMQ.
  "Password": "1qaz@WSX",

  // Конечные точки RabbitMQ.
  "Endpoints": [
    {
      // IP-адрес или доменное имя RabbitMQ.
      "Hostname": "rabbitmq.ru",

      // Порт RabbitMQ. Порт по умолчанию: 5672.
      // Укажите 5671 при использовании TLS.
      "Port": 5671,

      // Адрес API управления RabbitMQ для мониторинга очередей.
      // Для client-api это поле можно не заполнять.
      "ApiAddress": "https://rabbitmq.ru:15671",

      // Требование использования mTLS.
      // Если false, значения остальных полей Ssl* не имеет значения.
      "SslEnabled": true,

      // Путь к клиентскому сертификату в формате PFX.
      "SslCertPath": "/home/cp/downloads/cproar.pfx",

      // Пароль от PFX.
      "SslCertPassphrase": "<password>",

      // Доменное имя сервера, к которому проводится подключение.
      "SslServerName": "rabbitmq.ru"
    }
  ]
}
}
}

```

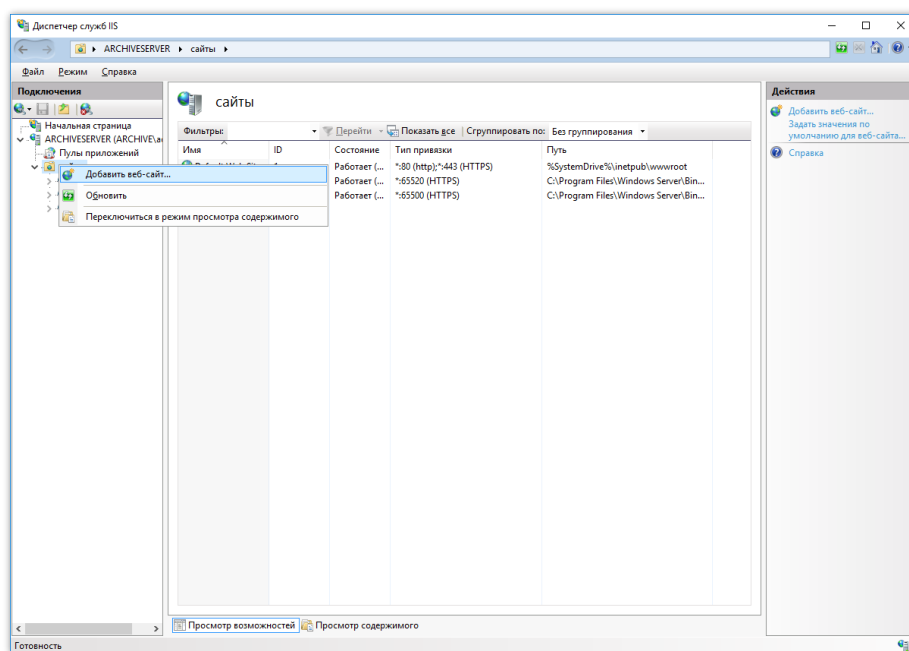
3.6 Настройка frontend

В данном разделе описана настройка административной панели КристоПро Архив. Панель представляет собой графический веб-интерфейс для управления КристоПро Архив. Панель связывается с подсистемой admin-api, которая может быть установлена как на данном сервере, так и на удалённом.

Для настройки frontend необходим КристоПро Архив в конфигурациях «Полная установка» или «Подсистема приёма подписей». Также необходим локальный или удалённый доступ к программе admin-api. В примерах ниже предполагается установка компонентов Архива по стандартным путям. Если пути не совпадают с выбранными на этапе установки, измените их на соответствующие. Для защиты соединения с приложением frontend рекомендуется использовать односторонний TLS. Для этого дополнительно потребуется сертификат проверки подлинности сервера.

3.6.1 Добавление приложения IIS

На ОС семейства Windows Server компонент frontend работает в качестве приложения IIS. Для добавления приложения откройте IIS, правой кнопкой нажмите «сайты», затем «Добавить веб-сайт...»:



Параметры, которые необходимо заполнить, приведены в таблице ниже.

Имя параметра	Значение
Имя сайта	frontend
Физический путь	C:\inetpub\cp-archive\frontend
Привязка: Тип	https
Привязка: Порт	443
SSL-сертификат	Необходимо указать сертификат проверки подлинности сервера

Пример заполнения страницы:

Добавить веб-сайт

Имя сайта: frontend Пул приложений: frontend Выбрать...

Каталог содержимого

Физический путь: C:\inetpub\archive\frontend ...

Проверка подлинности

Подкл. как... Тест настроек...

Привязка

Тип: https IP-адрес: Все неназначенные Порт: 443

Имя узла:

☐ Требовать обозначение имени сервера

☐ Отключить HTTP/2

☐ Отключить OCSP-сшивание

SSL-сертификат: archive-cryptopro.ru Выбрать... Вид...

☒ Запустить веб-сайт сейчас

OK Отмена

Нажать «ОК». Настройка приложения IIS завершена.

3.6.2 Конфигурационный файл

Конфигурационный файл расположен по пути C:\inetpub\sr-archive\frontend\custom-config.json. Этот JSON-файл поддерживает комментарии: строки, начинающиеся с «//», не учитываются. После изменения конфигурации перезапустите соответствующую службу в IIS.

```
{
  // Внешний адрес admin-api. По этому адресу браузер администратора
  // будет делать запросы к admin-api.
  "baseUrl": "https://admin-api:32764/api",

  // Текст внизу страницы.
  "footerText": "000 \"Кристо-Про\" 2000-2026",

  // Период автоматического опроса admin-api для получения статусов
  // контейнеров в секундах.
  "statusUpdateIntervalSec": 0,

  // Период автоматического опроса admin-api для получения количества
  // контейнеров, находящихся в статусе «Ошибка обработки подписи».
  "warnCountUpdateIntervalSec": 0,

  // Период автоматического опроса admin-api для получения уведомлений
  // суперпользователя.
  "messageListUpdateIntervalSec": 0,

  // Таймаут запросов к admin-api.
  "apiTimeoutSec": 30
}
```

3.7 Настройка signature-updater

В данном разделе приведена настройка программы signature-updater, отвечающей за усовершенствование подписей до формата CAdES-A. Для настройки потребуется установленный на сервере КриптоПро Архив в конфигурации «Полная установка» (установлены все компоненты) или «Подсистема обеспечения доказательствами подлинности» (установлен только signature-updater). В примерах ниже предполагается установка компонентов Архива по стандартным путям. Если пути не совпадают с выбранными на этапе установки, измените их на соответствующие.

signature-updater работает в несколько потоков. Количество потоков указывается в конфигурационном файле. Существуют 3 группы потоков:

1. Группа потоков, проводящих первое усовершенствование. Количество этих потоков регулируется параметром NumberOfThreadsForIncomingDocuments.
2. Группа потоков для повторного усовершенствования.
3. Поток для опроса БД и отметки контейнеров, подлежащих повторному усовершенствованию.

Такое разделение позволяет избежать ситуации, когда все потоки заняты повторными усовершенствованиями, и для первого усовершенствования новых созданных контейнеров не хватает ресурсов.

3.7.1 Добавление службы

На ОС семейства Windows Server программа signature-updater работает как служба Windows. Для добавления службы выполните в PowerShell от лица администратора следующие команды:

```
New-Service -Name signature-updater -BinaryPathName C:\inetpub\cp-  
archive\signature-updater\Archive.SignUpdaterService.exe -StartupType Automatic  
  
Start-Service -Name signature-updater
```

Обратите внимание на указание полного пути до исполняемого файла.

3.7.2 Конфигурационный файл

Конфигурационный файл расположен по пути C:\inetpub\ср-archive\signature-updater\appsettings.json. Этот JSON-файл поддерживает комментарии: строки, начинающиеся с «//», не учитываются. После изменения конфигурации перезапустите службу.

