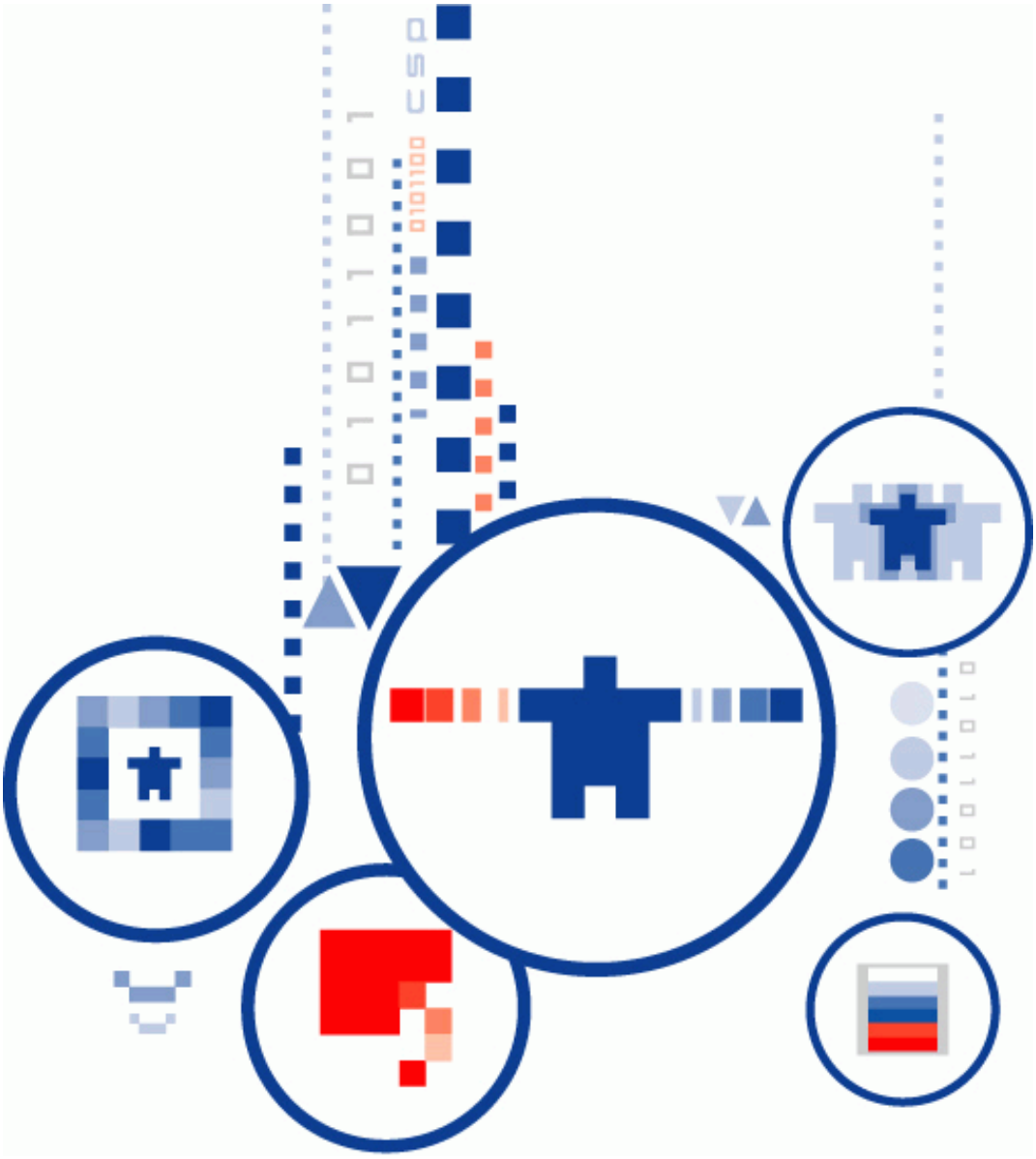


Программный комплекс

«КриптоПро Архив»

Руководство администратора

ЖТЯИ.00117-01 92 01

Оглавление

1 Описание 6
1.1 Аннотация 6
1.2 Общие сведения 7
1.3 Архитектура решения 8
1.3.1 ОС семейства Windows Server 8
1.3.2 ОС семейства Linux 9
1.4 Опциональная подсистема Архив УЦ 11
2 Установка 12
2.1 Описание процесса установки КриптоПро Архив 12
2.1.1 ОС семейства Windows Server 12
2.1.2 Astra Linux 13
2.2 Установка КриптоПро CSP 15
2.2.1 Установка КриптоПро CSP на ОС семейства Windows Server 15
2.2.2 Установка КриптоПро CSP и ГОСТ NGINX на Astra Linux 16
2.3 Установка Elasticsearch 18
2.3.1 Установка Elasticsearch на ОС семейства Windows Server 18
2.3.2 Установка Elasticsearch на Astra Linux 19
2.4 Установка Kibana 21
2.4.1 Установка Kibana на ОС семейства Windows Server 21
2.4.2 Установка Kibana на Astra Linux 23
2.5 Установка RabbitMQ 25
2.5.1 Установка RabbitMQ на ОС семейства Windows Server 25
2.5.2 Установка RabbitMQ на Astra Linux 28
2.7 Установка Microsoft Hosting Bundle 31
2.7.1 Установка Microsoft Hosting Bundle на ОС семейства Windows Server 31
2.8 Установка PostgreSQL 32
2.8.1 Установка PostgreSQL на ОС семейства Windows Server 32

2.8.2 Установка PostgreSQL на Astra Linux SE 1.7 37
2.8.3 Установка PostgreSQL на Astra Linux 38
2.9 Установка КриптоПро Архив 39
2.9.1 Установка КриптоПро Архив на ОС семейства Windows Server 39
2.9.2 Установка КриптоПро Архив на ОС семейства Linux 42
2.10 Установка Erlang 43
2.10.1 Установка Erlang OTP на ОС семейства Windows Server 43
2.10.2 Установка ESL Erlang на Astra Linux 46
2.11 Установка Python 3 47
2.11.1 Установка Python 3 на ОС семейства Windows Server 47
2.12 Установка NSSM 49
2.12.1 Установка NSSM на ОС семейства Windows Server 49
3 Настройка 53
3.1 Настройка RabbitMQ 53
3.1.1 Настройка RabbitMQ на ОС семейства Windows Server 53
3.1.2 Настройка RabbitMQ на ОС семейства Linux 57
3.2 Настройка Elasticsearch 58
3.2.1 Настройка Elasticsearch на ОС семейства Windows Server 58
3.2.2 Настройка Elasticsearch на ОС семейства Linux 59
3.3 Настройка PostgreSQL 60
3.3.1 Настройка PostgreSQL на ОС семейства Windows Server 60
3.3.2 Настройка PostgreSQL на Astra Linux 1.7 66
3.3.3 Настройка PostgreSQL на Astra Linux 68
3.4 Настройка Oracle Database 71
3.4.1 Настройка Oracle Database на ОС семейства Windows Server 71
3.4.2 Настройка Oracle Database на ОС семейства Linux 73
3.5 Настройка admin-api и client-api 75
3.5.1 Настройка admin-api и client-api на ОС семейства Windows Server 75

3.5.2 Настройка admin-api и client-api на ОС семейства Linux 89
3.6 Настройка frontend 95
3.6.1 Настройка frontend на ОС семейства Windows Server 95
3.6.2 Настройка frontend на ОС семейства Linux 97
3.7 Настройка signature-updater 100
3.7.1 Настройка signature-updater на ОС семейства Windows Server 100
3.7.2 Настройка signature-updater на ОС семейства Linux 105
3.8 Настройка consumer 111
3.8.1 Настройка consumer на ОС семейства Windows Server 111
3.8.2 Настройка consumer на ОС семейства Linux 114
3.10 Управление лицензиями 118
3.10.1 Управление лицензиями на ОС семейства Windows Server 118
3.10.2 Управление лицензиями на ОС семейства Linux 119
3.11 Настройка Архив УЦ 122
3.11.1 Настройка Архив УЦ на ОС семейства Windows Server 122
3.11.2 Настройка Архив УЦ на ОС семейства Linux 129
3.12 Настройка журналирования 136
3.12.1 Настройка отправки журналов в Elasticsearch 136
3.12.2 Настройка отправки журналов в ManticoreSearch 137
3.12.3 Настройка отправки журналов в файл 138
3.12.4 Отображение журналов в административном интерфейсе 139
3.13 Настройка дополнительных служб OCSP 141
3.14 Настройка хранилищ и информационных систем 145
3.14.1 Общее описание 145
3.14.2 Первичная настройка 146
3.14.3 Права информационных систем 149
4 Обновление 150
4.1 Обновление КриптоПро Архив на ОС семейства Windows Server 150

4.1.1 Остановка запущенных служб 150
4.1.2 Обновление КриптоПро Архив 150
4.1.3 Обновление базы данных 150
4.1.4 Запуск служб 152
4.2 Обновление КриптоПро Архив на ОС семейства Linux 153
4.2.1 Остановка запущенных служб 153
4.2.2 Обновление КриптоПро Архив 153
4.2.3 Обновление базы данных 153
4.2.4 Запуск служб 155
4.3 Особенности обновления версий 156
4.3.1 Особенности обновления до версии 1.5.4 156
5 Дополнительные инструкции 158
5.1 Проверка работоспособности Elasticsearch 158
5.2 Проверка работоспособности Python 3 160
5.2.1 Проверка работоспособности Python 3 на ОС семейства Windows Server 160
5.3 Проверка работоспособности RabbitMQ 161
5.3.1 Проверка работоспособности RabbitMQ на ОС семейства Windows Server 161
5.4 Проверка работоспособности Kibana 163
5.5 Выпуск тестового сертификата сервера с использованием тестового УЦ компании КриптоПро 164

1 Описание

В данной главе приведено общее описание ПК КриптоПро Архив.

1.1 Аннотация

В настоящее время почти каждая организация использует электронный документооборот — как внешний, так и внутренний. При этом определить истинное авторство документа и убедиться в том, что он не был изменён в процессе своего жизненного цикла позволяет использование электронной подписи. Хранение, в том числе и долговременное, является частью жизненного цикла многих видов электронных документов, подписанных электронной подписью. Однако, для этого необходимо решить задачу сохранения юридической значимости документа, подписанного электронной подписью, в процессе хранения.

Настоящий документ содержит Руководство администратора программного комплекса КриптоПро Архив, который предназначен для подготовки электронных подписей документов, к долговременному хранению и сохранению юридической значимости документов.

В документе описан процесс установки и настройки ПО. Документ предназначен для администраторов как руководящий материал перед установкой и эксплуатацией программного обеспечения КриптоПро Архив.

1.2 Общие сведения

Программный комплекс КриптоПро Архив предназначен для

- подготовки электронной подписи документов, к временному (до 10 лет), долговременному (свыше 10 лет) и постоянному централизованному хранению,
- усовершенствования электронных подписей документов форматов CAdES-BES, CAdES-T, CAdES-C, CAdES-XLT1 до формата CAdES-E-A, для обеспечения юридической значимости документов при их длительном хранении за счёт использования хранящихся в подписи доказательств подлинности и заверяющих их архивных меток (штампов) времени,
- контроля сроков действия доказательств юридической значимости документов при их длительном хранении и при необходимости — их автоматическое обновление,
- приёма и передачи информации о контейнерах электронных документов временного, долговременного и постоянного хранения между Системой и внешними ИС,
- контроля сроков хранения контейнеров документов, установленных законодательством.

1.3 Архитектура решения

Ниже приведён список компонентов КриптоПро Архив.

Название компонента	Краткое описание
admin-api	Программа приёма документов и управления объектами КриптоПро Архив (для администраторов)
client-api	Программа приёма документов (для информационных систем)
signature-updater	Программа обеспечения подписей доказательствами подлинности
frontend	Графический административный веб-интерфейс
consumer	Программа обработки очередей
config	Программа для централизованной настройки компонентов КриптоПро Архив

1.3.1 ОС семейства Windows Server

Приведём схему работы КриптоПро Архив на устройствах под управлением ОС семейства Windows Server. Линиями указан поток информации (в частности, подписей и их метаданных) от компонента к компоненту. Компонент Elasticsearch может быть заменён на ManticoreSearch и используется всеми частями системы. КриптоПро Архив работает под управлением веб-сервера IIS.

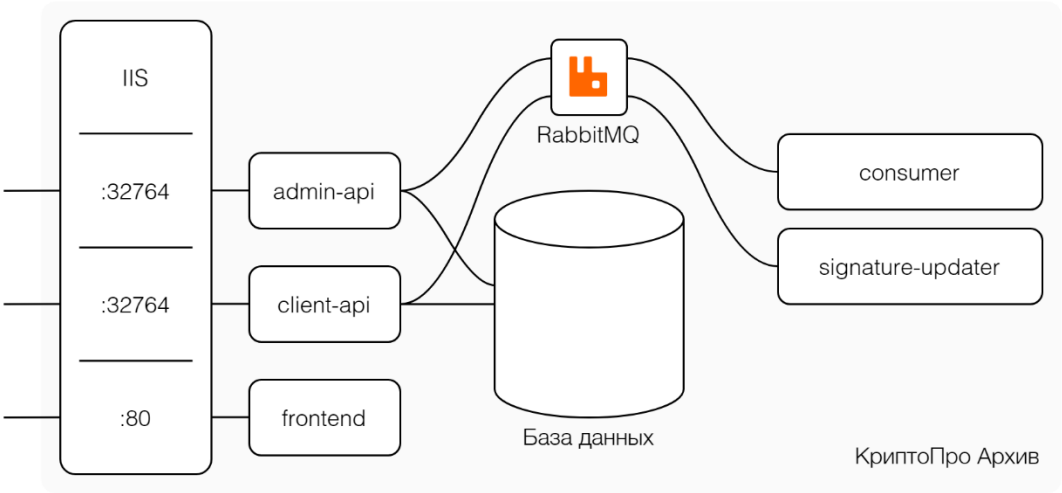


Рисунок 1. Схема взаимодействия компонентов КриптоПро Архив на ОС семейства Windows Server

1.3.2 ОС семейства Linux

Приведём схему работы КриптоПро Архив на устройствах под управлением ОС семейства Linux. Линиями указан поток информации (в частности, подписей и их метаданных) от компонента к компоненту. Компонент Elasticsearch может быть заменён на ManticoreSearch и используется всеми частями системы.

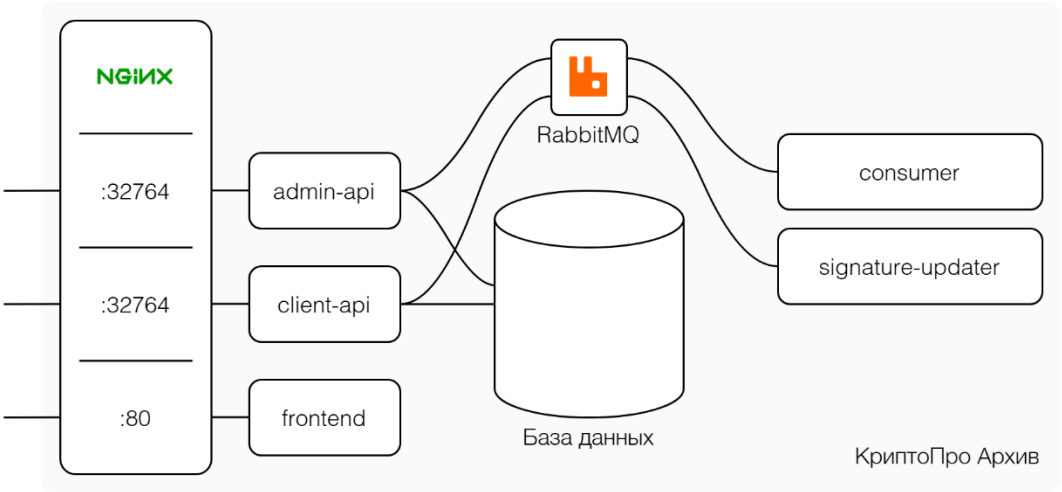


Рисунок 2. Схема взаимодействия компонентов КриптоПро Архив на ОС семейства Linux

В такой конфигурации NGINX выступает в качестве прокси между пользователем и API КриптоПро Архив и перенаправляет запросы, приходящие на внешние порты (32764 и 32767 в примере на рисунке 2 — указанные порты

должны быть открыты), на локально работающие службы (например, на портах 5000 и 5001 соответственно).

1.4 Опциональная подсистема Архив УЦ

В данном разделе приведено описание архитектуры опциональной подсистемы Архив УЦ.

Архив УЦ представляет собой подсистему хранения подписанных документов. Документы хранятся в базах данных, управление которыми происходит через admin-api и consumer.

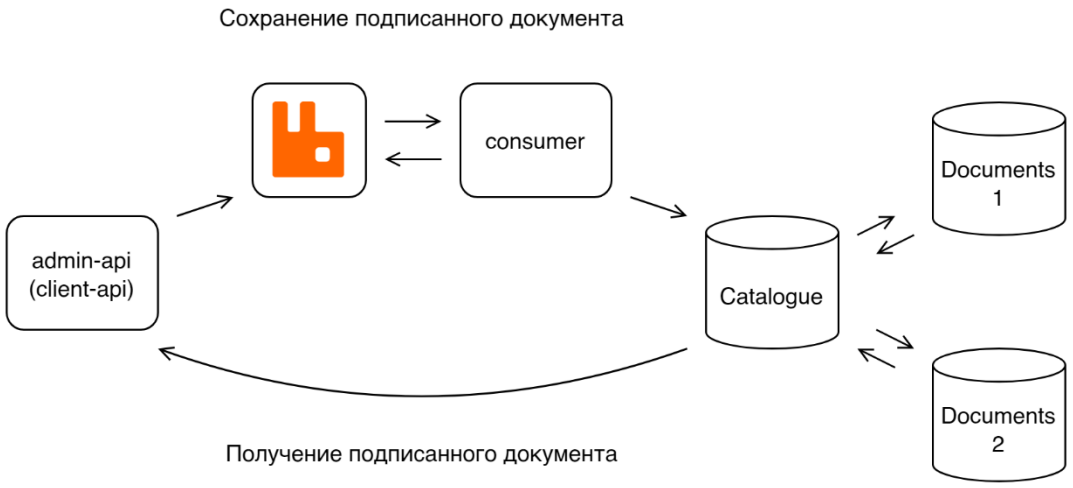


Рисунок 3. Схема взаимодействия компонентов Архив и Архив УЦ

Схема взаимодействия компонентов представлена на рисунке 3. Для надёжной загрузки документа admin-api (client-api) отправляет его в очередь RabbitMQ, откуда его забирает программа consumer, которая пробует сохранить его в базе данных. Если документ загрузить не удаётся, он помещается обратно в очередь. Для скачивания документа admin-api взаимодействует со справочником баз данных (Catalogue), который в свою очередь содержит расположения (адреса баз данных или пути, указанные в плагинах) всех документов.

2 Установка

2.1 Описание процесса установки КриптоПро Архив

В данном разделе приведено описание процесса установки КриптоПро Архив для различных операционных систем с ссылками на конкретные инструкции. Если в инструкциях по установке того или иного компонента присутствует Ваша конкретная ОС, эти инструкции приоритетны над другими.

2.1.1 ОС семейства Windows Server

ВАЖНО: не проводить установку от лица администратора сервера (пользователь Администратор). Создать пользователя с правами администратора и выполнять установку от его лица.

Для установки КриптоПро Архив на ОС семейства Windows Server необходимо установить следующие компоненты (предполагается, что IIS уже установлен на сервере):

1. Для работы потребуется **СУБД** PostgreSQL версии не ниже 11 или Oracle Database 12c. Если СУБД не установлена, предлагается установить PostgreSQL. См. раздел 2.8.1 Установка PostgreSQL на ОС семейства Windows Server
2. **КриптоПро CSP** и **КриптоПро ЭЦП Browser plug-in**. См. раздел 2.2.1 Установка КриптоПро CSP на ОС семейства Windows Server
3. **Elasticsearch**. См. раздел 2.3.1 Установка Elasticsearch на ОС семейства Windows Server
4. **RabbitMQ**. См. раздел 2.5.1 Установка RabbitMQ на ОС семейства Windows Server
5. **Microsoft Hosting Bundle**. См. раздел 2.7.1 Установка Microsoft Hosting Bundle на ОС семейства Windows Server
6. **КриптоПро Архив**. См. раздел 2.9.1 Установка КриптоПро Архив на ОС семейства Windows Server

После установки компонентов их необходимо настроить. Перед настройкой рекомендуется ознакомиться с введением к разделу 3 Настройка. Настройку рекомендуется производить в следующем порядке:

1. **Развёртывание базы данных**. См. разделы
   - 3.3.1 Настройка PostgreSQL на ОС семейства Windows Server
   - 3.4.1 Настройка Oracle Database на ОС семейства Windows Server
2. **Elasticsearch**. См. раздел 3.2.1 Настройка Elasticsearch на ОС семейства Windows Server
3. **RabbitMQ**. См. раздел 3.1.1 Настройка RabbitMQ на ОС семейства Windows Server
4. **Компоненты КриптоПро Архив**. См. разделы
   - 3.5.1 Настройка admin-api и client-api на ОС семейства Windows Server
   - 3.6.1 Настройка frontend на ОС семейства Windows Server
   - 3.7.1 Настройка signature-updater на ОС семейства Windows Server
   - 3.8.1 Настройка consumer на ОС семейства Windows Server

Инструкция по вводу лицензий приведена в разделе 3.10.1 Управление лицензиями на ОС семейства Windows Server.

2.1.2 Astra Linux

Для установки КриптоПро Архив на Astra Linux необходимо установить следующие компоненты:

1. Для работы потребуется **СУБД** PostgreSQL версии не ниже 11 или Oracle Database 12c. Если СУБД не установлена, предлагается установить PostgreSQL. См. разделы 2.8.2 Установка PostgreSQL на Astra Linux SE 1.7 и 2.8.3 Установка PostgreSQL на Astra Linux
2. **КриптоПро CSP** и **ГОСТ NGINX**. См. раздел 2.2.2 Установка КриптоПро CSP и ГОСТ NGINX на Astra Linux
3. **Elasticsearch**. См. раздел 2.3.2 Установка Elasticsearch на Astra Linux
4. **RabbitMQ**. См. раздел 2.5.2 Установка RabbitMQ на Astra Linux
5. **КриптоПро Архив**. См. раздел 2.9.2 Установка КриптоПро Архив на ОС семейства Linux.

После установки компонентов их необходимо настроить. Перед настройкой рекомендуется ознакомиться с введением к разделу 3 Настройка. Настройку рекомендуется производить в следующем порядке:

1. **Развёртывание базы данных**. См. разделы
   - 3.3.2 Настройка PostgreSQL на Astra Linux 1.7
   - 3.3.3 Настройка PostgreSQL на Astra Linux
   - 3.4.2 Настройка Oracle Database на ОС семейства Linux
2. **Elasticsearch**. См. раздел 3.2.2 Настройка Elasticsearch на ОС семейства Linux
3. **RabbitMQ**. См. раздел 3.1.2 Настройка RabbitMQ на ОС семейства Linux
4. **Компоненты КриптоПро Архив**. См. разделы
   - 3.5.2 Настройка admin-api и client-api на ОС семейства Linux
   - 3.6.2 Настройка frontend на ОС семейства Linux
   - 3.7.2 Настройка signature-updater на ОС семейства Linux
   - 3.8.2 Настройка consumer на ОС семейства Linux

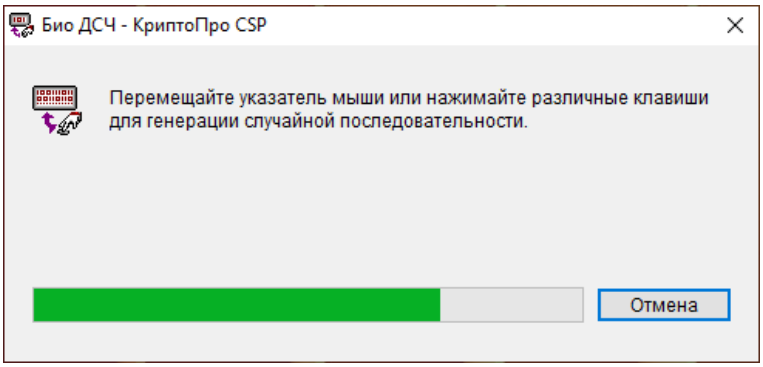
Инструкция по вводу лицензий приведена в разделе 3.10.2 Управление лицензиями на ОС семейства Linux.

2.2 Установка КриптоПро CSP

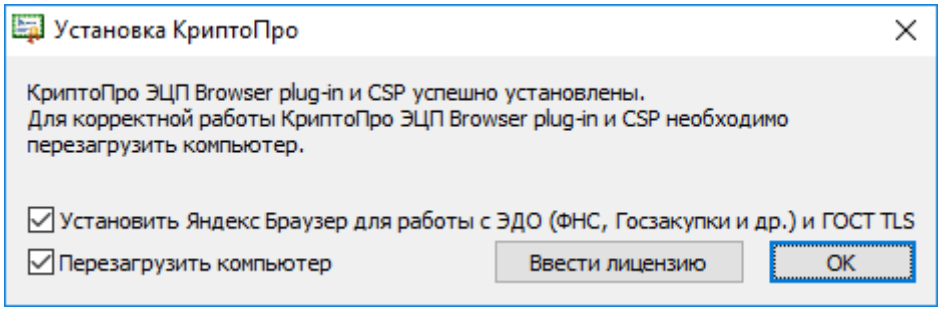
В данном разделе кратко приведены инструкции по установке КриптоПро CSP и КриптоПро ЭЦП Browser plug-in. Для более подробного и точного описания процесса установки обратитесь к документации КриптоПро CSP (раздел **Документация**).

2.2.1 Установка КриптоПро CSP на ОС семейства Windows Server

Для установки КриптоПро CSP вместе с КриптоПро ЭЦП Browser plug-in сперва необходимо скачать актуальную версию КриптоПро CSP. Запустите скачанный установочный файл от имени администратора. Во время установки следуйте инструкциям:



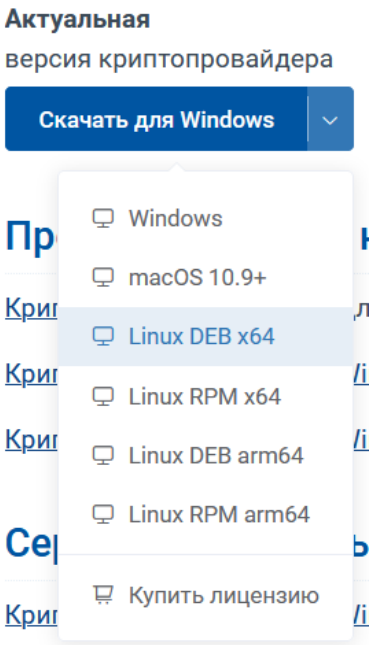
По завершению будут показаны сообщение об успешной установке и предложения по дальнейшим шагам:



Оба пункта рекомендуется оставить отмеченными для упрощения отладки.

2.2.2 Установка КриптоПро CSP и ГОСТ NGINX на Astra Linux

Для установки КриптоПро CSP вместе с КриптоПро ЭЦП Browser plug-in сперва необходимо скачать актуальную версию КриптоПро CSP для ОС семейства Debian:



Разархивировать скачанный файл:

```
tar -xf linux-amd64_deb.tgz
```

В текущей директории появится разархивированная папка `linux-amd64_deb`. Перейти в неё:

```
cd linux-amd64_deb
```

Установить программу, выполнив:

```
sudo ./install.sh
```

В результате успешной установки в конце вывода на экране будет написано `Пакеты КриптоПро CSP успешно установлены`. Далее необходимо установить библиотеку cades. Для этого выполните

```
sudo dpkg -i cprocsp-pki-cades-64_<version>_amd64.deb
```

Где <version> — версия библиотеки (может различаться в зависимости от дистрибутива CSP). Успешная установка завершится указанием установленных лицензий. Далее необходимо установить ГОСТ NGINX:

```
sudo dpkg -i cprocsp-nginx-64_<version>_amd64.deb
```

Где <version> — версия программы (может различаться в зависимости от дистрибутива CSP). Программа установлена успешно, если отсутствуют ошибки при установке. Запустите сервер:

```
sudo systemctl enable cpnginx.service --now
```

Проверить работоспособность можно, выполнив

```
sudo systemctl status cpnginx.service
```

В случае успеха в выводе среди прочего будет указано `Active: active (running)`.

2.3 Установка Elasticsearch

В данном разделе кратко приведены инструкции по установке Elasticsearch версии 7.17. Для более подробного описания процесса установки обратитесь к онлайн-документации Elasticsearch.

2.3.1 Установка Elasticsearch на ОС семейства Windows Server

Для установки Elasticsearch 7.17.16 разархивировать содержимое архива `redist\elasticsearch-7.17.16-windows-x86_64.zip` из папки с дистрибутивом КриптоПро Архив в `C:\Program Files`. Для установки и запуска службы Elasticsearch запустить PowerShell от имени администратора и выполнить следующие команды:

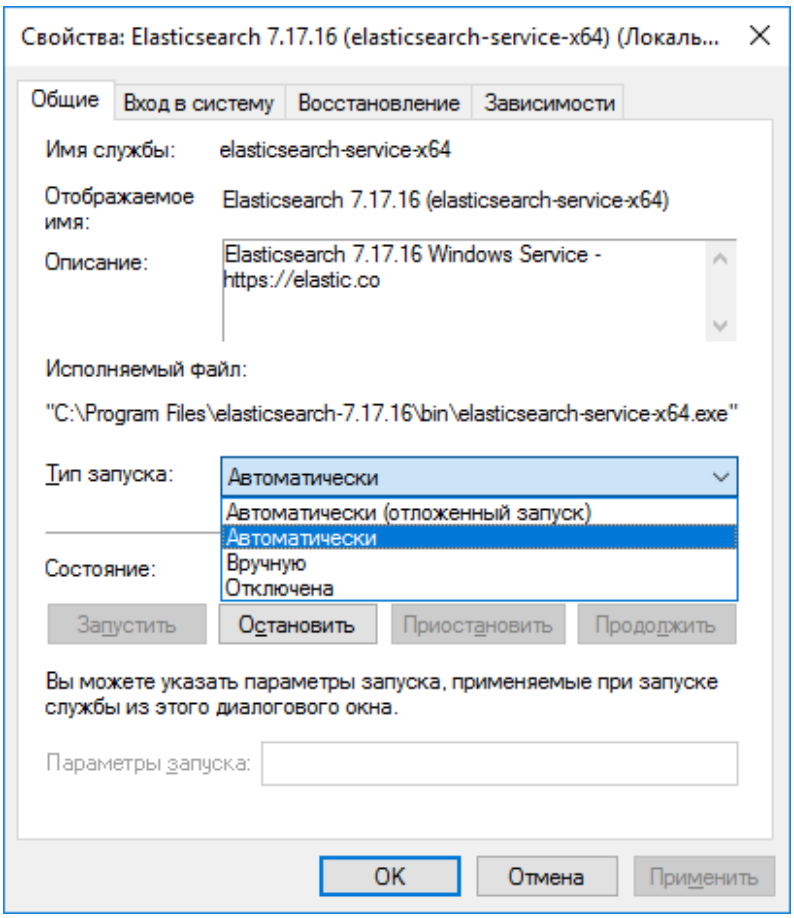
```
cd 'C:\Program Files\elasticsearch-7.17.16\bin'
.\elasticsearch-service.bat install
```

После выполнения в конце вывода должно быть написано `The service 'elasticsearch-service-x64' has been installed`. Для запуска службы выполнить

```
.\elasticsearch-service.bat start
```

После успешного запуска должно быть написано `The service 'elasticsearch-service-x64' has been started`. При возникновении ошибки внимательно прочитать текст ошибки и попробовать установить/запустить сервис повторно.

По умолчанию служба устанавливается с типом запуска **Вручную**. Чтобы это изменить и сделать запуск Elasticsearch автоматическим, откройте программу **Службы**, нажмите правой кнопкой мыши на службу **Elasticsearch 7.17.16 (elasticsearch-service-x64)** и выберите пункт **Свойства**. Установите тип запуска **Автоматически**:



Нажмите **Применить** и **ОК**.

Проверить работу сервиса можно в приложении **Службы**. Подробнее о проверке работоспособности кластера Elasticsearch см. в разделе 5.1 Проверка работоспособности Elasticsearch.

2.3.2 Установка Elasticsearch на Astra Linux

Установочный файл Elasticsearch распространяется вместе с дистрибутивом КриптоПро Архив и расположен в папке с дистрибутивом. Для установки Elasticsearch 7.17.16 в папке с дистрибутивом выполнить

```
sudo dpkg -i elasticsearch-7.17.16-amd64.deb
```

Успешный вывод команды установки выглядит следующим образом:

```
Выбор ранее не выбранного пакета elasticsearch.
(Чтение базы данных ... на данный момент установлено 168238 файлов и каталогов.)
Подготовка к распаковке elasticsearch-7.17.16-amd64.deb ...
Creating elasticsearch group... OK
```

```
Creating elasticsearch user... OK
Распаковывается elasticsearch (7.17.16) ...
Настраивается пакет elasticsearch (7.17.16) ...
### NOT starting on installation, please execute the following statements to configure
elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
Обрабатываются триггеры для systemd (241-7~deb10u8astra.se28) ...
```

Запустить службу systemd:

```
sudo systemctl daemon-reload

sudo systemctl start elasticsearch.service
```

Для автоматического запуска Elasticsearch на старте операционной системы выполнить

```
sudo systemctl enable elasticsearch.service
```

Проверить состояние сервиса можно командой

```
sudo systemctl status elasticsearch.service
```

В случае успеха в выводе среди прочего будет указано `Active: active (running)`. Более подробно проверка работоспособности Elasticsearch описана в разделе 5.1 Проверка работоспособности Elasticsearch.

2.4 Установка Kibana

В данном разделе кратко описана установка опционального ПО для просмотра журналов в Elasticsearch под названием Kibana. Для более подробного описания процесса установки обратитесь к официальной онлайн-документации Kibana.

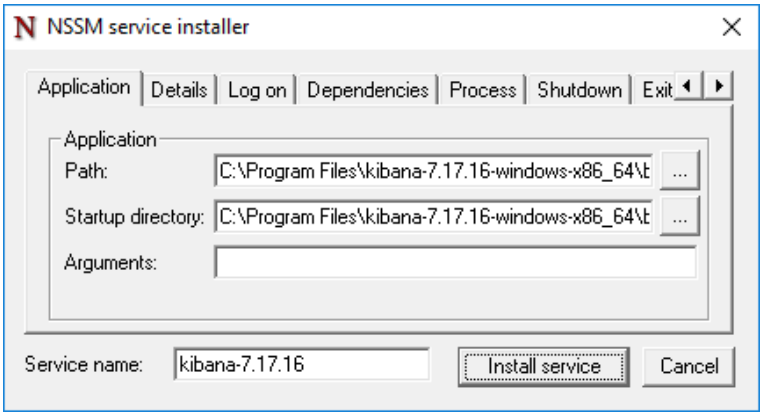
2.4.1 Установка Kibana на ОС семейства Windows Server

Для установки Kibana 7.17.16 разархивировать содержимое архива `redist\kibana-7.17.16-windows-x86_64.zip` из папки с дистрибутивом КриптоПро Архив в `C:\Program Files`.

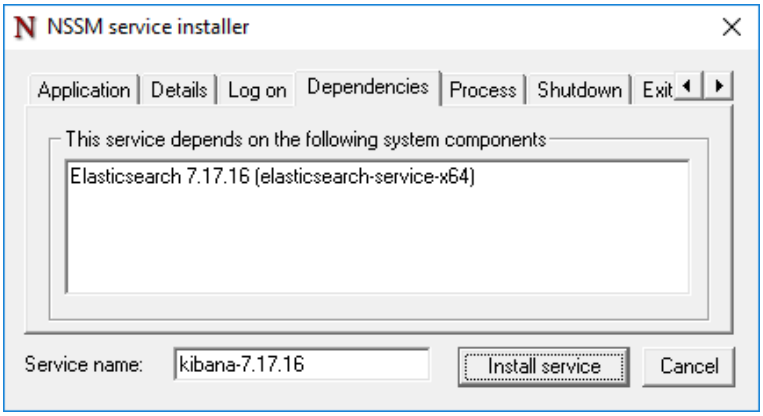
Для того, чтобы зарегистрировать Kibana как службу Windows, недостаточно стандартных средств, установленных в Windows Server по умолчанию. Для регистрации Kibana необходимо установить программу NSSM (см. раздел 2.12.1 Установка NSSM на ОС семейства Windows Server). После установки откройте PowerShell от имени администратора и выполните

```
nssm install kibana-7.17.16
```

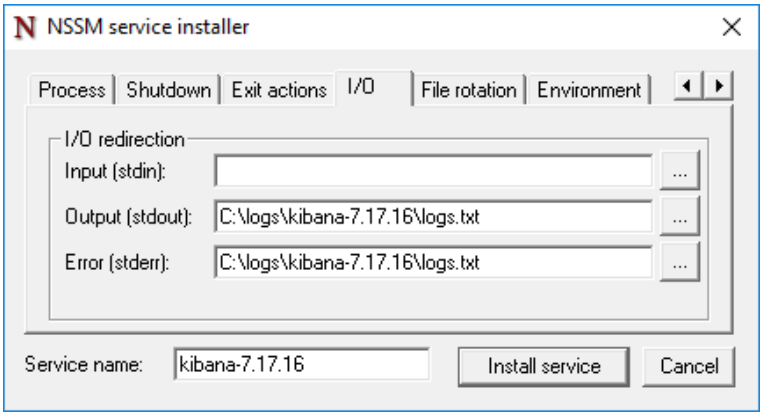
В открывшемся окне во вкладке **Application** в поле **Path** указать путь `C:\Program Files\kibana-7.17.16-windows-x86_64\bin\kibana.bat`, в поле Startup directory указать `C:\Program Files\kibana-7.17.16-windows-x86_64\bin`:



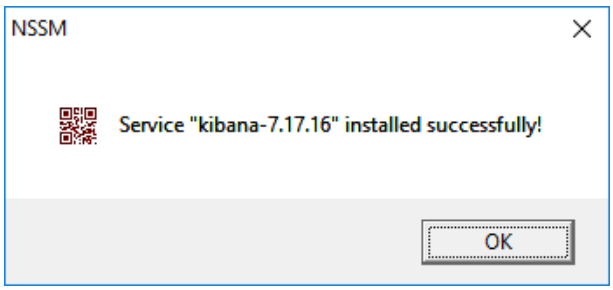
Далее, если Elasticsearch установлен на данном сервере, во вкладке **Dependencies** указать имя службы Elasticsearch (по умолчанию **Elasticsearch 7.17.16 (elasticsearch-service-x64)**; имя можно найти в программе **Службы**):



Во вкладке **I/O** в полях **Output (stdout)** и **Error (stderr)** указать пути до файлов, которые будут использованы для ведения журналов (в примере `C:\logs\kibana-7.17.16\logs.txt`):



Изменение остальных параметров не обязательно. Нажать **Install service**. После успешной установки появится диалоговое окно



Нажать **OK**. Служба Kibana установлена. По умолчанию служба не запускается. Запустите её вручную, используя команду

```
nssm start kibana-7.17.16
```

В случае успешного запуска на экран будет выведено сообщение `kibana-7.17.16: START: Операция успешно завершена`. Для проверки работоспособности см. раздел 5.4 Проверка работоспособности Kibana. Для редактирования установленных параметров используйте команду

```
nssm edit kibana-7.17.16
```

2.4.2 Установка Kibana на Astra Linux

Установочный файл Kibana распространяется вместе с дистрибутивом КриптоПро Архив и расположен в папке с дистрибутивом. Для установки Kibana 7.17.16 в папке с дистрибутивом выполнить

```
sudo dpkg -i kibana-7.17.16-amd64.deb
```

Успешный вывод команды установки выглядит следующим образом:

```
Выбор ранее не выбранного пакета kibana.
(Чтение базы данных ... на данный момент установлено 169335 файлов и каталогов.)
Подготовка к распаковке kibana-7.17.16-amd64.deb ...
Распаковывается kibana (7.17.16) ...
Настраивается пакет kibana (7.17.16) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and
instructions on how to disable see
https://www.elastic.co/guide/en/kibana/7.17/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
Обрабатываются триггеры для systemd (241-7~deb10u8astra.se28) ...
```

Установить и запустить службу `systemd`:

```
sudo systemctl daemon-reload
sudo systemctl enable kibana.service --now
```

Проверить состояние сервиса можно командой

```
sudo systemctl status kibana.service
```

В случае успеха в выводе среди прочего будет указано `Active: active (running)`. Более подробно проверка работоспособности Kibana описана в разделе 5.4 Проверка работоспособности Kibana.

2.5 Установка RabbitMQ

В данном разделе приведено краткое описание инструкции по установке RabbitMQ версии 3.12. За более подробным описанием обратитесь на официальный сайт RabbitMQ. Версия RabbitMQ должна быть не ниже 3.12.