```
{
  // Настройки логирования.
  "Serilog": {
    "Using": [
      "Serilog.Sinks.Console",
      "Serilog.Sinks.File",
      "Serilog.Sinks.Elasticsearch",
      "Serilog.Sinks.ManticoreSearch"
    ],
    "MinimumLevel": {
      // Общий уровень логирования.
      "Default": "Debug",

      // Переопределение уровней логирования для компонентов.
      "Override": {
        "Microsoft.EntityFrameworkCore": "Warning",
        "Microsoft.EntityFrameworkCore.Query": "Warning",
        "Microsoft.AspNetCore": "Warning"
      }
    },

    // Перечисление мест, куда писать логи.
    "WriteTo": [
      {
        // Пример настройки логирования в файл.
        // Рекомендуется использовать именно логирование в файл.
        "Name": "File",
        "Args": {
          // Путь к файлу, в который будут записаны логи.
          // Путь должен быть доступен для записи сервисом.
          "path": "<path>",

          // Как часто менять файл логов.
          "rollingInterval": "Day",

          // Менять файл логов при превышении размера текущего файла.
          "rollOnFileSizeLimit": true,

          // Сколько файлов оставлять. Будут сохранены только последние файлы.
          "retainedFileCountLimit": 31,

          // (опционально) JSON-формат логов. Удалите или закомментируйте это
          // поле для записи логов в обычном формате.
          "outputTemplate": "[{Timestamp:HH:mm:ss} {Level:u3}] {Message:lj}
{Properties:lj}{NewLine}{Exception}"
        }
      },
      {
        // Пример настройки логирования в Elasticsearch.

```

```

// Удалите эту секцию, если не используете Elasticsearch.
"Name": "Elasticsearch",
"Args": {
  // Адрес Elasticsearch.
  "nodeUri": "http://localhost:9200",

  // Имя индекса Elasticsearch.
  "indexFormat": "archive.consumer-{0:yyyy.MM.dd}",

  // Поля, необходимые для совместимости.
  "autoRegisterTemplateVersion": "ESv7",
  "autoRegisterTemplate": true
}
},
{
  // Пример настройки логирования в ManticoreSearch.
  // Удалите эту секцию, если не используете ManticoreSearch.
  "Name": "ManticoreSearch",
  "Args": {
    // Адрес ManticoreSearch.
    "basePath": "http://127.0.0.1:9308",

    // Имя индекса ManticoreSearch.
    "indexName": "archive_logs",

    // Имя кластера в случае использования кластера.
    "clusterName": null
  }
}
],
},

"ConnectionStrings": {
  // Строка подключения к БД.
  "DefaultConnection": "<main_connection_string>"
},

// Основная секция настроек signature-updater.
"Enhancer": {
  // Адрес TSP, которая будет использована при усовершенствовании.
  "TSPAddress": "<tsp_url>",

  // Флаг, включающий использование стандартного адреса OCSP,
  // указанного с помощью политики DefaultOCSPURL клиента OCSP
  // в случае отсутствия адреса OCSP в сертификате подписанта.
  "CadesUseOcspAuthorizedPolicy": true,

  // В КриптоПро Архив есть два статуса контейнера, обозначающих ошибку:
  // «Ошибка проверки подписи» и «Ошибка обработки подписи».
  // В случае возникновения ошибки как минимум с одной подписью
  // ни одна подпись в контейнере не будет усовершенствована.
  //
  // Первый статус означает, что как минимум одна подпись в контейнере
  // не прошла проверку подлинности. Иногда, тем не менее,
  // такой статус может быть присвоен в связи с ошибкой, которая
  // в данном конкретном сценарии вызвана не ошибкой проверки,
  // а ошибкой обработки подписи. Для того, чтобы в этом случае внести
  // коррективы в получаемый контейнером статус, добавьте hex-строку с
  // кодом ошибки в этот список.
  "ErrorCodes": ["0x00000000"],

  // Количество дней перед временем истечения срока действия подписи,

```

```

// определяющее временной интервал, в который система КриптоПро Архив
// повторно обеспечит подпись доказательствами подлинности. Подпись,
// дата окончания срока действительности которой попала в этот интервал,
// считается подлежащей обновлению.
"NumberOfDaysBeforeExpirationDate": 90,

// Число потоков, используемых для первого усовершенствования подписей.
"NumberOfThreadsForIncomingDocuments": 1,

// Число потоков, используемых для повторного усовершенствования
// подписей.
"NumberOfThreadsForExistingDocuments": 1,

// Число контейнеров, запрашиваемых каждым потоком из числа
// NumberOfThreadsForExistingDocuments для последовательного
// повторного усовершенствования.
"NumberOfExistingDocuments": 100,

// Число контейнеров, запрашиваемых каждым потоком из числа
// NumberOfThreadsForIncomingDocuments для последовательного
// первого усовершенствования.
"NumberOfIncomingDocuments": 100,

// Время в миллисекундах, которое каждый поток будет ждать до
// следующей попытки получить контейнеры для первого усовершенствования.
"IncomingThreadDelayMs": 50,

// Время в миллисекундах, которое каждый поток будет ждать до
// следующей попытки получить контейнеры для повторного усовершенствования.
"ExistingThreadDelayMs": 50,

// Время в секундах, которое поток ждёт между опросами БД для установки
// статуса «Требуется обновление подписи».
"NumberOfSecondsToWaitExpirationCheck": 60
},

"General": {
  // СУБД. Возможные значения: PostgreSQL, Oracle.
  "DatabaseProvider": "PostgreSql"
},

"RabbitMq": {
  // Виртуальный хост RabbitMQ.
  "VirtualHost": "archive",

  // Имя пользователя RabbitMQ.
  "Username": "archive",

  // Пароль пользователя RabbitMQ.
  "Password": "1qaz@WSX",

  // Конечные точки RabbitMQ.
  "Endpoints": [
    {
      // IP-адрес или доменное имя RabbitMQ.
      "Hostname": "rabbitmq.ru",

      // Порт RabbitMQ. Порт по умолчанию: 5672.
      // Укажите 5671 при использовании TLS.
      "Port": 5671,

      // Адрес API управления RabbitMQ для мониторинга очередей.

```

```

// Для client-api это поле можно не заполнять.
"ApiAddress": "https://rabbitmq.ru:15671",

// Требование использования mTLS.
// Если false, значения остальных полей Ssl* не имеет значения.
"SslEnabled": true,

// Путь к клиентскому сертификату в формате PFX.
"SslCertPath": "/home/cp/downloads/cproar.pfx",

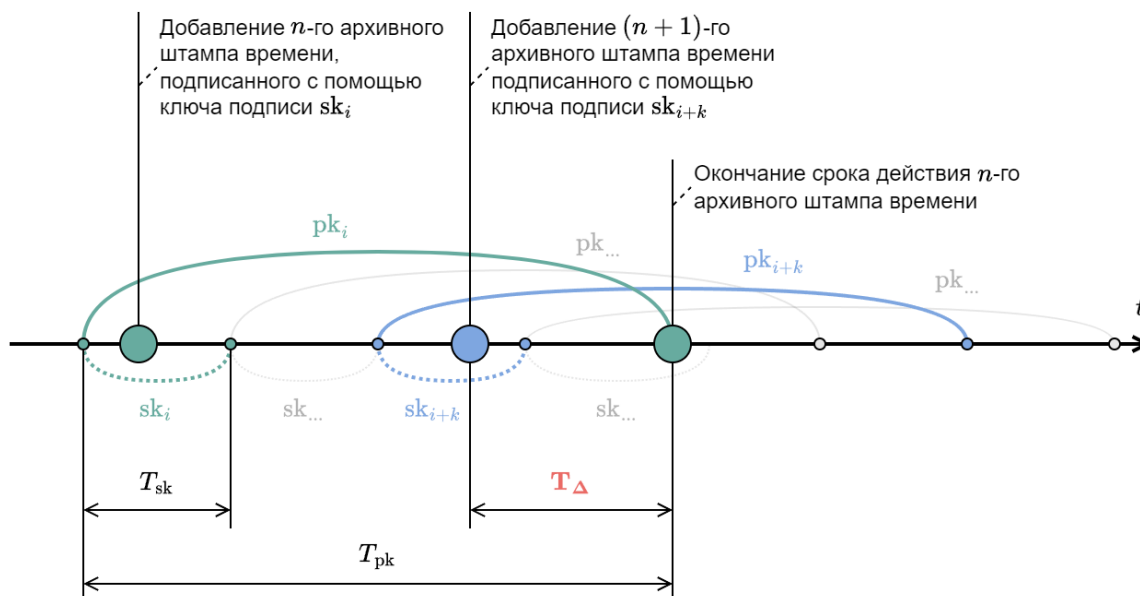
// Пароль от PFX.
"SslCertPassphrase": "<password>",

// Доменное имя сервера, к которому проводится подключение.
"SslServerName": "rabbitmq.ru"
}
]
}
}

```

ВАЖНО

Если сертификат службы штампов времени действует дольше 1 года 3 месяцев, рекомендуется установить значение параметра NumberOfDaysBeforeExpirationDate в 500.



$sk_i, sk_{...}, sk_{i+k}$	ключи подписи службы TSP
$pk_i, pk_{...}, pk_{i+k}$	сертификаты службы TSP
T_{sk}	срок действия ключа подписи службы TSP
T_{pk}	срок действия сертификата службы TSP
T_{Δ}	параметр КриптоПро Архив, указывающий, за какое время до истечения сертификата службы TSP необходимо добавить очередной архивный штамп времени

Для более подробного пояснения значения параметра

`$.Enhancer.NumberOfDaysBeforeExpirationDate` обратимся к рисунку. Параметру `NumberOfDaysBeforeExpirationDate` соответствует значение T_{Δ} . Если $T_{\Delta} > T_{pk} - T_{sk}$ (другими словами, повторное усовершенствование подписи будет происходить на том же ключе подписи службы TSP, что и предыдущее, и, соответственно, дата истечения подписи не изменится после добавления архивного штампа), усовершенствование подписи произведено не будет, а контейнер перейдёт в статус «Ошибка обработки подписи».

3.8 Настройка consumer

В данном разделе приведена настройка программы consumer. Программа представляет собой приёмник сообщений RabbitMQ. Каждой очереди соответствует свой тип обработчика. Параметры обработчика можно настраивать в конфигурационном файле программы:

- Очередь на отправку уведомлений. Тип обработчика: Notification.
- Очередь на сохранение подписанных документов в опциональной подсистеме Архив УЦ. Тип обработчика: Document.
- Очередь на использование плагинов обработки подписей после усовершенствования (успешного или неуспешного). Тип обработчика: Signature.
- Очередь на создание отчётов. Тип обработчика: ReportCalculator.

Для настройки программы потребуется установленный на сервере КриптоПро Архив в конфигурации «Полная установка» (установлены все компоненты) или «Обработчики очередей» (установлен только consumer), а также RabbitMQ на данном или удалённом сервере.

3.8.1 Добавление службы

На ОС семейства Windows Server программа consumer работает как служба Windows. Для добавления службы выполните в PowerShell от лица администратора следующие команды:

```
New-Service -Name consumer -BinaryPathName C:\inetpub\cp-  
archive\consumer\CryptoPro.Archive.Consumer.Service.exe -StartupType Automatic  
  
Start-Service -Name consumer
```

Обратите внимание на указание полного пути до исполняемого файла.

3.8.2 Конфигурационный файл

Конфигурационный файл расположен по пути C:\inetpub\cp-archive\consumer\appsettings.json. Этот JSON-файл поддерживает комментарии: строки, начинающиеся с «//», не учитываются. После изменения конфигурации перезапустите службу.

```

{
  // Настройки логирования.
  "Serilog": {
    "Using": [
      "Serilog.Sinks.Console",
      "Serilog.Sinks.File",
      "Serilog.Sinks.Elasticsearch",
      "Serilog.Sinks.ManticoresSearch"
    ],
    "MinimumLevel": {
      // Общий уровень логирования.
      "Default": "Debug",

      // Переопределение уровней логирования для компонентов.
      "Override": {
        "Microsoft.EntityFrameworkCore": "Warning",
        "Microsoft.EntityFrameworkCore.Query": "Warning",
        "Microsoft.AspNetCore": "Warning"
      }
    },
  },

  // Перечисление мест, куда писать логи.
  "WriteTo": [
    {
      // Пример настройки логирования в файл.
      // Рекомендуется использовать именно логирование в файл.
      "Name": "File",
      "Args": {
        // Путь к файлу, в который будут записаны логи.
        // Путь должен быть доступен для записи сервисом.
        "path": "<path>",

        // Как часто менять файл логов.
        "rollingInterval": "Day",

        // Менять файл логов при превышении размера текущего файла.
        "rollOnFileSizeLimit": true,

        // Сколько файлов оставлять. Будут сохранены только последние файлы.
        "retainedFileCountLimit": 31,

        // (опционально) JSON-формат логов. Удалите или закомментируйте это
        // поле для записи логов в обычном формате.
        "outputTemplate": "[{Timestamp:HH:mm:ss} {Level:u3}] {Message:l}j"
      },
      {Properties:j}{NewLine}{Exception}"
    },
    {
      // Пример настройки логирования в Elasticsearch.
      // Удалите эту секцию, если не используете Elasticsearch.
      "Name": "Elasticsearch",
      "Args": {
        // Адрес Elasticsearch.
        "nodeUri": "http://localhost:9200",

        // Имя индекса Elasticsearch.
        "indexFormat": "archive.consumer-{0:yyyy.MM.dd}",

        // Поля, необходимые для совместимости.

```

```

        "autoRegisterTemplateVersion": "ESv7",
        "autoRegisterTemplate": true
    }
},
{
    // Пример настройки логирования в ManticoreSearch.
    // Удалите эту секцию, если не используете ManticoreSearch.
    "Name": "ManticoreSearch",
    "Args": {
        // Адрес ManticoreSearch.
        "basePath": "http://127.0.0.1:9308",

        // Имя индекса ManticoreSearch.
        "indexName": "archive_logs",

        // Имя кластера в случае использования кластера.
        "clusterName": null
    }
}
]
},

"ConnectionStrings": {
    // Строка подключения к БД.
    "DefaultConnection": "<main_connection_string>"
},

"General": {
    // СУБД. Возможные значения: PostgreSQL, Oracle.
    "DatabaseProvider": "PostgreSQL"
},

// Основная секция.
"RabbitMq": {
    "Consumers": [
        {
            // Включен ли данный приёмник.
            "Enabled": false,

            // Отображаемое в логах имя приёмника.
            "Name": "Archive Report Calculator",

            // Тип приёмника.
            "Type": "ReportCalculator",

            // Имя пользователя RabbitMQ.
            "Username": "<username>",

            // Пароль
            "Password": "<password>",

            // Задержка в миллисекундах перед повторной
            // попыткой при возникновении ошибки.
            "DelayMs": 5000,

            // Имя очереди RabbitMQ.
            "QueueName": "archive.reports.requests.queue",

            // Имя обменника RabbitMQ.
            "ExchangeName": "archive.reports.requests.exchange",

            // Имя виртуального хоста RabbitMQ.

```

```

    "VirtualHost": "archive",

    // Конечные точки RabbitMQ.
    "Endpoints": [
        {
            // IP-адрес или доменное имя RabbitMQ.
            "Hostname": "rabbitmq.ru",

            // Порт RabbitMQ. Порт по умолчанию: 5672.
            // Укажите 5671 при использовании TLS.
            "Port": 5671,

            // Адрес API управления RabbitMQ для мониторинга очередей.
            // Для client-api это поле можно не заполнять.
            "ApiAddress": "https://rabbitmq.ru:15671",

            // Требование использования mTLS.
            // Если false, значения остальных полей Ssl* не имеет значения.
            "SslEnabled": true,

            // Путь к клиентскому сертификату в формате PFX.
            "SslCertPath": "/home/cp/downloads/cproar.pfx",