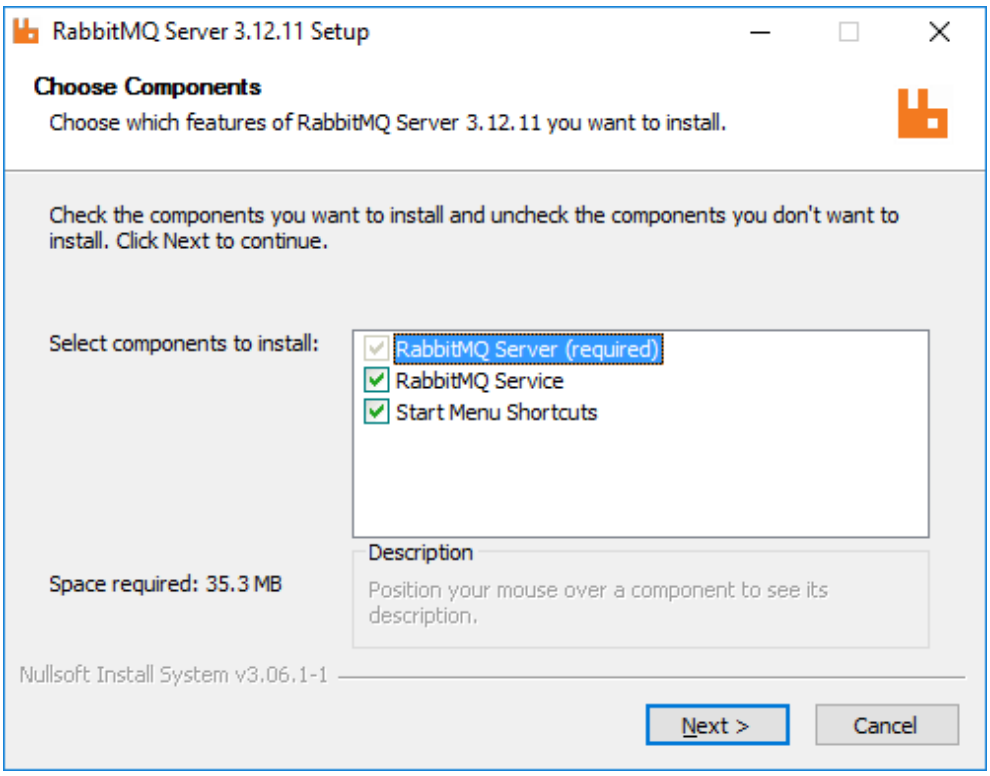
2.5.1 Установка RabbitMQ на ОС семейства Windows Server

ВАЖНО: не выполнять дальнейшие действия, находясь в учётной записи администратора сервера (пользователь Администратор). Создать пользователя с правами администратора и выполнять установку от его лица.

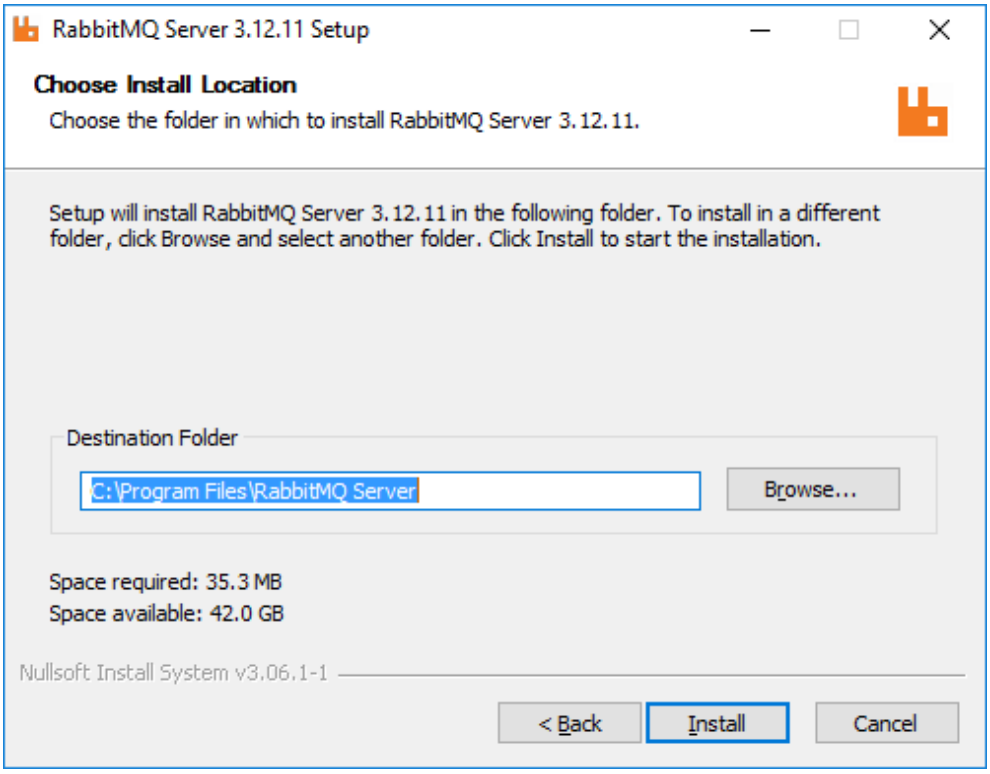
Для установки RabbitMQ с требуемой функциональностью, совместимого с Архивом, потребуется предварительно скачать и установить несколько зависимостей:

- Erlang OTP 25 (см. раздел 2.10.1 Установка Erlang OTP на ОС семейства Windows Server),
- Python 3 (см. раздел 2.11.1 Установка Python 3 на ОС семейства Windows Server),
- RabbitMQ Delayed Message Exchange Plugin

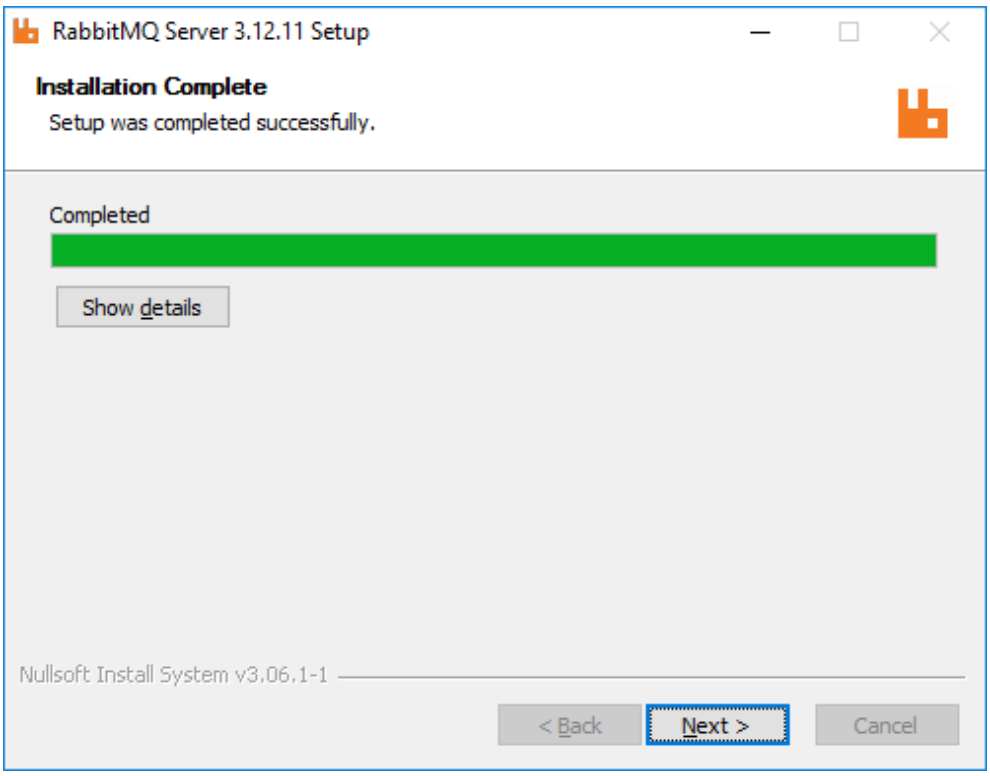
Скачайте RabbitMQ Delayed Message Exchange Plugin версии 3.12.0. После установки всех зависимостей скачайте RabbitMQ 3.12.11 с официального сайта и запустите установочный файл от имени администратора:



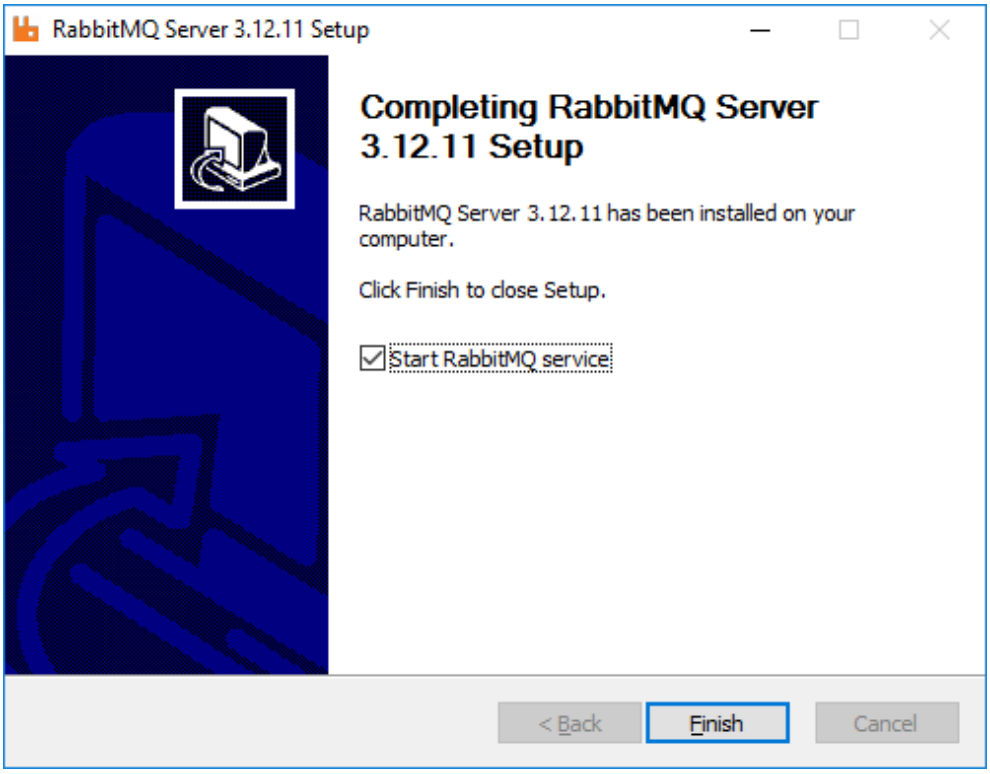
Оставить все пункты отмеченными и нажать **Next**.



Оставить пусть установки по умолчанию и нажать **Install**. После завершения установки диалоговое окно будет иметь следующее содержание:



Нажать Next. Последнее окно:



Оставить пункт **Start RabbitMQ service** отмеченным и нажать **Finish**. Установка завершена.

Проверка работоспособности RabbitMQ описана в разделе 5.3.1 Проверка работоспособности RabbitMQ на ОС семейства Windows Server.

Установите скачанный RabbitMQ Delayed Message Exchange Plugin. Для этого переместите скачанный ранее файл с плагином в папку `C:\Program Files\RabbitMQ Server\rabbitmq_server-3.12.11\plugins`. После этого активируйте плагин, выполнив в PowerShell от лица администратора

```
cd 'C:\Program Files\RabbitMQ Server\rabbitmq_server-3.12.11\sbin'

.\rabbitmq-plugins.bat enable rabbitmq_delayed_message_exchange
```

Успешный вывод программы выглядит следующим образом:

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

set 4 plugins.
Offline change; changes will take effect at broker restart.
```

Перезапустите службу в приложении **Службы** для применения изменений. Установка RabbitMQ завершена.

2.5.2 Установка RabbitMQ на Astra Linux

Для Astra Linux RabbitMQ распространяется вместе с дистрибутивом КриптоПро Архив и расположен в папке с дистрибутивом. Для установки RabbitMQ потребуется сперва установить

- ESL Erlang (см. раздел 2.10.2 Установка ESL Erlang на Astra Linux)

RabbitMQ Delayed Message Exchange Plugin распространяется вместе с дистрибутивом КриптоПро Архив и расположен в папке с дистрибутивом. Для установки RabbitMQ в папке с дистрибутивом выполните команду

```
sudo dpkg -i rabbitmq-server_3.12.11-1_all.deb
```

После успешной установки на экран будет выведено следующее:

```
Выбор ранее не выбранного пакета rabbitmq-server.
(Чтение базы данных ... на данный момент установлено 229487 файлов и каталогов.)
Подготовка к распаковке rabbitmq-server_3.12.11-1_all.deb ...
Распаковывается rabbitmq-server (3.12.11-1) ...
Настраивается пакет rabbitmq-server (3.12.11-1) ...
Добавляется группа «rabbitmq» (GID 129) ...
Готово.
Добавляется системный пользователь «rabbitmq» (UID 117) ...
Добавляется новый пользователь «rabbitmq» (UID 117) в группу «rabbitmq» ...
Не создаётся домашний каталог «/var/lib/rabbitmq».
Created symlink /etc/systemd/system/multi-user.target.wants/rabbitmq-server.service →
/lib/systemd/system/rabbitmq-server.service.
Обрабатываются триггеры для systemd (241-7~deb10u8astra.se28) ...
Обрабатываются триггеры для man-db (2.8.5-2) ...
```

Проверить работоспособность RabbitMQ можно, выполнив

```
sudo systemctl status rabbitmq-server.service
```

В случае успеха в выводе среди прочего будет указано `Active: active (running)`. Дополнительно можно проверить вывод команды

```
sudo rabbitmqctl status
```

В случае успешного выполнения будет выведена информация о системе, об установленных плагинах и так далее.

Далее, необходимо установить плагин для управления RabbitMQ: rabbitmq_management. Для этого в папке с дистрибутивом выполните

```
sudo mkdir /usr/lib/rabbitmq/plugins

sudo mv rabbitmq_delayed_message_exchange-3.12.0.ez /usr/lib/rabbitmq/plugins

sudo rabbitmq-plugins enable rabbitmq_management rabbitmq_delayed_message_exchange
```

После успешной активации на экран будет выведено следующее:

```
Enabling plugins on node rabbit@astra-se:
```

```
rabbitmq_management
rabbitmq_delayed_message_exchange
The following plugins have been configured:
  rabbitmq_delayed_message_exchange
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_web_dispatch
Applying plugin configuration to rabbit@astra-se...
The following plugins have been enabled:
  rabbitmq_delayed_message_exchange
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_web_dispatch

started 4 plugins.
```

При появлении ошибок, связанных с тем, что плагин `rabbitmq_delayed_message_exchange` не найден, убедитесь что файл `rabbitmq_delayed_message_exchange-3.12.0.ez` именно с таким именем расположен в директории `/usr/lib/rabbitmq/plugins`. После этого повторите последнюю команду.

Далее, выполните

```
sudo curl -fsSL http://127.0.0.1:15672/cli/rabbitmqadmin -o
/usr/local/bin/rabbitmqadmin

sudo chmod u+x /usr/local/bin/rabbitmqadmin
```

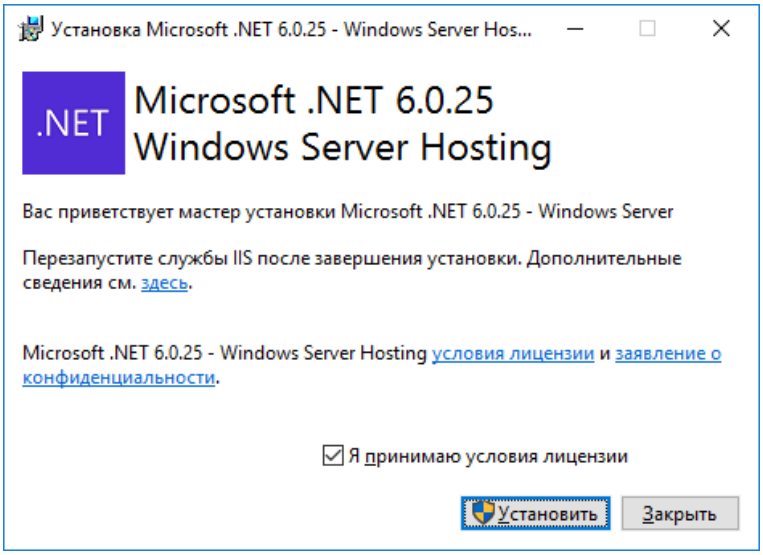
Установка RabbitMQ завершена.

2.7 Установка Microsoft Hosting Bundle

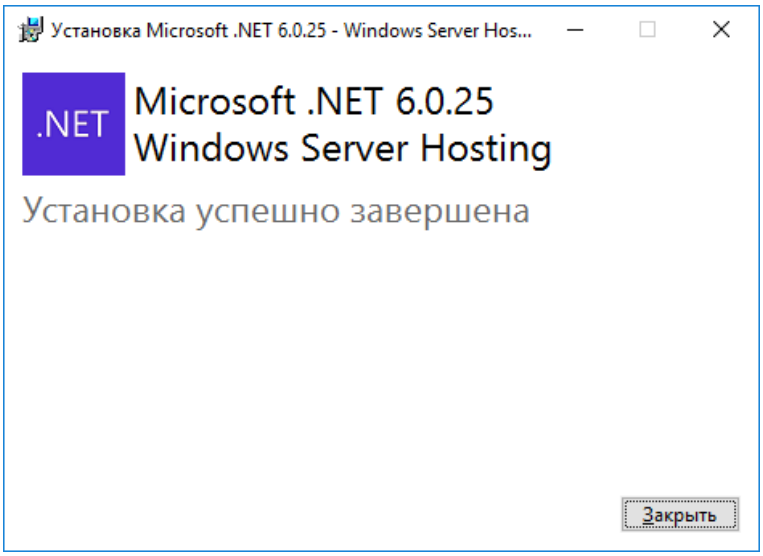
В данном разделе приведены инструкции по установке Microsoft Hosting Bundle, позволяющего управлять компонентами КриптоПро Архив через IIS на ОС семейства Windows Server.

2.7.1 Установка Microsoft Hosting Bundle на ОС семейства Windows Server

Для установки скачать Microsoft Hosting Bundle 6.0.25 с официального сайта Microsoft. Запустить установочный файл от имени администратора:



Отметить пункт **Я принимаю условия лицензии** и нажать **Установить**. Результат успешной установки:

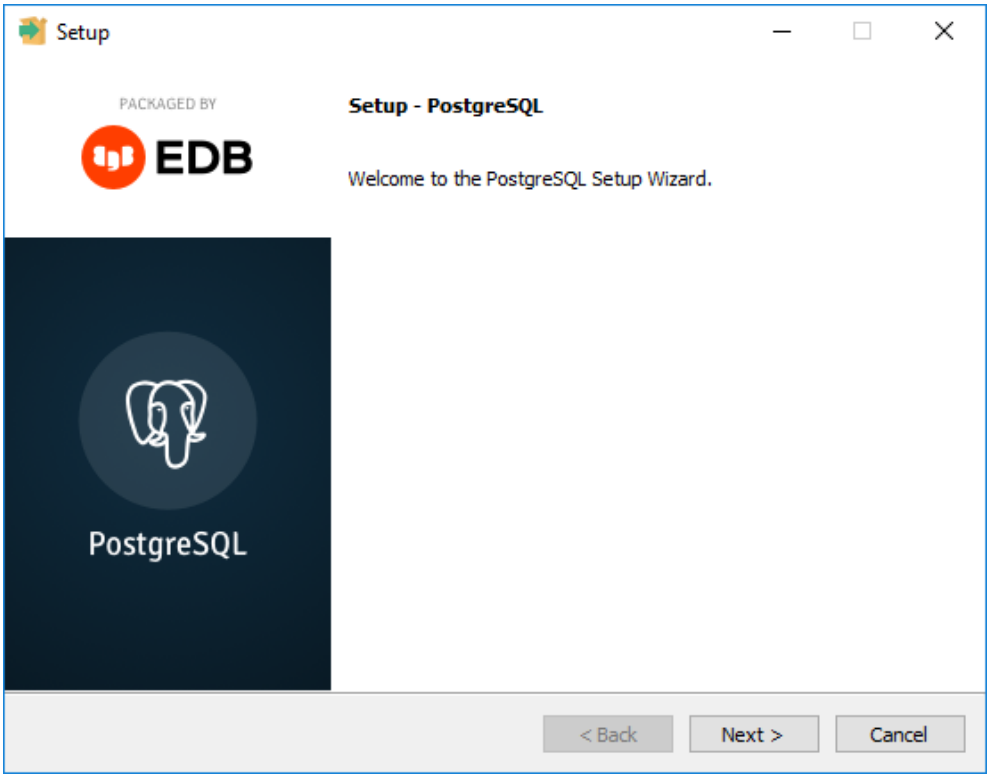


2.8 Установка PostgreSQL

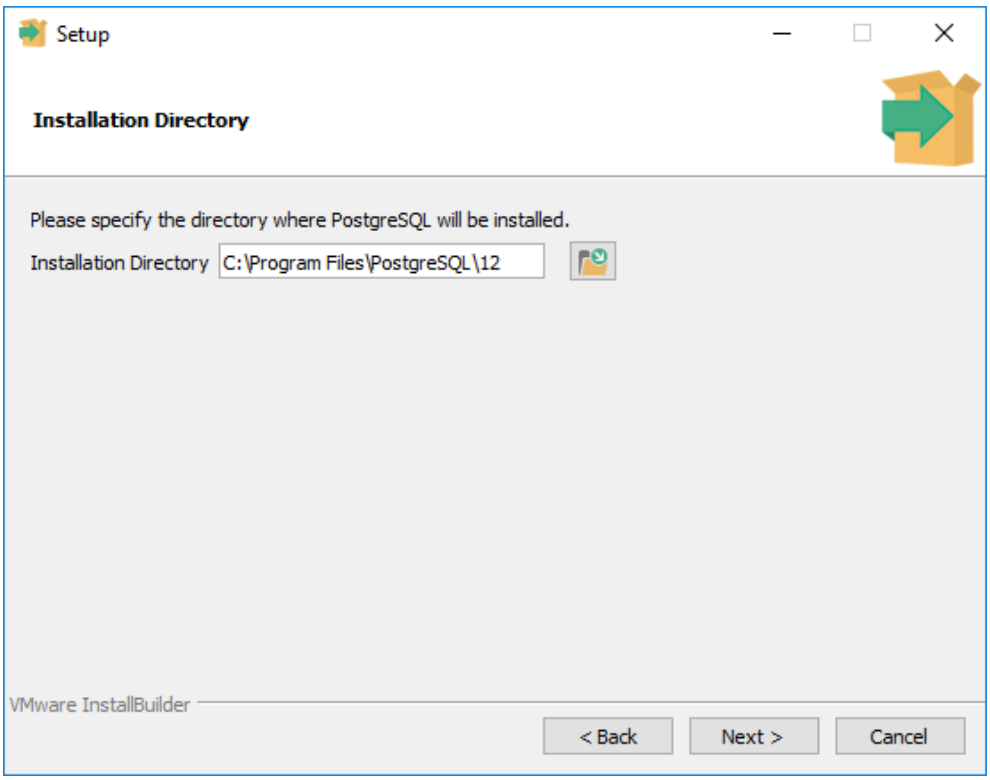
КриптоПро Архив поддерживает работу с СУБД PostgreSQL версии не ниже 11. В данном разделе приведены инструкции по установке PostgreSQL на различные операционные системы.

2.8.1 Установка PostgreSQL на ОС семейства Windows Server

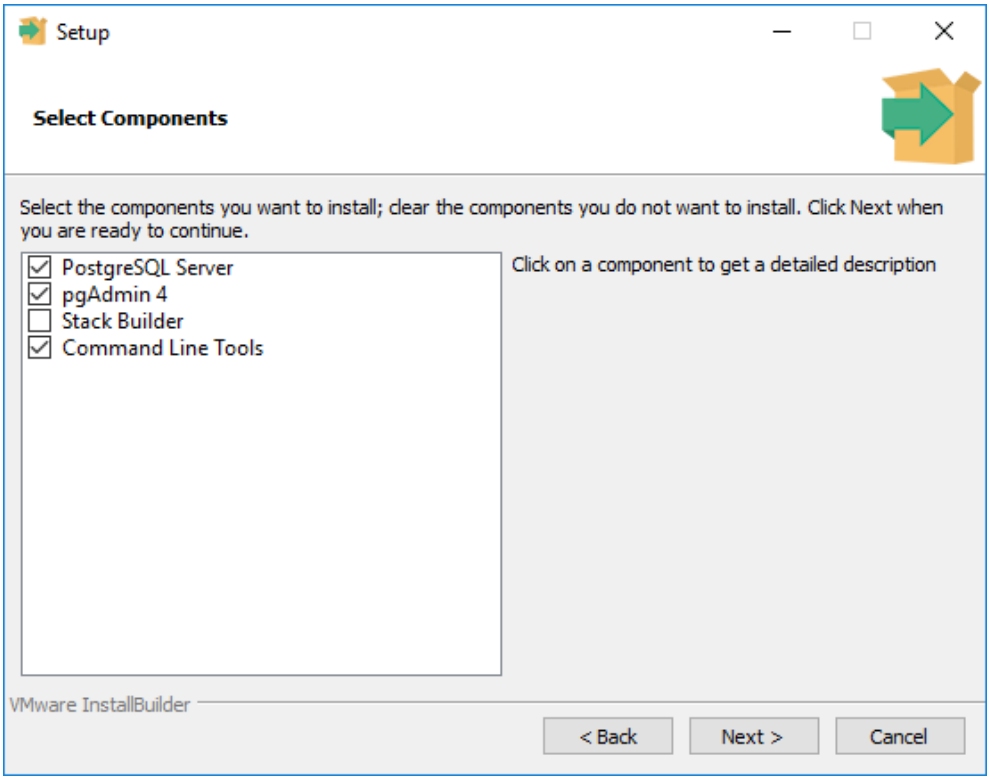
Для установки PostgreSQL на ОС семейства Windows Server скачайте PostgreSQL версии не ниже 11. В примере ниже используется PostgreSQL 12. Запустить скачанный установочный файл от имени администратора. Откроется окно:



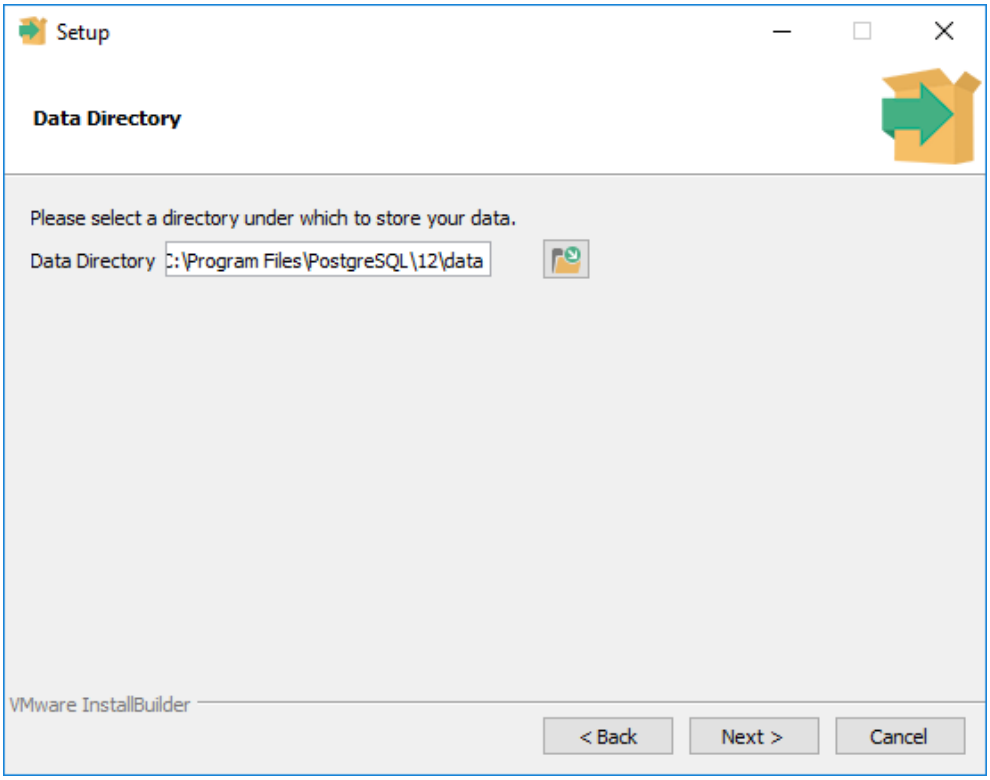
Нажать **Next**:



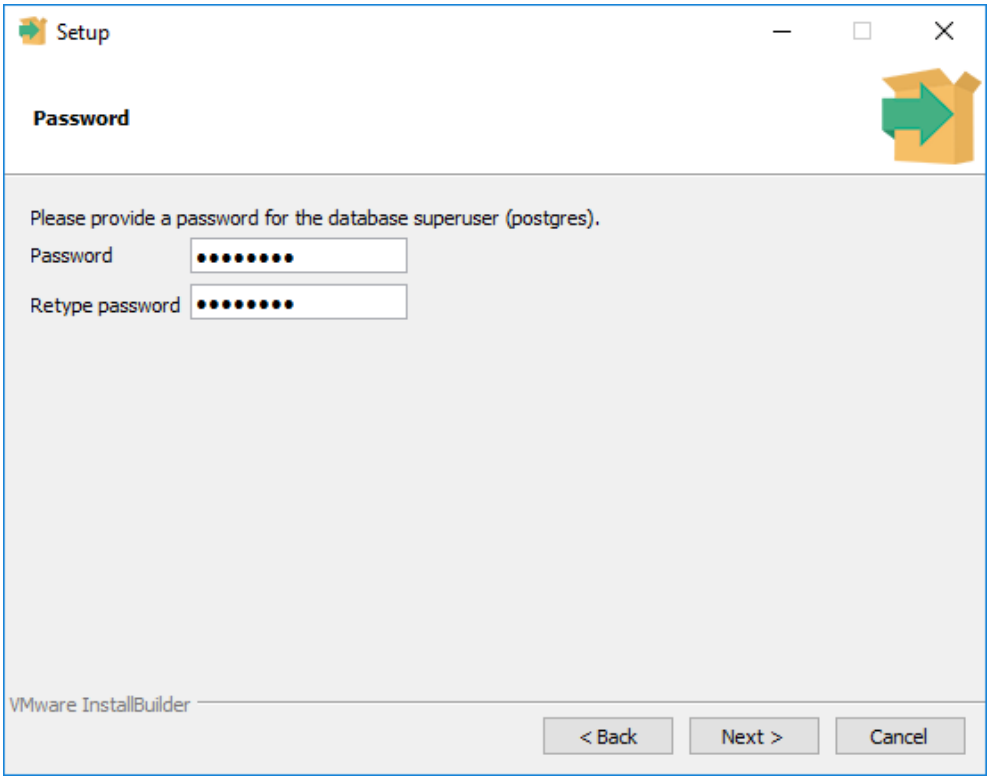
Оставить путь установки по умолчанию. Нажать **Next**:



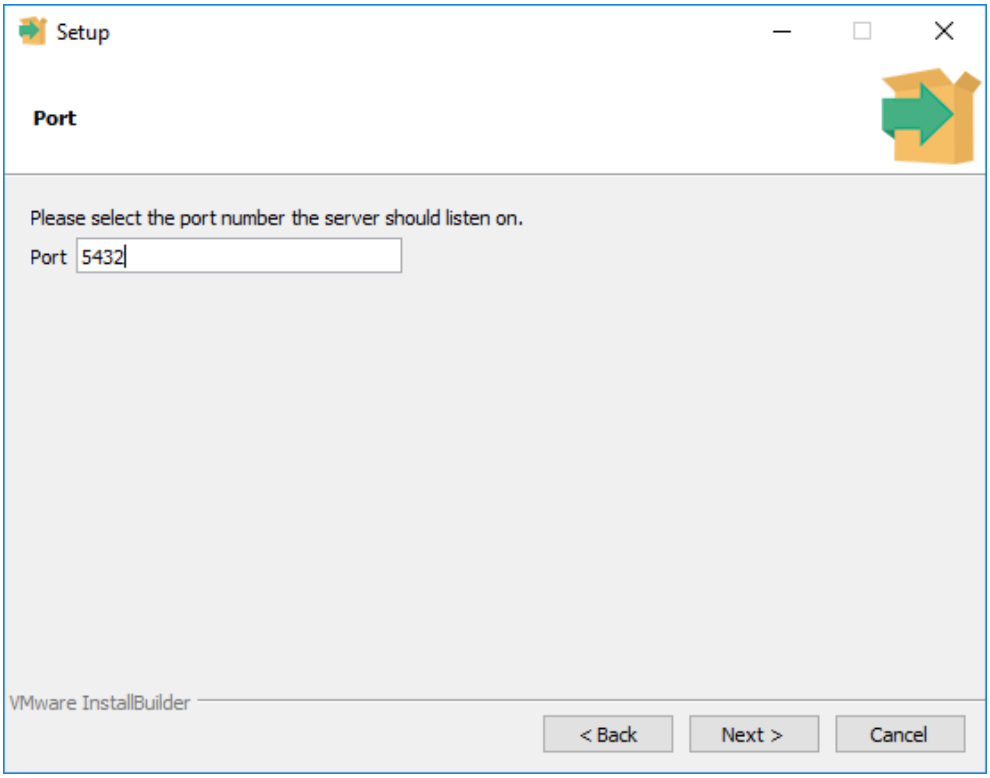
Снять выделение с Stack Builder, так как эта функциональность не потребуется. Нажать **Next**:



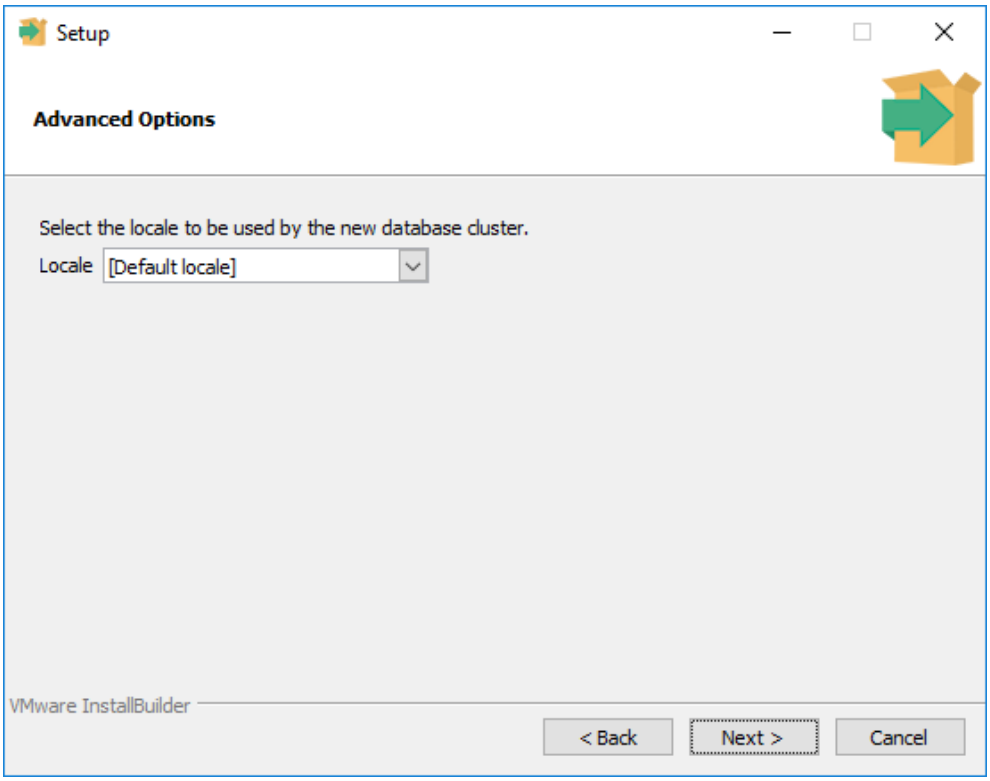
Оставить путь по умолчанию. Нажать **Next**:



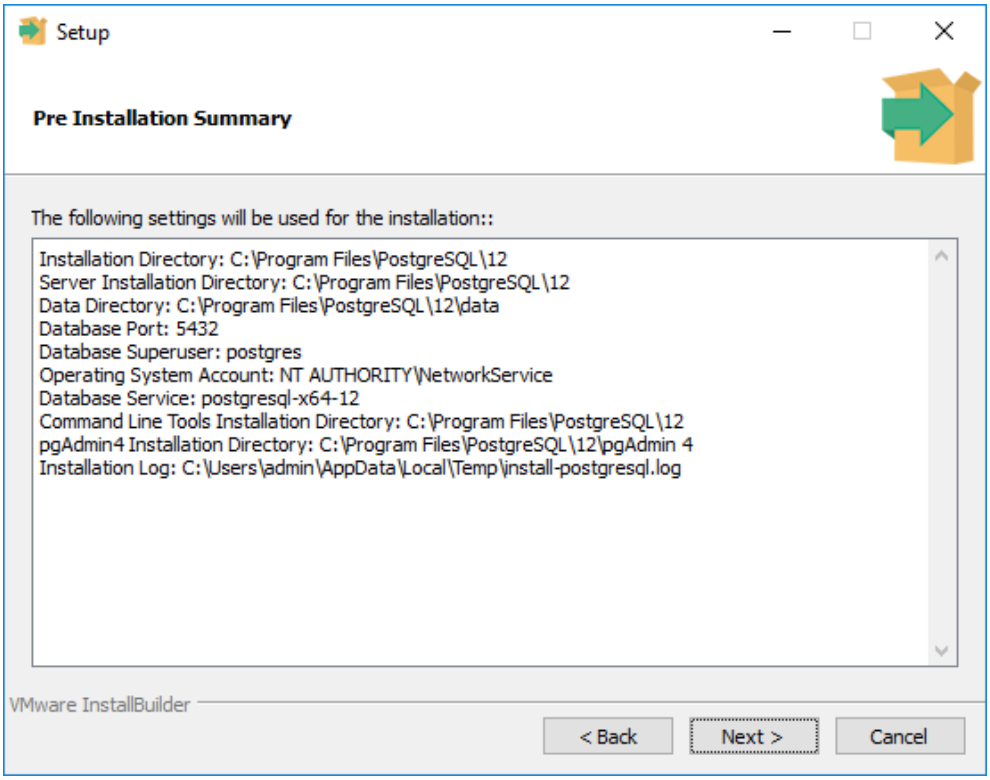
Задать пароль пользователю `postgres`. Нажать **Next**:



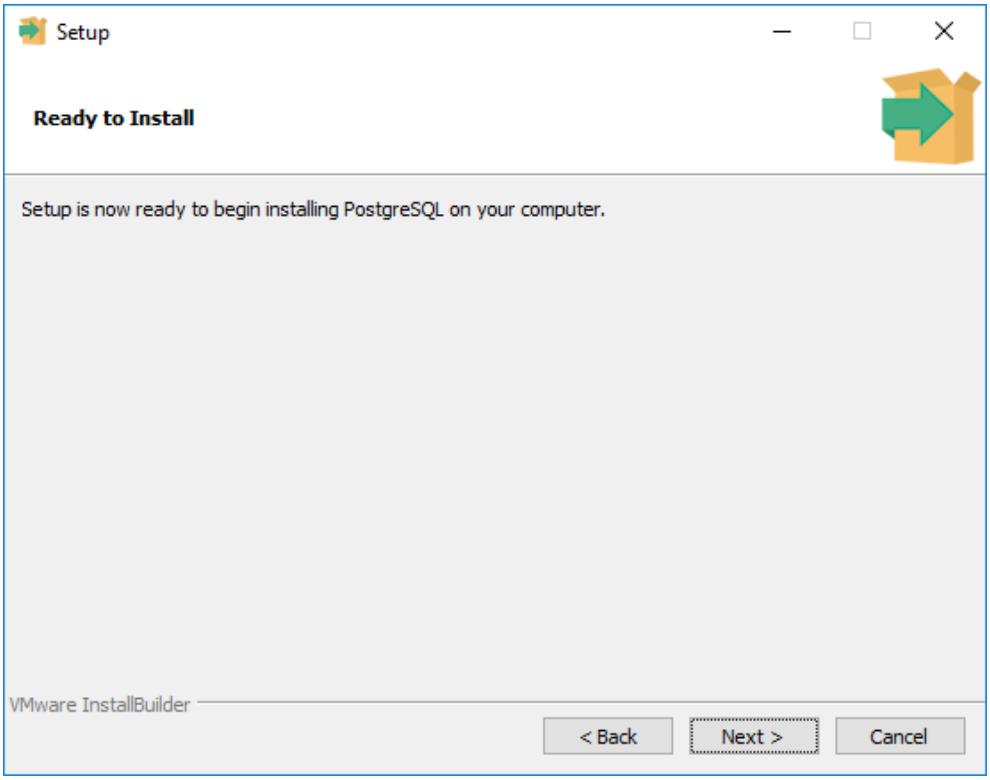
Оставить порт без изменений. Нажать **Next**:



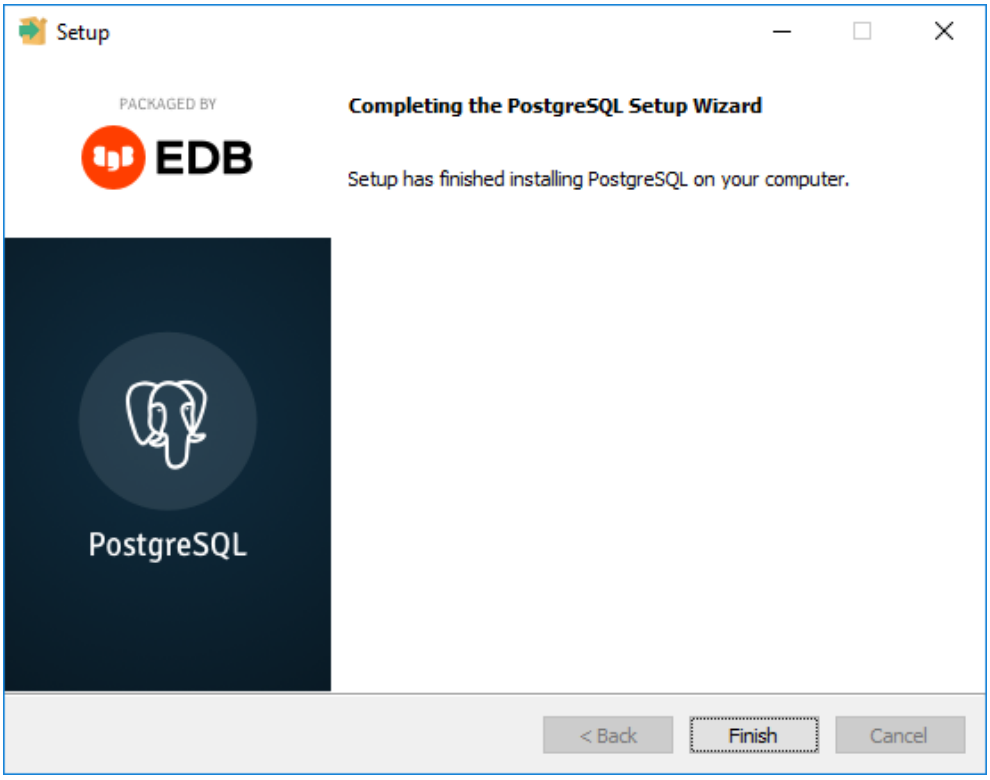
Оставить значение локали по умолчанию. Нажать **Next**:



Проверьте все выбранные настройки и нажмите **Next**:



Нажмите **Next**. Процесс установки будет запущен. По завершению установки диалоговое окно примет следующий вид:



Нажмите **Finish**. Установка PostgreSQL завершена.

2.8.2 Установка PostgreSQL на Astra Linux SE 1.7

Для установки PostgreSQL на Astra Linux SE 1.7 выполнить