            // Пароль от PFX.
            "SslCertPassphrase": "<password>",

            // Доменное имя сервера, к которому проводится подключение.
            "SslServerName": "rabbitmq.ru"
        }
    ],
},
{
    "Enabled": false,
    "Name": "Archive CA Document Consumer",
    "Username": "<username>",
    "Password": "<password>",
    "QueueName": "archive.ca.documents.queue",
    "ExchangeName": "archive.ca.documents.exchange",
    "VirtualHost": "archive",
    "Type": "Document",
    "DelayMs": 5000,
    "Endpoints": [
        {
            "HostName": "localhost",
            "Port": 5672,
            "SslEnabled": false,
            "SslCertPath": "/path/to/certificate.pfx",
            "SslCertPassphrase": "<pin>",
            "SslServerName": "<domain>"
        }
    ],
},
{
    "Enabled": false,
    "Name": "Notification Consumer",
    "Username": "<username>",
    "Password": "<password>",
    "QueueName": "archive.notifications.queue",
    "ExchangeName": "archive.notifications.exchange",
    "VirtualHost": "archive",
    "Type": "Notification",
    "DelayMs": 5000,
    "Endpoints": [
        {
            "HostName": "localhost",

```

```

        "Port": 5672,
        "SslEnabled": false,
        "SslCertPath": "/path/to/certificate.pfx",
        "SslCertPassphrase": "<pin>",
        "SslServerName": "<domain>"
    ]
},
{
    "Enabled": false,
    "Name": "Signatures Consumer",
    "Username": "<username>",
    "Password": "<password>",
    "QueueName": "archive.signatures.queue",
    "ExchangeName": "archive.signatures.exchange",
    "VirtualHost": "archive",
    "Type": "Signature",
    "DelayMs": 5000,
    "Endpoints": [
        "HostName": "localhost",
        "Port": 5672,
        "SslEnabled": false,
        "SslCertPath": "/path/to/certificate.pfx",
        "SslCertPassphrase": "<pin>",
        "SslServerName": "<domain>"
    ]
}
],
},

// Настройка сохранения подписанных документов.
"ArchiveCa": {
    // Активна ли функциональность.
    // Если false, остальные значения в этой секции не имеют значения.
    // Для работы необходим RabbitMQ и программа consumer.
    "UseArchiveCa": false,

    "ConnectionStrings": {
        // Строка подключения к каталогу БД.
        // СУБД должна быть та же, что указана в секции General.
        "DatabaseCatalogue": "<catalogue_connection_string>"
    }
}
}

```

Если не включить ни один приёмник из секции Consumers, программа выдаст ошибку в логи при запуске.

4 Обновление

В данной главе приведены инструкции по обновлению компонентов Архива. Выборочное обновление компонентов возможно, но не рекомендуется. Для обновления последовательно выполните следующие шаги:

1. Перед обновлением остановите работающие компоненты Архива:
 - admin-api (остановка производится в приложении IIS)
 - client-api (остановка производится в приложении IIS)
 - signature-updater (остановка производится в приложении **Службы**)
 - consumer (остановка производится в приложении **Службы**)
2. Установите новую версию программы, не удаляя предыдущую.
3. Выполните миграцию на новую версию базы данных для всех используемых баз данных. Для этого воспользуйтесь инструкциями ниже в зависимости от используемой СУБД.
4. Запустите остановленные ранее службы.

Обновление Архива завершено.

4.1 Обновление базы данных PostgreSQL.

Выполните следующую команду в PowerShell от лица администратора. В этой и следующей командах замените строку подключения (параметр `--connection-string`) на используемую:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
  --database `
  --mode upgrade `
  --database-provider PostgreSQL `
  --connection-string "username = <username>; password = <password>; host =
  <host>; database = <database>"
```

При использовании подсистемы Архив УЦ проведите миграцию для каталога баз данных Архива УЦ:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
  --database `
  --mode upgrade `
  --database-provider PostgreSQL `
```

```
--connection-string "username = <username>; password = <password>; host =
<host>; database = <catalogue_database>" `
--ca `
--type catalogue
```

А также для каждой базы данных с подписанными документами (повторите команду ниже для каждой базы данных с подписанными документами):

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
--database `
--mode upgrade `
--database-provider PostgreSQL `
--connection-string "username = <username>; password = <password>; host =
<host>; database = <storage_database>" `
--ca `
--type storage
```

4.2 Обновление базы данных Oracle Database

В случае использования Oracle Database выполните следующую команду в PowerShell от лица администратора. В этой и следующей командах замените строку подключения (параметр `--connection-string`) и имя используемой базы данных (параметр `--target`) на используемые:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
--database `
--mode upgrade `
--database-provider Oracle `
--connection-string "User ID = SYS; DBA Privilege = SYSDBA; Password =
<password>; Data Source = <data_source>" `
--target <username>
```

При использовании подсистемы Архив УЦ проведите миграцию для каталога баз данных Архива УЦ:

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
--database `
--mode upgrade `
--database-provider Oracle `
--connection-string "User ID = SYS; DBA Privilege = SYSDBA; Password =
<password>; Data Source = <data_source>" `
--target <catalogue_database> `
--ca `
--type catalogue
```

А также для каждой базы данных с подписанными документами (повторите команду ниже для каждой базы данных с подписанными документами):

```
C:\inetpub\cp-archive\config\Archive.Config migrate `
--database `
--mode upgrade `
--database-provider Oracle `
```

```
--connection-string "User ID = SYS; DBA Privilege = SYSDBA; Password =  
<password>; Data Source = <data_source>" `--target <storage_database> `  
--ca `  
--type storage
```

5 Администрирование

5.1 Настройка хранилищ и информационных систем

В данном разделе описана настройка хранилищ и информационных систем в КриптоПро Архив, рассмотрены принципы взаимодействия информационных систем и хранилищ.

5.1.1 Общее описание

КриптоПро Архив хранит подписи в *контейнере*. Контейнер представляет собой совокупность подписи или нескольких подписей документа и набора метаданных, таких как, например, дата и время следующего усовершенствования этих подписей. Один контейнер может содержать в себе подписи только одного документа. Контейнер всегда содержит только усовершенствованные (последние актуальные) подписи документа: после усовершенствования старые подписи уничтожаются. Контейнер не содержит в себе подписанного документа. Для хранения подписанных документов существует опциональная подсистема Архив УЦ. Контейнеры объединены в *хранилище*. Хранилищ может быть несколько.

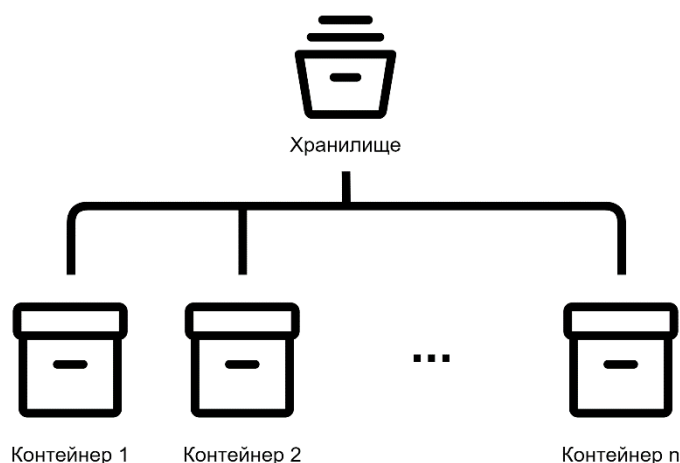


Рисунок 3. Хранилище с контейнерами.

К хранилищу прикреплены *информационные системы*. В КриптоПро Архив информационная система представляет собой набор данных о зарегистрированных СЭДО (или аналогичных ИС) или отдельных

пользователях. К одному хранилищу может быть прикреплено несколько информационных систем. Разные информационные системы могут иметь разные права по отношению к данному хранилищу.