```
sudo apt install postgresql-11
```

Убедиться, что сервис запущен, с помощью команды

```
sudo systemctl status postgresql.service
```

В выводе должно быть написано `Active: active (exited)`. Если это не так, попробуйте запустить службу вручную с помощью команды

```
sudo systemctl start postgresql.service
```

2.8.3 Установка PostgreSQL на Astra Linux

Для установки PostgreSQL на ОС семейства Debian Linux сперва необходимо добавить в пакетный менеджер репозиторий с PostgreSQL:

```
sudo sh -c 'echo "deb http://apt-archive.postgresql.org/pub/repos/apt stretch-pgdg
main" > /etc/apt/sources.list.d/pgdg.list'

wget --no-check-certificate --quiet -O -
https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add
```

После этого обновить репозитории:

```
sudo apt update
```

Установить PostgreSQL (в примере ниже устанавливается версия 12):

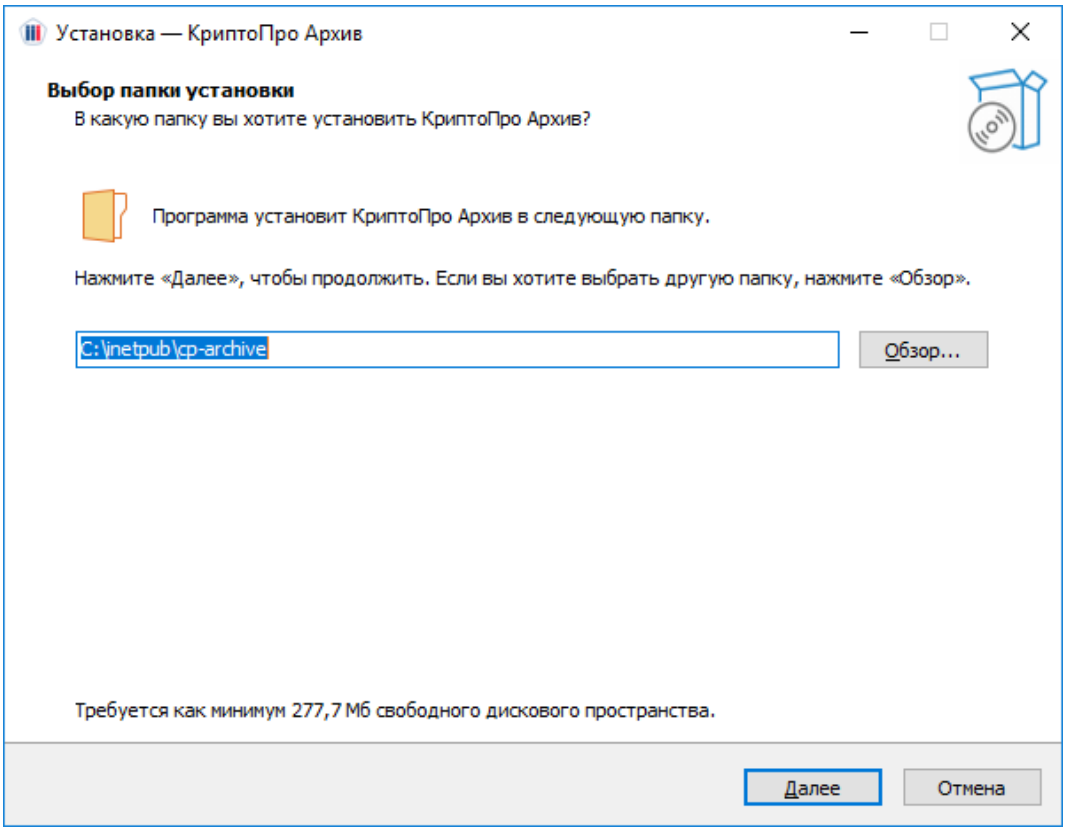
```
sudo apt install postgresql-12
```

2.9 Установка КриптоПро Архив

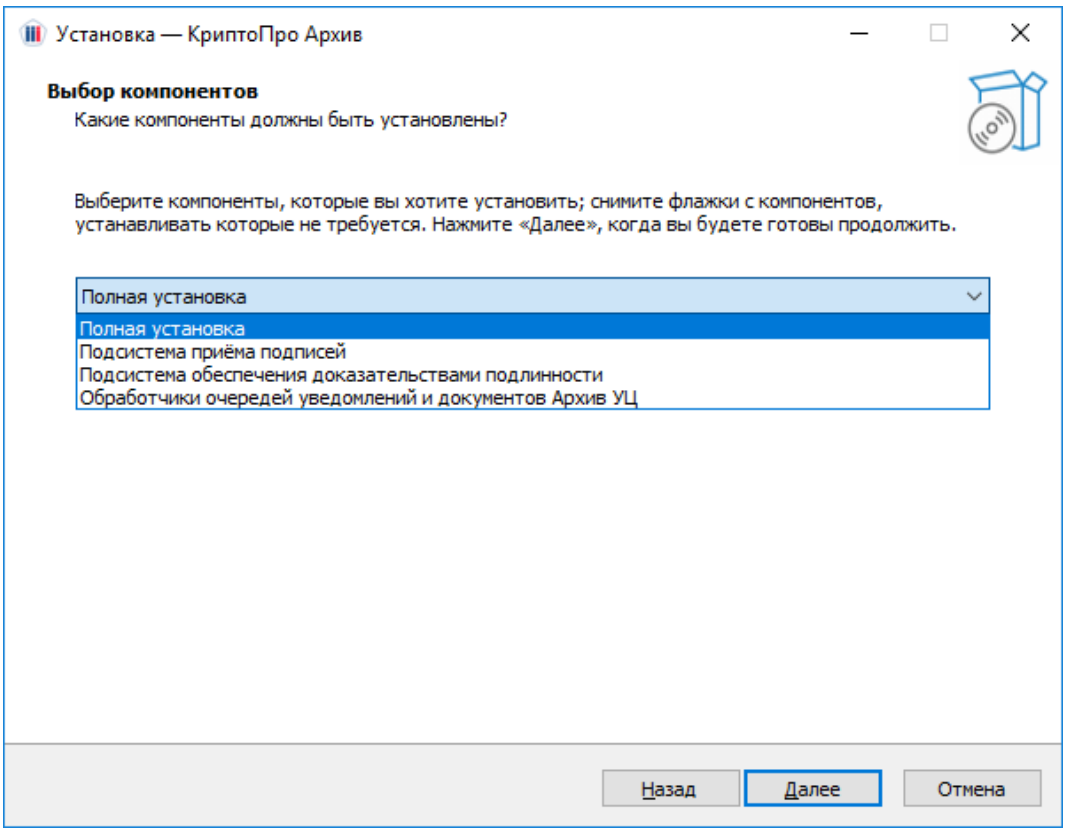
В данном разделе описано, как устанавливать КриптоПро Архив. Прежде чем переходить к этому шагу, убедитесь, что на целевом сервере установлены все необходимые зависимости (см раздел 2.1 Описание процесса установки КриптоПро Архив).

2.9.1 Установка КриптоПро Архив на ОС семейства Windows Server

Для установки КриптоПро Архив на ОС семейства Windows Server от имени администратора запустить установочный файл `cp-archive_<version>_win-x64.exe`, где `<version>` — версия дистрибутива. Появится окно:



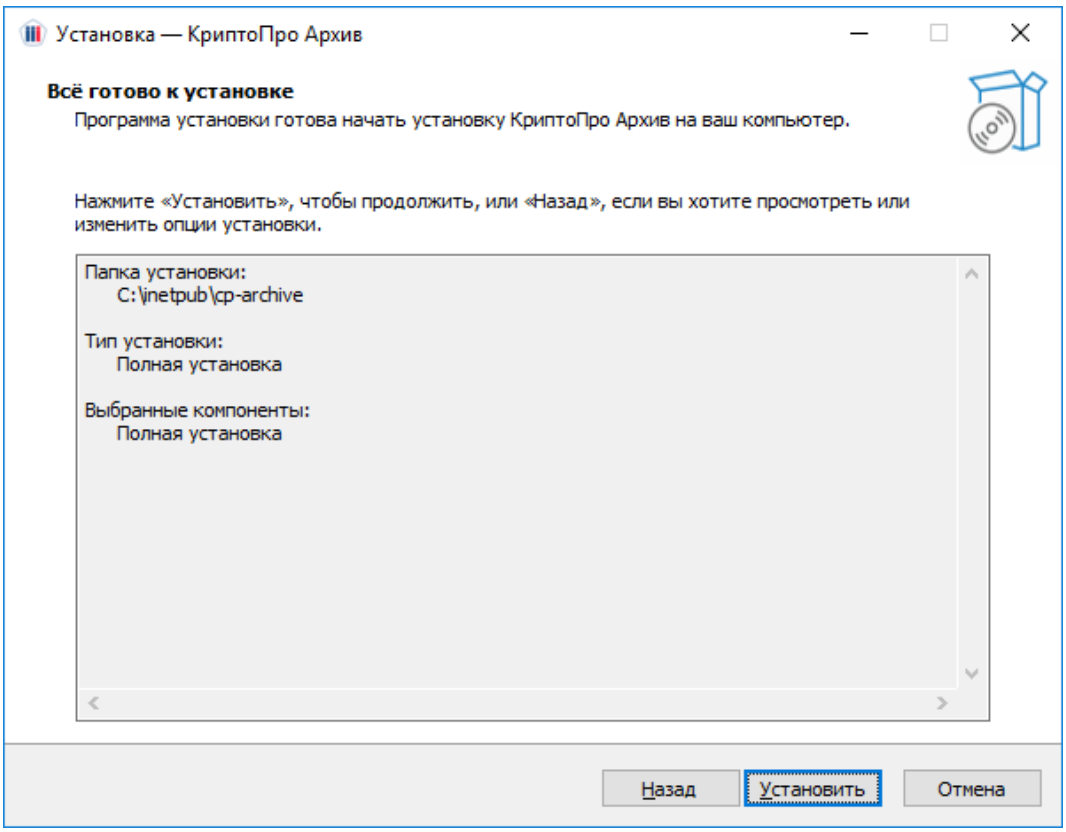
Рекомендуется оставить путь установки по умолчанию. Нажмите **Далее**:



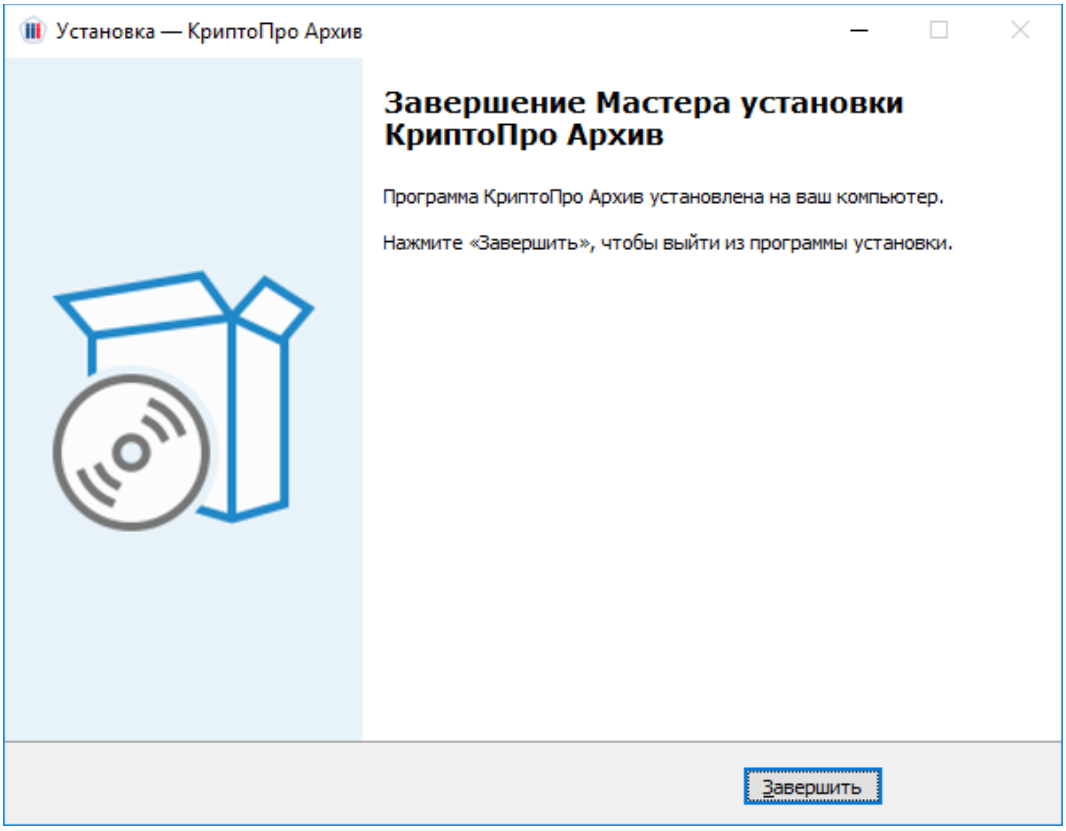
Возможен выбор компонентов для установки. Соответствие между названиями вариантов установки и набором устанавливаемых компонентов приведено в таблице (программа config будет установлена во всех сценариях):

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

Выберите подходящий вариант и нажмите **Далее**:



Нажать **Установить**. После успешного завершения установки диалоговое окно примет следующий вид:



Нажмите **Завершить**. Установка программы КриптоПро Архив завершена.

2.9.2 Установка КриптоПро Архив на ОС семейства Linux

Для установки КриптоПро Архив на ОС семейства Linux сперва распаковать содержимое пакета `cp-archive_<version>_linux-x64.tar.gz`, где `<version>` — версия дистрибутива:

```
tar -xf cp-archive_<version>_linux-x64.tar.gz
```

В результате выполнения в текущей папке появится папка `release`. Перейти в неё:

```
cd release
```

Для установки всех компонентов КриптоПро Архив выполнить

```
sudo ./install.sh
```

Также возможна установка выборочно нескольких компонентов. Например, для установки только admin-api и client-api выполнить

```
sudo ./install.sh -c admin-api -c client-api
```

Список всех доступных компонентов приведён в разделе 1.3 Архитектура решения.

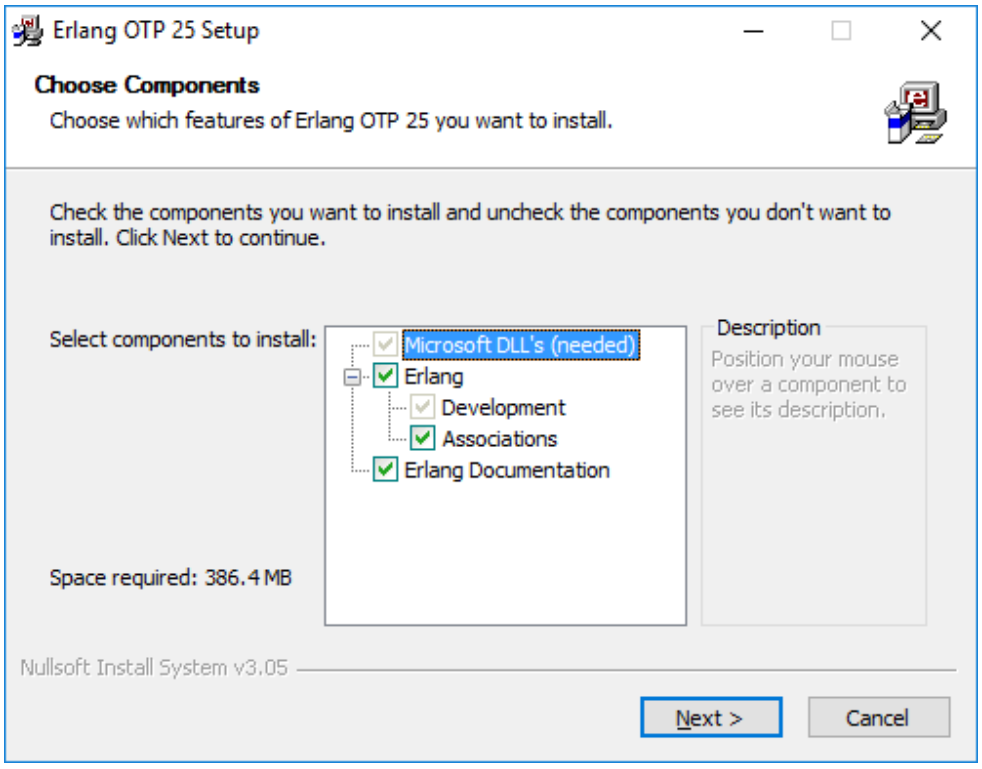
2.10 Установка Erlang

В данном разделе приведены инструкции по установке одной из зависимостей RabbitMQ: Erlang OTP 25.

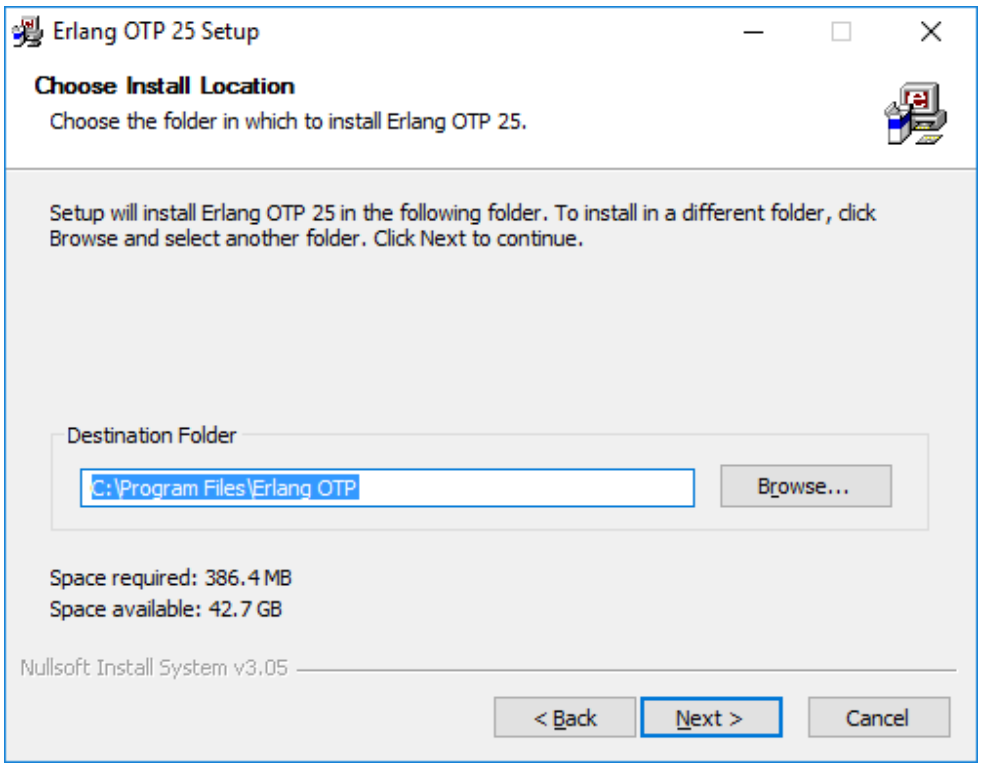
2.10.1 Установка Erlang OTP на ОС семейства Windows Server

ВАЖНО: не выполнять дальнейшие действия, находясь в учётной записи администратора сервера (пользователь Администратор). Создать пользователя с правами администратора и выполнять установку от его лица.

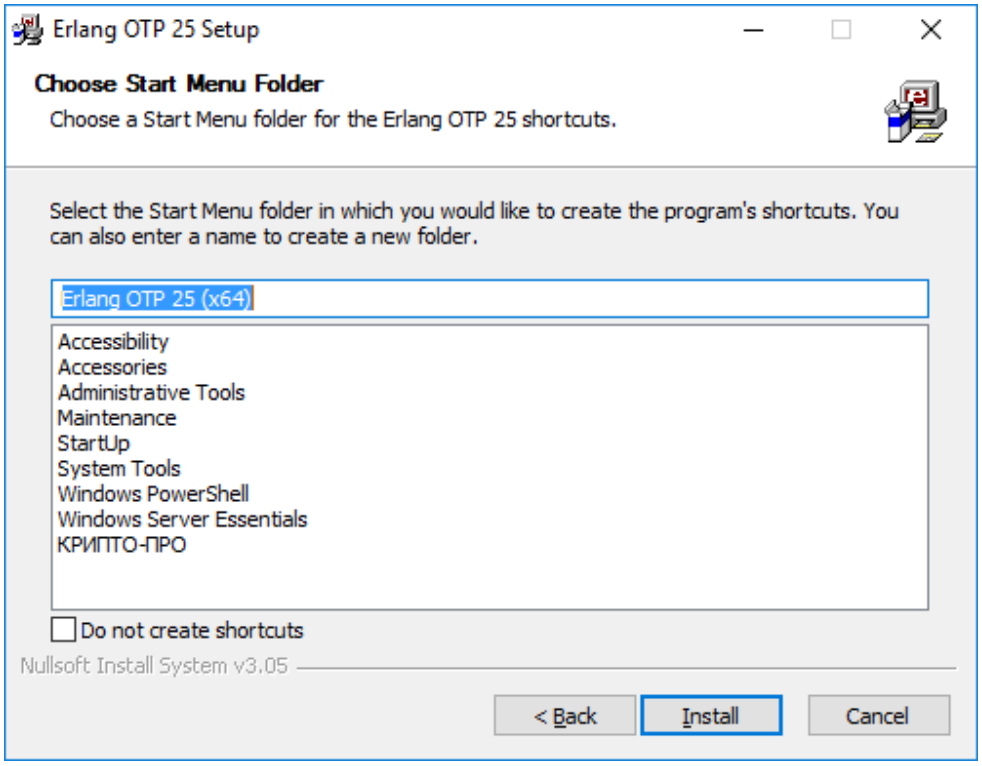
Для установки Erlang OTP 25.3.2.8 скачать его с официального сайта и запустить установочный файл от имени администратора:



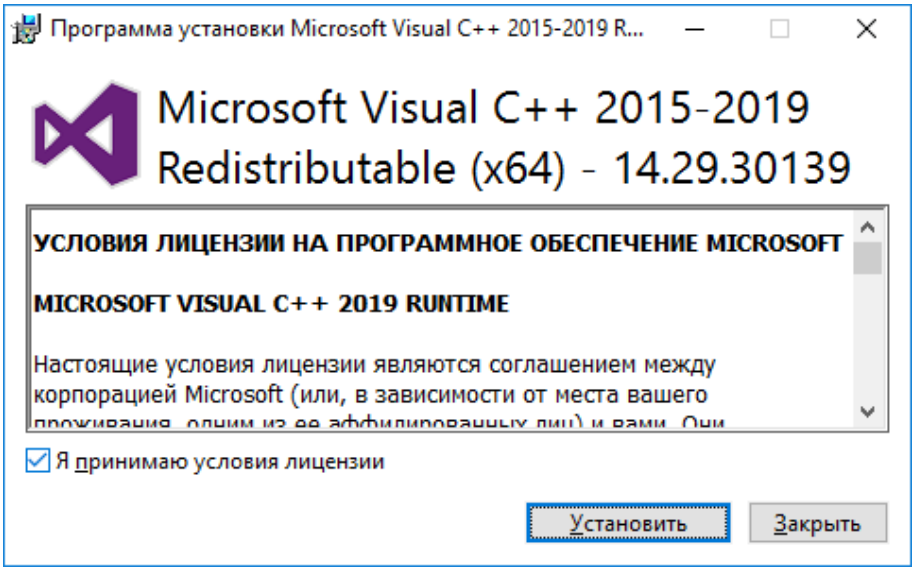
Оставить все пункты отмеченными и нажать **Next**.



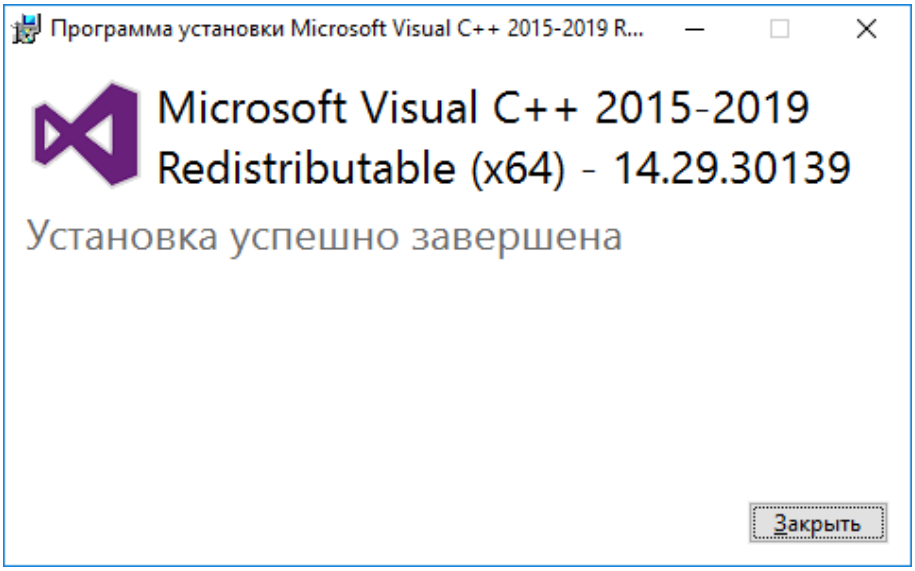
Оставить пусть установки по умолчанию и нажать **Next**.



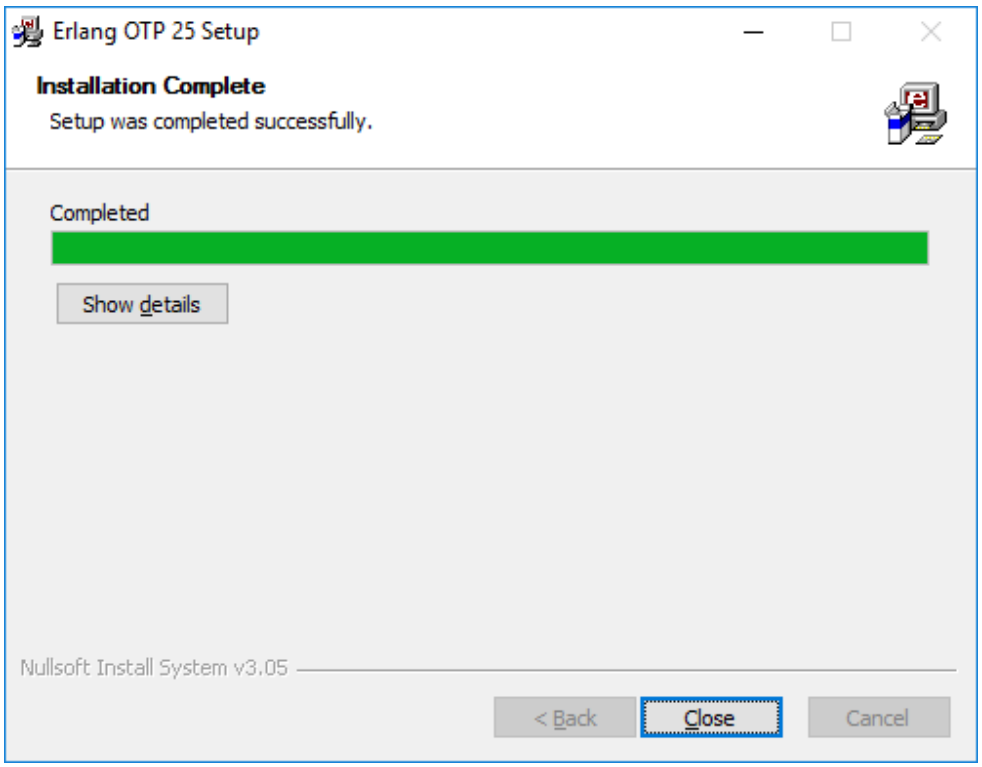
Оставить все настройки по умолчанию и нажать **Install**. Во время установки может появиться диалоговое окно с предложением установить Microsoft Visual C++ Redistributable:



Отметить пункт **Я принимаю условия лицензии** и нажать **Установить**. После завершения установки Microsoft Visual C++ Redistributable появится окно



Нажать **Закрыть**. Установка Erlang OPT 25 продолжится автоматически. После завершения установки диалоговое окно будет выглядеть следующим образом:



Нажать **Close**. Установка завершена.

2.10.2 Установка ESL Erlang на Astra Linux

ESL Erlang 25.3.2 для Astra Linux распространяется вместе с дистрибутивом КриптоПро Архив и расположен в папке с дистрибутивом. Для установки в файле `/etc/apt/sources.list` необходимо раскомментировать или добавить следующую строку:

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64
main contrib non-free
```

После этого в папке дистрибутива выполните

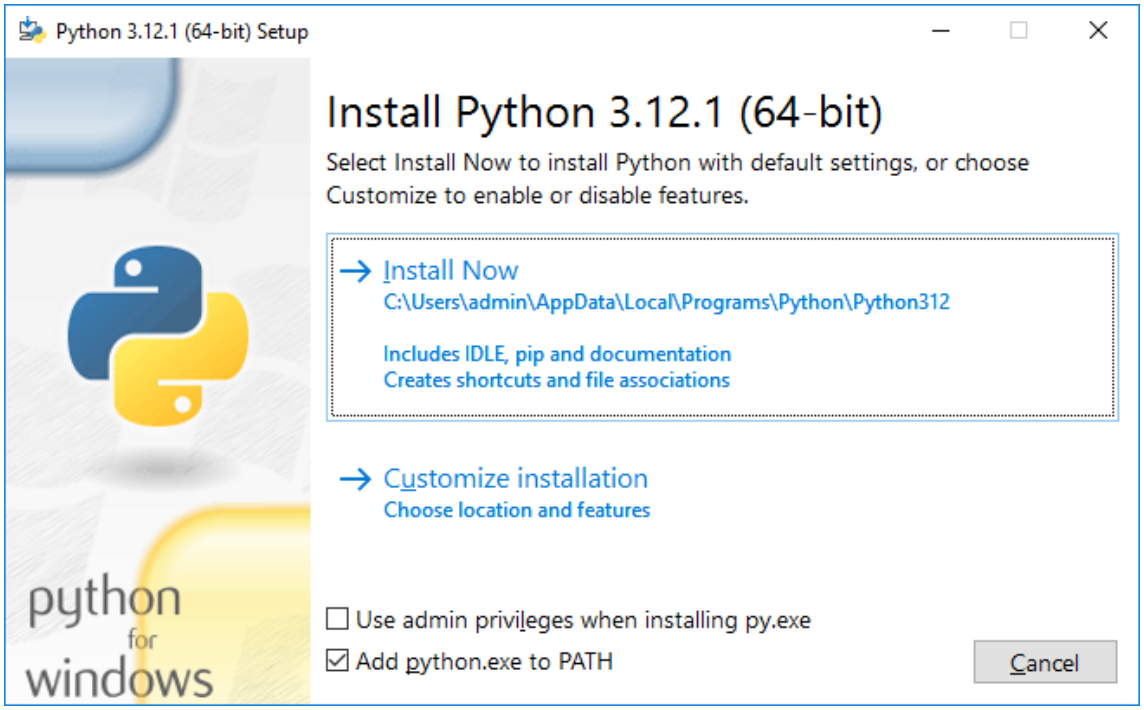
```
sudo apt update

sudo apt install libtinfo5 libncurses5 libsctp1

sudo dpkg -i esl-erlang_25.3.2-1~debian~buster_amd64.deb
```

2.11 Установка Python 3

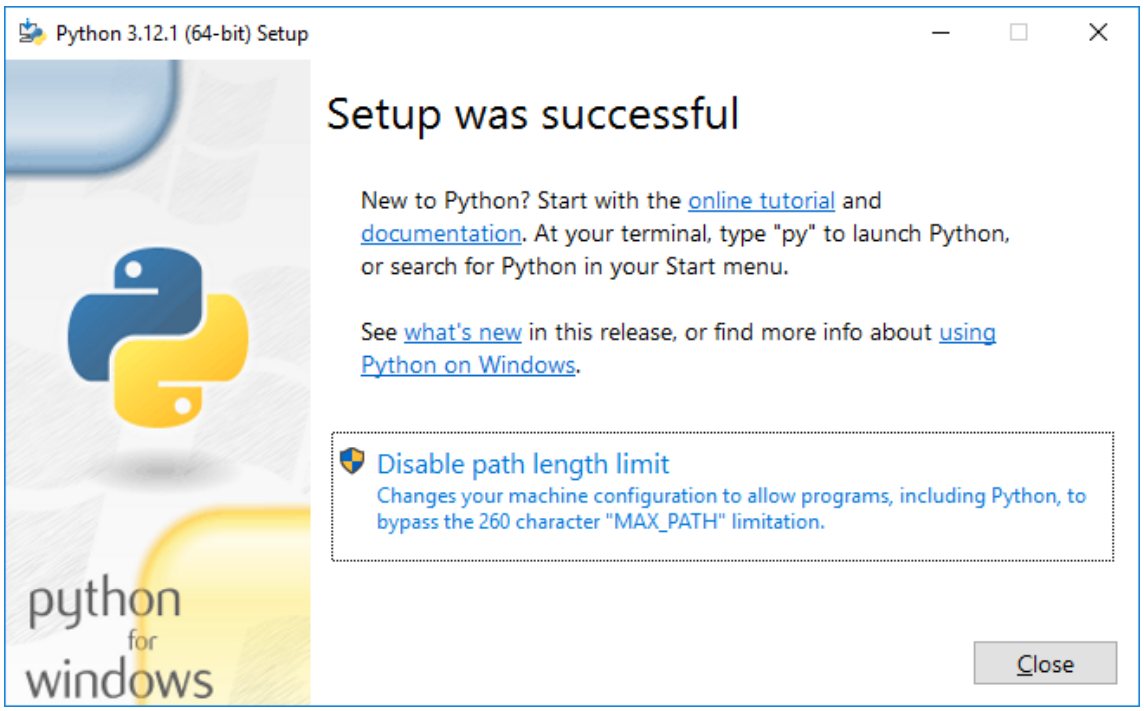
В данном разделе приведены инструкции по установке одной из зависимостей RabbitMQ: Python 3.

2.11.1 Установка Python 3 на ОС семейства Windows Server

Для установки Python 3.12.1 скачать его с официального сайта и запустить установочный файл от имени администратора:



Отметить пункт **Add python.exe to PATH** и нажать **Install Now**. После завершения установки диалоговое окно будет иметь следующее содержание:



Нажать **Close**. Установка завершена.

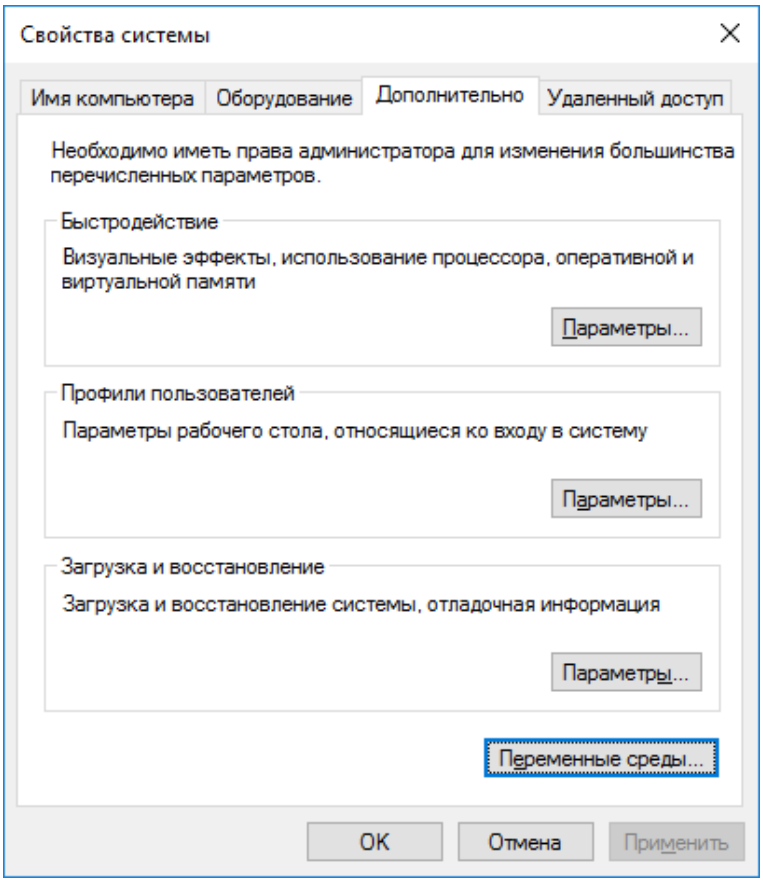
2.12 Установка NSSM

В данном разделе описана установка NSSM — опционального дополнительного ПО для более удобной регистрации служб на ОС семейства Windows Server.

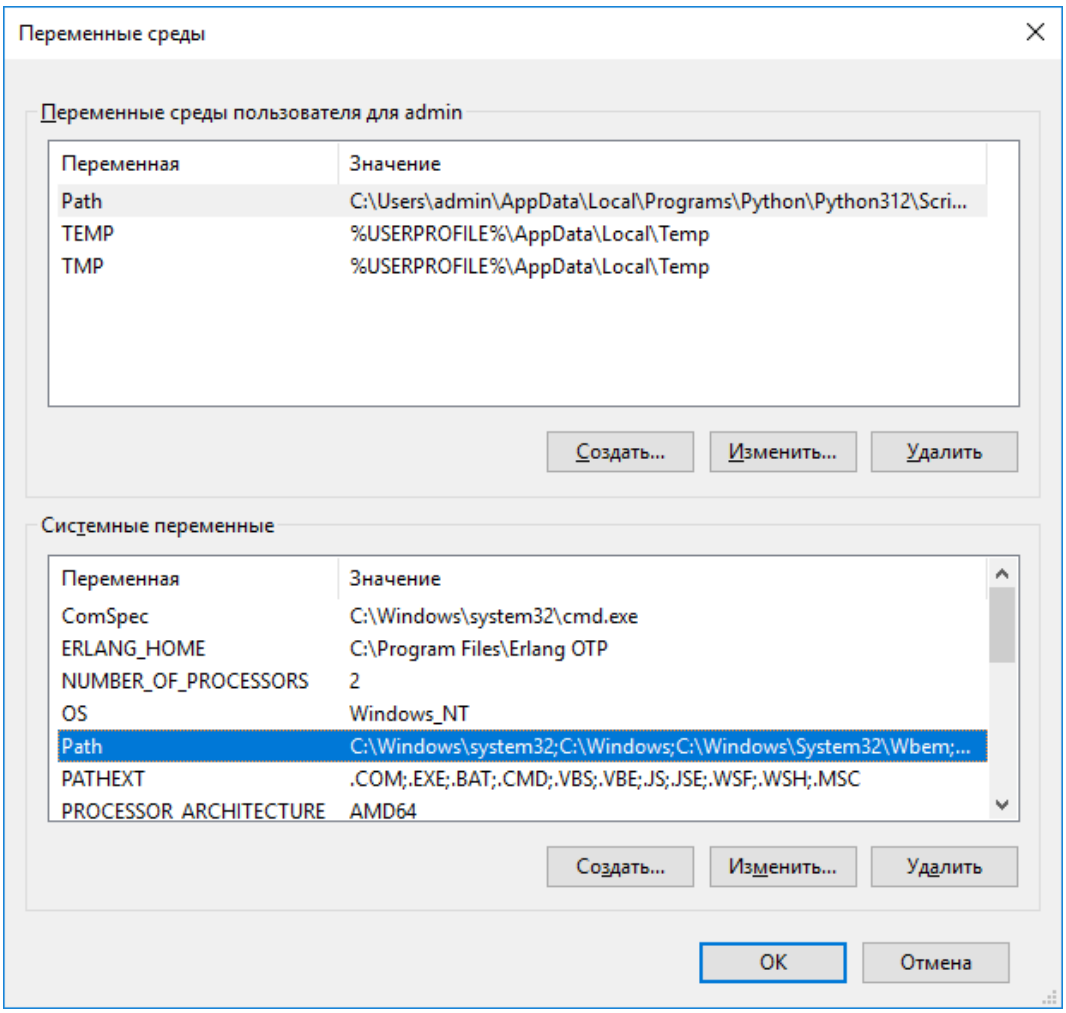
2.12.1 Установка NSSM на ОС семейства Windows Server

Для установки NSSM 2.24 на ОС семейства Windows Server скачайте архив с программой с официального сайта проекта. Разархивируйте содержимое архива в папку `C:\Program Files`.