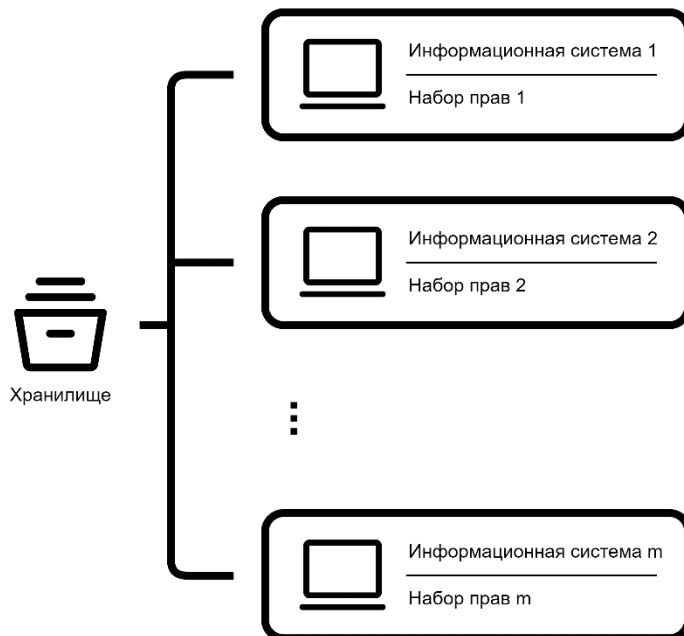
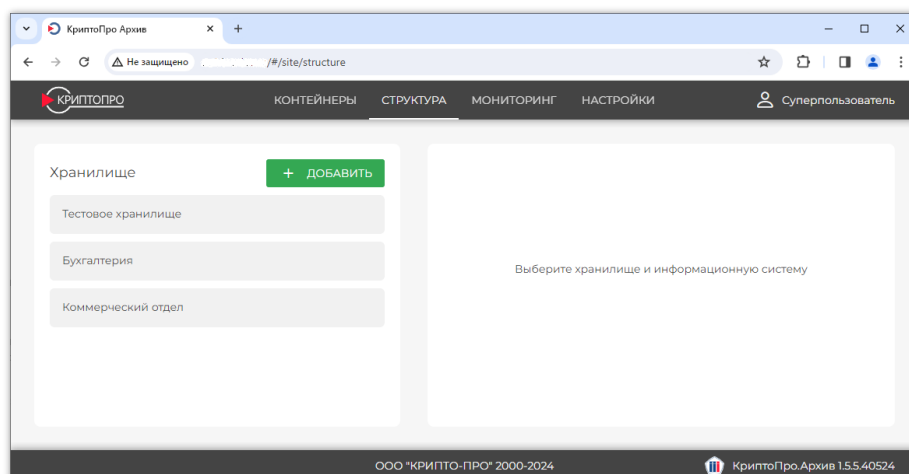


Рисунок 4. Хранилище с прикреплёнными к нему информационными системами.

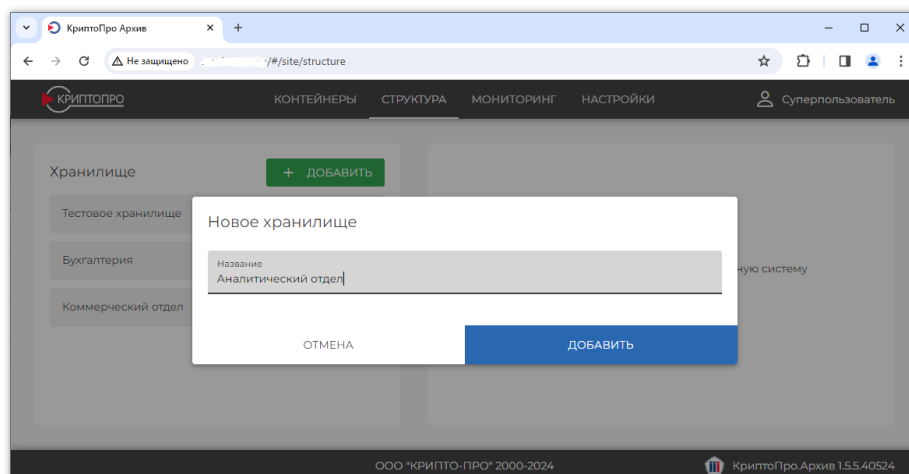
5.1.2 Первичная настройка

В данном подразделе описан процесс создания хранилищ и информационных систем. Для выполнения дальнейших действий потребуются права суперпользователя КристоПро Архив.

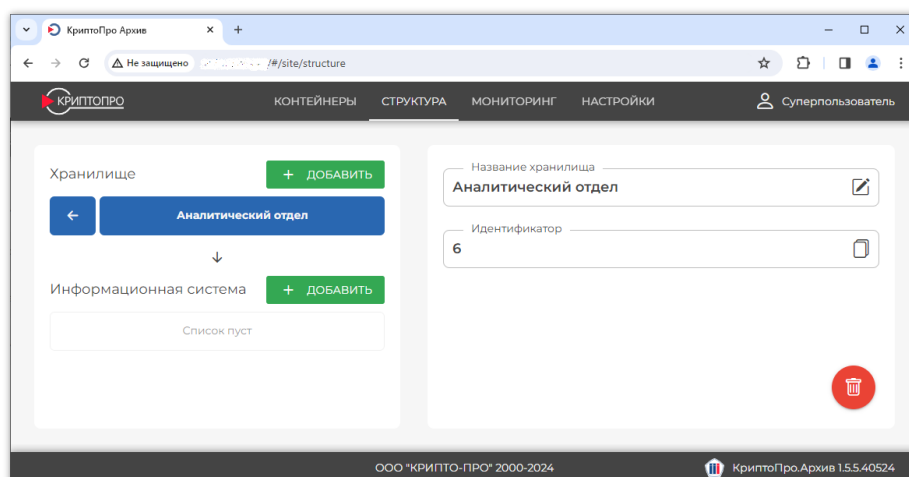
Для создания хранилища зайдите в административную панель от лица суперпользователя и перейдите на вкладку «Структура»:



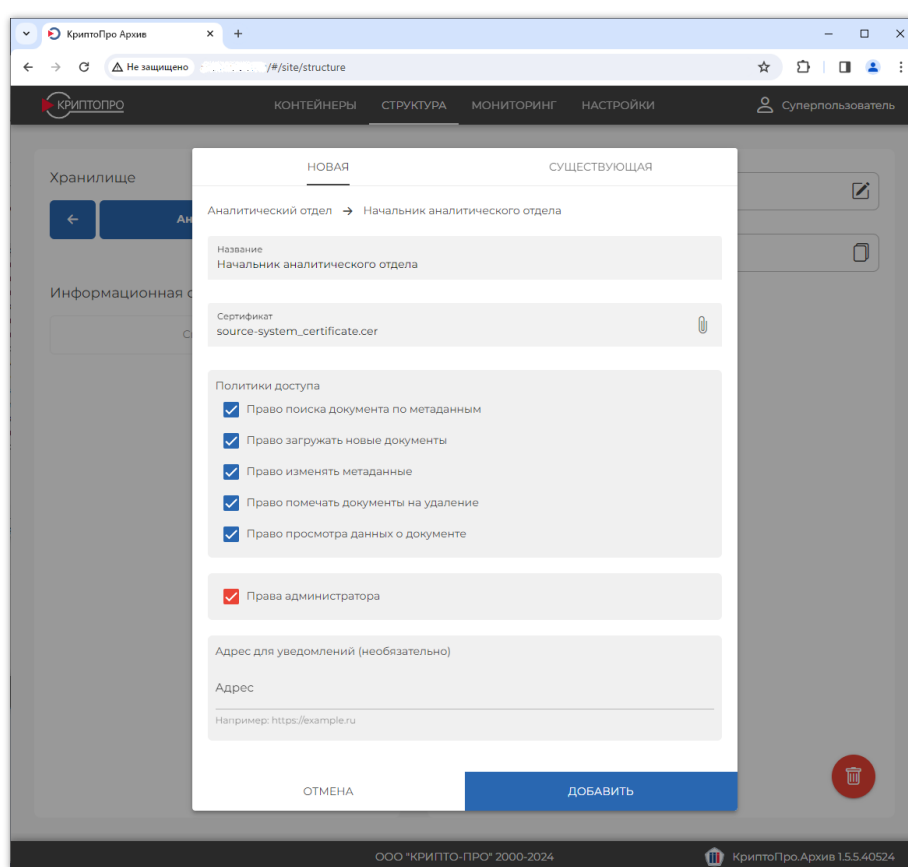
Нажмите «Добавить». В появившемся окне введите имя хранилища и нажмите «Добавить»:



Созданное хранилище появится в списке хранилищ. Нажмите на него:



Откроется меню управления хранилищем, где его можно переименовать. Далее необходимо создать информационную систему. В примере ниже будет создана управляющая информационная система. Для каждого хранилища рекомендуется создать как минимум одну управляющую информационную систему для упрощения процесса отладки. Для создания информационной системы слева напротив нажмите «Добавить». Введите название создаваемой информационной системы, укажите ещё сертификат, отметьте все политики доступа. Поле «Адрес для уведомлений» оставьте пустым.