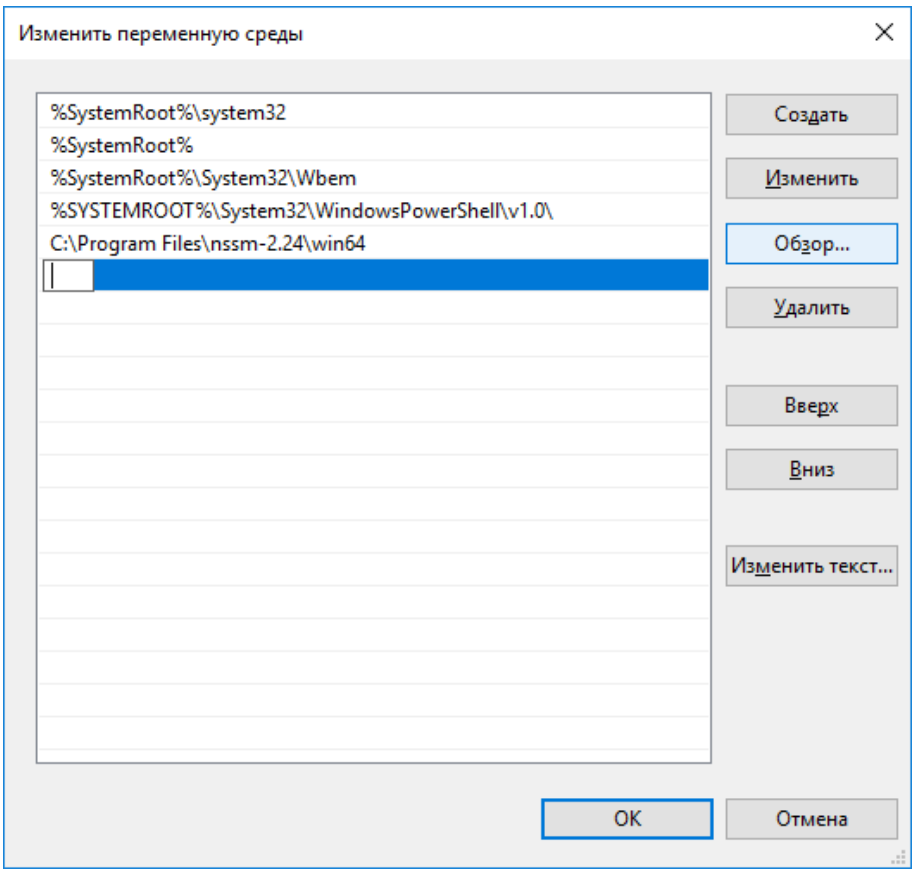
Рекомендуется добавить путь к исполняемому файлу в переменную PATH для доступа к программе из любой папки на компьютере. Для этого откройте **Панель управления** и перейдите по пути `Панель управления\Система и безопасность\Система`. На панели слева найдите и откройте **Дополнительные параметры**:



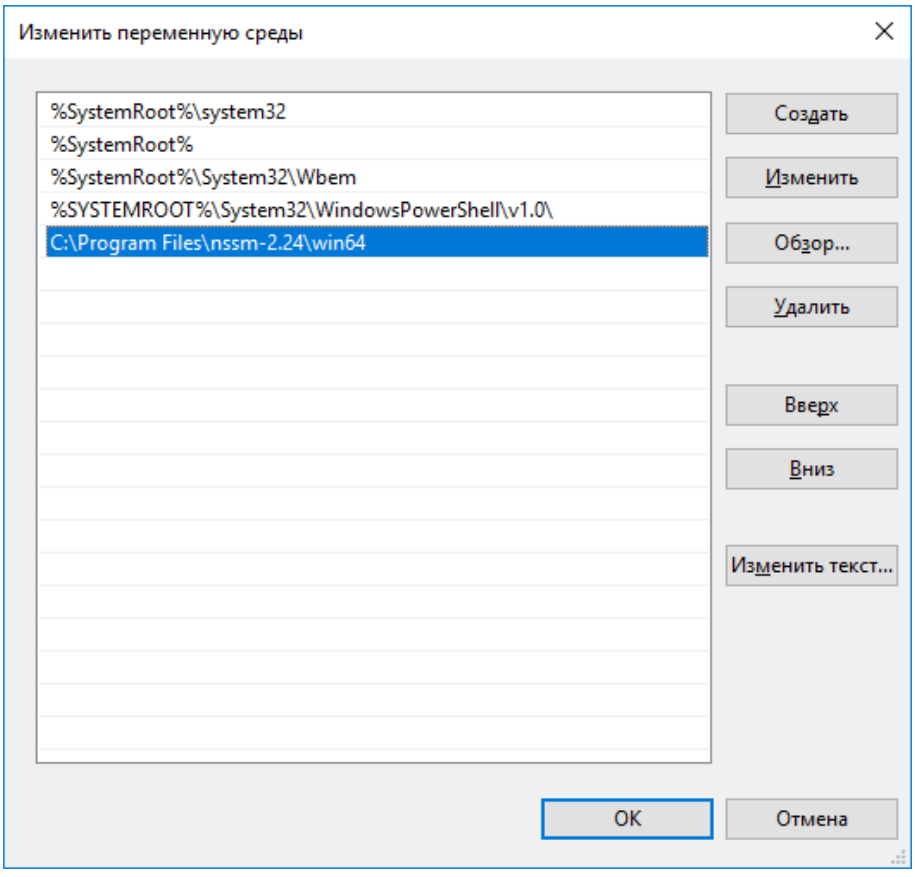
Нажмите **Переменные среды**:



В разделе **Системные переменные** дважды нажмите на переменную **Path**. В появившемся окне нажмите **Создать** и укажите путь до папки `C:\Program Files\nssm-2.24\win64`. Путь также можно выбрать, нажав **Обзор**.



После ввода значения переменной экран будет выглядеть следующим образом:



Нажмите **ОК** несколько раз, чтобы закрыть все открытые в процессе установки переменной среды окна. Настройка переменной среды завершена. Теперь вызывать программу можно просто введя в терминале `nssm`.

3 Настройка

В данной главе описана настройка компонентов КриптоПро Архив. К настройке следует переходить, если все необходимые компоненты установлены. Для списка необходимых компонентов обратитесь к разделу 2.1 Описание процесса установки КриптоПро Архив.

Для описания путей в JSON-файлах используется нотация JSONPath. Например, для обращения к значению `"Petya"` из примера ниже используется синтаксис `$.Person.Children[0].Name`:

```
{
  "Person": {
    "Name": "Ivan",
    "Children": [
      {
        "Name": "Petya",
        "Age": 10
      }
    ]
    "Age": 35,
    "Employed": true
  }
}
```

Цвета указывают тип переменной. Строки обозначаются оранжевым цветом с кавычками, числа — синим цветом, булевы значения — зелёным.

3.1 Настройка RabbitMQ

В данном разделе описана настройка RabbitMQ. Предполагается, что программа установлена на сервере. Инструкции по установке см. в разделе 2.5 Установка RabbitMQ.

3.1.1 Настройка RabbitMQ на ОС семейства Windows Server

Для настройки RabbitMQ выполните сценарий `ConfigureRabbitMq.ps1`, расположенный в папке с дистрибутивом КриптоПро Архив. Для этого откройте PowerShell в этой папке от лица администратора и выполните следующий сценарий. Задайте параметры `<username>` и `<password>`. Они определяют имя создаваемого пользователя и его пароль:

```
.\ConfigureRabbitMq.ps1 -username <username> -password <password>
```

Сценарий принимает опциональные параметры. Измените их при необходимости в соответствии с настройками на сервере.

Имя параметра	Описание	Значение по умолчанию
`-username`	Имя создаваемого пользователя	`cryptopro_app`
`-password`	Пароль создаваемого пользователя	`cryptopro`
`-version`	Установленная версия RabbitMQ (изменить в случае несоответствия)	`3.12.11`
`-path`	Путь к папке с сценариями для управления RabbitMQ (изменить в случае установки RabbitMQ не по стандартному пути)	`C:\Program Files\RabbitMQ Server\rabbitmq_server-$version\sbin`

Сценарий создаст виртуальный хост `archive`, пользователя и активирует плагин для управления RabbitMQ через административную панель с графическим веб-интерфейсом. Рекомендуется изменить имя и пароль создаваемого пользователя (параметры `-username` и `-password`).

Пример вызова сценария с параметрами:

```
.\ConfigureRabbitMq.ps1 -username <username> -password <password> -version 3.12.10
```

При возникновении ошибок, связанных с **Execution Policy**, выполнить в директории со сценарием (больше информации по ссылке)

```
Unblock-File -Path .\ConfigureRabbitMq.ps1
```

Пример успешного выполнения сценария:

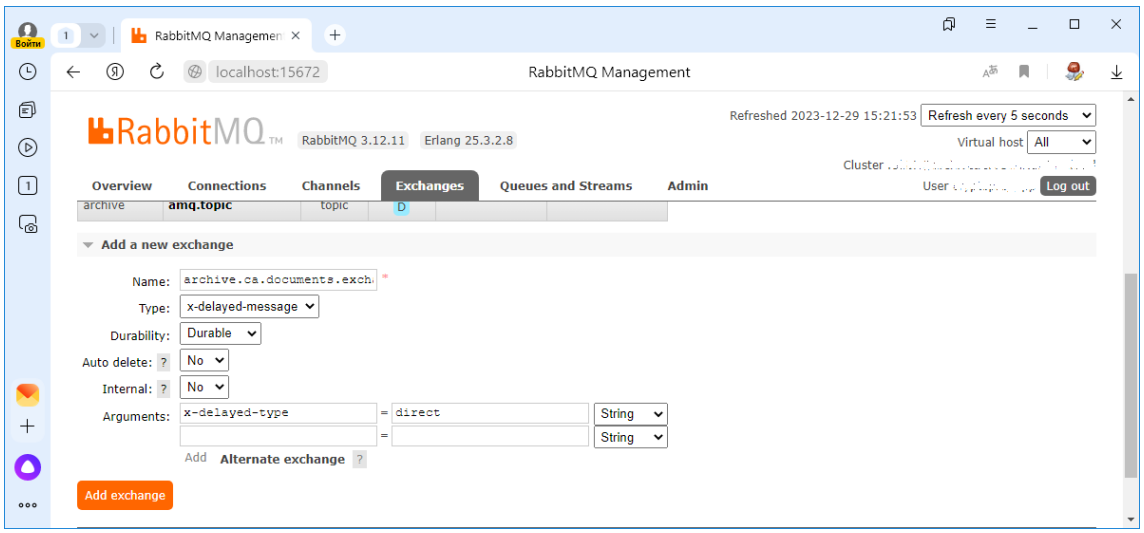
```
Adding user "<username>" ...
Done. Don't forget to grant the user permissions to some virtual hosts! See
'rabbitmqctl help set_permissions' to learn more.
Setting tags for user "<username>" to [management] ...
Adding vhost "archive" ...
Setting permissions for user "<username>" in vhost "archive" ...
```

```
Enabling plugins on node <node_name>:
rabbitmq_management
The following plugins have been configured:
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_web_dispatch
Applying plugin configuration to <node_name>...
The following plugins have been enabled:
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_web_dispatch

started 3 plugins.
```

Административный интерфейс расположен по адресу `http://localhost:15672`. Перейдите туда и войдите под созданным пользователем. Перейдите на вкладку **Exchanges** (обмены) и раскройте меню **Add a new exchange**. Создайте два обмена: `archive.ca.documents.exchange`, `archive.notifications.exchange` и `archive.signatures.exchange` с идентичными настройками, различающиеся только именем. Заполните поля следующим образом:

Имя поля	Значение
Name	`archive.ca.documents.exchange`, `archive.notifications.exchange` или `archive.signatures.exchange` (необходимо создать все три)
Type	`x-delayed-message`
Durability	Durable
Auto delete	No
Internal	No
Arguments	`x-delayed-type=direct`

Пример заполнения формы для обмена `archive.ca.documents.exchange`:

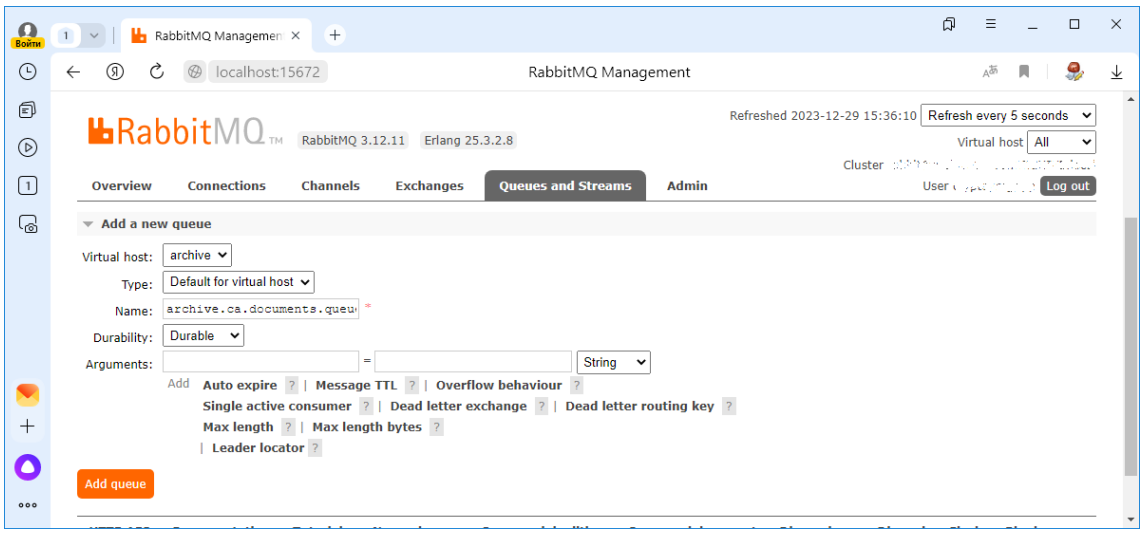


Нажмите **Add exchange** для создания обмена.

Перейдите на вкладку **Queues and Streams** для создания необходимых очередей и раскройте меню **Add a new queue**. Создайте две очереди с именами `archive.ca.documents.queue`, `archive.notifications.queue` и archive.signatures.queue с идентичными настройками, различающиеся только именем. Заполните поля следующим образом:

Имя поля	Значение
Virtual host	`archive`
Type	Default for virtual host
Name	`archive.ca.documents.queue`, `archive.notifications.queue` или `archive.signatures.queue` (необходимо создать все три)
Durability	Durable
Arguments	

Пример заполнения формы для очереди `archive.ca.documents.queue`:



Нажмите **Add queue** для создания очереди. Настройка RabbitMQ завершена.

3.1.2 Настройка RabbitMQ на ОС семейства Linux

Перед выполнением настройки убедитесь, что RabbitMQ установлен в соответствии с инструкцией, приведённой в разделе 2.5 Установка RabbitMQ. Настройка RabbitMQ на ОС семейства Linux заключается в выполнении сценария `rabbitmq.sh` в директории с дистрибутивом:

```
chmod +x rabbitmq.sh

./rabbitmq.sh \
    --username <username> \
    --password <password>
```

Где `<username>` — имя создаваемого пользователя, а `<password>` — его пароль. Значения по умолчанию: `cryptopro_app` и `cryptopro` соответственно. Пример вывода после успешного выполнения сценария:

```
Adding user "<username>" ...
Done. Don't forget to grant the user permissions to some virtual hosts! See
'rabbitmqctl help set_permissions' to learn more.
Setting tags for user "<username>" to [management] ...
Adding vhost "archive" ...
Setting permissions for user "<username>" in vhost "archive" ...
queue declared
queue declared
queue declared
exchange declared
exchange declared
exchange declared
```

3.2 Настройка Elasticsearch

В данном разделе описана настройка Elasticsearch. Предполагается, что программа установлена на сервере. Инструкции по установке см. в разделе 2.3 Установка Elasticsearch. Инструкции ниже предполагают установленную версию 7.17.16. При несовпадении заменить версию в командах на ту, которая установлена на сервере. Более подробно про настройку Elasticsearch можно прочитать в официальной онлайн-документации. Разработчики также приводят список настроек, на которые рекомендуется обратить внимание перед запуском кластера.

3.2.1 Настройка Elasticsearch на ОС семейства Windows Server

Стандартные настройки Elasticsearch, такие как порт и адрес прослушивания определены и прокомментированы в файле `C:\Program Files\elasticsearch-7.17.16\config\elasticsearch.yml`. Для изменения выбранной настройки раскомментировать строку с ней и установить требуемое значение.

В некоторых случаях может быть желательно настроить количество потребляемой оперативной памяти, так как по умолчанию Elasticsearch может занимать всю свободную оперативную память. Перед тем, как это делать, рекомендуется ознакомиться с онлайн-документацией по изменению подобных расширенных параметров, так как разработчики Elasticsearch не рекомендуют менять эти параметры в большинстве случаев. Также рекомендуется ознакомиться с содержимым файла `C:\Program Files\elasticsearch-7.17.16\config\jvm.options`.

Для настройки создать файл `limits.options` в папке `C:\Program Files\elasticsearch-7.17.16\config\jvm.options.d` и указать там следующие строки:

```
-Xms4g
-Xmx4g
```

Число 4 указывает количество ГБ. Изменить его при необходимости. После этого перезапустить службу Elasticsearch.

3.2.2 Настройка Elasticsearch на ОС семейства Linux

Стандартные настройки Elasticsearch, такие как порт и адрес прослушивания определены и прокомментированы в файле `/etc/elasticsearch/elasticsearch.yml`. Для изменения выбранной настройки раскомментировать строку с ней и установить требуемое значение.

В некоторых случаях может быть желательно настроить количество потребляемой оперативной памяти, так как по умолчанию Elasticsearch может занимать всю свободную оперативную память. Перед тем, как это делать, рекомендуется ознакомиться с онлайн-документацией по изменению подобных расширенных параметров, так как разработчики Elasticsearch не рекомендуют менять эти параметры в большинстве случаев. Также рекомендуется ознакомиться с содержимым файла `/etc/elasticsearch/jvm.options`.

Для настройки создать файл `limits.options` в папке `/etc/elasticsearch/jvm.options.d` и указать там следующие строки:

```
-Xms4g
-Xmx4g
```

Число 4 указывает количество ГБ. Изменить его при необходимости. После этого перезапустить службу Elasticsearch:

```
sudo systemctl restart elasticsearch.service
```

3.3 Настройка PostgreSQL

В данном разделе приведены инструкции по настройке PostgreSQL для работы с КриптоПро Архив. Для настройки потребуются установленные СУБД PostgreSQL версии не ниже 11, pgAdmin4 и КриптоПро Архив в любой конфигурации. Предполагается, что программы установлены по стандартным путям, как указано в инструкциях по установке. В противном случае в примерах ниже заменить эти пути на соответствующие.

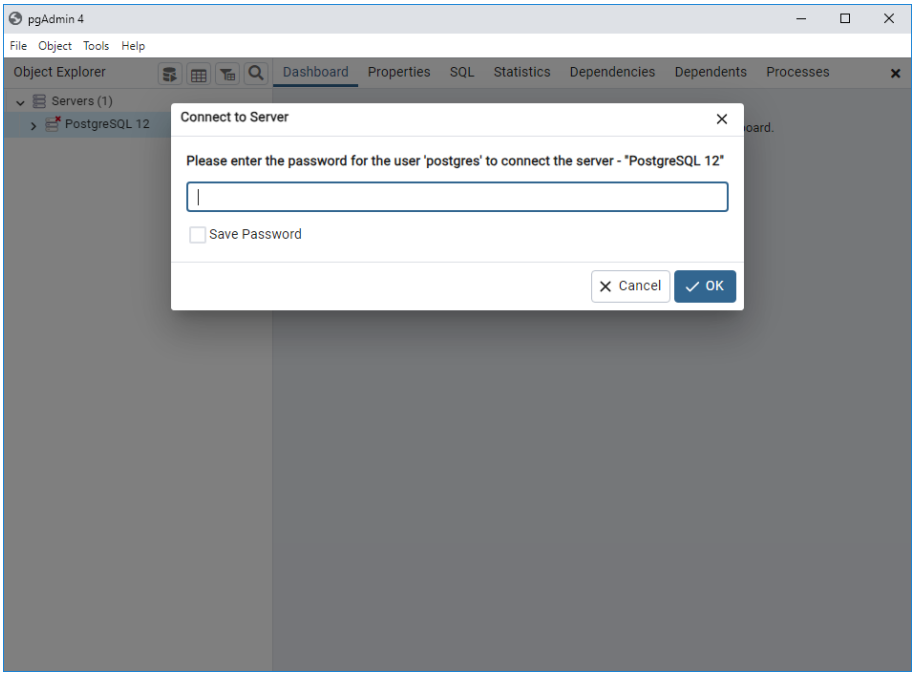
Замечание: ниже описана инструкция по созданию пользователя и базы данных, владельцем которой является созданный пользователь. Если такого ограничения недостаточно с точки зрения безопасности, пользователя можно не делать владельцем базы данных. В таком случае минимальные права, требуемые пользователю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

- на каждую таблицу права `INSERT`, `SELECT`, `UPDATE`, `DELETE`
- на хранимые функции право `EXECUTE`

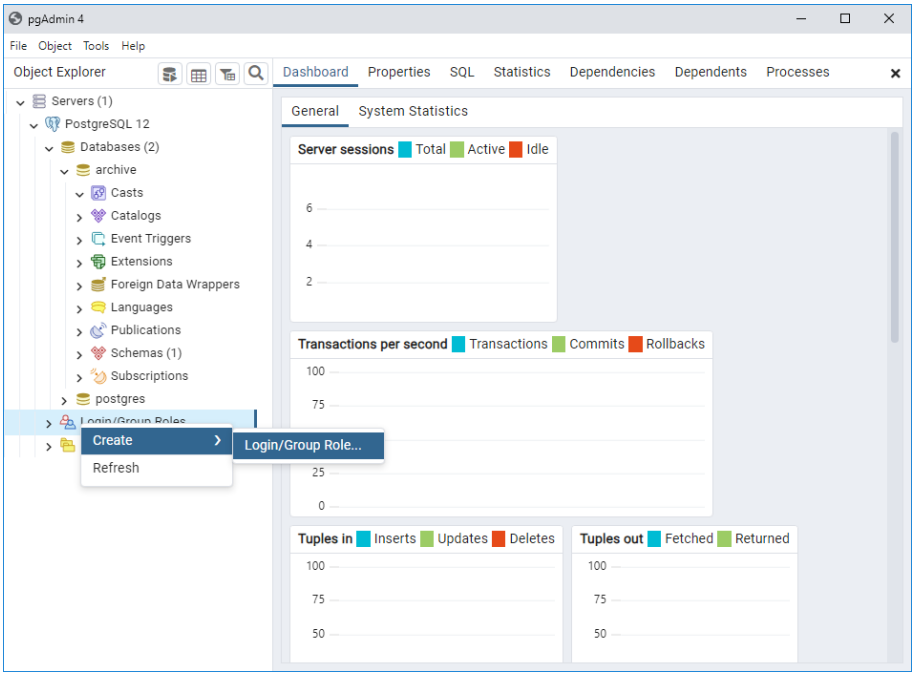
Замечание: настоятельно рекомендуется производить резервное копирование всех создаваемых баз данных.

3.3.1 Настройка PostgreSQL на ОС семейства Windows Server

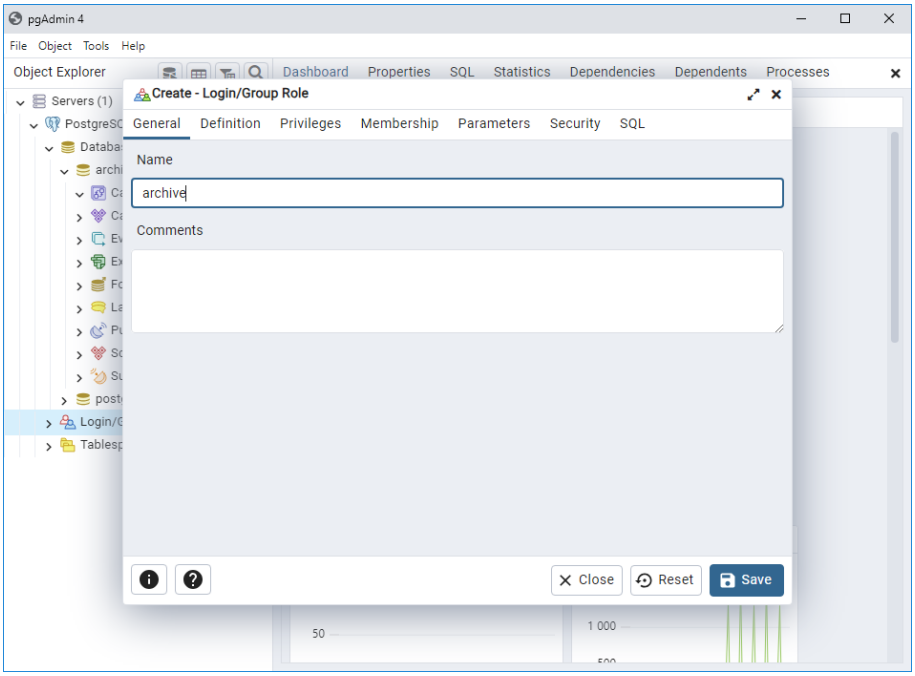
Для создания базы данных PostgreSQL, совместимой с КриптоПро Архив, сперва создайте пользователя, от лица которого будет происходить подключение к базе данных со стороны Архива. Для этого откройте pgAdmin4, разверните вкладку **Servers** и введите пароль пользователя `postgres`:



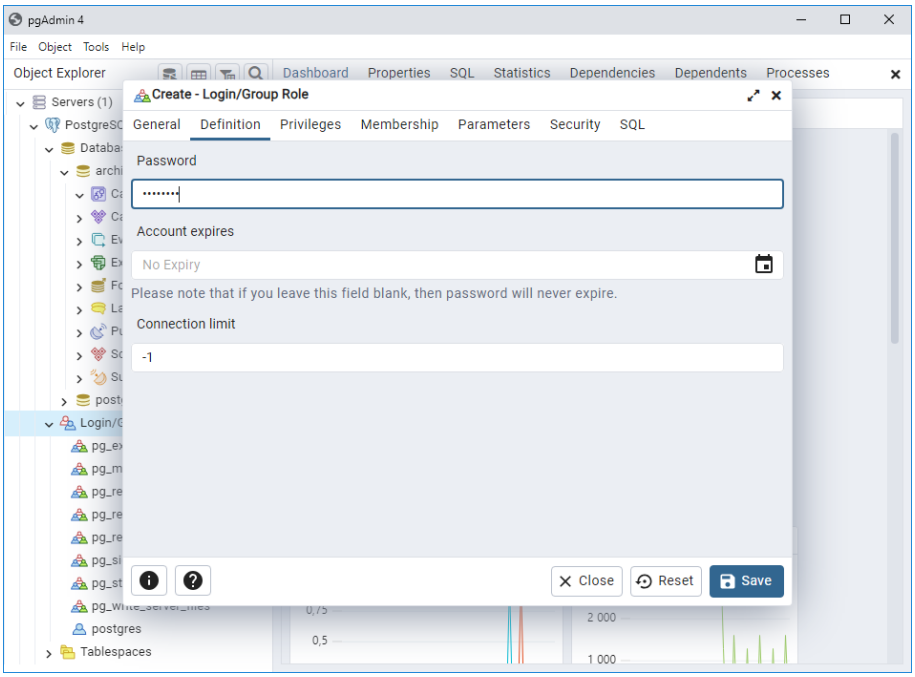
Создайте пользователя `archive`. Для этого откройте **Login/Group Roles** > **Create** > **Login/Group Role…**:



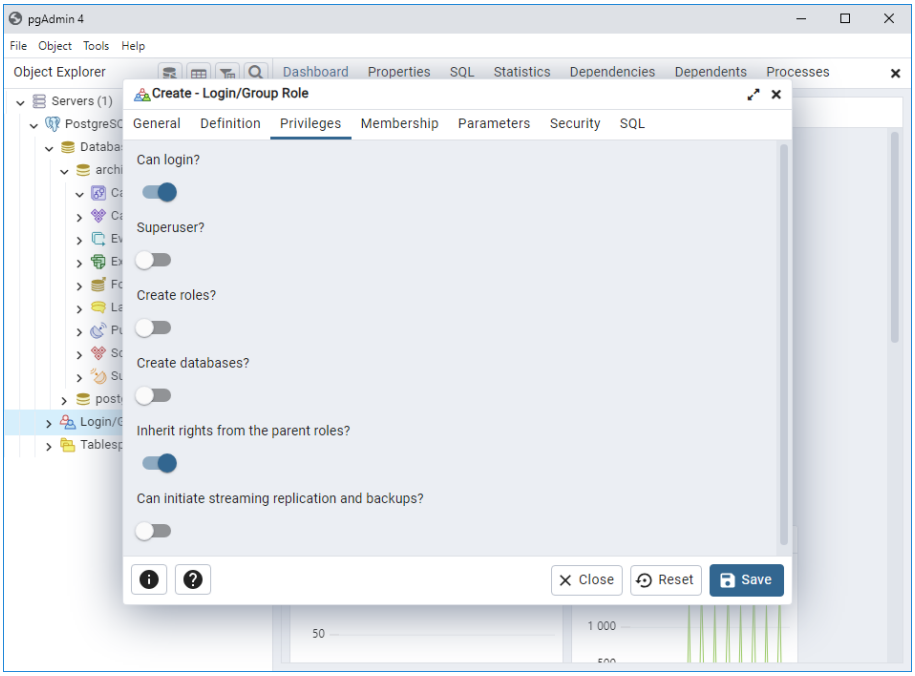
В открывшемся окне на вкладке **General** введите имя пользователя. В примере ниже используется `archive`. Это значение рекомендуется изменить:



Придумайте пароль создаваемого пользователя и введите его во вкладке **Definition**:

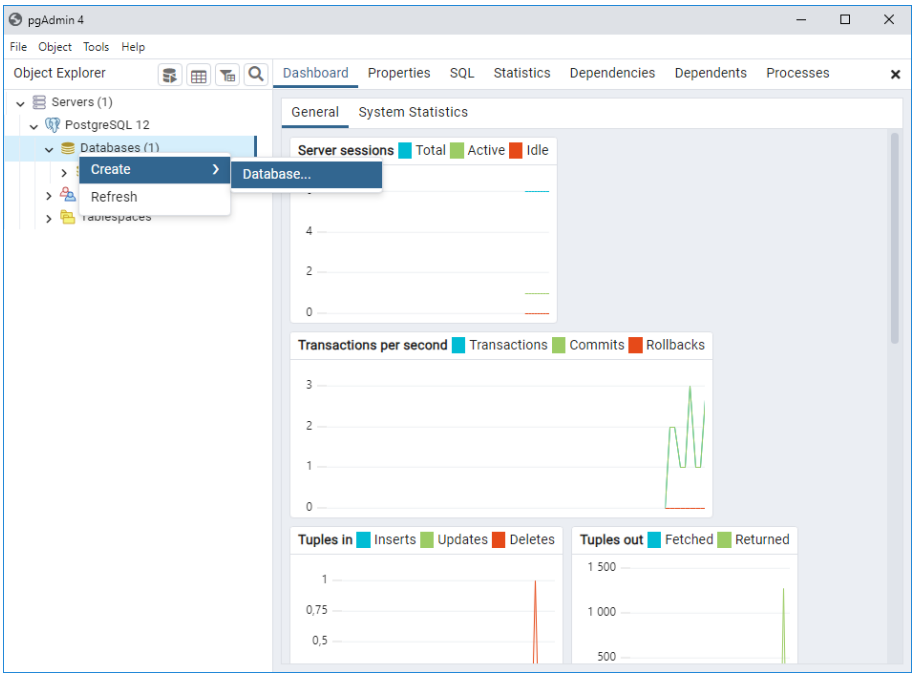


Откройте вкладку **Privileges** и отметьте пункт **Can login**:

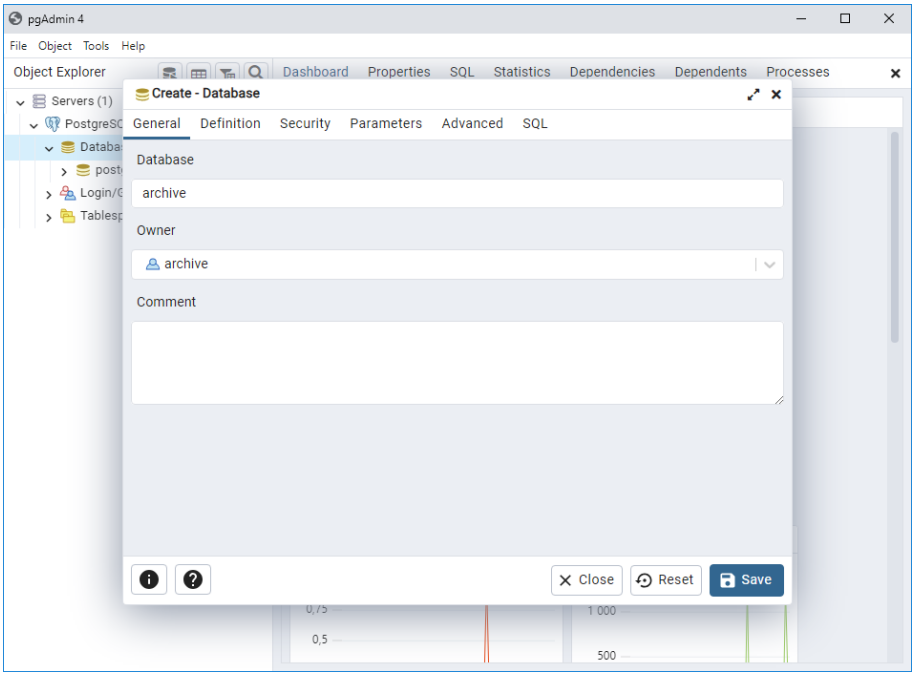


Нажмите **Save**. Пользователь создан. Теперь он будет отображаться в списке **Login/Group Roles**.

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



Введите имя базы данных. В примере ниже — `archive`. Его рекомендуется изменить.



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
--database	Указание на то, что требуется выполнить миграцию базы данных
--mode	Режим миграции. Определяет, нужно ли создать новую базу данных (значение create), заполнить существующую (use) или обновить существующую заполненную до новой версии (upgrade)

`--database-provider`	Имя провайдера баз данных. Должно быть указано `PostgreSql`
`--connection-string`	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 КриптоПро 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.

3.3.2 Настройка PostgreSQL на Astra Linux 1.7

Для создания базы данных PostgreSQL, совместимой с КриптоПро Архив, сперва создайте пользователя, от лица которого будет происходить подключение к базе данных со стороны Архива. Для этого запустите `psql` от лица администратора баз данных — пользователя `postgres`:

```
sudo -u postgres psql
```

Создайте пользователя и базу данных. Назначьте созданного пользователя владельцем созданной базы данных:

```
CREATE USER <username> PASSWORD '<password>';
CREATE DATABASE <database> OWNER <username>;
exit
```

Обратите внимание на кавычки вокруг `<password>`. Выдайте пользователю `postgres` права на чтение мандатных меток:

```
sudo pdpl-user -z archive
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb /etc/parsec/capdb
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb /etc/parsec/capdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb /etc/parsec/capdb
```

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

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

Программа заполнит 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 КриптоПро Архив, выполните следующие команды, заменив `<username>` на имя пользователя, `<password>` на пароль пользователя, `<host>` на адрес сервера с PostgreSQL и `<database>` на имя базы данных:

```
sudo /opt/cp-archive/config/Archive.Config set \
    --database-provider PostgreSql

sudo /opt/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

```
sudo /opt/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.

3.3.3 Настройка PostgreSQL на Astra Linux

Для создания базы данных PostgreSQL, совместимой с КриптоПро Архив, сперва создайте пользователя `archive`, от лица которого будет происходить подключение к базе данных со стороны Архива. Для этого запустите `psql` от лица администратора баз данных — пользователя `postgres`:

```
sudo -u postgres psql
```

Создайте пользователя и базу данных. Назначьте созданного пользователя владельцем созданной базы данных:

```
CREATE USER <username> PASSWORD '<password>';

CREATE DATABASE <database> OWNER <username>;

exit
```

Обратите внимание на кавычки вокруг `<password>`.

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

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

Программа заполнит 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 КриптоПро Архив, выполните следующие команды, заменив `<username>` на имя пользователя, `<password>` на пароль пользователя, `<host>` на адрес сервера с PostgreSQL и `<database>` на имя базы данных:

```
sudo /opt/cp-archive/config/Archive.Config set \
    --database-provider PostgreSql

sudo /opt/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

```
sudo /opt/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.

3.4 Настройка Oracle Database

В данном разделе приведено описание настройки Oracle Database для работы с КриптоПро Архив. Для настройки потребуются установленные КриптоПро Архив в любой конфигурации и Oracle Database 12c Release 2. Предполагается, что программы установлены по стандартным путям, как указано в инструкциях по установке. В противном случае в примерах ниже заменить эти пути на соответствующие.

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

3.4.1 Настройка Oracle Database на ОС семейства Windows Server

Для быстрого автоматического создания пользователя и схемы, достаточных для работы с КриптоПро 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
--database	Указание на то, что требуется выполнить миграцию базы данных
--mode	Режим миграции. Определяет, нужно ли создать новую базу данных (значение create), заполнить существующую (use) или обновить существующую заполненную до новой версии (upgrade)
--database-provider	Имя провайдера баз данных. Должно быть указано Oracle

`--connection-string`	Строка подключения к базе данных. Обратите внимание на то, что подключение должно производиться к существующему пользователю/схеме
`--target`	Имя создаваемого пользователя

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>
```

Настройка базы данных Oracle Database завершена.

3.4.2 Настройка Oracle Database на ОС семейства Linux

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

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

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, заменив <password> на пароль пользователя <username> и <data_source> на адрес сервера с Oracle:

```
sudo /opt/cp-archive/config/Archive.Config set \
    --database-provider Oracle

sudo /opt/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

```
sudo /opt/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>
```

Настройка базы данных Oracle Database завершена.

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

В примерах ниже предполагается установка компонентов Архива по стандартным путям. Если пути не совпадают с выбранными на этапе установки, измените их на соответствующие.

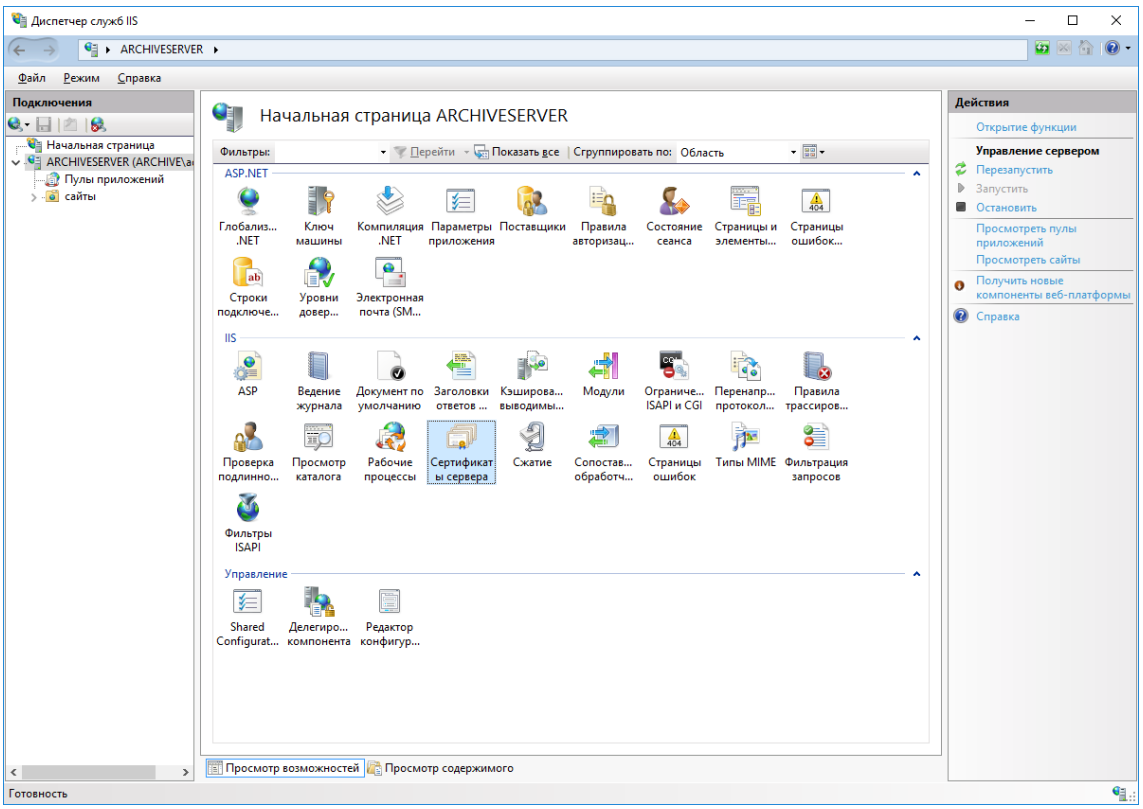
3.5.1 Настройка admin-api и client-api на ОС семейства Windows Server

Предполагается, что на сервере, помимо указанных выше, установлены программы IIS и Microsoft Hosting Bundle. 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.

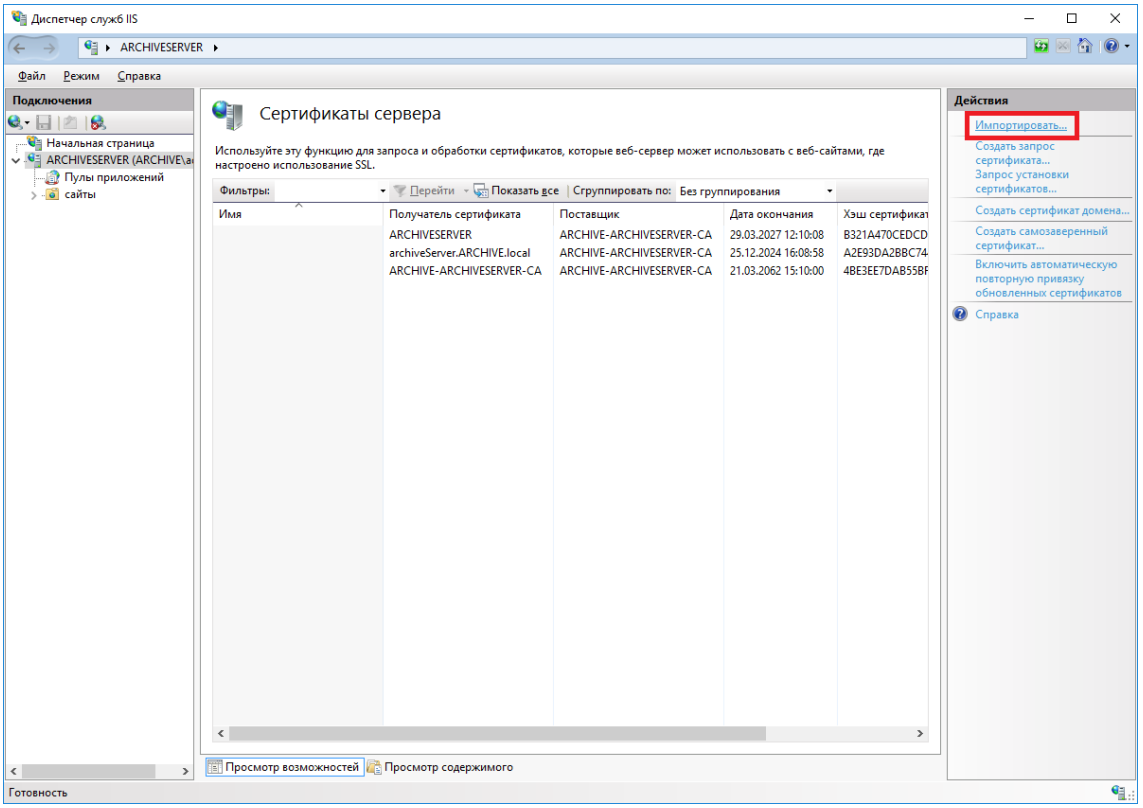
Инструкции ниже разделены на секции, однако при первой настройке рекомендуется читать их последовательно.