Нажмите «Добавить». Созданная информационная система появится в списке информационных систем, привязанных к данному хранилищу. Справа можно просмотреть и изменить параметры информационной системы.

Для входа от лица созданной информационной системы её сертификат должен быть установлен на компьютере. Далее закройте браузер и откройте его заново. Выберите сертификат созданной информационной системы.

5.1.3 Права и роли

В терминах Архива:

- **Информационная система (ИС, Пользователь)** — автоматизированная система, использующая функции Архива для работы с Контейнерами. Инструкция по созданию ИС приведена в подразделе 5.1.2 Первичная настройка.
- **Администратор** (управляющая ИС) — лицо, которое имеет доступ к управлению выделенным ему хранилищем, созданию собственных хранилищ, подключению ИС к этим хранилищам, управлению их правами по отношению к этим хранилищам, а также дополнительными службами УЦ для этих ИС. Для создания Администратора создайте ИС и выдайте ей право управления хранилищем.
- **Суперпользователь** — лицо, которое настраивает Архив, может управлять Администраторами и осуществлять любые настройки Архива. Суперпользователь не может создавать контейнеры, но может управлять всеми созданными контейнерами. Для инструкции по созданию суперпользователя см. раздел 5.5 Управление суперпользователями.

В данном подразделе приведены возможные права информационной системы по отношению к хранилищу и соответствующие им допустимые действия.

Имя права	Допустимые действия
Право поиска документа по метаданным	• Поиск списка контейнеров с набором фильтров.
Право загружать новые документы	• Создание контейнеров.
Право изменять метаданные	• Изменение метаданных контейнеров.

Право помечать

документы на

удаление

- Удаление контейнеров.

Право просмотра

данных о

документе

- Просмотр подробной информации о контейнерах.

Данное право превращает ИС в Администратора.

Право управления

хранилищем

- Отправка контейнеров на повторную обработку.
- Создание информационных систем без прав администратора в рамках хранилища.
- Создание хранилищ.
- Управление дополнительными службами УЦ для ИС, состоящих в данном хранилище.

5.2 Настройка дополнительных служб УЦ

В данном разделе описана настройка дополнительных служб OCSP и TSP. Данная функциональность предоставляет возможность явно указать, какие пары адресов служб OCSP и опционально TSP необходимо использовать для издателя данного сертификата подписанта. Можно добавить дополнительные службы УЦ глобально для всех информационных систем, создающих контейнеры, а можно привязать эти службы к конкретной информационной системе. Пользователь с правом управления хранилищем может управлять дополнительными службами УЦ для информационных систем в этом хранилище.

КриптоПро Архив обращается к парам служб OCSP/TSP в следующем порядке до первого успеха (до первого определённого ответа о статусе сертификата):

1. Дополнительные адреса служб УЦ для данной ИС (если адрес TSP не указан, он берётся из настроек signature-updater).
2. Глобальные дополнительные адреса служб УЦ (если адрес TSP не указан, он берётся из настроек signature-updater).
3. Адрес OCSP, указанный в сертификате подписанта и адрес TSP, указанный в настройках signature-updater.
4. Адрес, указанный в групповой политике клиента OCSP.

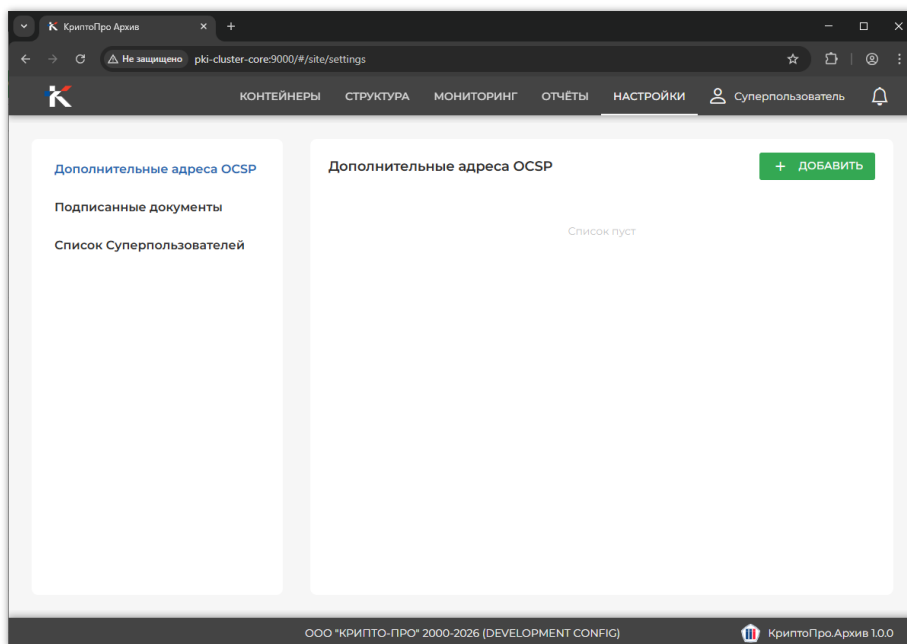
Адреса OCSP и TSP указываются парами. Указание адреса TSP не обязательно. Если дополнительно к адресу OCSP указан адрес TSP, он будет использован для получения меток времени. Если адрес TSP не указан, для получения меток времени будет использован адрес из настроек программы signature-updater.

Таким образом, функциональность позволяет указать, какие адреса служб OCSP и TSP следует использовать для издателя данного сертификата подписанта. Издатель определяется по CN.

Для выполнения дальнейших шагов на настраиваемом сервере потребуется установленный КриптоПро Архив в конфигурации «Полная установка»

ЖТЯИ.00117-01 92 03. КриптоПро Архив. Руководство администратора Windows (установлены все компоненты) или «Подсистема приёма подписей» (установлены admin-api, client-api и frontend).

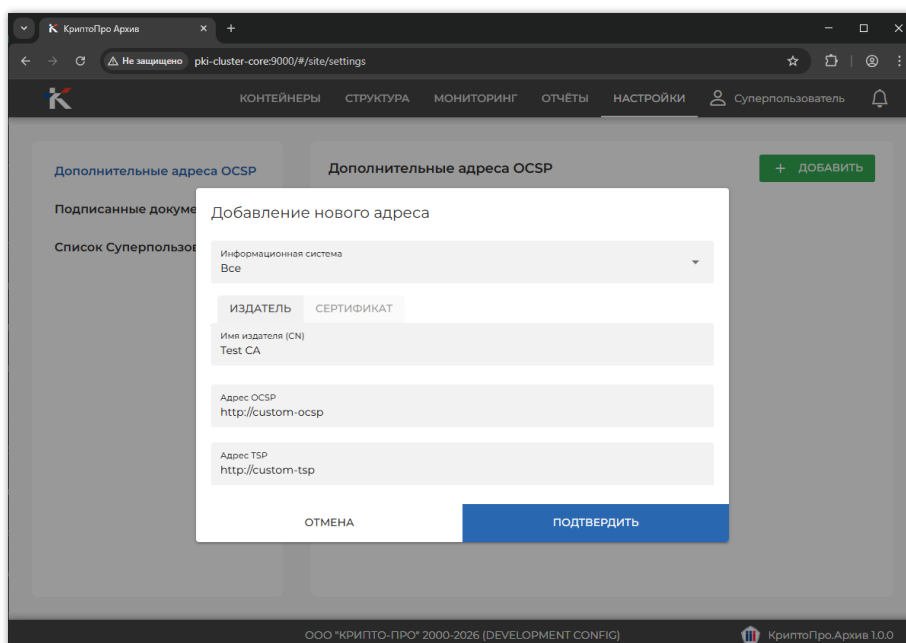
Для настройки дополнительных служб откройте административную панель КриптоПро Архив от лица суперпользователя и перейдите в раздел «Настройки». Слева выберите вкладку «Дополнительные адреса OCSP»:



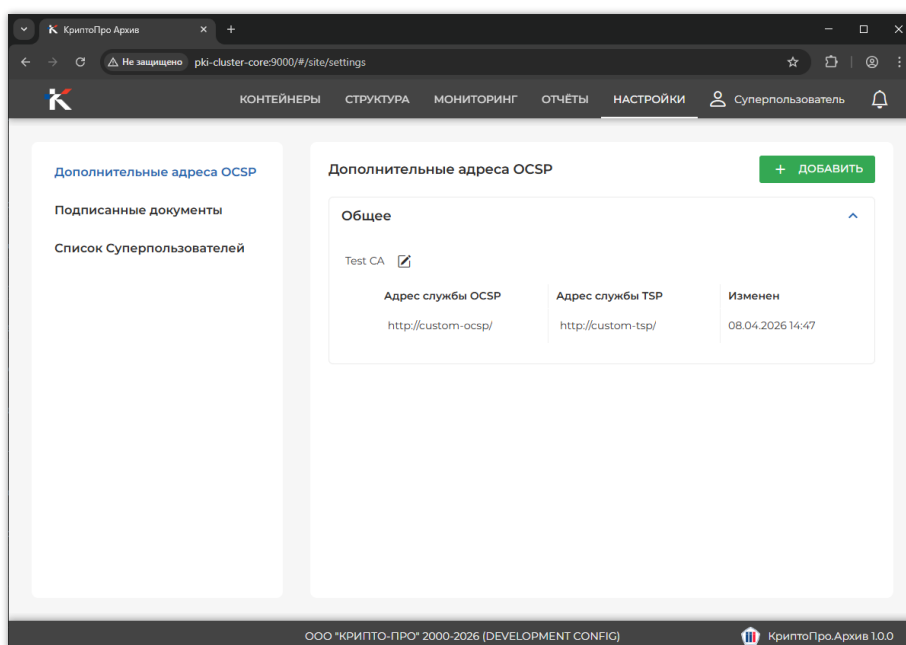
Нажмите «Добавить». Далее необходимо указать CN издателя, адрес дополнительной службы OCSP и опционально адрес службы TSP. Имя издателя можно указать двумя способами, которым соответствуют вкладки над этим полем:

- ввести имя издателя вручную,
- получить имя издателя с помощью любого сертификата, выпущенного этим издателем.

Пример заполнения вручную:



Нажмите «Подтвердить». После этого в списке появятся добавленные дополнительные адреса службы OSCP и TSP:



При добавлении нескольких адресов для одного издателя обращения будут происходить в порядке, указанном на этой странице сверху вниз. Элементы можно переставить местами.

5.3 Сохранение подписанных документов (ранее Архив УЦ)

В данном разделе приведена настройка опциональной подсистемы хранения подписанных документов (ранее Архив УЦ). Описание подсистемы приведено в разделе.

Для работы подсистеме необходимы установленные компоненты admin-api (для настройки) и consumer (для отложенного сохранения подписанных документов в базу данных). Также обязательно использование очереди. В инструкциях ниже предполагается, что на настраиваемом сервере установлены эти компоненты. В некоторых сценариях компоненты могут быть установлены на разных серверах, однако процесс настройки в этом случае идентичен. Также предполагается доступ к базе данных PostgreSQL версии не ниже 11 или Oracle Database 12c.

ЗАМЕЧАНИЕ

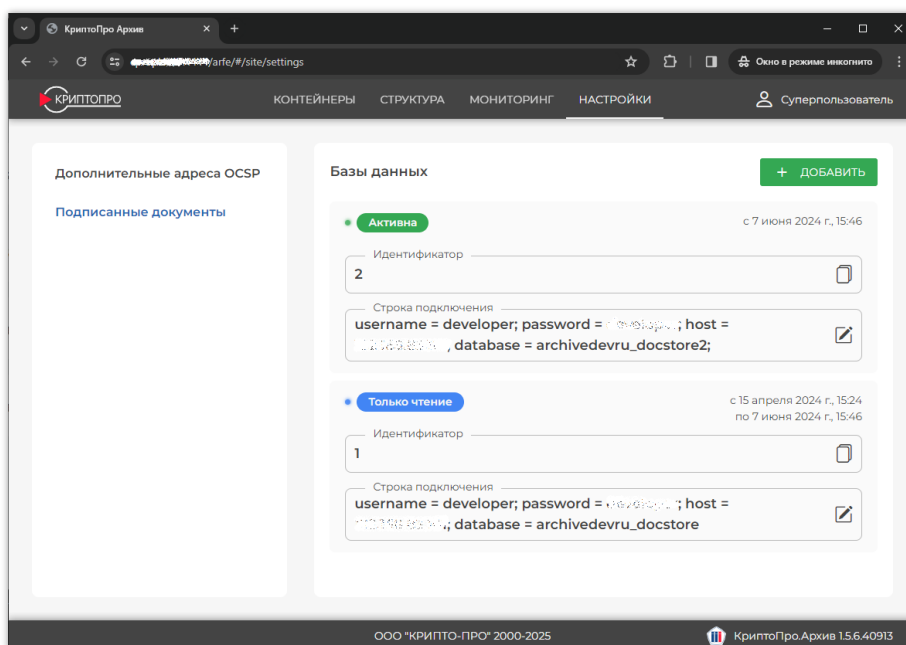
Идентификаторы подписанных документов в подсистеме Архив УЦ совпадают с идентификаторами соответствующих контейнеров в КриптоПро Архив.

Заполните секцию ArchiveCa в конфигурационных файлах компонентов admin-api, client-api и consumer. Пример заполненной секции:

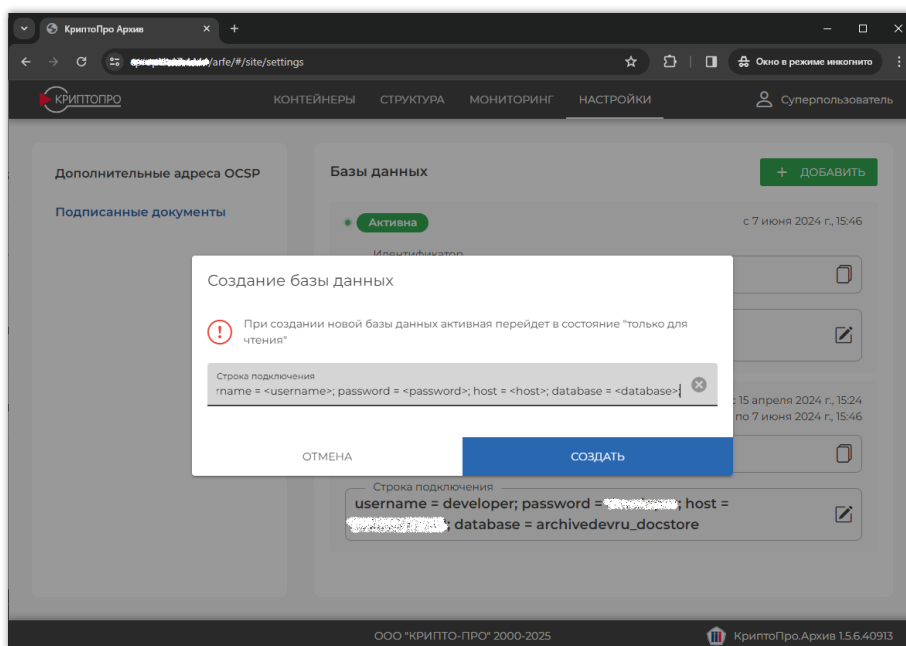
```
// Настройка сохранения подписанных документов.
"ArchiveCa": {
  // Активна ли функциональность.
  // Если false, остальные значения в этой секции не имеют значения.
  // Для работы необходим RabbitMQ и программа consumer.
  "UseArchiveCa": true,

  "ConnectionStrings": {
    // Строка подключения к каталогу БД.
    // СУБД должна быть та же, что указана в секции General.
    "DatabaseCatalogue": "<catalogue_connection_string>"
  }
}
```

Перейдите в веб-интерфейс администратора в раздел Настройки > Подписанные документы:



Нажмите «Добавить». Введите строку подключения к созданному ранее хранилищу подписанных документов. В примере ниже используется строка подключения к базе данных PostgreSQL: «**username** = <username>; **password** = <password>; **host** = 127.0.0.1; **database** = <database_name>». Пример строки подключения для базы данных Oracle Database: «**User ID** = <username>; **Password** = <password>; **Data Source** = 127.0.0.1:1521/ORCL». При заполнении кавычки указывать не нужно.



Нажмите «Создать». Программа проверит доступность и формат базы данных и добавит её в список баз данных, если проверка будет пройдена успешно.

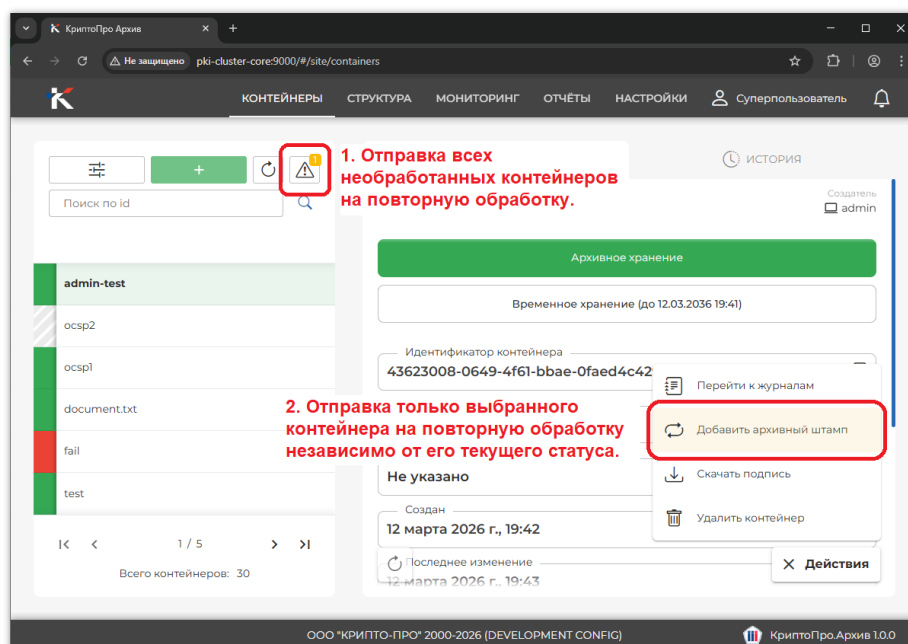
Настройка подсистемы Архив УЦ завершена.

5.4 Повторная обработка контейнеров

Для удобства в этом разделе будем называть контейнеры в статусе «Ошибка обработки подписи» *необработанными*, а контейнеры в статусе «Ошибка проверки подписи» — *недействительными*.

В ходе работы Архива может возникнуть ситуация, когда контейнер по той или иной причине не был обработан (т.е. подписи в этом контейнере не были усовершенствованы). Например, недоступны службы УЦ или подпись изначально недействительна. В этом случае контейнер станет необработанным или недействительным. Для того, чтобы повторить обработку контейнера, необходимо открыть веб-интерфейс администратора и перейти в раздел контейнеры. Далее есть два варианта:

1. Над списком контейнеров расположена кнопка, позволяющая отправить на повторную обработку все необработанные контейнеры, находящиеся в администрируемых текущим пользователем хранилищах. Число в углу указывает количество контейнеров, которые будут затронуты.
2. Для отправки только выбранного контейнера на повторную обработку в карточке контейнера нажмите Действия > Добавить архивный штамп.



На текущий момент в Архиве нет возможности автоматически отправлять контейнеры на повторную обработку. Это мотивируется тем, что любая ошибка, полученная в процессе усовершенствования подписей, должна быть внимательно рассмотрена администратором. Перед повторной обработкой необходимо устранить причину ошибки.

5.5 Управление суперпользователями

В Архиве можно создать несколько суперпользователей. Они равноправны и «видят» друг друга в веб-интерфейсе. При создании нового суперпользователя все существующие суперпользователи получают уведомление.

Управление суперпользователями осуществляется только через консольную программу admin-api. Для получения актуальной справки по командам выполните

```
C:\inetpub\cp-archive\admin-api\Archive.AdminApi help
```

Для вывода списка суперпользователей выполните

```
C:\inetpub\cp-archive\admin-api\Archive.AdminApi list -t superuser
```

Пример вывода:

Id	Thumbprint	Name
2	bf4eb66f30e1cdc9ac6f8c8acf5417c9d2b4780e	superuser
3	261b9476c2ed89e4cb7f3230f2b375feab837e51	superuser

Для создания нового суперпользователя выполните

```
C:\inetpub\cp-archive\admin-api\Archive.AdminApi add -t superuser --thumbprint
<thumbprint> --name <name>
```

где <thumbprint> — отпечаток сертификата, с которым будет заходить суперпользователь, <name> — опциональное произвольное отображаемое имя (по умолчанию superuser).

Для удаления суперпользователя выполните

```
C:\inetpub\cp-archive\admin-api\Archive.AdminApi remove -t superuser --id <id>
```

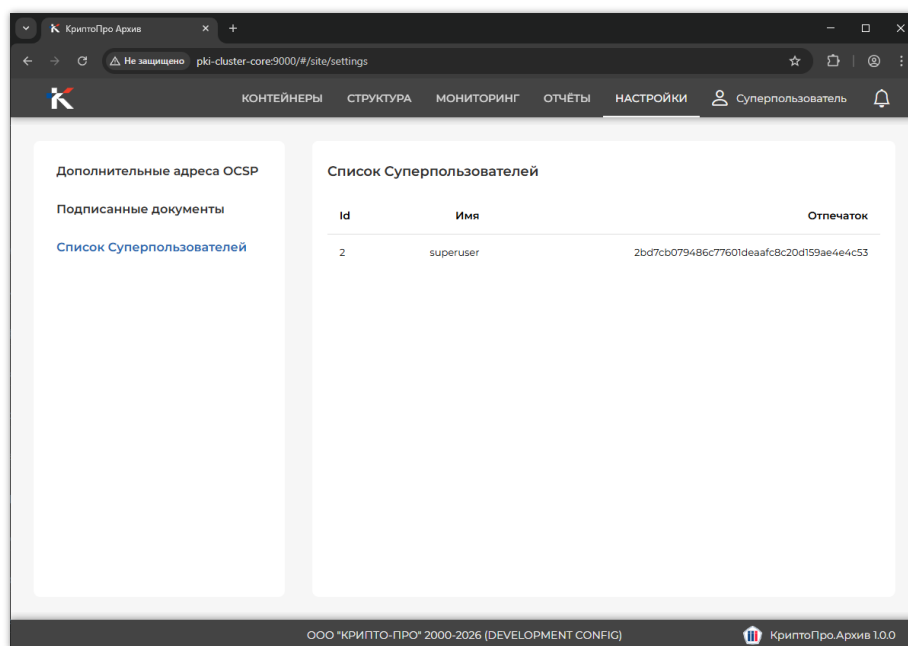
где <id> — идентификатор суперпользователя, полученный из веб-интерфейса администратора или из вывода подпрограммы list.

Для изменения отпечатка сертификата или отображаемого имени суперпользователя выполните

```
C:\inetpub\cp-archive\admin-api\Archive.AdminApi edit -t superuser --id <id> --
thumbprint <new_thumbprint> --name <new_name>
```

где `<id>` — идентификатор суперпользователя, полученный из веб-интерфейса или подпрограммы `list`, `<new_thumbprint>` — новый отпечаток суперпользователя (если не указан, не будет изменён), `<new_name>` — новое отображаемое имя пользователя (если не указано, не будет изменено).

Для просмотра списка зарегистрированных суперпользователей в веб-интерфейсе перейдите в раздел Настройки > Список Суперпользователей:



Этот список нельзя изменять из веб-интерфейса.