3.5.1.1 Добавление серверного сертификата

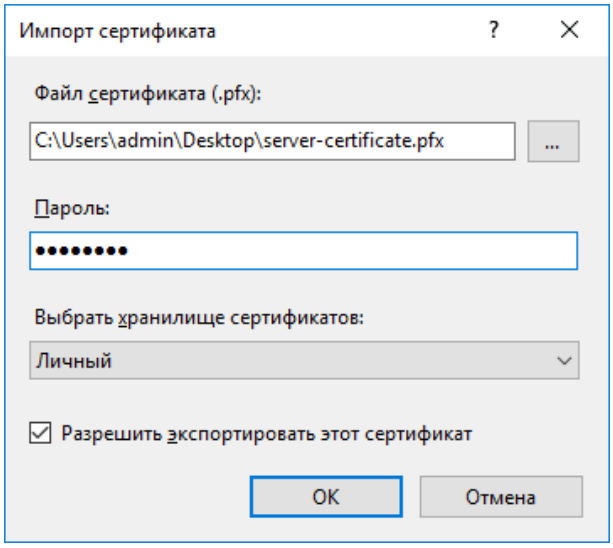
Сперва необходимо добавить сертификат проверки подлинности сервера в IIS. Если он уже был добавлен, повторно этого делать не нужно — используйте добавленный. Для добавления откройте IIS, выберите слева вкладку с именем сервера и дважды нажмите на **Сертификаты сервера**:



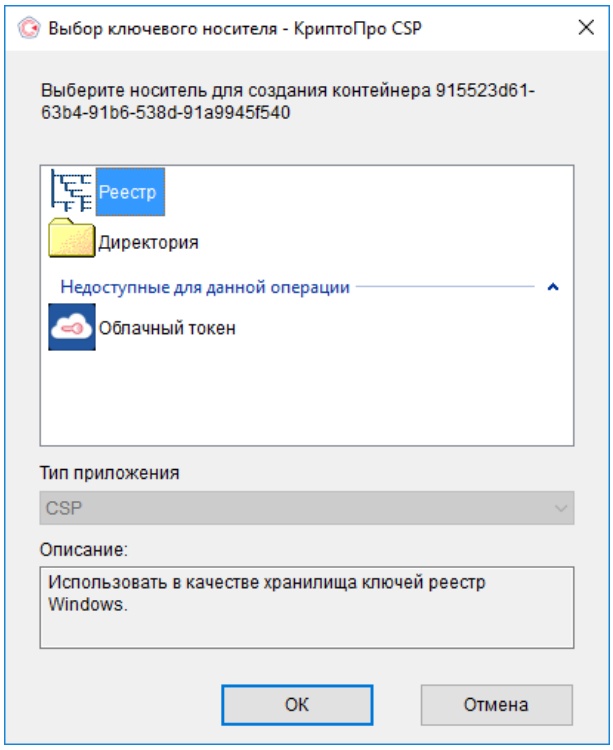
В меню справа выберите **Импортировать**:



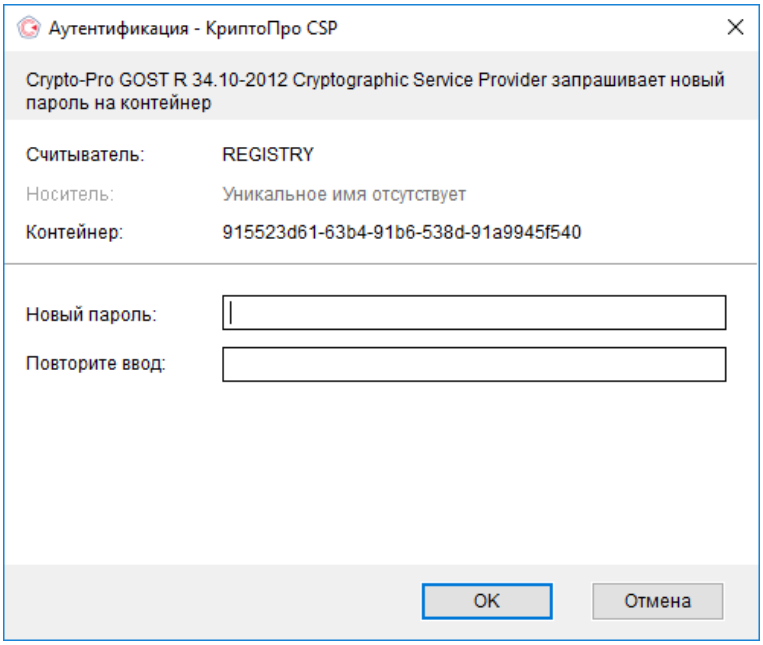
В появившемся окне укажите путь к сертификату и введите пароль:



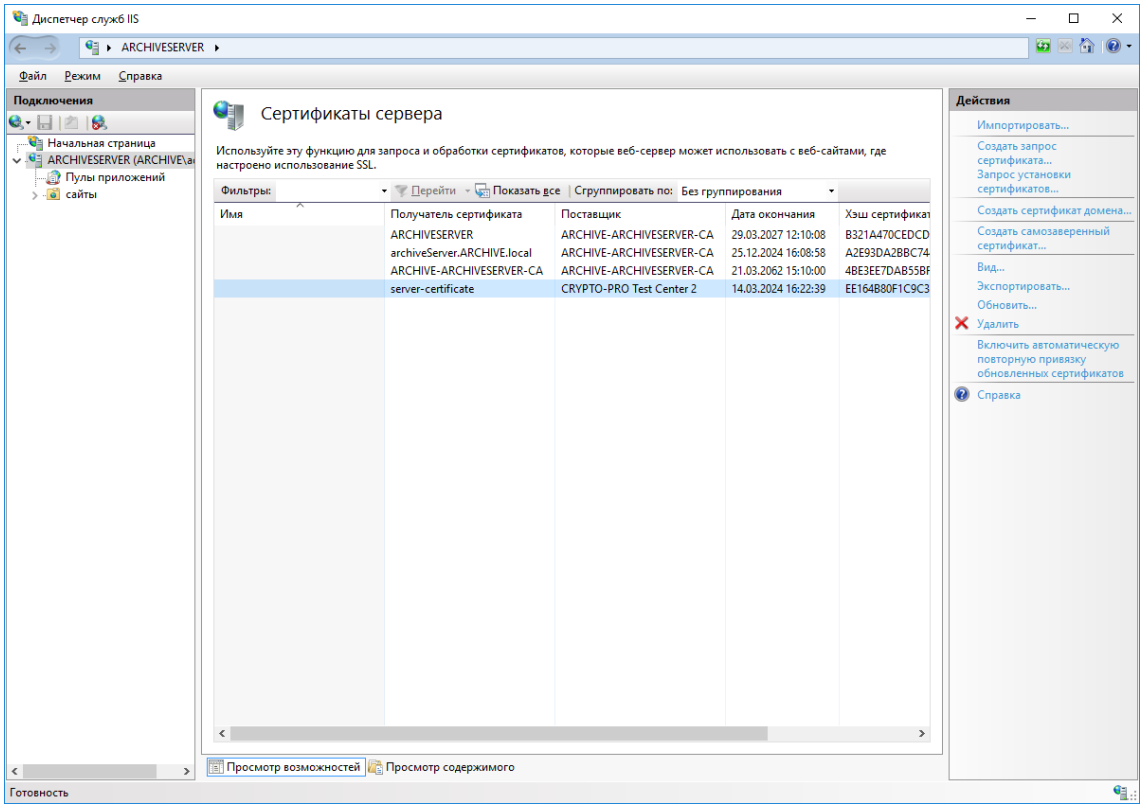
Нажмите **ОК**. В качестве носителя выберите **Реестр**:



Нажмите **ОК**. Опционально придумайте введите пароль для контейнера. В примерах ниже пароль не задаётся. Нажмите **ОК**:



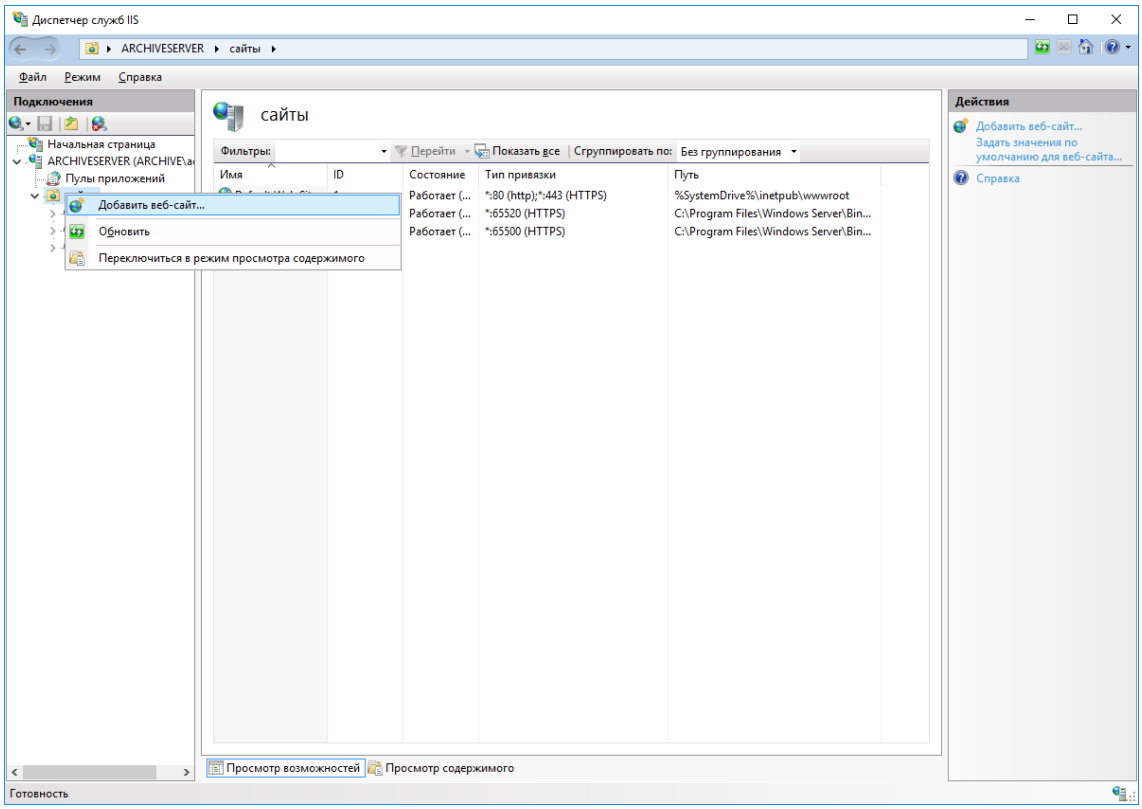
Сертификат появится среди добавленных:



Добавление серверного сертификата завершено.

3.5.1.2 Добавление приложения IIS

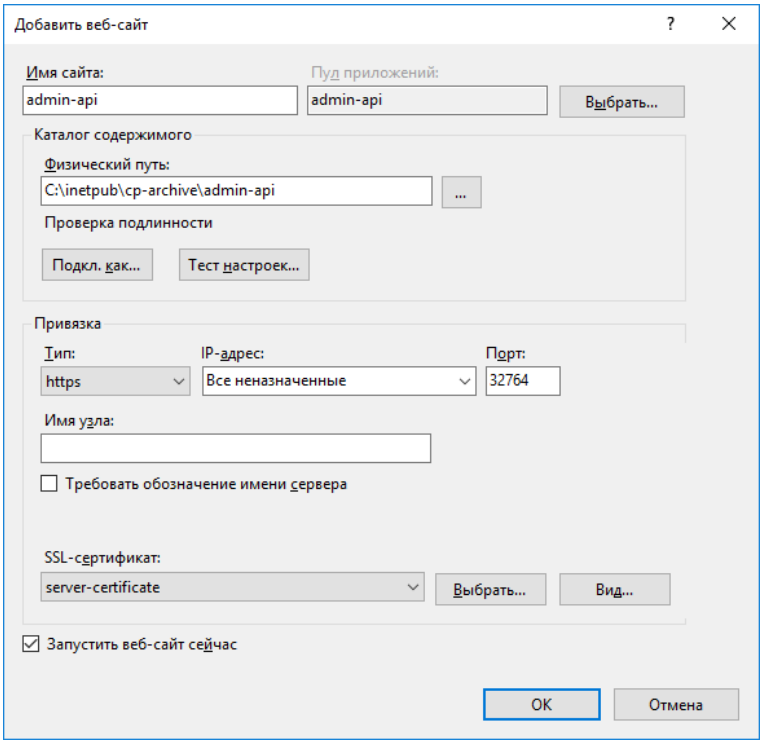
Служба admin-api (client-api) работает через IIS. Для добавления admin-api (client-api) как приложения IIS правой кнопкой мыши нажмите **сайты**, затем **Добавить веб-сайт…**:



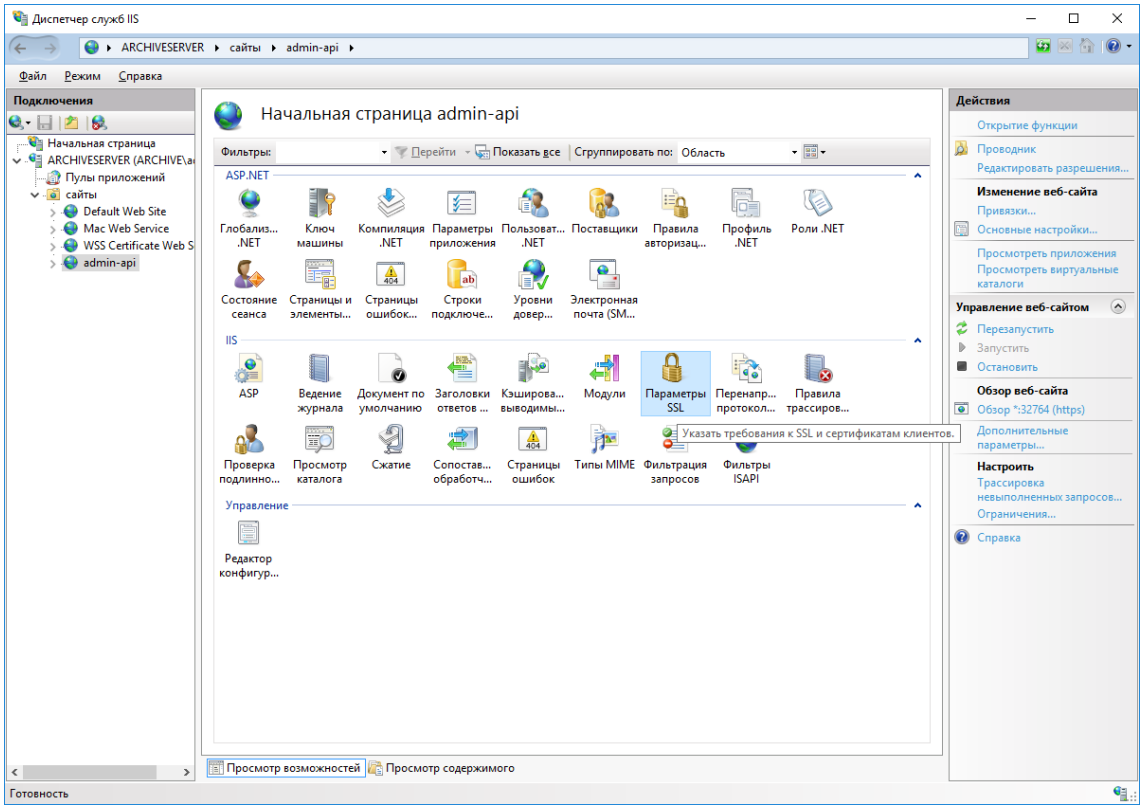
Параметры, которые необходимо заполнить, приведены в таблице ниже.

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`).

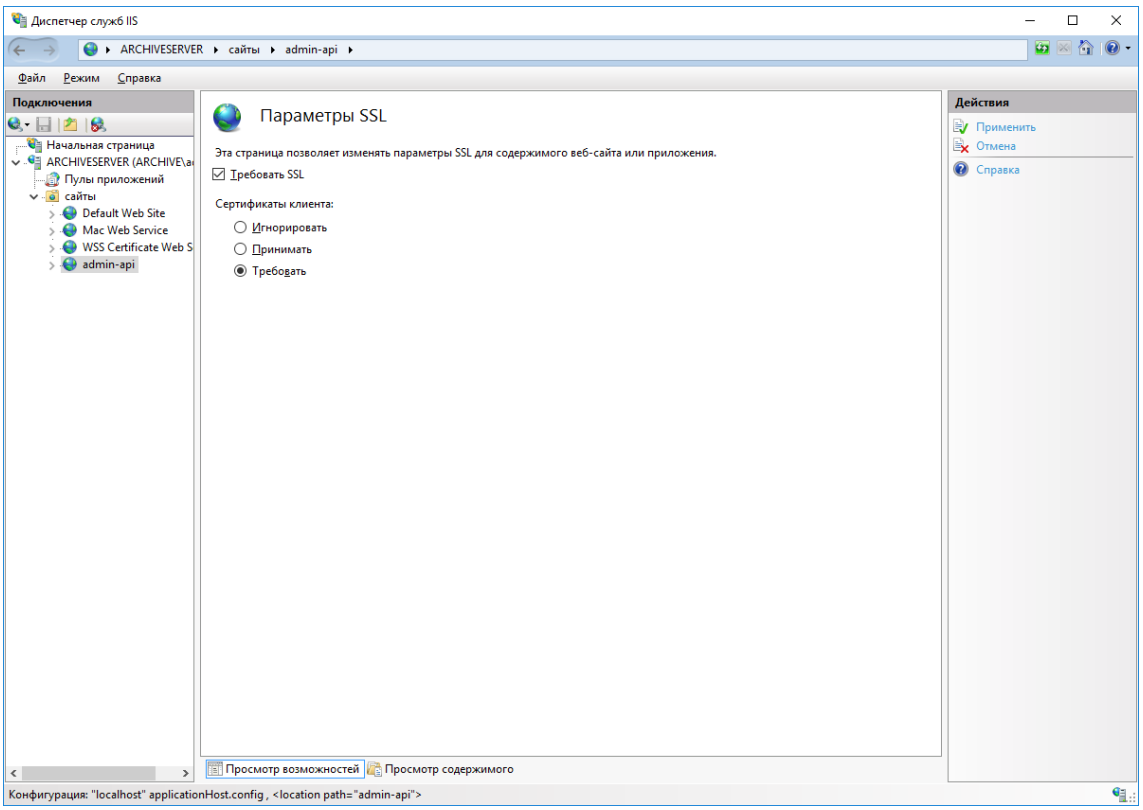
Пример заполнения страницы:



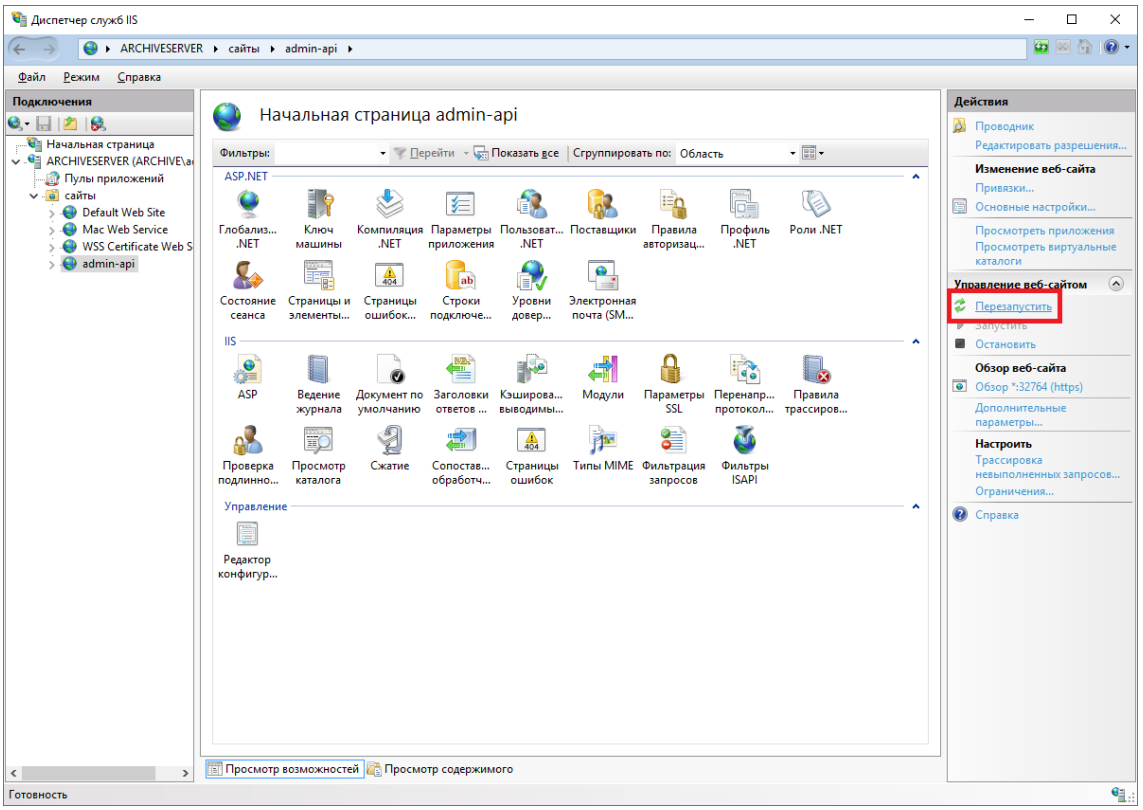
Нажмите **ОК**. Откройте в IIS страницу созданного приложения и дважды нажмите **Параметры SSL**:



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.

3.5.1.3 Настройка строки подключения

Сперва убедитесь, что установлена правильная строка подключения. Для проверки текущей строки подключения выполните в PowerShell от лица администратора

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

Пример вывода:

```
admin-api: <connection_string>
client-api: <connection_string>
consumer: <connection_string>
signature-updater: <connection_string>
```

Здесь указаны строки подключения, заданные для каждого компонента. Если строка подключения задана неверно, укажите используемую СУБД и задайте строку подключения явно с помощью команд

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

C:\inetpub\cp-archive\config\Archive.Config set `
    --connection-string "<connection_string>"
```

Где `<database_provider>` — `PostgreSql` или `Oracle`, `<connection_string>` — строка подключения к созданной и настроенной для КриптоПро Архив базе данных. Инструкции по настройке базы данных приведены в разделах 3.3.1 Настройка PostgreSQL на ОС семейства Windows Server и 3.4.1 Настройка Oracle Database на ОС семейства Windows Server.

3.5.1.4 Настройка RabbitMQ

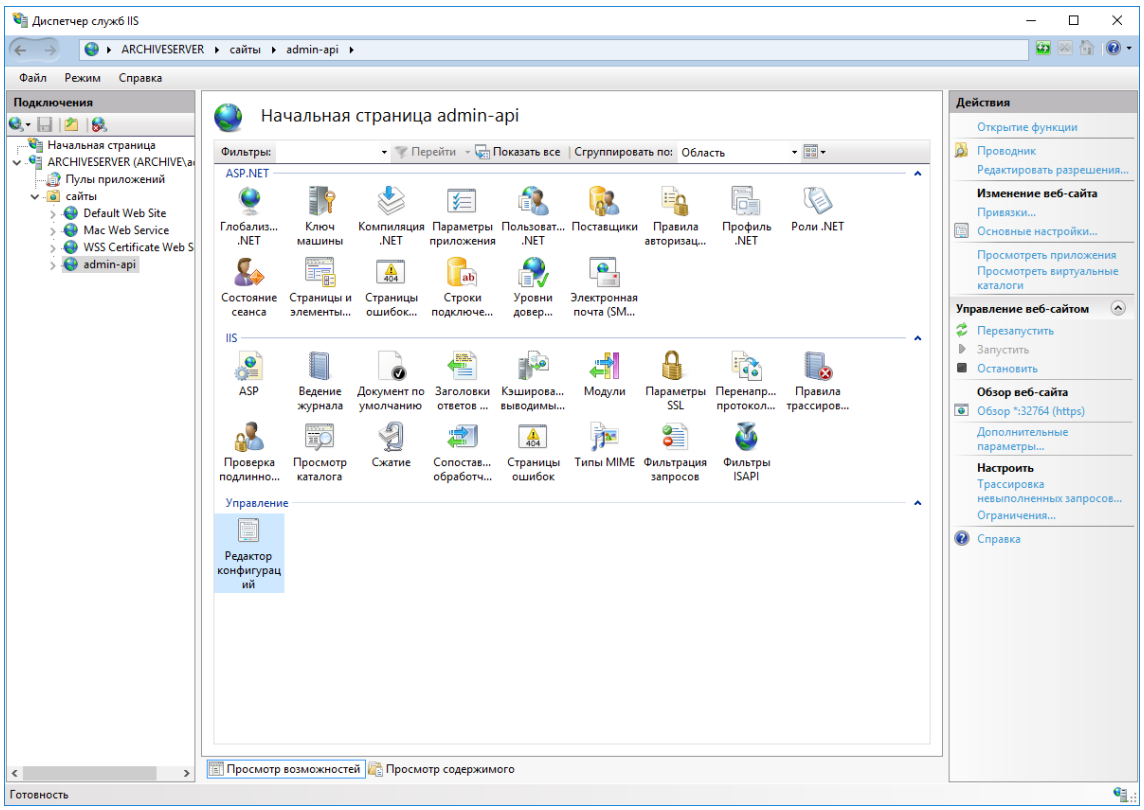
Текстовым редактором откройте конфигурационный файл `C:\inetpub\cp-archive\admin-api\appsettings.json` (для client-api: `C:\inetpub\cp-archive\client-api\appsettings.json`). Для настройки подключения к RabbitMQ измените параметры секции `$.RabbitMq`. Ниже приведены описания

параметров. При стандартной установке достаточно изменить поля `$.RabbitMq.Username` и `$.RabbitMq.Password`.

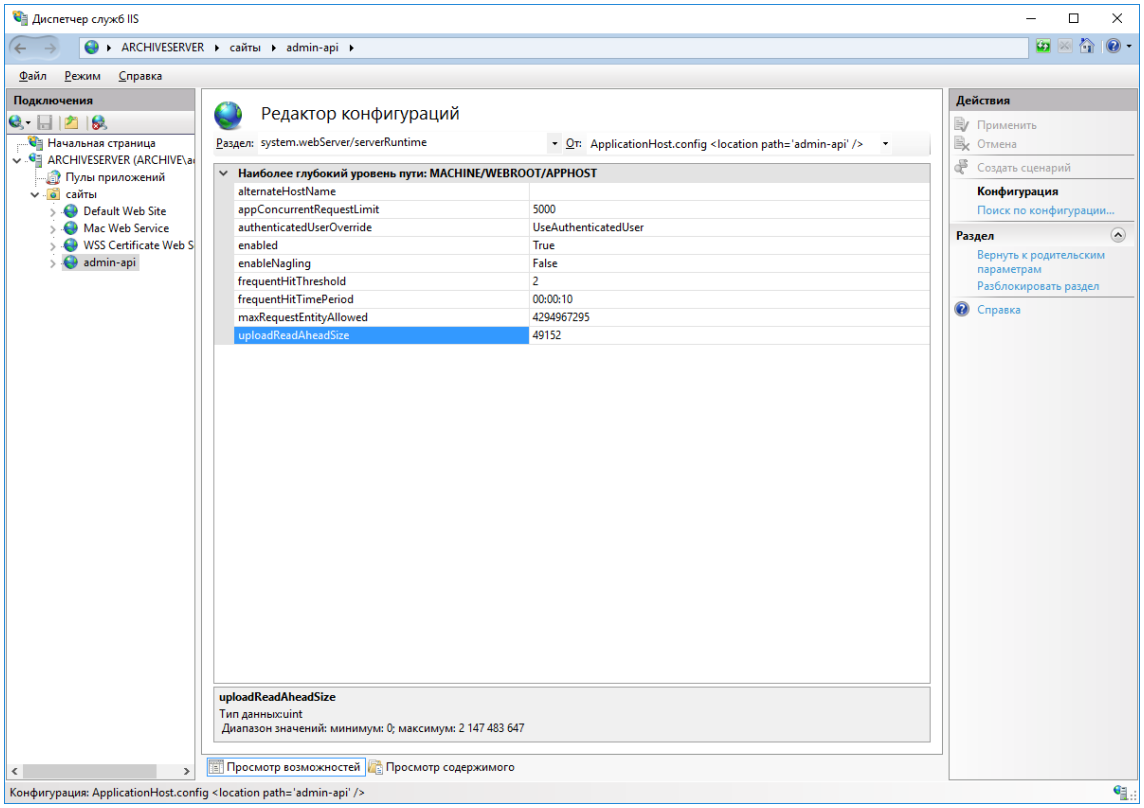
Имя параметра	Описание
`$.RabbitMq.Username`	Имя пользователя RabbitMQ. Значение по умолчанию: `"cryptopro_app"`
`$.RabbitMq.Password`	Пароль пользователя RabbitMQ. Значение по умолчанию: `"cryptopro"`
`$.RabbitMq.VirtualHost`	Имя виртуального хоста. Значение по умолчанию: `"archive"`
`$.RabbitMq.HostName`	Имя/адрес сервера, на котором расположен RabbitMQ. Значение по умолчанию: `"localhost"`
`$.RabbitMq.ApiAddress`	Адрес API панели администратора RabbitMQ из плагина `rabbitmq_management`. Значение по умолчанию: `"http://localhost:15672"`

3.5.1.6 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**:



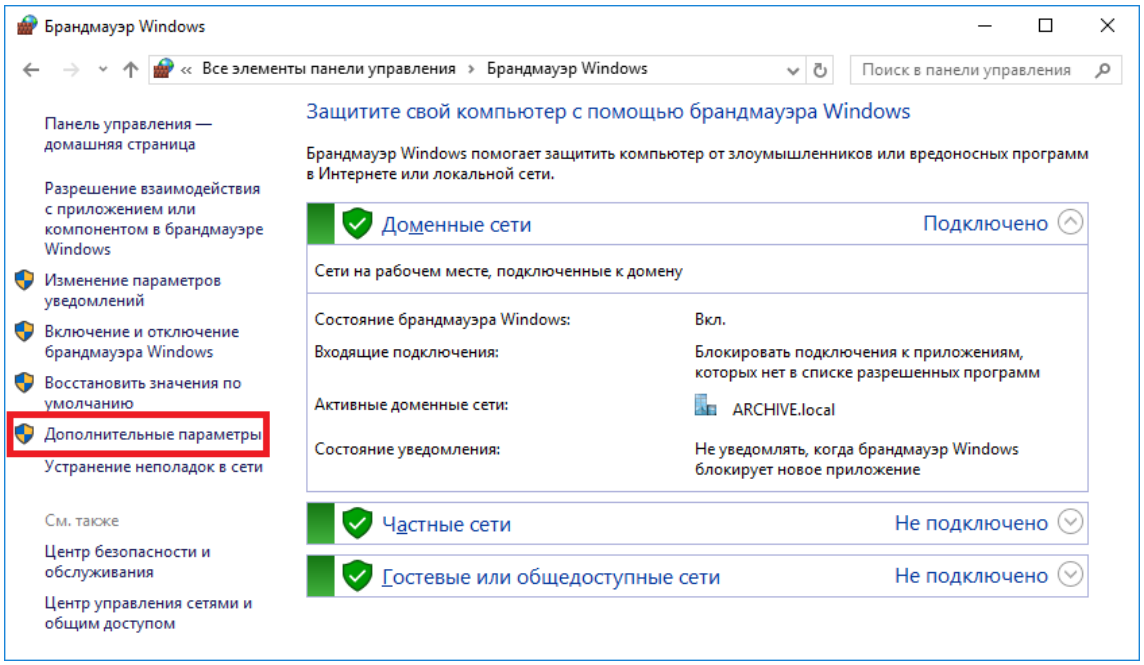
В поле **Раздел** введите `system.webServer/serverRuntime` и нажмите **Enter**:



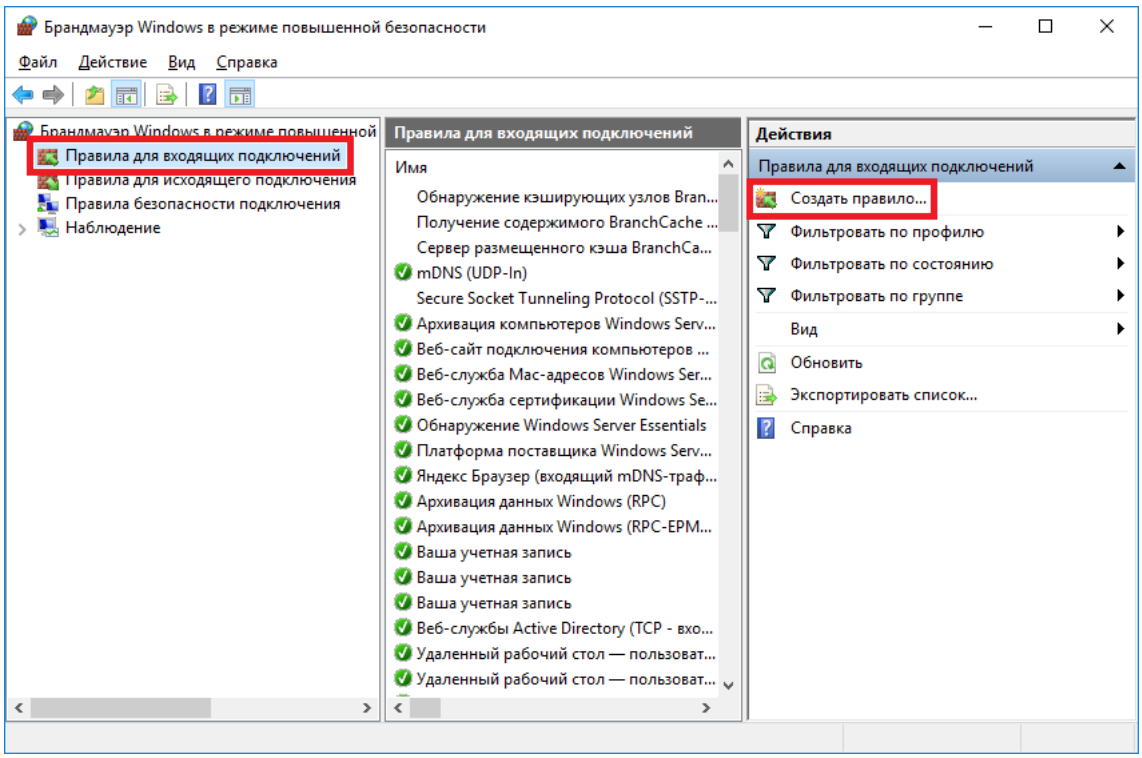
Необходимо изменить значение поля `uploadReadAheadSize` на требуемое значение. В этом поле указывается количество Байт, определяющее размер буфера для чтения пользовательского запроса. Максимальное значение: 2147483647. Более подробно с этим и другими параметрами можно ознакомиться в официальной онлайн-документации.

3.5.1.7 Настройка брандмауэра Windows

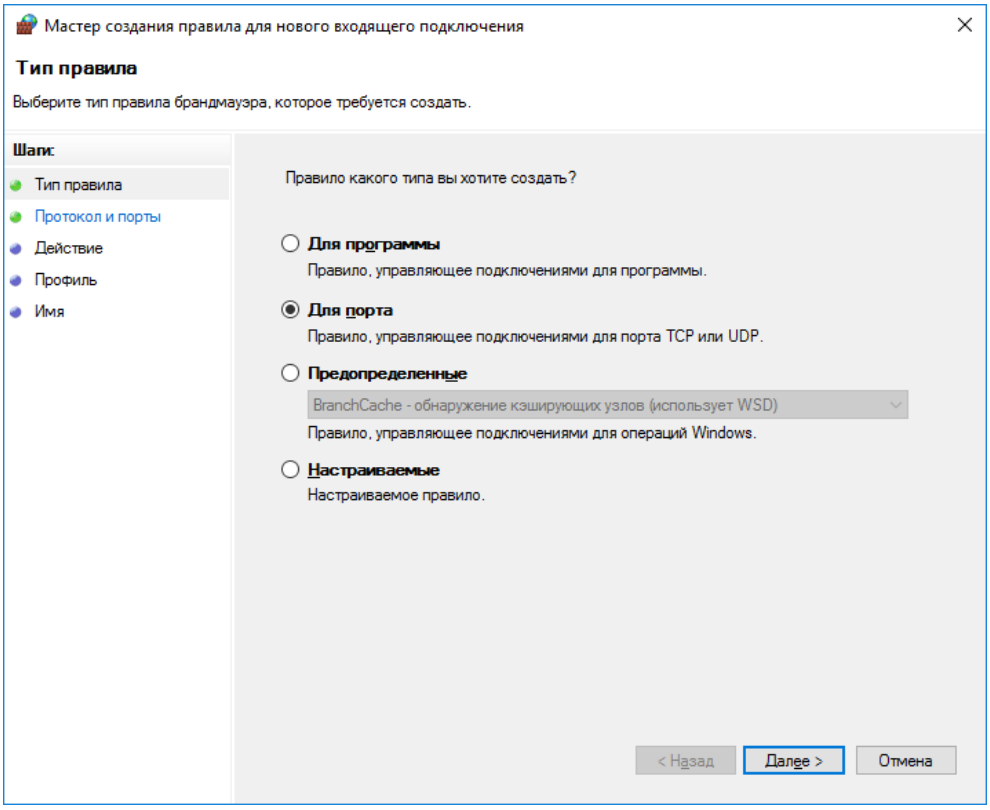
Для того, чтобы открыть порты служю admin-api и client-api, запустите программу **Брандмауэр Windows** и выберите **Дополнительные параметры** слева:



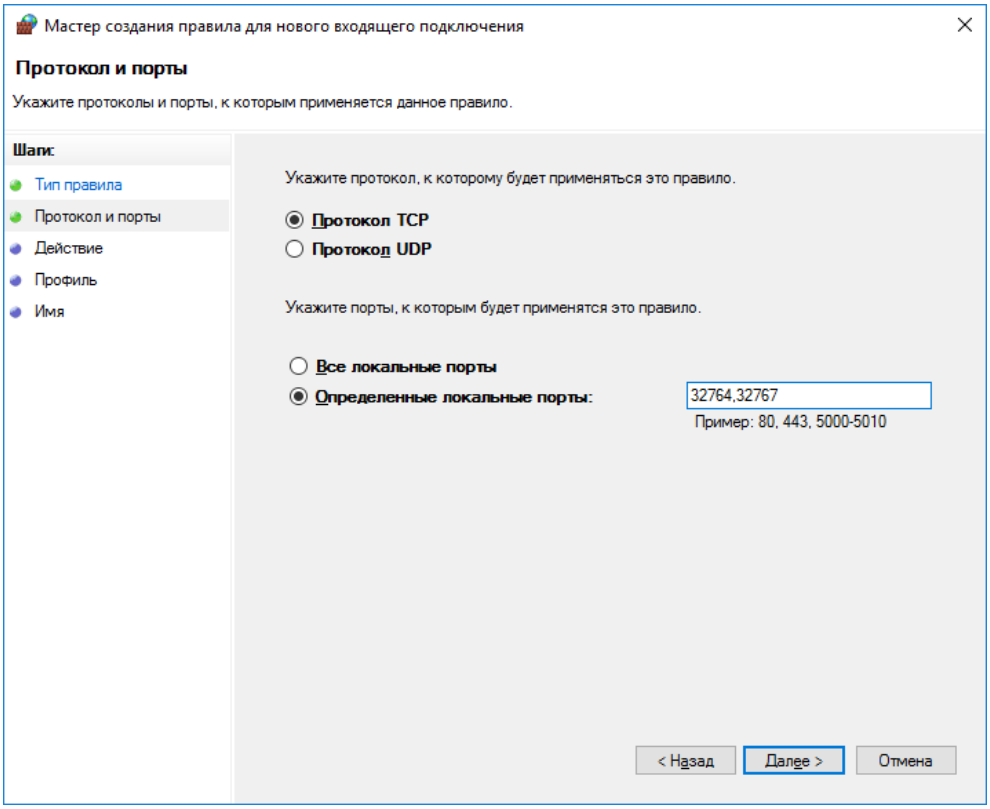
Выберите вкладку **Правила для входящих подключений** слева и нажмите **Создать правило…** справа:



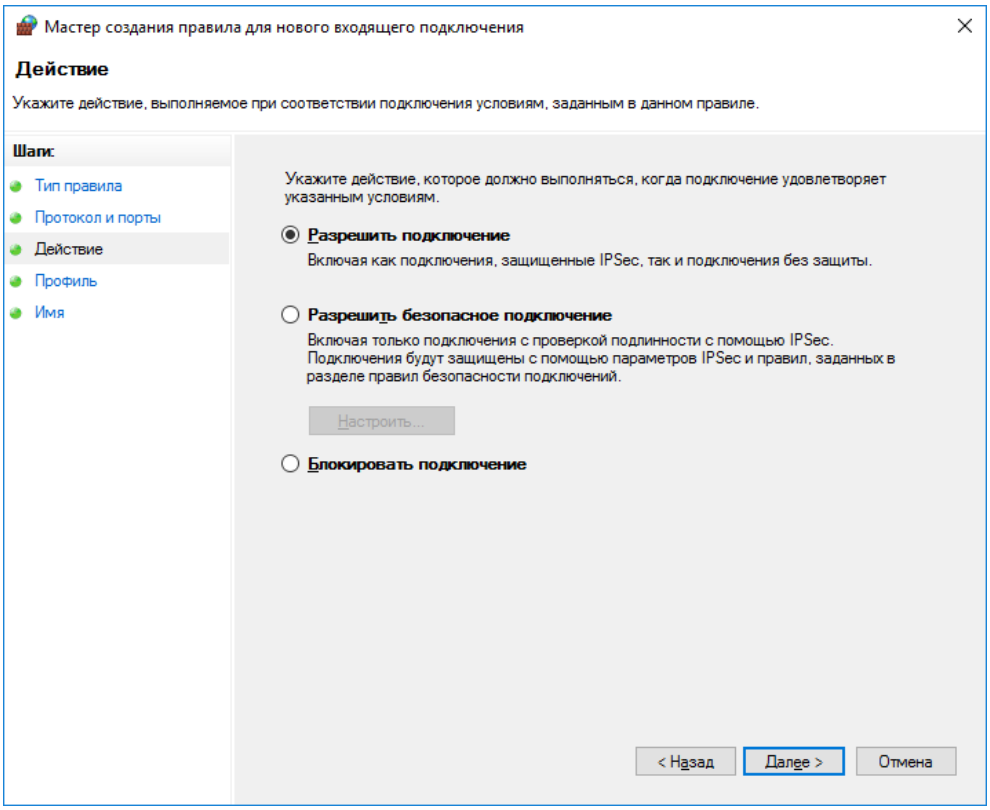
В появившемся окне отметьте пункт **Для порта** и нажмите **Далее**:



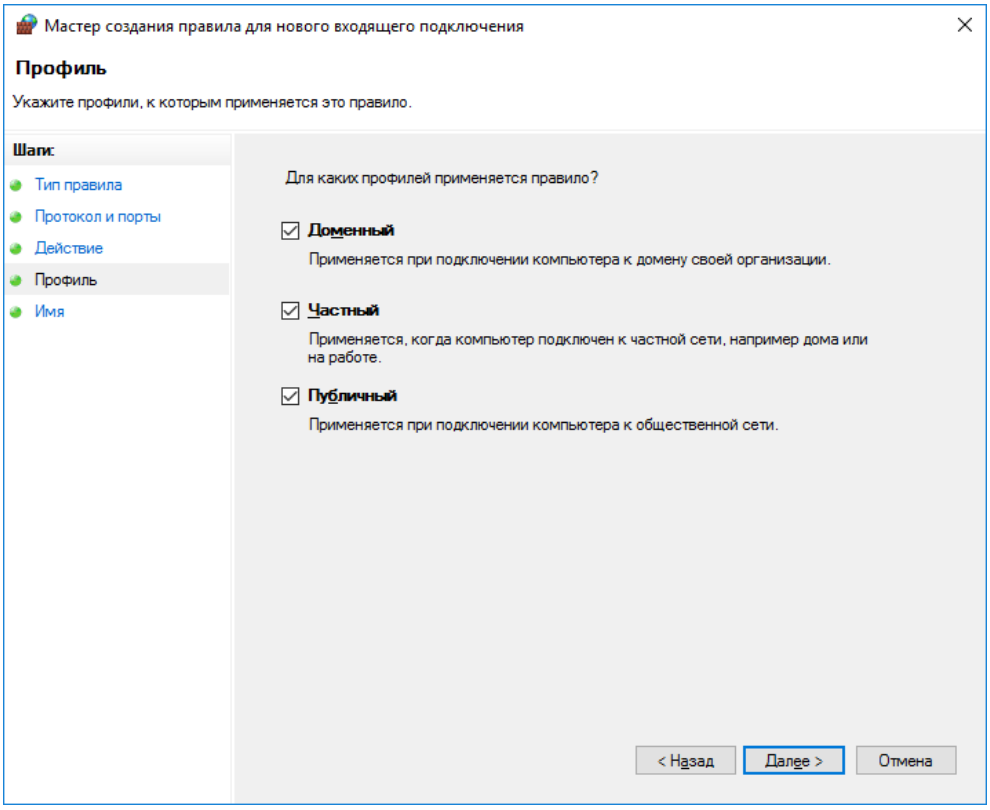
Выберите пункты **Протокол TCP**, **Определенные локальные порты** и укажите значение 32764,32767 и нажмите **Далее**:



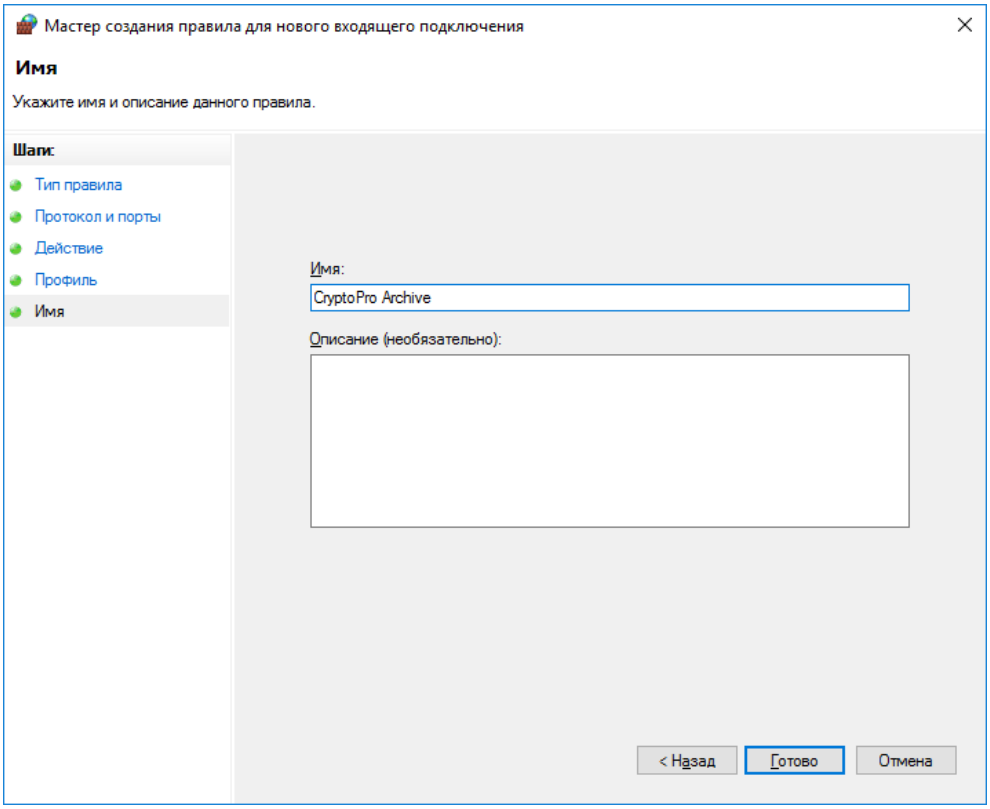
Выберите пункт **Разрешать подключение** и нажмите **Далее**:



Отметьте все пункты и нажмите **Далее**:



Введите имя правила (в примере ниже `CryptoPro Archive`) и нажмите **Готово**:



Настройка правила **Брандмауэра Windows** завершена.

3.5.1.8 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.

3.5.2 Настройка admin-api и client-api на ОС семейства Linux

Предполагается, что на сервере, помимо указанных выше, установлена программа ГОСТ NGINX (cpnginx). 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.

3.5.2.1 Добавление серверного сертификата

Сперва необходимо добавить сертификат проверки подлинности сервера в ГОСТ NGINX. Если он уже был добавлен, повторно этого делать не нужно — используйте добавленный. Для добавления сертификата выполните команду

```
sudo -u cpnginx /opt/cprocsp/bin/amd64/certmgr \
    -install \
    -file server-certificate.pfx \
    -pfx \
    -pin <pfx_pin> \
    -store umy
```

При добавлении сертификата будет предложено установить пароль на создаваемый контейнер. Задание пароля можно пропустить, оставив поле пустым и нажав **Enter**. В данном примере пароль не задаётся.

После успешного добавления сертификата будет выведена информация о нём и строка `[ErrorCode: 0x00000000]` в конце.

Установить также корневой и промежуточные сертификаты для сертификата проверки подлинности сервера. Для установки корневого сертификата (в примере ниже — `root.cer`) выполнить:

```
sudo -u cpnginx /opt/cprocsp/bin/amd64/certmgr \
    -install \
    -file root.cer \
    -store uroot
```

Для установки промежуточного сертификата (в примере ниже — `sub.cer`) выполнить:

```
sudo -u cpnginx /opt/cprocsp/bin/amd64/certmgr \
    -install \
    -file sub.cer \
    -store uca
```

3.5.2.2 Настройка ГОСТ NGINX

Откройте текстовым редактором конфигурационный файл cpnginx: `/etc/opt/cprocsp/cpnginx/cpnginx.conf`. В секции `http` добавьте следующую строку, если она там отсутствует:

```
include /etc/opt/cp-archive/nginx.conf.d/*.conf;
```

Скопируйте серийный номер сертификата проверки подлинности сервера. Для этого выполните следующую команду, найдите добавленный сертификат и скопируйте значение поля `Серийный номер`:

```
sudo -u cpnginx /opt/cprocsp/bin/amd64/certmgr \
    -list \
    -store umy
```

Текстовым редактором откройте файл конфигурационный файл NGINX для admin-api: `/etc/opt/cp-archive/nginx.conf.d/cp-archive_admin-api.conf` (для client-api: `/etc/opt/cp-archive/nginx.conf.d/cp-archive_client-api.conf`). В секции `server` замените значение поля `sspi_certificate` на скопированный серийный номер сертификата. Список параметров, которые также можно изменить, приведён ниже. За дополнительной информацией обратитесь к документации по настройке ГОСТ NGINX.

Имя параметра	Описание
`listen`	Адрес службы. Должен быть доступен при использовании межсетевого экрана. По умолчанию рекомендуется значение `32764` для admin-api и `32767` для client-api без указания адреса или с указанием `0.0.0.0`. Подробнее о параметре
`server_name`	Доменное имя сервера. В простых сценариях рекомендуется оставить значение `_`. С помощью этого параметра NGINX определяет, какая секция `server` будет обрабатывать запрос в случае совпадения у разных секций `server` параметра `listen`. Подробнее о том, за что отвечает параметр `server_name`, а также как NGINX обрабатывает запросы, можно узнать из официальной документации. Подробнее о параметре
`sspi_certificate`	Серийный номер сертификата проверки подлинности сервера. Подробнее о параметре
`proxy_pass`	Адрес внутреннего сервера Kestrel, на котором работает служба admin-api. Для большинства сценариев достаточно оставить значение по умолчанию: `http://localhost:5000` (для client-api: `http://localhost:5001`). Подробнее о параметре

Перезапустите NGINX:

```
sudo systemctl restart cpnginx.service
```

При возникновении ошибок после перезапуска убедитесь, что конфигурационный файл имеет правильный формат. Частая ошибка: отсутствие точки с запятой в конце строки. После исправления ошибок перезапустите службу.

3.5.2.3 Настройка строки подключения

Сперва убедитесь, что установлена правильная строка подключения. Для проверки текущей строки подключения выполните

```
sudo /opt/cp-archive/config/Archive.Config get --connection-string
```

Пример вывода:

```
admin-api: <connection_string>
client-api: <connection_string>
consumer: <connection_string>
signature-updater: <connection_string>
```

Здесь указаны строки подключения, заданные для каждого компонента. Если строка подключения задана неверно, укажите используемую СУБД и задайте строку подключения явно с помощью команд

```
sudo /opt/cp-archive/config/Archive.Config set \
    --database-provider <database_provider>

sudo /opt/cp-archive/config/Archive.Config set \
    --connection-string "<connection_string>"
```

Где `<database_provider>` — `PostgreSql` или `Oracle`, `<connection_string>` — строка подключения к созданной и настроенной для КриптоПро Архив базе данных. Инструкции по настройке базы данных приведены в разделах 3.3.2 Настройка PostgreSQL на Astra Linux 1.7 и 3.4.2 Настройка Oracle Database на ОС семейства Linux.

3.5.2.4 Настройка RabbitMQ

Текстовым редактором откройте конфигурационный файл `/etc/opt/cp-archive/admin-api/appsettings.json` (для client-api: `/etc/opt/cp-archive/client-api/appsettings.json`). Для настройки подключения к RabbitMQ измените параметры секции `$.RabbitMq`. Ниже приведены описания параметров. При стандартной установке достаточно изменить поля `$.RabbitMq.Username` и `$.RabbitMq.Password`.

Имя параметра	Описание

`$.RabbitMq.Username`	Имя пользователя RabbitMQ. Значение по умолчанию: `"cryptopro_app"`
`$.RabbitMq.Password`	Пароль пользователя RabbitMQ. Значение по умолчанию: `"cryptopro"`
`$.RabbitMq.VirtualHost`	Имя виртуального хоста. Значение по умолчанию: `"archive"`
`$.RabbitMq.HostName`	Имя/адрес сервера, на котором расположен RabbitMQ. Значение по умолчанию: `"localhost"`
`$.RabbitMq.ApiAddress`	Адрес API панели администратора RabbitMQ из плагина `rabbitmq_management`. Значение по умолчанию: `"http://localhost:15672"`

3.5.2.6 Настройка максимального размера запроса

Так как NGINX выступает в роли обратного прокси, для изменения максимального допустимого размера запроса необходимо отредактировать конфигурации NGINX и Kestrel, на котором работают службы admin-api и client-api.

Для настройки максимального размера тела запроса в NGINX текстовым редактором откройте файл конфигурационный файл NGINX для admin-api: `/etc/opt/cp-archive/nginx.conf.d/cp-archive_admin-api.conf` (для client-api: `/etc/opt/cp-archive/nginx.conf.d/cp-archive_client-api.conf`). Измените параметр `client_max_body_size`, который указывает максимальный размер тела запроса в мегабайтах. Например,

```
client_max_body_size 500M;
```

Более подробное описание параметра можно найти в официальной документации.

Для изменения максимального размера запроса Kestrel текстовым редактором откройте конфигурационный файл `/etc/opt/cp-archive/admin-api/appsettings.json` (для client-api: `/etc/opt/cp-archive/client-api/appsettings.json`). Добавьте параметр

`$.Kestrel.Limits.MaxRequestBodySize` с указанием максимального размера тела запроса в байтах. Например, `100000000`.

Так как контейнеры загружаются в систему с типом `multipart/form-data`, необходимо также изменить максимальный допустимый размер тела запроса с таким типом. Для этого в том же конфигурационном файле добавьте параметр `$.FormOptions.MultipartBodyLengthLimit`, значение которого указывает размер запроса с типом `multipart/form-data` в байтах. Например, `100000000`.

3.5.2.7 Настройка службы systemd

Программы admin-api и client-api работают в качестве служб systemd. Для обеспечения автоматического запуска служб выполнить

```
sudo systemctl enable cp-archive_admin-api.service
sudo systemctl enable cp-archive_client-api.service
```

Для запуска служб выполнить

```
sudo systemctl start cp-archive_admin-api.service
sudo systemctl start cp-archive_client-api.service
```

3.5.2.8 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`):

```
sudo /opt/cp-archive/config/Archive.Config set \
    --superuser \
    --thumbprint <thumbprint> \
    --database-provider <provider>
```

После успешного выполнения на экран будет выведено сообщение `Значение успешно изменено`.

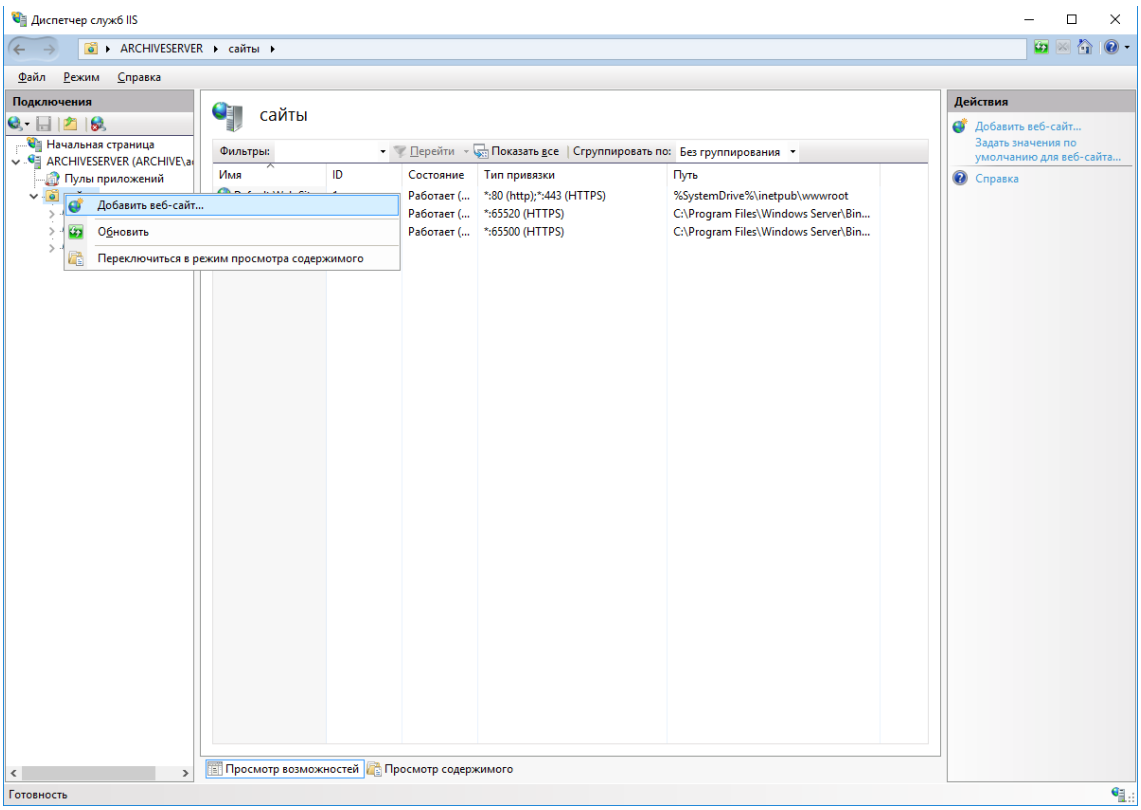
3.6 Настройка frontend

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

Для настройки frontend необходим КриптоПро 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.

3.6.1 Настройка frontend на ОС семейства Windows Server

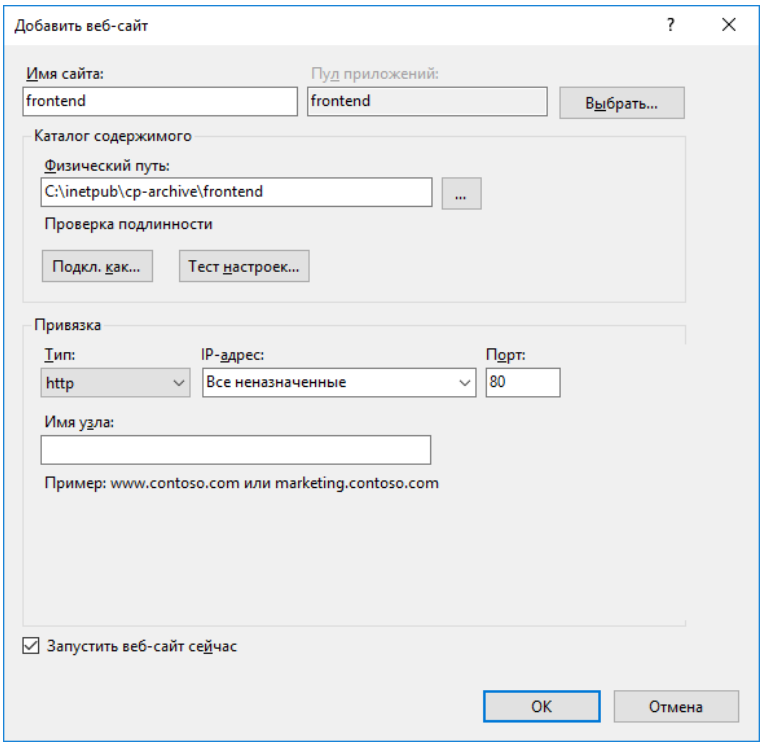
На ОС семейства Windows Server компонент frontend работает в качестве приложения IIS. Для добавления приложения откройте IIS, правой кнопкой нажмите **сайты**, затем **Добавить веб-сайт…**:



Параметры, которые необходимо заполнить, приведены в таблице ниже.

Имя параметра	Значение
Имя сайта	frontend
Физический путь	`C:\inetpub\cp-archive\frontend`
Привязка: Тип	http
Привязка: Порт	`80`

Пример заполнения страницы:



Нажать **ОК**. Настройка приложения IIS завершена.

Откройте текстовым редактором конфигурационный файл компонента frontend: `C:\inetpub\cp-archive\frontend\custom-config.json`. В поле `$.baseURL` введите адрес admin-api таким, каким он виден для других систем. Например, если обращение к admin-api с рабочего места администратора происходит по адресу `https://api.servername.ru:32764/api`, именно этот адрес и необходимо ввести в конфигурационном файле несмотря на то, что службы frontend и admin-api могут работать на одном сервере.

В некоторых случаях может быть желательно изменить частоту опроса API для обновления статусов контейнеров на текущей открытой странице. Для этого предназначен параметр `$.statusUpdateIntervalSec`, указывающий интервал опроса API в секундах. Для отключения автоматического опроса установите значение `0`.

Перечень всех параметров приведён в таблице ниже. После изменения настроек перезапустите приложение frontend в IIS.

Имя параметра	Описание
`$.baseURL`	Внешний адрес службы admin-api
`$.statusUpdateIntervalSec`	Интервал опроса API для автоматического обновления статуса отображаемых контейнеров. Для отключения автоматического опроса API установите значение `0`. Значение по умолчанию: `10`
`$.footerText`	Текст внизу административной панели

3.6.2 Настройка frontend на ОС семейства Linux

Предполагается, что на сервере, помимо указанных выше, установлена программа ГОСТ NGINX (cpnginx).

Откройте текстовым редактором конфигурационный файл cpnginx: `/etc/opt/cprocsp/cpnginx/cpnginx.conf`. В секции `http` добавьте следующую строку, если она там отсутствует:

```
include /etc/opt/cp-archive/nginx.conf.d/*.conf;
```

Сервер cpnginx содержит настроенную по умолчанию страницу на порте 80. Чтобы не возникало конфликта с этой страницей и веб-интерфейсом КриптоПро Архив, можно либо сменить порт стандартной страницы, например, на `8080`, либо установить порт веб-интерфейса КриптоПро Архив на другой порт, например `8080`. Для изменения порта страницы NGINX по умолчанию откройте конфигурационный файл `/etc/opt/cprocsp/cpnginx/conf.d/default.conf` и

измените значение параметра `listen` на `8080`, после чего перезапустите cpnginx.

Для изменения параметров сервера отредактируйте конфигурационный файл `/etc/opt/cp-archive/nginx.conf.d/cp-archive_frontend.conf`, содержащий конфигурацию NGINX для frontend. Ниже указаны параметры, которые в некоторых специальных сценариях может быть желательно изменить.

Имя параметра	Описание
`listen`	Адрес службы. Должен быть доступен при использовании межсетевого экрана. По умолчанию рекомендуется значение `80` без указания адреса или с указанием `0.0.0.0`. Подробнее о параметре
`server_name`	Доменное имя сервера. В простых сценариях рекомендуется оставить значение `_`. С помощью этого параметра NGINX определяет, какая секция `server` будет обрабатывать запрос в случае совпадения у разных секций `server` параметра `listen`. Подробнее о том, за что отвечает параметр `server_name`, а также как NGINX обрабатывает запросы, можно узнать из официальной документации. Подробнее о параметре

Откройте текстовым редактором конфигурационный файл компонента frontend: `/etc/opt/cp-archive/frontend/custom-config.json`. В поле `$.baseURL` введите адрес admin-api таким, каким он виден для других систем. Например, если обращение к admin-api с рабочего места администратора происходит по адресу `https://api.servername.ru:32764/api`, именно этот адрес и необходимо ввести в конфигурационном файле несмотря на то, что службы frontend и admin-api могут работать на одном сервере.

В некоторых случаях может быть желательно изменить частоту опроса API для обновления статусов контейнеров на текущей открытой странице. Для этого предназначен параметр `$.statusUpdateIntervalSec`, указывающий интервал опроса API в секундах. Для отключения автоматического опроса установите значение `0`.

Перечень всех параметров приведён в таблице ниже. После изменения настроек перезапустите NGINX:

```
sudo systemctl restart cpnginx.service
```

Имя параметра	Описание
`$.baseURL`	Внешний адрес службы admin-api
`$.statusUpdateIntervalSec`	Интервал опроса API для автоматического обновления статуса отображаемых контейнеров. Для отключения автоматического опроса API установите значение `0`. Значение по умолчанию: `10`
`$.footerText`	Текст внизу административной панели

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.

3.7.1 Настройка signature-updater на ОС семейства Windows Server

На ОС семейства Windows Server программа signature-updater работает как служба Windows. Ниже приведены инструкции по настройке службы и параметров усовершенствования подписей.

3.7.1.1 Настройка строки подключения

Сперва убедитесь, что установлена правильная строка подключения. Для проверки текущей строки подключения выполните в PowerShell от лица администратора

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

Пример вывода:

```
admin-api: <connection_string>
client-api: <connection_string>
consumer: <connection_string>
signature-updater: <connection_string>
```

Здесь указаны строки подключения, заданные для каждого компонента. Обратите внимание на строку, начинающуюся с `signature-updater`. Если строка подключения задана неверно, укажите используемую СУБД и задайте строку подключения явно с помощью команд

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

C:\inetpub\cp-archive\config\Archive.Config set `
    --connection-string "<connection_string>"
```

Где <database_provider> — PostgreSql или Oracle, <connection_string> — строка подключения к созданной и настроенной для КриптоПро Архив базе данных. Инструкции по настройке базы данных приведены в разделах 3.3.1 Настройка PostgreSQL на ОС семейства Windows Server и 3.4.1 Настройка Oracle Database на ОС семейства Windows Server.

3.7.1.2 Настройка адреса службы TSP

Текстовым редактором откройте конфигурационный файл C:\inetpub\cp-archive\signature-updater\appsettings.json. Укажите адрес службы TSP, используемой для получения архивных штампов времени с помощью параметра $.Enchancer.TSPAddress. Пример значения параметра: "http://localhost/tsp/tsp.srf".

3.7.1.3 Настройка службы Windows

Для запуска приложения как службы Windows выполните в PowerShell от лица администратора следующую команду:

```
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.

3.7.1.4 Использование стандартного адреса службы OCSP

При отсутствии адреса OCSP в сертификате подписанта проверяемой подписи возможно использование стандартного адреса OCSP, указанного с помощью политики DefaultOCSPURL клиента OCSP. Для этого текстовым редактором откройте конфигурационный файл C:\inetpub\cp-archive\signature-updater\appsettings.json и установите параметр $.Enchancer.CadesUseOcspAuthorizedPolicy в значение true (без кавычек).

3.7.1.5 Изменение статуса контейнера при возникновении ошибки

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, в конфигурационном файле `C:\inetpub\cp-archive\signature-updater\appsettings.json` существует параметр `$.Enchancer.ErrorCodes`, значение которого — список с hex-строками, представляющими собой значения ошибок. Пример заполнения поля (значения ошибок в примере приведены только для иллюстрации формата):

```
{
  "Enchancer": {
    "ErrorCodes": [
      "0x800b0101",
      "0x800b0102"
    ]
  }
}
```

3.7.1.7 Настройка производительности

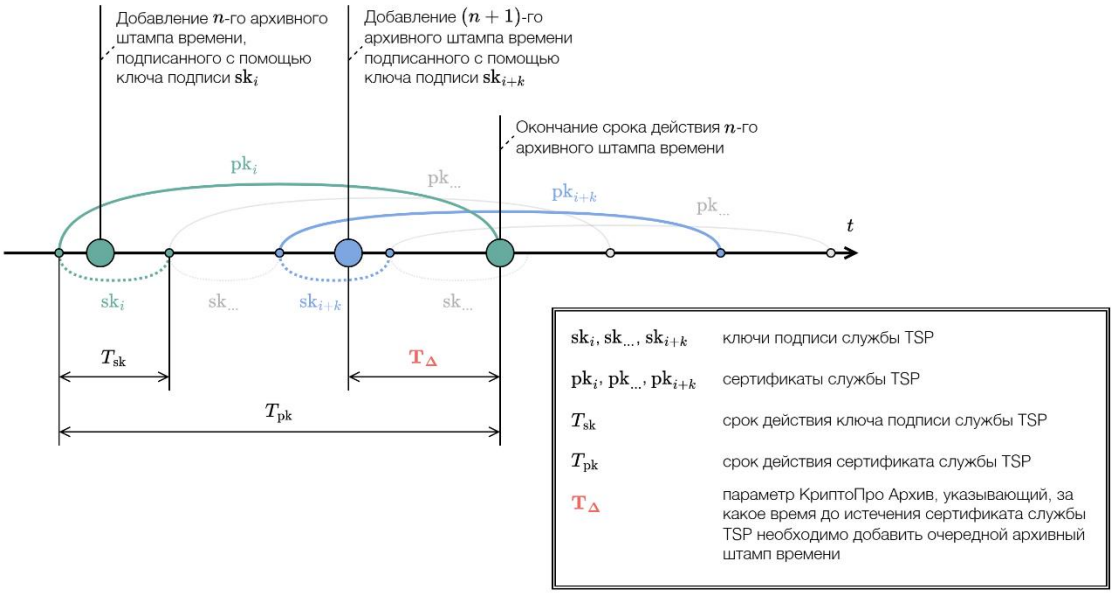
Настройки, приведённые ниже, используются для установки параметров производительности программы signature-updater, таких как количество потоков, используемых для обработки контейнеров, время ожидания потоков и количество резервируемых каждым потоком контейнеров для последовательной обработки.

Название параметра	Описание параметра
`$.Enchancer .NumberOfThreadsForExistingDocuments`	Число потоков, используемых для усовершенствования подписи документов. Значение по умолчанию: `2`
`$.Enchancer .NumberOfExistingDocuments`	Число документов, запрашиваемых одним потоком для последовательного улучшения. Значение по умолчанию: `50`
`$.Enchancer .NumberOfSecondsToWaitExistingThread`	Время в секундах, которое каждый поток будет ждать до следующей

	проверки по истечению доступных в базе данных документов для улучшения. Значение по умолчанию: 5
$.Enchancer .NumberOfThreadsForIncomingDocuments	Число потоков, используемых для усовершенствования подписи документов. Значение по умолчанию: 2
$.Enchancer .NumberOfIncomingDocuments	Число документов, запрашиваемых одним потоком для последовательного улучшения. Значение по умолчанию: 50
$.Enchancer .NumberOfSecondsToWaitIncomingThread	Время в секундах, которое каждый поток будет ждать до следующей проверки по истечению доступных в базе данных документов для улучшения. Значение по умолчанию: 5
$.Enchancer .NumberOfArchiveExpirationDocuments	Количество документов, одновременно помечаемых подлежащими обновлению, если они такими являются. Значение по умолчанию: 1000
$.Enchancer .NumberOfSecondsToWaitExpirationCheck	Время в секундах, которое поток ждёт между запросами на выставление подлежащим обновлению документам соответствующего статуса. Значение по умолчанию: 1
$.Enchancer .NumberOfDaysBeforeExpirationDate	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. Значение по умолчанию: 90 *

* **ВАЖНО**: если сертификат службы штампов времени действует дольше 1 года 3 месяцев, рекомендуется установить значение параметра `$.Enchancer.NumberOfDaysBeforeExpirationDate` в `500`.

Для более подробного пояснения значения параметра `$.Enchancer.NumberOfDaysBeforeExpirationDate` обратимся к рисунку:



Параметру `$.Enchancer.NumberOfDaysBeforeExpirationDate` соответствует значение T_Δ. Если $T_\Delta > T_{\mathrm{pk}} - T_{\mathrm{sk}}$ (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**.

3.7.1.8 Настройка RabbitMQ

Текстовым редактором откройте конфигурационный файл `C:\inetpub\cp-archive\signature-updater\appsettings.json`. Для настройки подключения к RabbitMQ измените параметры секции `$.RabbitMq`. Ниже приведены описания параметров. При стандартной установке достаточно изменить поля `$.RabbitMq.Username` и `$.RabbitMq.Password`.

Имя параметра	Описание
`$.RabbitMq.Username`	Имя пользователя RabbitMQ. Значение по умолчанию: `"cryptopro_app"`
`$.RabbitMq.Password`	Пароль пользователя RabbitMQ. Значение по умолчанию: `"cryptopro"`
`$.RabbitMq.VirtualHost`	Имя виртуального хоста. Значение по умолчанию: `"archive"`
`$.RabbitMq.HostName`	Имя/адрес сервера, на котором расположен RabbitMQ. Значение по умолчанию: `"localhost"`

3.7.2 Настройка signature-updater на ОС семейства Linux

На ОС семейства Linux программа signature-updater работает как служба systemd. Ниже приведены инструкции по настройке службы и параметров усовершенствования подписей.

3.7.2.1 Настройка строки подключения

Сперва убедитесь, что установлена правильная строка подключения. Для проверки текущей строки подключения выполните в PowerShell от лица администратора

```
sudo /opt/cp-archive/config/Archive.Config get --connection-string
```

Пример вывода:

```
admin-api: <connection_string>
client-api: <connection_string>
consumer: <connection_string>
signature-updater: <connection_string>
```

Здесь указаны строки подключения, заданные для каждого компонента. Обратите внимание на строку, начинающуюся с `signature-updater`. Если строка подключения задана неверно, укажите используемую СУБД и задайте строку подключения явно с помощью команд

```
sudo /opt/cp-archive/config/Archive.Config set \
    --database-provider <database_provider>
```

```
sudo /opt/cp-archive/config/Archive.Config set \
    --connection-string "<connection_string>"
```

Где <database_provider> — PostgreSql или Oracle, <connection_string> — строка подключения к созданной и настроенной для КриптоПро Архив базе данных. Инструкции по настройке базы данных приведены в разделах 3.3.2 Настройка PostgreSQL на Astra Linux 1.7 и 3.4.2 Настройка Oracle Database на ОС семейства Linux.

3.7.2.2 Настройка адреса службы TSP

Текстовым редактором откройте конфигурационный файл /etc/opt/cp-archive/signature-updater/appsettings.json. Укажите адрес службы TSP, используемой для получения архивных штампов времени с помощью параметра $.Enchancer.TSPAddress. Пример значения параметра: "http://localhost/tsp/tsp.srf".

3.7.2.3 Настройка службы systemd

Для обеспечения автоматического запуска приложения выполните

```
sudo systemctl enable cp-archive_signature-updater.service
```

Для запуска приложения как службы выполните

```
sudo systemctl start cp-archive_signature-updater.service
```

3.7.2.4 Использование стандартного адреса службы OCSP

При отсутствии адреса OCSP в сертификате подписанта проверяемой подписи возможно использование стандартного адреса OCSP, указанного с помощью политики DefaultOCSPURL клиента OCSP. Для этого текстовым редактором откройте конфигурационный файл /etc/opt/cp-archive/signature-updater/appsettings.json и установите параметр $.Enchancer.CadesUseOcspAuthorizedPolicy в значение true (без кавычек).

3.7.2.5 Изменение статуса контейнера при возникновении ошибки

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, в конфигурационном файле `/etc/opt/cp-archive/signature-updater/appsettings.json` существует параметр `$.Enchancer.ErrorCodes`, значение которого — список с hex-строками, представляющими собой значения ошибок. Пример заполнения поля (значения ошибок в примере приведены только для иллюстрации формата):

```
{
  "Enchancer": {
    "ErrorCodes": [
      "0x800b0101",
      "0x800b0102"
    ]
  }
}
```

3.7.2.7 Настройка производительности

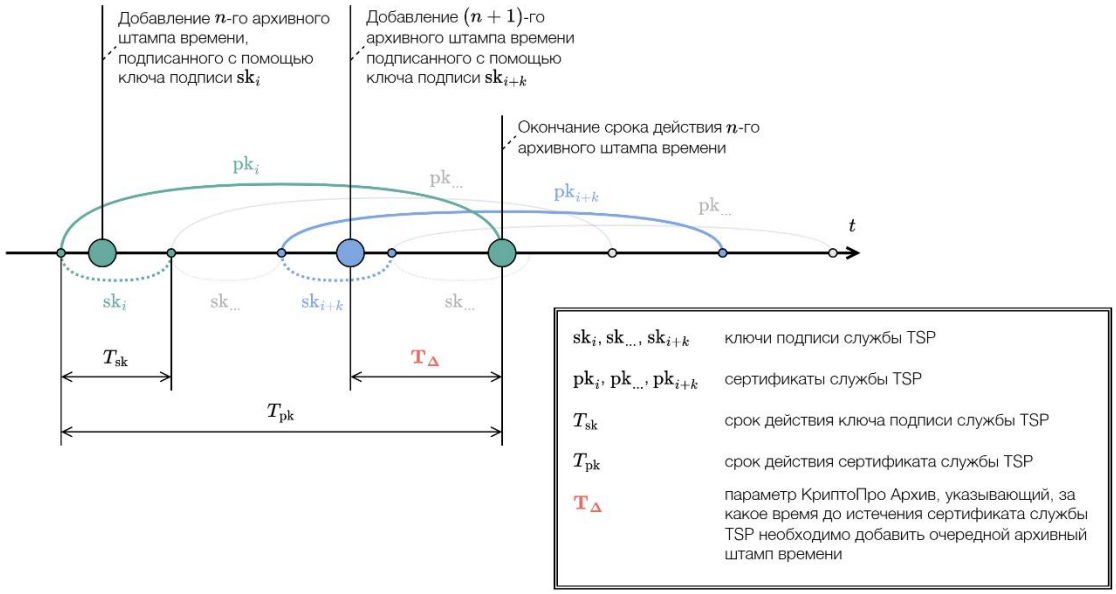
Настройки, приведённые ниже, используются для установки параметров производительности программы signature-updater, таких как количество потоков, используемых для обработки контейнеров, время ожидания потоков и количество резервируемых каждым потоком контейнеров для последовательной обработки.

Название параметра	Описание параметра
`$.Enchancer .NumberOfThreadsForExistingDocuments`	Число потоков, используемых для усовершенствования подписи документов. Значение по умолчанию: `2`
`$.Enchancer .NumberOfExistingDocuments`	Число документов, запрашиваемых одним потоком для последовательного улучшения. Значение по умолчанию: `50`
`$.Enchancer .NumberOfSecondsToWaitExistingThread`	Время в секундах, которое каждый поток будет ждать до следующей

	проверки по истечению доступных в базе данных документов для улучшения. Значение по умолчанию: 5
$.Enchancer .NumberOfThreadsForIncomingDocuments	Число потоков, используемых для усовершенствования подписи документов. Значение по умолчанию: 2
$.Enchancer .NumberOfIncomingDocuments	Число документов, запрашиваемых одним потоком для последовательного улучшения. Значение по умолчанию: 50
$.Enchancer .NumberOfSecondsToWaitIncomingThread	Время в секундах, которое каждый поток будет ждать до следующей проверки по истечению доступных в базе данных документов для улучшения. Значение по умолчанию: 5
$.Enchancer .NumberOfArchiveExpirationDocuments	Количество документов, одновременно помечаемых подлежащими обновлению, если они такими являются. Значение по умолчанию: 1000
$.Enchancer .NumberOfSecondsToWaitExpirationCheck	Время в секундах, которое поток ждёт между запросами на выставление подлежащим обновлению документам соответствующего статуса. Значение по умолчанию: 1
$.Enchancer .NumberOfDaysBeforeExpirationDate	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. Значение по умолчанию: 90 *

* **ВАЖНО**: если сертификат службы штампов времени действует дольше 1 года 3 месяцев, рекомендуется установить значение параметра `$.Enchancer.NumberOfDaysBeforeExpirationDate` в `500`.

Для более подробного пояснения значения параметра `$.Enchancer.NumberOfDaysBeforeExpirationDate` обратимся к рисунку:



Параметру `$.Enchancer.NumberOfDaysBeforeExpirationDate` соответствует значение T_Δ. Если $T_\Delta > T_{\mathrm{pk}} - T_{\mathrm{sk}}$ (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**.

3.7.2.8 Настройка RabbitMQ

Текстовым редактором откройте конфигурационный файл `/etc/opt/cp-archive/signature-updater/appsettings.json`. Для настройки подключения к RabbitMQ измените параметры секции `$.RabbitMq`. Ниже приведены описания параметров. При стандартной установке достаточно изменить поля `$.RabbitMq.Username` и `$.RabbitMq.Password`.

Имя параметра	Описание
`$.RabbitMq.Username`	Имя пользователя RabbitMQ. Значение по умолчанию: `"cryptopro_app"`
`$.RabbitMq.Password`	Пароль пользователя RabbitMQ. Значение по умолчанию: `"cryptopro"`
`$.RabbitMq.VirtualHost`	Имя виртуального хоста. Значение по умолчанию: `"archive"`
`$.RabbitMq.HostName`	Имя/адрес сервера, на котором расположен RabbitMQ. Значение по умолчанию: `"localhost"`

3.8 Настройка consumer

В данном разделе приведена настройка программы consumer. Программа представляет собой приёмник сообщений RabbitMQ. Программа поддерживает работу с тремя очередями. 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

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. В примерах ниже предполагается установка компонентов Архива по стандартным путям. Если пути не совпадают с выбранными на этапе установки, измените их на соответствующие.

3.8.1 Настройка consumer на ОС семейства Windows Server

На ОС семейства Windows Server программа consumer работает как служба Windows. Ниже приведены инструкции по настройке службы.

3.8.1.1 Настройка службы Windows

Для запуска приложения как службы Windows выполните в PowerShell от лица администратора следующую команду:

```
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.

3.8.1.2 Настройка соединений RabbitMQ

Программа позволяет настроить подключение к нескольким очередям RabbitMQ. Для этого используется секция `$.RabbitMq` конфигурационного файла `C:\inetpub\cp-archive\consumer\appsettings.json`. Ниже приведены общие настройки для всех типов обработчика, после чего каждый тип обработчика описан отдельно.

Текстовым редактором откройте конфигурационный файл `C:\inetpub\cp-archive\consumer\appsettings.json`. Для настройки подключения к RabbitMQ измените параметры секции `$.RabbitMq`. Ниже приведены описания параметров.

В таблице ниже указаны доступные настройки для подключения к RabbitMQ. Символом `i` обозначен индекс конкретного объекта подключения в файле настройки (обозначения описаны в начале главы 3 Настройка).

Имя параметра	Описание
`$.RabbitMq .Consumers[i] .Enabled`	Флаг, определяющий, активно ли текущее соединение. Если указано `false`, программа будет игнорировать это соединение при запуске. Значение по умолчанию: `false`
`$.RabbitMq .Consumers[i] .Name`	Имя этого соединения для упрощения отладки. Может быть произвольной строкой. Значение по умолчанию: `"unnamed"`
`$.RabbitMq .Consumers[i] .Username`	Имя пользователя RabbitMQ. Значение по умолчанию: `"cryptopro_app"`
`$.RabbitMq .Consumers[i] .Password`	Пароль пользователя RabbitMQ. Значение по умолчанию: `"cryptopro"`
`$.RabbitMq .Consumers[i] .VirtualHost`	Имя виртуального хоста. Значение по умолчанию: `"archive"`
`$.RabbitMq .Consumers[i] .HostName`	Имя/адрес сервера, на котором расположен RabbitMQ. Значение по умолчанию: `"localhost"`

`$.RabbitMq .Consumers[i] .ExchangeName`	Имя обмена в RabbitMQ. Должно быть установлено одно из значений `"archive.ca.documents.exchange"`, `"archive.notifications.exchange"` или `"archive.signatures.exchange"` в зависимости от типа обработчика
`$.RabbitMq .Consumers[i] .QueueName`	Имя очереди в RabbitMQ. Должно быть установлено одно из значений `"archive.ca.documents.queue"`, `"archive.notifications.queue"` или `"archive.signatures.queue"` в зависимости от типа обработчика
`$.RabbitMq .Consumers[i] .Port`	Порт службы RabbitMQ. Значение по умолчанию: `5672`
`$.RabbitMq .Consumers[i] .Type`	Тип обработчика очереди (см. ниже). Должно быть указано обязательно. Доступные значения: `"Document"`, `"Notification"`, `"Signature"`
`$.RabbitMq .Consumers[i] .DelayMs`	Задержка отложенного добавления в очередь в миллисекундах. Значение по умолчанию: `5000`

При возникновении ошибки во время обработки сообщения, полученного из очереди, обработчик автоматически возвращает это сообщение обратно в очередь для повторной обработки через определённое время. Это время регулируется параметром `$.RabbitMq.Consumers[i].DelayMs`, значение которого представляет собой задержку отложенного добавления в очередь в миллисекундах. Значение по умолчанию: `5000` (5 секунд). Например, если обработка сообщения была прервана с ошибкой, это сообщение будет возвращено в очередь через 5 секунд.

3.8.1.2.1 Обработчик уведомлений (тип: Notification)

Обработчик используется для отложенной отправки уведомлений о результате усовершенствования подписей на указанный адрес.

3.8.1.2.1 Обработчик подписанных документов опциональной подсистемы Архив УЦ (тип: Document)

Обработчик используется подсистемой Архив УЦ для отложенного сохранения подписанных документов в базу данных или во внешнюю систему хранения данных с использованием механизма подключаемых модулей.

Замечание: Обработчик используется только подсистемой Архив УЦ. Настройка Архив УЦ описана в разделе 3.11 Настройка Архив УЦ.

3.8.1.2.1 Обработчик усовершенствованных подписей (тип: Signature)

Обработчик используется для отложенной обработки усовершенствованных (успешно или неуспешно) подписей через механизм подключаемых модулей.

3.8.2 Настройка consumer на ОС семейства Linux

На ОС семейства Linux программа consumer работает как служба systemd. Ниже приведены инструкции по настройке службы и параметров сохранения подписанных документов.

3.8.2.1 Настройка службы systemd

Для обеспечения автоматического запуска приложения как службы systemd выполните

```
sudo systemctl enable cp-archive_consumer.service
```

Для запуска службы выполните

```
sudo systemctl start cp-archive_consumer.service
```

3.8.2.2 Настройка RabbitMQ

Программа позволяет настроить подключение к нескольким очередям RabbitMQ. Для этого используется секция `$.RabbitMq` конфигурационного файла `/etc/opt/cp-archive/consumer/appsettings.json`. Ниже приведены общие настройки для всех типов обработчика, после чего каждый тип обработчика описан отдельно.

Текстовым редактором откройте конфигурационный файл /etc/opt/cp-archive/consumer/appsettings.json. Для настройки подключения к RabbitMQ измените параметры секции $.RabbitMq. Ниже приведены описания параметров.

В таблице ниже указаны доступные настройки для подключения к RabbitMQ. Символом i обозначен индекс конкретного объекта подключения в файле настройки (обозначения описаны в начале главы 3 Настройка).

Имя параметра	Описание
$.RabbitMq .Consumers[i] .Enabled	Флаг, определяющий, активно ли текущее соединение. Если указано false, программа будет игнорировать это соединение при запуске. Значение по умолчанию: false
$.RabbitMq .Consumers[i] .Name	Имя этого соединения для упрощения отладки. Может быть произвольной строкой. Значение по умолчанию: "unnamed"
$.RabbitMq .Consumers[i] .Username	Имя пользователя RabbitMQ. Значение по умолчанию: "cryptopro_app"
$.RabbitMq .Consumers[i] .Password	Пароль пользователя RabbitMQ. Значение по умолчанию: "cryptopro"
$.RabbitMq .Consumers[i] .VirtualHost	Имя виртуального хоста. Значение по умолчанию: "archive"
$.RabbitMq .Consumers[i] .HostName	Имя/адрес сервера, на котором расположен RabbitMQ. Значение по умолчанию: "localhost"
$.RabbitMq .Consumers[i] .ExchangeName	Имя обмена в RabbitMQ. Должно быть установлено одно из значений "archive.ca.documents.exchange", "archive.notifications.exchange" или "archive.signatures.exchange" в зависимости от типа обработчика
$.RabbitMq .Consumers[i] .QueueName	Имя очереди в RabbitMQ. Должно быть установлено одно из значений "archive.ca.documents.queue", "archive.notifications.queue" или

	"archive.signatures.queue" в зависимости от типа обработчика
$.RabbitMq .Consumers[i] .Port	Порт службы RabbitMQ. Значение по умолчанию: 5672
$.RabbitMq .Consumers[i] .Type	Тип обработчика очереди (см. ниже). Должно быть указано обязательно. Доступные значения: "Document", "Notification", "Signature"
$.RabbitMq .Consumers[i] .DelayMs	Задержка отложенного добавления в очередь в миллисекундах. Значение по умолчанию: 5000

При возникновении ошибки во время обработки сообщения, полученного из очереди, обработчик автоматически возвращает это сообщение обратно в очередь для повторной обработки через определённое время. Это время регулируется параметром $.RabbitMq.Consumers[i].DelayMs, значение которого представляет собой задержку отложенного добавления в очередь в миллисекундах. Значение по умолчанию: 5000 (5 секунд). Например, если обработка сообщения была прервана с ошибкой, это сообщение будет возвращено в очередь через 5 секунд.

3.8.1.2.1 Обработчик уведомлений (тип: Notification)

Обработчик используется для отложенной отправки уведомлений о результате усовершенствования подписей на указанный адрес.

3.8.1.2.1 Обработчик подписанных документов опциональной подсистемы Архив УЦ (тип: Document)

Обработчик используется подсистемой Архив УЦ для отложенного сохранения подписанных документов в базу данных или во внешнюю систему хранения данных с использованием механизма подключаемых модулей.

Замечание: Обработчик используется только подсистемой Архив УЦ. Настройка Архив УЦ описана в разделе 3.11 Настройка Архив УЦ.

3.8.1.2.1 Обработчик усовершенствованных подписей (тип: Signature)

Обработчик используется для отложенной обработки усовершенствованных (успешно или неуспешно) подписей через механизм подключаемых модулей.

3.10 Управление лицензиями

В данном разделе описан ввод и просмотр лицензий на программный комплекс КриптоПро Архив и подсистему Архив УЦ. Лицензия представляет собой набор из 25 символов и имени организации.

3.10.1 Управление лицензиями на ОС семейства Windows Server

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 'ООО \"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.
```

3.10.2 Управление лицензиями на ОС семейства Linux

Для ввода лицензии выполните

```
sudo /opt/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. Например,

```
sudo /opt/cp-archive/config/Archive.Config set \
    --license \
    --serial '01234-56789-01234-56789-01234' \
    --org 'ООО "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

```
sudo /opt/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.
```

3.11 Настройка Архив УЦ

В данном разделе приведена настройка опциональной подсистемы Архив УЦ. Описание подсистемы приведено в разделе 1.4 Опциональная подсистема Архив УЦ.

Для работы подсистеме необходимы установленные компоненты admin-api (для настройки) и consumer (для отложенного сохранения подписанных документов в базу данных). 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.

3.11.1 Настройка Архив УЦ на ОС семейства Windows Server

Предполагается, что изначальная настройка основной базы данных КриптоПро Архив была проведена в соответствии с инструкцией в одном из разделов

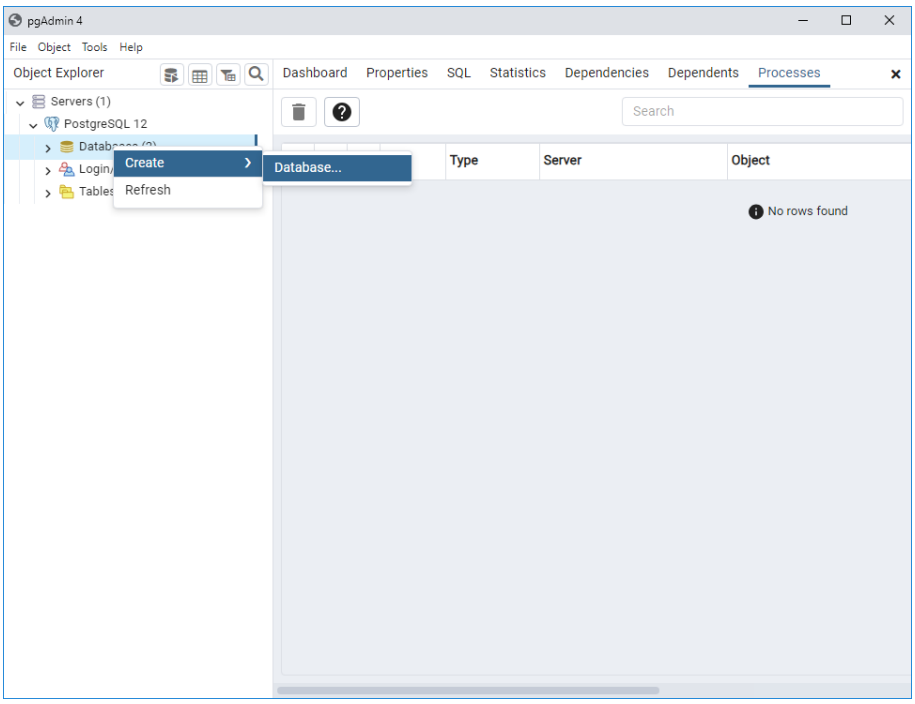
- 3.3.1 Настройка PostgreSQL на ОС семейства Windows Server
- 3.4.1 Настройка Oracle Database на ОС семейства Windows Server

3.11.1.1 Создание баз данных

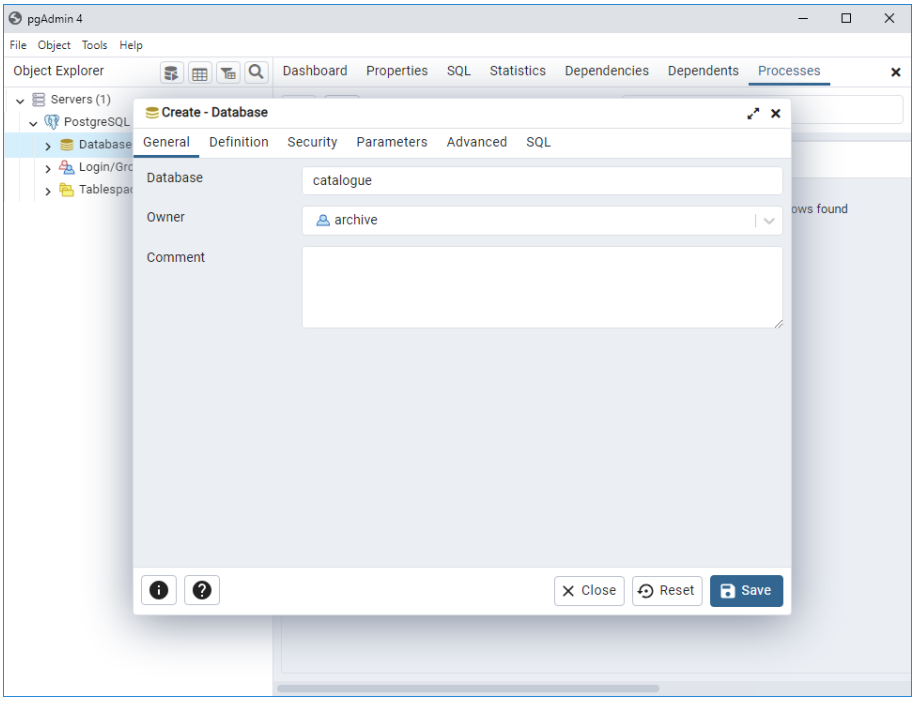
Для настройки Архив УЦ на ОС семейства Windows Server необходимо создать базы данных. В соответствии с описанием подсистемы Архив УЦ (см. раздел 1.4 Опциональная подсистема Архив УЦ) необходимо создать каталог баз данных и базу данных для хранения подписанных документов.

3.11.1.1.1 PostgreSQL

При использовании PostgreSQL для создания каталога базы данных откройте pgAdmin 4, подключитесь к серверу баз данных как пользователь `postgres` (администратор) и выберите **Databases** > **Create** > **Database…**:



Введите имя базы данных (в примере ниже — `catalogue`), укажите в качестве владельца пользователя, от лица которого предполагается подключение к базе данных (в примере ниже — `archive`) и нажмите **Save**:



Тем же образом создайте базу данных для хранения подписанных документов.

Для создания необходимых объектов в каталоге баз данных выполните следующую команду. Здесь флаг `--ca` указывает на работу с базой данных подсистемы Архив УЦ, а флаг `--type` указывает тип создаваемой базы данных (возможные значения: `catalogue` и `storage`). Также замените `<username>`, `<password>`, `<host>` и `<database>` на имя пользователя, пароль пользователя, адрес сервера с PostgreSQL и имя созданного пустого каталога баз 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>" `
    --ca `
    --type catalogue
```

После успешного выполнения миграции на экране будет написано `Миграция успешно выполнена`. Для создания необходимых объектов в хранилище подписанных документов выполните следующую команду, заменив `<username>`, `<password>`, `<host>` и `<database>` на имя пользователя, пароль пользователя, адрес сервера с PostgreSQL и имя созданной пустой базы данных для хранения подписанных документов 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>" `
    --ca `
    --type storage
```

После успешного выполнения миграции на экране будет написано `Миграция успешно выполнена`.

3.11.1.1.2 Oracle Database

При использовании Oracle Database создайте каталог баз данных с помощью следующей команды. Здесь флаг `--ca` указывает на работу с базой данных подсистемы Архив УЦ, а флаг `--type` указывает тип создаваемой базы данных

(возможные значения: catalogue и storage). Также замените <password>, <data_source> и <catalogue_username> на пароль пользователя SYS, источник данных (Data Source) Oracle Database и имя создаваемого пользователя для каталога баз данных соответственно. Команда создаёт каталог баз данных:

```
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
```

После успешного выполнения миграции на экране будет написано Миграция успешно выполнена. Соответственно, для создания необходимых объектов в хранилище подписанных документов выполните следующую команду, заменив <password>, <data_source> и <storage_username> на пароль пользователя SYS, источник данных (Data Source) Oracle Database и имя создаваемого пользователя для хранилища подписанных документов соответственно. Команда создаст базу данных для хранения подписанных документов:

```
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
```

После успешного выполнения миграции на экране будет написано Миграция успешно выполнена.

3.11.1.2 Настройка компонентов КриптоПро Архив

Для настройки Архив УЦ в конфигурационных файлах следующих компонентов КриптоПро Архив предусмотрена идентичная секция $.ArchiveCa:

- admin-api (конфигурационный файл: `C:\inetpub\cp-archive\admin-api\appsettings.json`)
- client-api (`C:\inetpub\cp-archive\client-api\appsettings.json`)
- consumer (`C:\inetpub\cp-archive\consumer\appsettings.json`)

Для настройки подсистемы Архив УЦ необходимо отредактировать секцию `$.ArchiveCa` во всех указанных выше файлах. Список параметров секции приведён в таблице ниже.

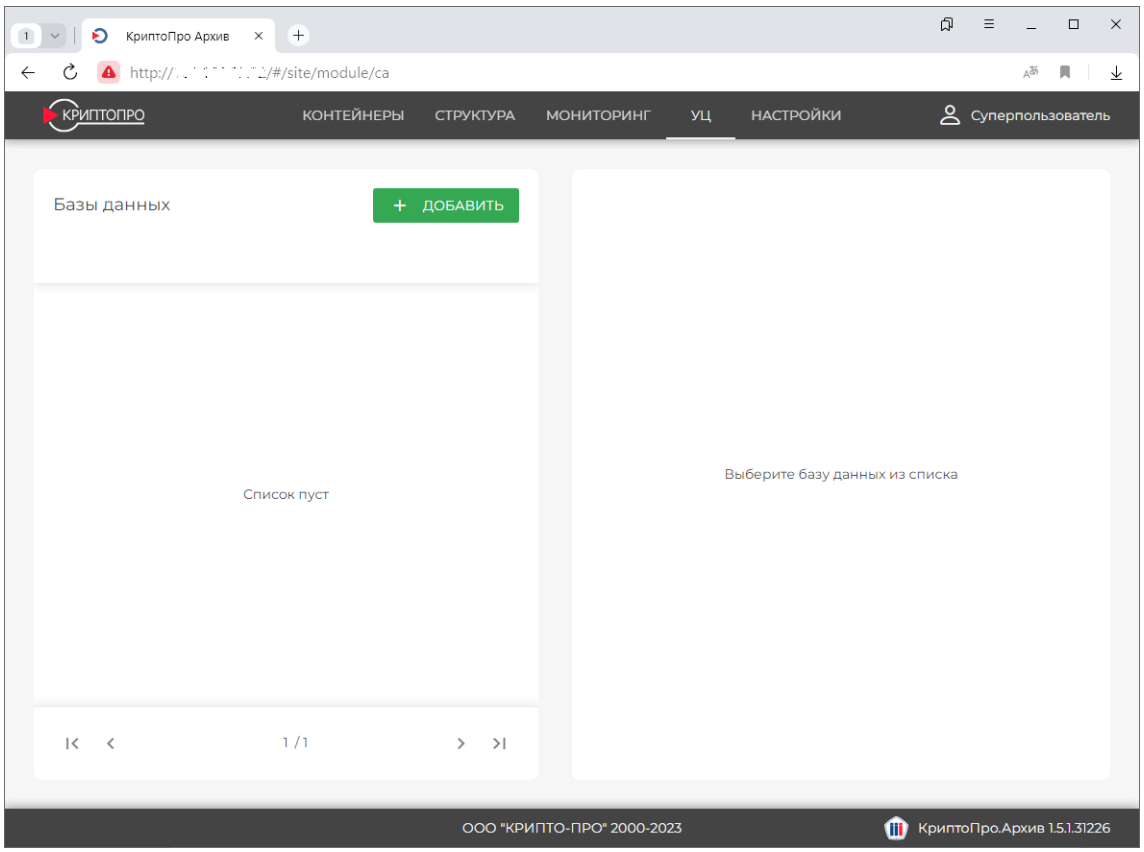
Имя параметра	Описание
`$.ArchiveCa.UseArchiveCa`	Флаг, указывающий, активна ли подсистема Архив УЦ. Значение по умолчанию: `false`
`$.ArchiveCa.ConnectionStrings.DatabaseCatalogue`	Строка подключения к каталогу баз данных
`$.ArchiveCa.MaxSmallFileSizeBytes`	Размер в байтах, файлы меньше которого считать маленькими. Маленькие файлы записываются в базу данных и читаются из неё не поточно. Файлы больше этого размера — поточно. Значение по умолчанию: 10 МБ

Обязательно необходимо установить параметр `$.ArchiveCa.UseArchiveCa` в значение `true` и указать строку подключения к созданному ранее каталогу баз данных в параметре `$.ArchiveCa.ConnectionStrings.DatabaseCatalogue`.

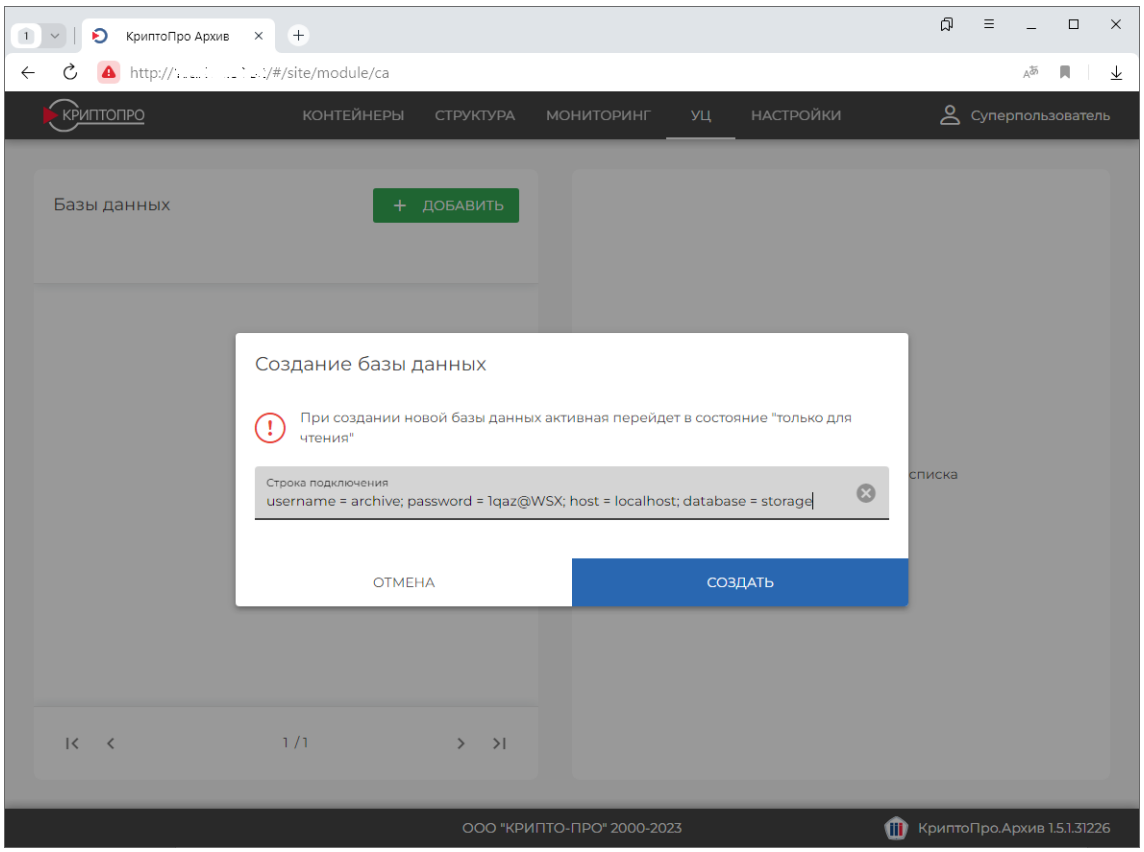
После настройки секции `$.ArchiveCa` в конфигурационных файлах указанных программ перезапустите эти программы.

3.11.1.3 Подключение хранилища документов к подсистеме Архив УЦ

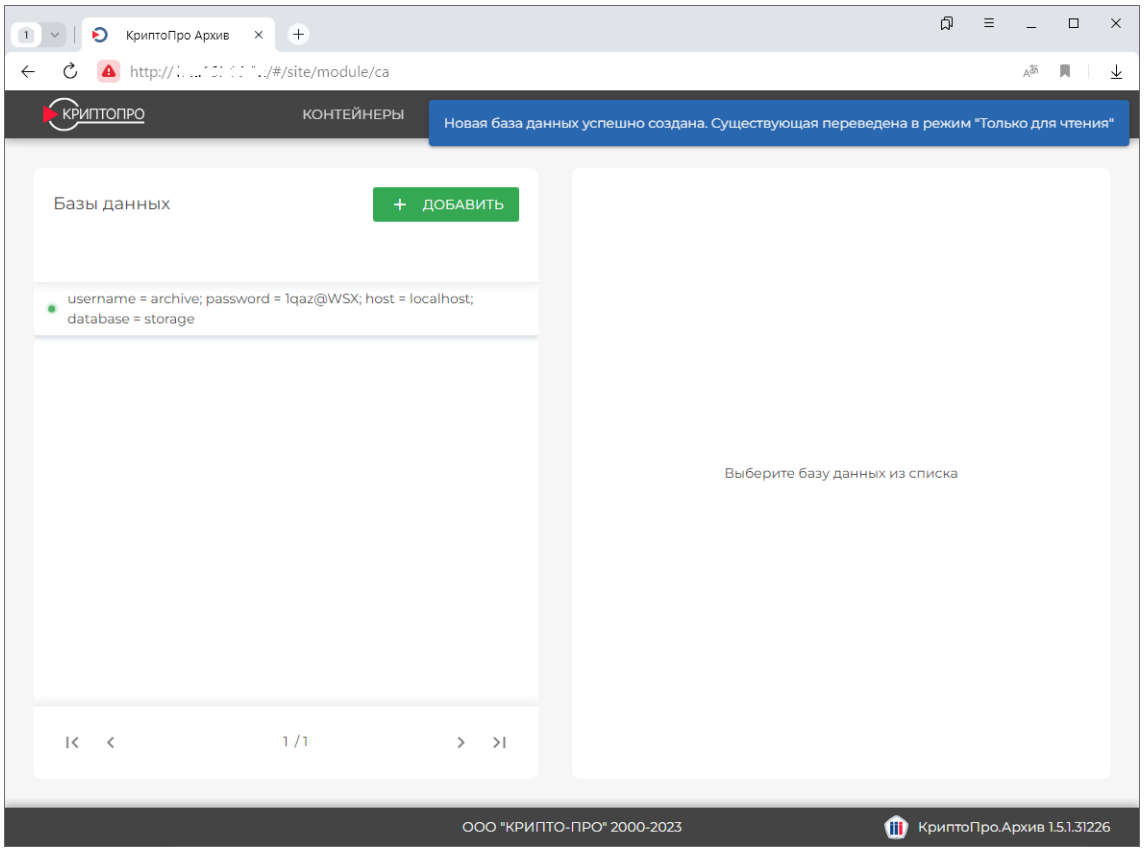
После активации подсистемы Архив УЦ в конфигурационном файле admin-api и при правильной настройке каталога баз данных в веб-интерфейсе появится вкладка **УЦ**. Зайдите в веб-интерфейс, приложив сертификат суперпользователя, и перейдите на вкладку **УЦ**:



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.

3.11.2 Настройка Архив УЦ на ОС семейства Linux

Предполагается, что изначальная настройка основной базы данных КриптоПро Архив была проведена в соответствии с инструкцией в одном из разделов

- 3.3.2 Настройка PostgreSQL на Astra Linux 1.7
- 3.3.3 Настройка PostgreSQL на Astra Linux
- 3.4.2 Настройка Oracle Database на ОС семейства Linux

3.11.2.1 Создание баз данных

Для настройки Архив УЦ на ОС семейства Linux необходимо создать базы данных. В соответствии с описанием подсистемы Архив УЦ (см. раздел 1.4 Опциональная подсистема Архив УЦ) необходимо создать каталог баз данных и базу данных для хранения подписанных документов.

3.11.2.1.1 PostgreSQL

При использовании PostgreSQL для создания необходимых баз данных, подключитесь к серверу баз данных как пользователь `postgres`:

```
sudo -u postgres psql
```

Создайте необходимые базы данных. Замените `<catalogue_database>` на имя каталога баз данных с подписанными документами, `<storage_database>` — на имя хранилища подписанных документов и `<username>` — на имя пользователя, от лица которого будет выполняться подключение:

```
CREATE DATABASE <catalogue_database> OWNER <username>;
CREATE DATABASE <storage_database> OWNER <username>;
exit
```

Для создания необходимых объектов в каталоге баз данных выполните следующую команду. Здесь флаг `--ca` указывает на работу с базой данных подсистемы Архив УЦ, а флаг `--type` указывает тип создаваемой базы данных

(возможные значения: catalogue и storage). Также замените <username>, <password>, <host> и <database> на имя пользователя, пароль пользователя, адрес сервера с PostgreSQL и имя созданного пустого каталога баз данных соответственно:

```
sudo /opt/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
```

После успешного выполнения миграции на экране будет написано Миграция успешно выполнена. Для создания необходимых объектов в хранилище подписанных документов выполните следующую команду, заменив <username>, <password>, <host> и <database> на имя пользователя, пароль пользователя, адрес сервера с PostgreSQL и имя созданной пустой базы данных для хранения подписанных документов соответственно:

```
sudo /opt/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
```

После успешного выполнения миграции на экране будет написано Миграция успешно выполнена.

3.11.2.1.2 Oracle Database

При использовании Oracle Database создайте каталог баз данных с помощью следующей команды. Здесь флаг --ca указывает на работу с базой данных подсистемы Архив УЦ, а флаг --type указывает тип создаваемой базы данных (возможные значения: catalogue и storage). Также замените <password>, <data_source> и <catalogue_username> на пароль пользователя SYS, источник

данных (Data Source) Oracle Database и имя создаваемого пользователя для каталога баз данных соответственно. Команда создаёт каталог баз данных:

```
sudo /opt/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
```

После успешного выполнения миграции на экране будет написано `Миграция успешно выполнена`. Соответственно, для создания необходимых объектов в хранилище подписанных документов выполните следующую команду, заменив `<password>`, `<data_source>` и `<storage_username>` на пароль пользователя SYS, источник данных (Data Source) Oracle Database и имя создаваемого пользователя для хранилища подписанных документов соответственно. Команда создаст базу данных для хранения подписанных документов:

```
sudo /opt/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
```

После успешного выполнения миграции на экране будет написано `Миграция успешно выполнена`.

3.11.2.2 Настройка компонентов КриптоПро Архив

Для настройки Архив УЦ в конфигурационных файлах следующих компонентов КриптоПро Архив предусмотрена идентичная секция `$.ArchiveCa`:

- admin-api (конфигурационный файл: `/etc/opt/cp-archive/admin-api/appsettings.json`)
- client-api (`/etc/opt/cp-archive/client-api/appsettings.json`)

- consumer (`/etc/opt/cp-archive/consumer/appsettings.json`)

Для настройки подсистемы Архив УЦ необходимо отредактировать секцию `$.ArchiveCa` во всех указанных выше файлах. Список параметров секции приведён в таблице ниже.

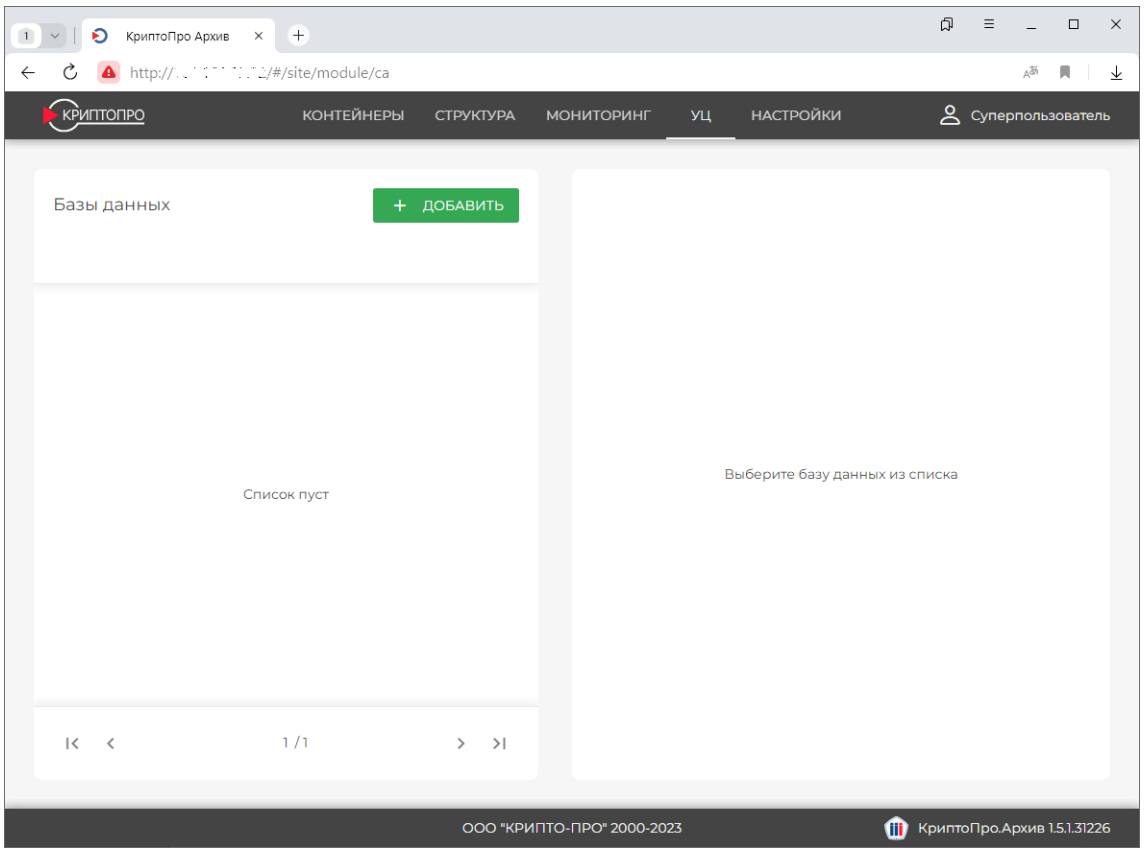
Имя параметра	Описание
`$.ArchiveCa .UseArchiveCa`	Флаг, указывающий, активна ли подсистема Архив УЦ. Значение по умолчанию: `false`
`$.ArchiveCa .ConnectionStrings .DatabaseCatalogue`	Строка подключения к каталогу баз данных
`$.ArchiveCa .MaxSmallFileSizeBytes`	Размер в байтах, файлы меньше которого считать маленькими. Маленькие файлы записываются в базу данных и читаются из неё не поточно. Файлы больше этого размера — поточно. Значение по умолчанию: 10 МБ

Обязательно необходимо установить параметр `$.ArchiveCa.UseArchiveCa` в значение `true` и указать строку подключения к созданному ранее каталогу баз данных в параметре `$.ArchiveCa.ConnectionStrings.DatabaseCatalogue`.

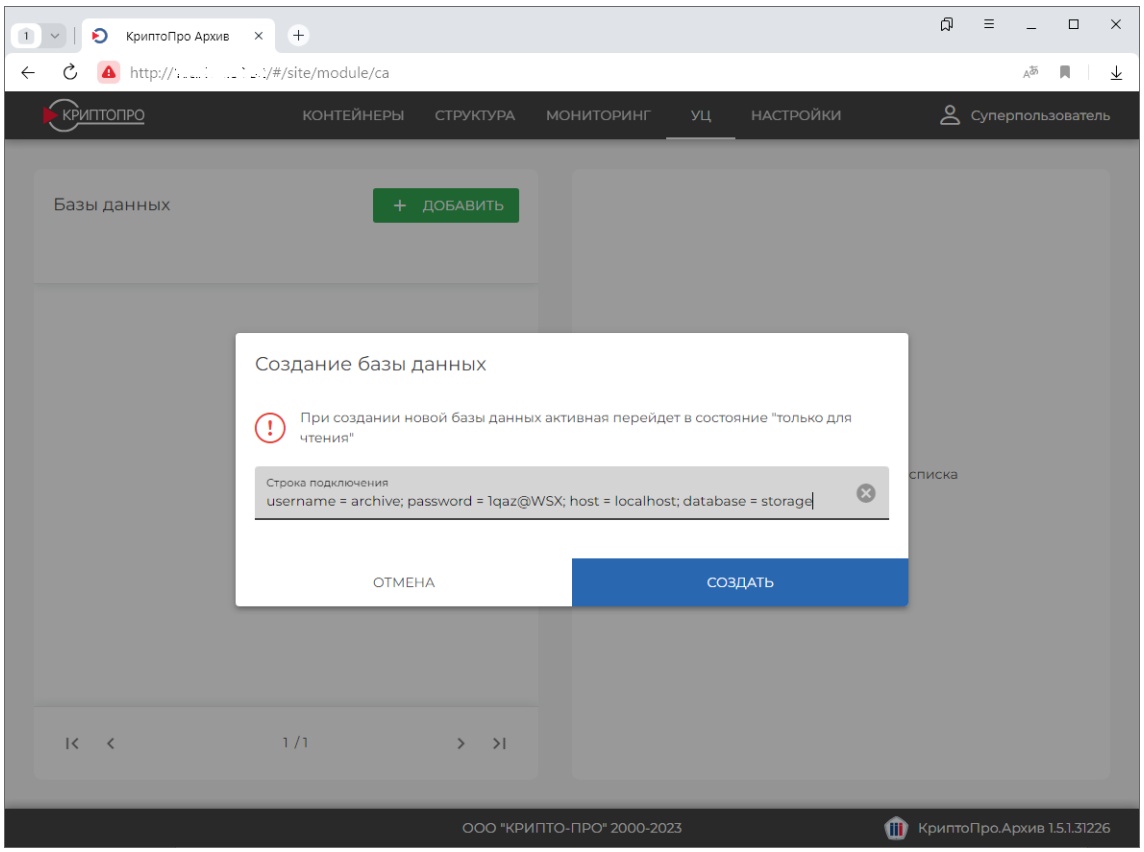
После настройки секции `$.ArchiveCa` в конфигурационных файлах указанных программ перезапустите эти программы.

3.11.2.3 Подключение хранилища документов к подсистеме Архив УЦ

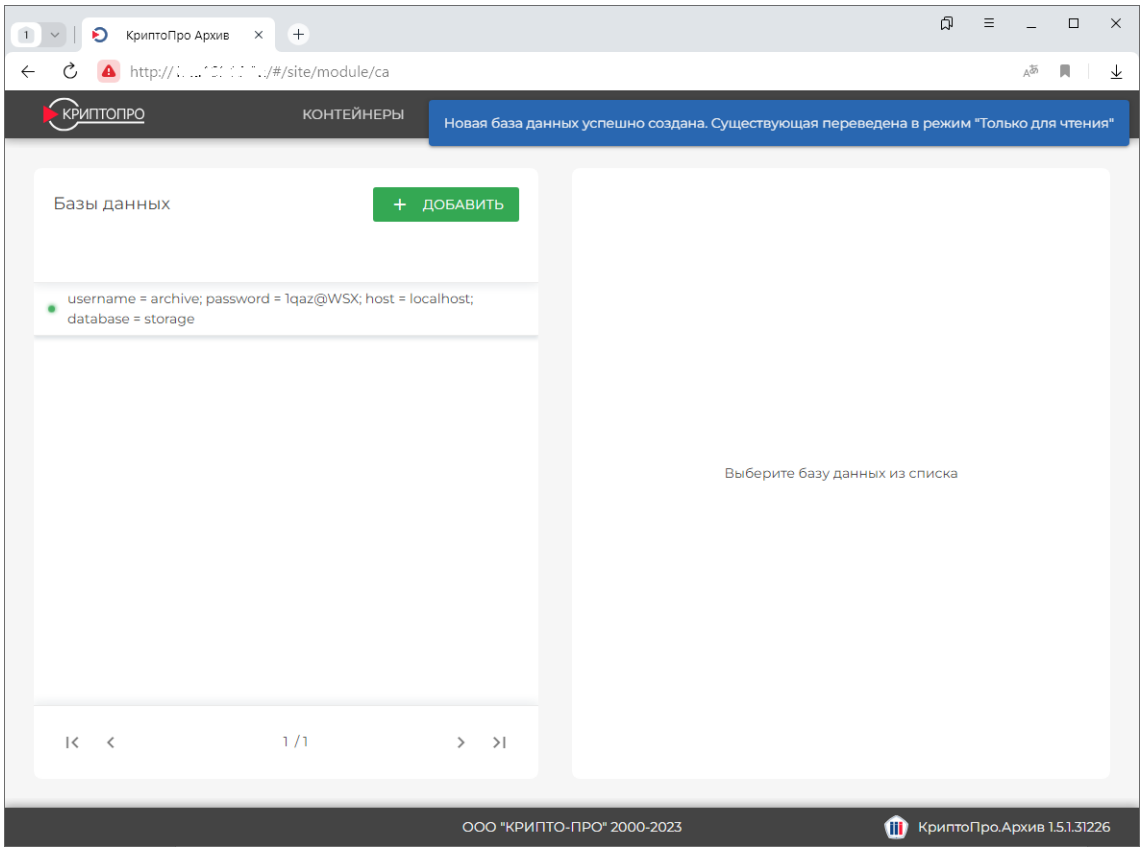
После активации подсистемы Архив УЦ в конфигурационном файле admin-api и при правильной настройке каталога баз данных в веб-интерфейсе появится вкладка **УЦ**. Зайдите в веб-интерфейс, приложив сертификат суперпользователя, и перейдите на вкладку **УЦ**:



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.

3.12 Настройка журналирования

В данном разделе описана настройка системы журналирования КриптоПро Архив. Для ведения журналов в КриптоПро Архив используется библиотека Serilog, позволяющая гибко настроить формат и параметры ведения журналов, а также указать несколько конечных точек для отправки в них записей журнала. Поддерживаемые конечные точки для записей журналов: Elasticsearch, ManticoreSearch, файл. Настройка системы журналирования производится с помощью секции `$.Serilog` в конфигурационном файле каждой службы. Пути к конфигурационным файлам служб КриптоПро Архив указаны в таблице ниже.

Имя службы	Путь к конфигурационному файлу
admin-api	**Windows**: `C:\inetpub\cp-archive\admin-api\appsettings.json` **Linux**: `/etc/opt/cp-archive/admin-api/appsettings.json`
client-api	**Windows**: `C:\inetpub\cp-archive\client-api\appsettings.json` **Linux**: `/etc/opt/cp-archive/client-api/appsettings.json`
signature-updater	**Windows**: `C:\inetpub\cp-archive\signature-updater\appsettings.json` **Linux**: `/etc/opt/cp-archive/signature-updater/appsettings.json`
consumer	**Windows**: `C:\inetpub\cp-archive\consumer\appsettings.json` **Linux**: `/etc/opt/cp-archive/consumer/appsettings.json`

Ниже приведены и описаны рекомендуемые параметры настройки ведения журналов для каждой конечной точки.

3.12.1 Настройка отправки журналов в Elasticsearch

Ниже приведён пример секции `$.Serilog` конфигурационного файла службы для настройки отправки журналов в Elasticsearch. Полный список доступных

параметров приведён в документации. Для указания адреса Elasticsearch используйте параметр $.Serilog.WriteTo[0].Args.nodeUris. Уровень ведения журналов указывается с помощью параметра $.Serilog.MinimumLevel.Default. При необходимости ведения журналов всех запросов и ответов сервера установите параметр $.Serilog.MinimumLevel.Override."Microsoft.AspNetCore" в значение "Information". Параметр $.indexFormat должен быть указан "archive.web-{0:yyyy.MM.dd}" для приложений admin-api, client-api и "archive.consumer-{0:yyyy.MM.dd}" для остальных приложений.

```
"Serilog": {
  "Using": [ "Serilog.Sinks.Elasticsearch" ],
  "MinimumLevel": {
    "Default": "Information",
    "Override": {
      "Microsoft.EntityFrameworkCore": "Warning",
      "Microsoft.EntityFrameworkCore.Query": "Error",
      "Microsoft.AspNetCore": "Warning"
    }
  },
  "WriteTo": [
    {
      "Name": "Elasticsearch",
      "Args": {
        "nodeUris": "http://localhost:9200",
        "indexFormat": "archive.web-{0:yyyy.MM.dd}",
        "autoRegisterTemplateVersion": "ESv7",
        "autoRegisterTemplate": true
      }
    }
  ]
}
```

3.12.2 Настройка отправки журналов в ManticoreSearch

Ниже приведён пример секции $.Serilog конфигурационного файла службы для настройки отправки журналов в ManticoreSearch. Полный список доступных параметров приведён после примера. Для указания адреса ManticoreSearch используйте параметр $.Serilog.WriteTo[0].Args.basePath. Уровень ведения журналов указывается с помощью параметра $.Serilog.MinimumLevel.Default. При необходимости ведения журналов всех запросов и ответов сервера установите параметр $.Serilog.MinimumLevel.Override."Microsoft.AspNetCore" в значение "Information".

```
"Serilog": {
```

```
    "Using": [ "Serilog.Sinks.ManticoreSearch" ],
    "MinimumLevel": {
      "Default": "Information",
      "Override": {
        "Microsoft.EntityFrameworkCore": "Warning",
        "Microsoft.EntityFrameworkCore.Query": "Error",
        "Microsoft.AspNetCore": "Warning"
      }
    },
    "WriteTo": [
      {
        "Name": "ManticoreSearch",
        "Args": {
          "basePath": "http://127.0.0.1:9308",
          "indexName": "archive_logs",
          "clusterName": null
        }
      }
    ]
  }
```

Имя параметра	Описание
basePath	Адрес службы ManticoreSearch. Значение по умолчанию: "http://127.0.0.1:9308"
indexName	Имя индекса ManticoreSearch. Значение по умолчанию: "archive_logs"
clusterName	Имя кластера ManticoreSearch. Значение по умолчанию: null

3.12.3 Настройка отправки журналов в файл

Ниже приведён пример секции $.Serilog конфигурационного файла службы для настройки отправки журналов в файл. Для указания пути к файлу используйте параметр $.Serilog.WriteTo[0].Args.path. Уровень ведения журналов указывается с помощью параметра $.Serilog.MinimumLevel.Default. При необходимости ведения журналов всех запросов и ответов сервера установите параметр $.Serilog.MinimumLevel.Override."Microsoft.AspNetCore" в значение "Information". Убедитесь, что у службы есть права на запись в указанный файл.

```
  "Serilog": {
    "Using": [ "Serilog.Sinks.File" ],
    "MinimumLevel": {
      "Default": "Information",
      "Override": {
```

```
        "Microsoft.EntityFrameworkCore": "Warning",
        "Microsoft.EntityFrameworkCore.Query": "Error",
        "Microsoft.AspNetCore": "Warning"
      }
    },
    "WriteTo": [
      {
        "Name": "File",
        "Args": {
          "path": "<path>",
          "rollingInterval": "Day",
          "rollOnFileSizeLimit": true,
          "retainedFileCountLimit": 31
        }
      }
    ]
  }
```

Где <path> — путь к файлу, в который необходимо сохранять журналы.

3.12.4 Отображение журналов в административном интерфейсе

Веб-интерфейс КриптоПро Архив поддерживает отображение журналов из источников Elasticsearch и ManticoreSearch.

Для настройки отображения журналов в административном интерфейсе в конфигурационном файле компонента admin-api сперва необходимо указать используемую службу хранения журналов в параметре $.General.LoggingService: "ManticoreSearch" или "Elasticsearch". После этого в зависимости от используемой службы заполнить разделы, как указано ниже.

3.12.4.1 В случае выбора ManticoreSearch

Для настройки отображения журналов ManticoreSearch в административном интерфейсе необходимо заполнить секцию $.ManticoreSearch. Список параметров секции с описанием приведён ниже.

Имя параметра	Описание
$.ManticoreSearch.ServiceAddress	Адрес службы ManticoreSearch. Значение по умолчанию: "http://127.0.0.1:9308"
$.ManticoreSearch.IndexName	Имя индекса ManticoreSearch. Значение по умолчанию: "archive_logs"

3.12.4.2 В случае выбора Elasticsearch

Для настройки отображения журналов ManticoreSearch в административном интерфейсе необходимо заполнить секцию `$.Elasticsearch`. Список параметров секции с описанием приведён ниже.

Имя параметра	Описание
`$.ElasticSearch.ServiceAddress`	Адрес службы Elasticsearch. Значение по умолчанию: `"http://localhost:9200"`

3.13 Настройка дополнительных служб OCSP

В данном разделе описана настройка дополнительных служб OCSP. Данная функциональность предоставляет возможность явно указать, какие адреса служб OCSP необходимо использовать для издателя данного сертификата подписанта.

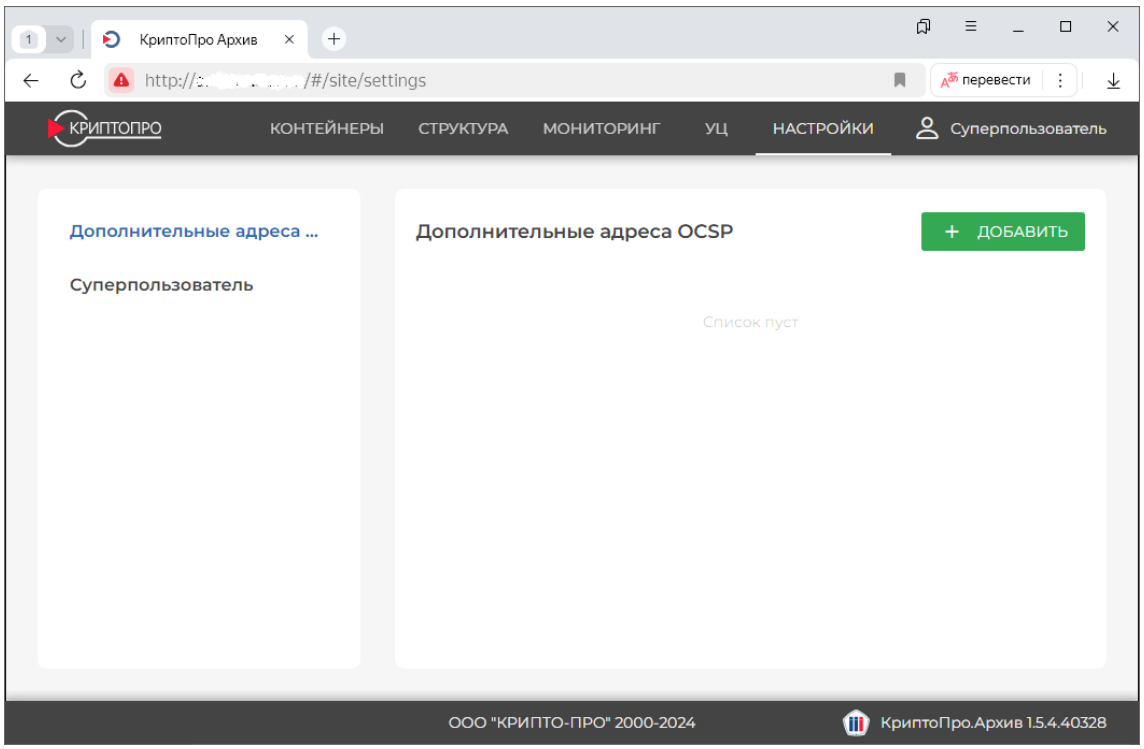
КриптоПро Архив обращается к службам OCSP в следующем порядке до первого успеха (до первого определённого ответа о статусе сертификата):

1. Дополнительные адреса служб OCSP
2. Адрес, указанный в сертификате подписанта
3. Адрес, указанный в групповой политике клиента OCSP

Таким образом, функциональность позволяет указать, к какому адресу OCSP следует обратиться для издателя данного сертификата подписанта.

Для выполнения дальнейших шагов на настраиваемом сервере потребуется установленный КриптоПро Архив в конфигурации «Полная установка» (установлены все компоненты) или «Подсистема приёма подписей» (установлены admin-api, client-api и frontend).

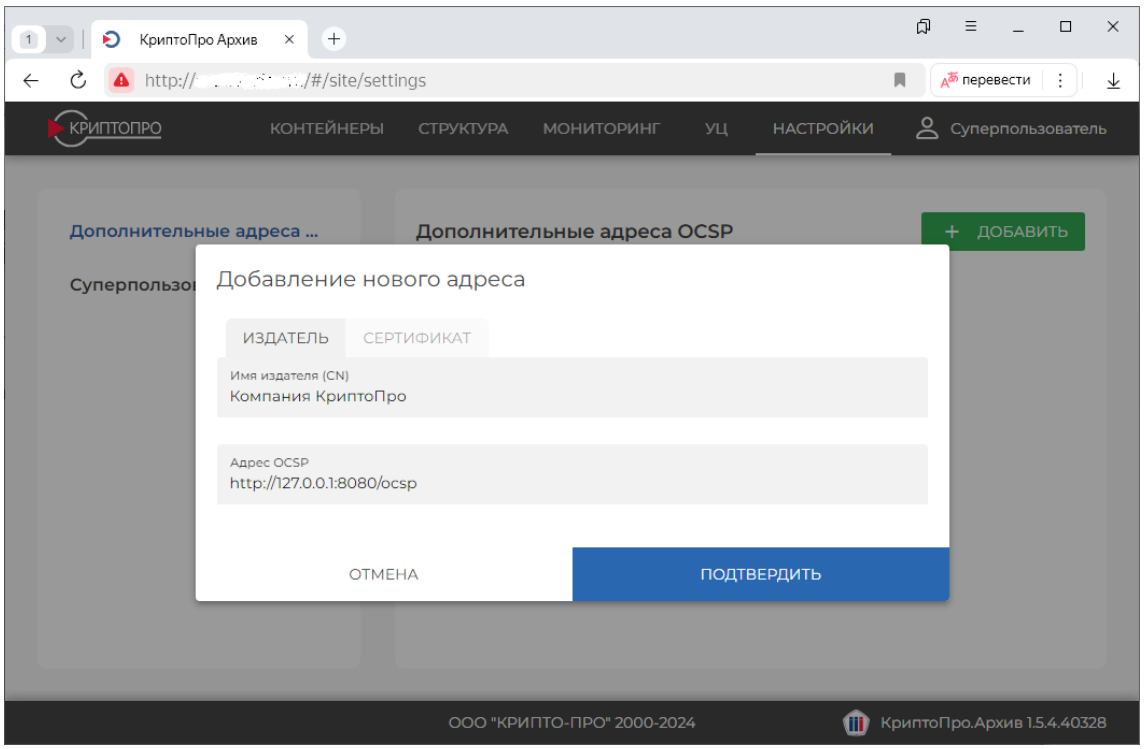
Для настройки дополнительных служб откройте административную панель КриптоПро Архив от лица суперпользователя и перейдите в раздел **Настройки**. Слева выберите вкладку **Дополнительные адреса OCSP**:



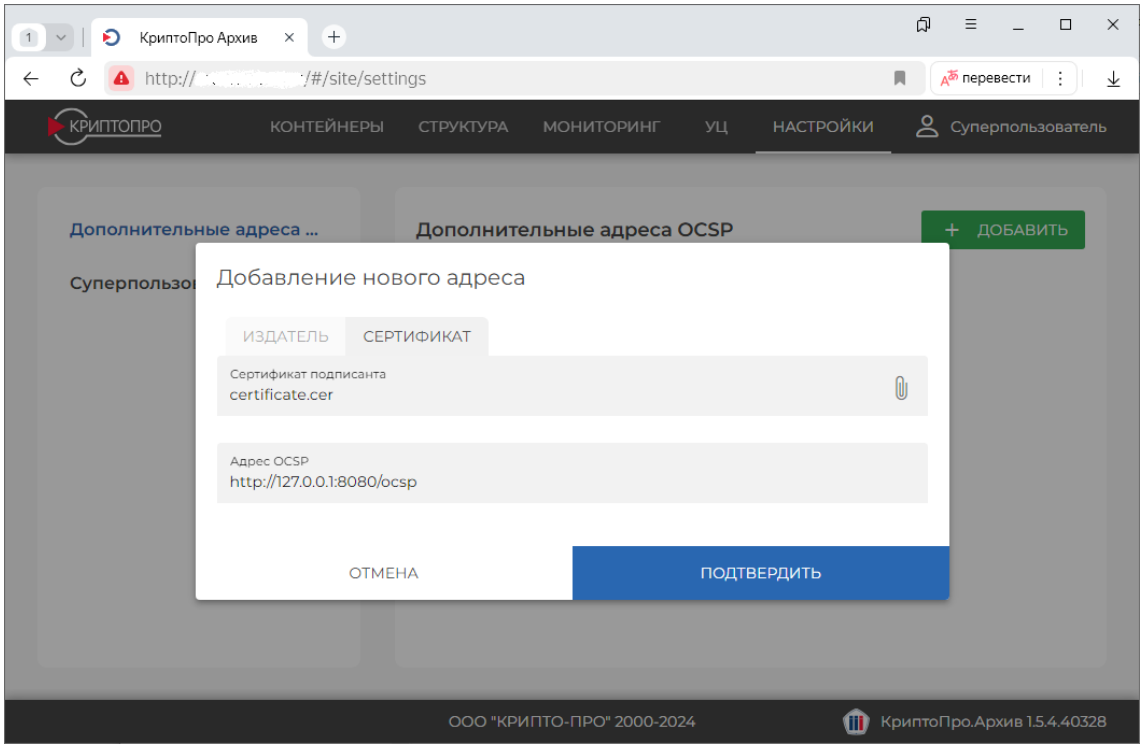
Нажмите **Добавить**. Далее необходимо указать имя издателя (более точно, CN издателя) и адрес дополнительной службы OCSP. Имя издателя можно указать двумя способами, которым соответствуют вкладки над этим полем:

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

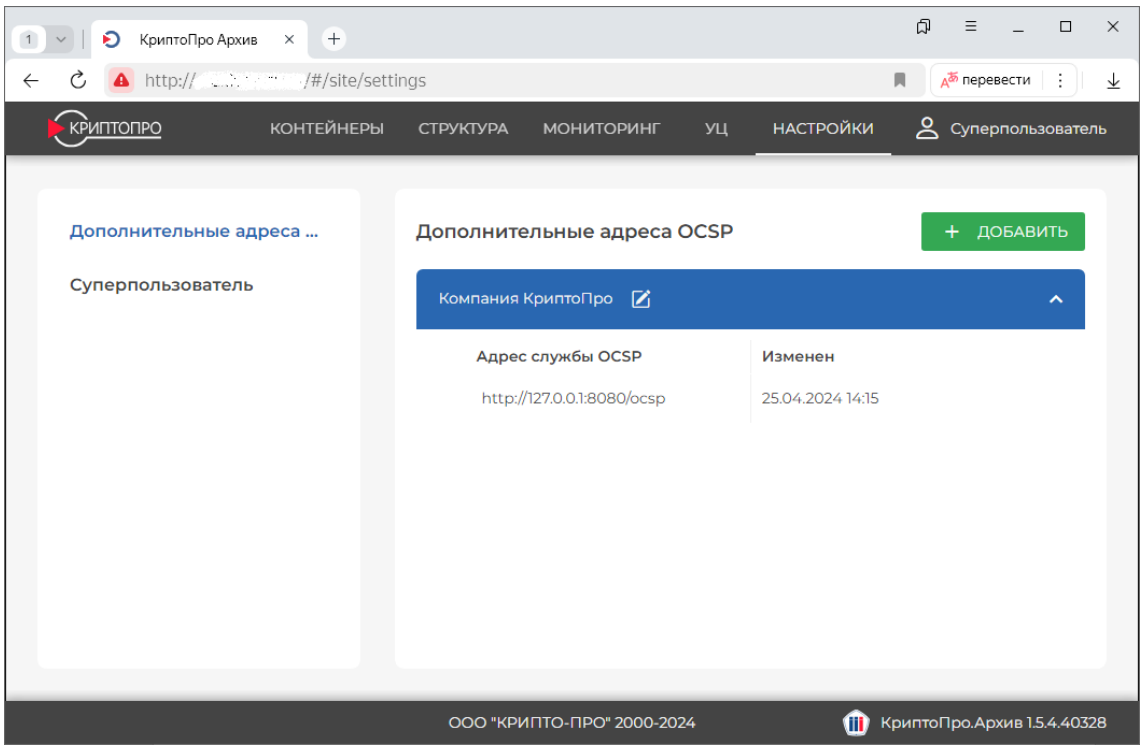
Пример заполнения вручную:



Пример указания сертификата:



Нажмите **Подтвердить**. После этого в списке появится добавленный дополнительный адрес службы OCSP:



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

3.14 Настройка хранилищ и информационных систем

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

3.14.1 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* (Рисунок 4). Хранилищ может быть несколько.

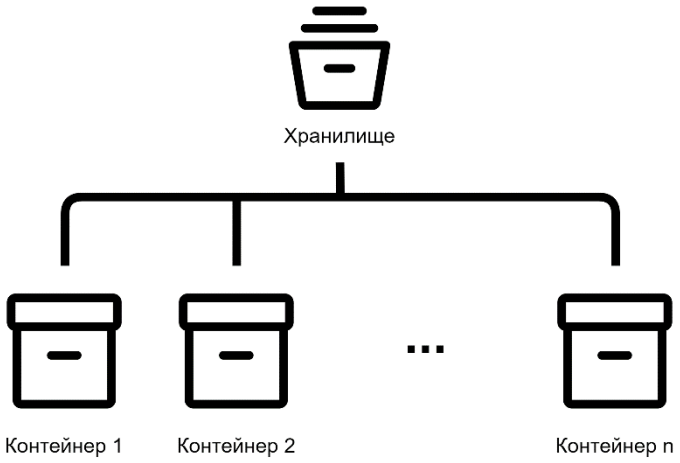


Рисунок 4. Хранилище с контейнерами

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 5).

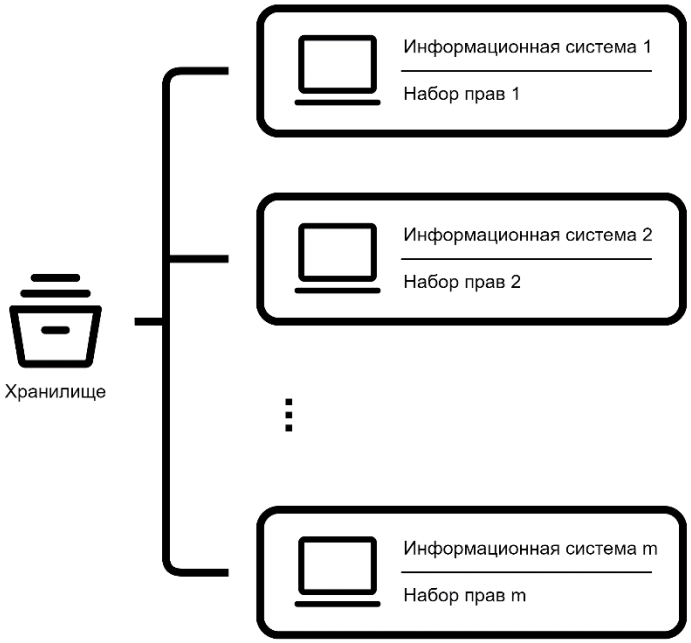
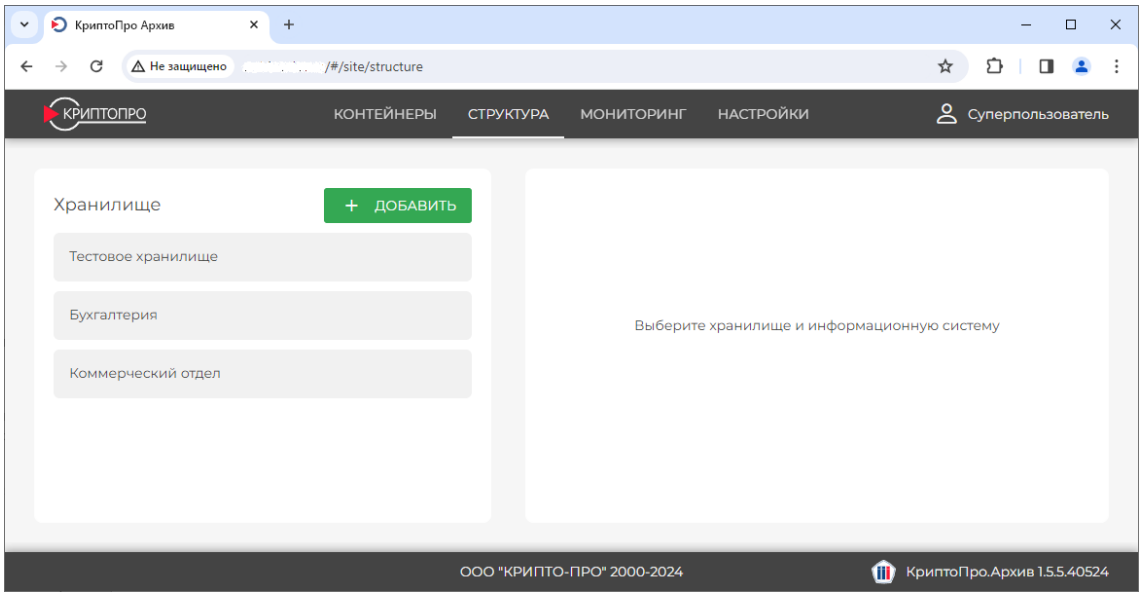


Рисунок 5. Хранилище с прикреплёнными к нему информационными системами

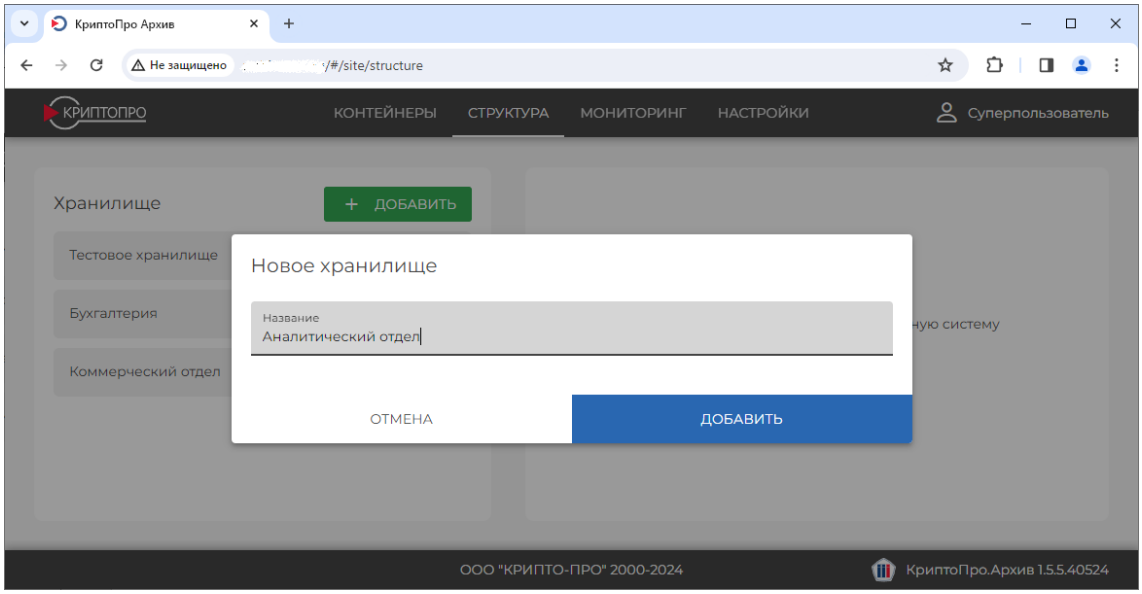
3.14.2 Первичная настройка

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

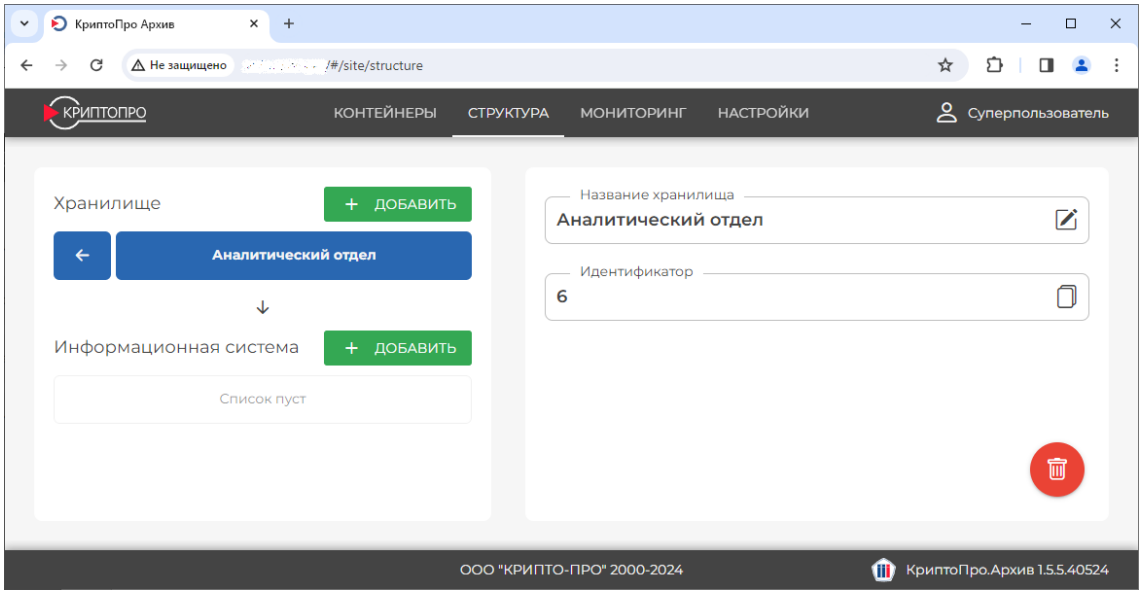
Для создания хранилища зайдите в административную панель от лица суперпользователя и перейдите на вкладку **Структура**:



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

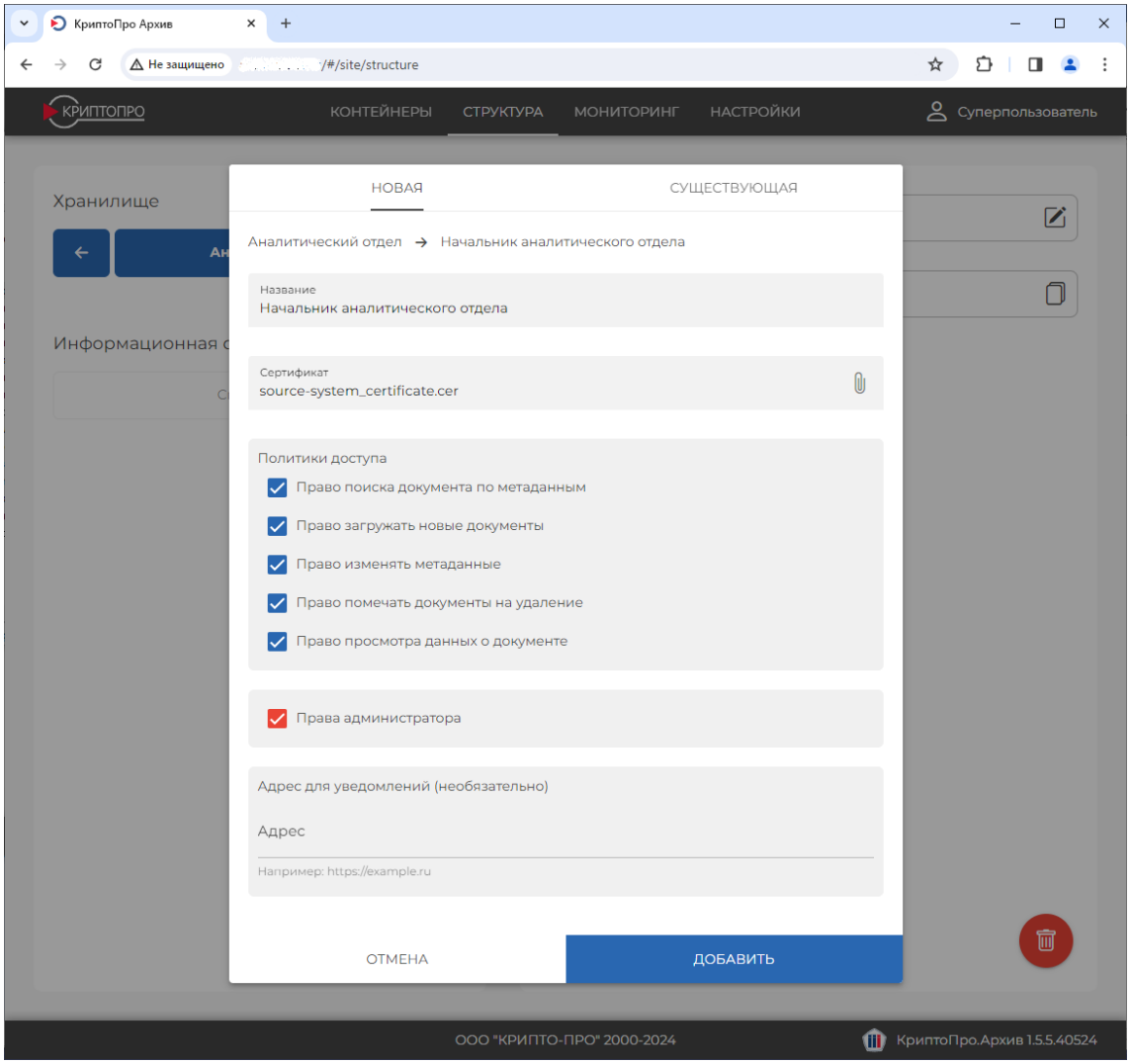


Созданное хранилище появится в списке хранилищ. Нажмите на него:



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. Дале закройте браузер и откройте его заново. Выберите сертификат созданной информационной системы.

3.14.3 Права информационных систем

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
Право управления хранилищем	• отправка контейнеров на повторную обработку • создание информационных систем без прав администратора в рамках хранилища

4 Обновление

В данной главе приведены инструкции по обновлению компонентов ПК КриптоПро Архив. Выборочное обновление компонентов возможно, но не рекомендуется.

4.1 Обновление КриптоПро Архив на ОС семейства Windows Server

В данном разделе приведена инструкция по обновлению ПК КриптоПро Архив на ОС семейства Windows Server.

4.1.1 Остановка запущенных служб

Перед обновлением остановите работающие компоненты КриптоПро Архив

- 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**)

4.1.2 Обновление КриптоПро Архив

Установите новую версию программы, не удаляя предыдущую.

4.1.3 Обновление базы данных

Выполните миграцию на новую версию базы данных для всех используемых баз данных.

4.1.3.1 Обновление базы данных PostgreSQL

Для этого в случае использования 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
```

4.1.3.2 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
```

4.1.4 Запуск служб

Запустите остановленные ранее службы.

4.2 Обновление КриптоПро Архив на ОС семейства Linux

В данном разделе приведена инструкция по обновлению ПК КриптоПро Архив на ОС семейства Linux.

4.2.1 Остановка запущенных служб

Перед обновлением остановите работающие компоненты КриптоПро Архив. Для этого выполните все или некоторые из следующих команд в зависимости от того, какие службы запущены на сервере:

```
sudo systemctl stop cp-archive_admin-api.service
sudo systemctl stop cp-archive_client-api.service
sudo systemctl stop cp-archive_signature-updater.service
sudo systemctl stop cp-archive_consumer.service
```

4.2.2 Обновление КриптоПро Архив

Установите новую версию программы, не удаляя предыдущую. Для этого в папке с новым дистрибутивом выполните

```
sudo ./install.sh
```

При необходимости обновите компоненты выборочно. Например, для обновления только admin-api и client-api выполните

```
sudo ./install.sh -c admin-api -c client-api
```

4.2.3 Обновление базы данных

Выполните миграцию на новую версию базы данных для всех используемых баз данных.

4.2.3.1 Обновление базы данных PostgreSQL

Для этого в случае использования PostgreSQL выполните следующую команду. В ней и в следующей командах замените строку подключения (параметр `--connection-string`) на используемую:

```
sudo /opt/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:

```
sudo /opt/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):

```
sudo /opt/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
```

4.2.3.2 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:

```
sudo /opt/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:

```
sudo /opt/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):

```
sudo /opt/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
```

4.2.4 Запуск служб

Запустите остановленные ранее службы. Для выполните все или некоторые из следующих команд в зависимости от того, какие службы были остановлены ранее:

```
sudo systemctl start cp-archive_admin-api.service
sudo systemctl start cp-archive_client-api.service
sudo systemctl start cp-archive_signature-updater.service
sudo systemctl start cp-archive_consumer.service
```

4.3 Особенности обновления версий

В данном разделе приведены дополнительные инструкции по обновлению.

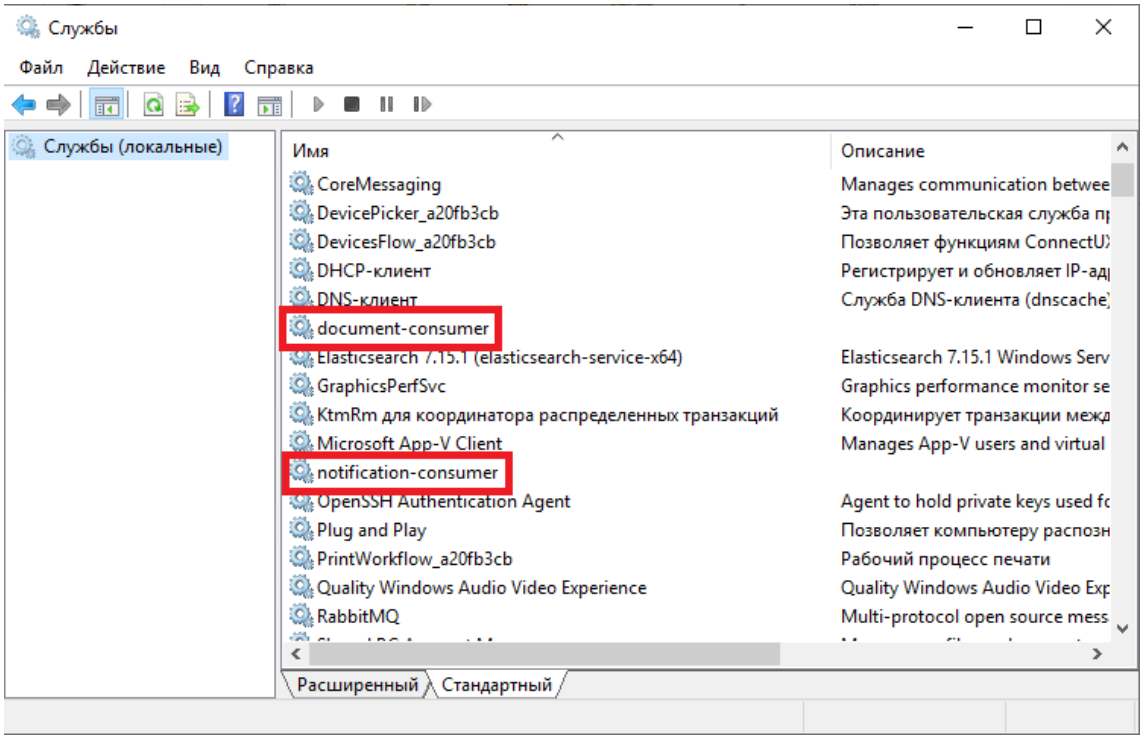
4.3.1 Особенности обновления до версии 1.5.4

Данное обновление объединяет программы document-consumer и notification-consumer в одну программу consumer с единой функциональностью. Не используемые более программы можно удалить штатным способом для используемой операционной системы. Ниже приведены подробные инструкции.

4.3.1.1 ОС семейства Windows Server

Для удаления более не используемых программ document-consumer и notification-consumer после обновления сперва остановите работающие службы, если они запущены, после чего удалите их. Для этого откройте приложение **Службы**, остановите и удалите службы, соответствующие приложениям document-consumer и notification-consumer. После этого в папке установки КриптоПро Архив (по умолчанию `C:\inetpub\cp-archive`) удалите папки document-consumer и notification-consumer.

В качестве проверки правильности выполнения действий убедитесь, что в приложении **Службы** отсутствуют выделенные ниже службы:



4.3.1.2 ОС семейства Linux

Для удаления более не используемых программ document-consumer и notification-consumer после обновления сперва остановите работающие службы, если они запущены:

```
sudo systemctl disable --now cp-archive_document-consumer.service
sudo systemctl disable --now cp-archive_notification-consumer.service
```

Далее удалите эти службы:

```
sudo apt remove cp-archive-document-consumer cp-archive-notification-consumer
```

Опционально удалите оставшиеся конфигурационные файлы служб:

```
sudo rm -r /etc/opt/cp-archive/document-consumer
sudo rm -r /etc/opt/cp-archive/notification-consumer

sudo rm -r /opt/cp-archive/document-consumer
sudo rm -r /opt/cp-archive/notification-consumer
```

5 Дополнительные инструкции

В данной главе содержатся дополнительные инструкции, которые помогут администратору отладить работу КриптоПро Архив.

5.1 Проверка работоспособности Elasticsearch

В данном разделе приведены инструкции для проверки работоспособности кластера Elasticsearch.

Предполагается доступ к серверу с установленным на нём Elasticsearch. По умолчанию служба работает по адресу `http://localhost:9200`. Для базовой проверки работоспособности можно отправить `GET`-запрос на этот адрес и получить в ответ JSON с следующим содержанием:


```
{
  "name": "<server_name>",
  "cluster_name": "elasticsearch",
  "cluster_uuid": "ZXop4rtISxmvmlzRBXkrVw",
  "version": {
    "number": "7.17.16",
    "build_flavor": "default",
    "build_type": "zip",
    "build_hash": "2b23fa076334f8d4651aeebe458a955a2ae23218",
    "build_date": "2023-12-08T10:06:54.672540567Z",
    "build_snapshot": false,
    "lucene_version": "8.11.1",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}
```


Для просмотра статуса («здоровья») кластера Elasticsearch выполните `GET`-запрос по адресу `http://localhost:9200/_cluster/health`. Пример содержимого ответа:


```
{
  "cluster_name": "elasticsearch",
  "status": "green",
  "timed_out": false,
  "number_of_nodes": 1,
  "number_of_data_nodes": 1,
  "active_primary_shards": 3,
  "active_shards": 3,
  "relocating_shards": 0,
  "initializing_shards": 0,
```

```
    "unassigned_shards": 0,
    "delayed_unassigned_shards": 0,
    "number_of_pending_tasks": 0,
    "number_of_in_flight_fetch": 0,
    "task_max_waiting_in_queue_millis": 0,
    "active_shards_percent_as_number": 100.0
}
```

Если в поле `$.status` ответа написано `"green"` или `"yellow"`, это означает, что кластер находится в функционирующем состоянии. Если написано `"red"`, это означает, что в работе кластера возникла ошибка. Подробнее о конечной точке `health` см. официальную документацию API Elasticsearch.

5.2 Проверка работоспособности Python 3

В данном разделе приведены инструкции проверки работоспособности Python 3.

5.2.1 Проверка работоспособности Python 3 на ОС семейства Windows Server

Для проверки работоспособности Python 3 на ОС семейства Windows Server откройте PowerShell от имени администратора и выполните команду `python`. Если Python работоспособен, должна запуститься REPL-среда, выглядящая примерно следующим образом:

```
Python 3.12.1 (tags/v3.12.1:2305ca5, Dec  7 2023, 22:03:25) [MSC v.1937 64 bit (AMD64)]
on win32
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Для выхода введите `exit()` и нажмите **Enter**.

5.3 Проверка работоспособности RabbitMQ

В данном разделе приведены инструкции по проверке работоспособности кластера RabbitMQ.

5.3.1 Проверка работоспособности RabbitMQ на ОС семейства Windows Server

Предполагается, что программа RabbitMQ версии 3.12.11 была установлена по стандартному пути `C:\Program Files\RabbitMQ Server`. При несовпадении этих настроек откорректируйте команды ниже.

Для проверки работоспособности RabbitMQ на ОС семейства Windows Server сперва откройте программу **Службы** и убедитесь, что служба **RabbitMQ** запущена. Далее откройте PowerShell от имени администратора и выполните следующие команды.

```
cd 'C:\Program Files\RabbitMQ Server\rabbitmq_server-3.12.11\sbin'
.\rabbitmqctl.bat status
```

Если ответ начинается с сообщения `Status of node <node_name> ...`, за которым следует описание параметров сервера, RabbitMQ работает исправно.

Если ответ начинается с сообщения `Error: unable to perform an operation on node '<node_name>'. Please see diagnostics information and suggestions below`, RabbitMQ не работает. В этом случае внимательно изучите сообщение, которое написано в выводе. Если очевидных сетевых ошибок не выявлено, попробуйте перезапустить службу с помощью команды

```
.\rabbitmq-server.bat -detached
```

Снова выполните `.\rabbitmqctl.bat status`. Если ошибка остаётся, переустановите службу. Для этого выполните

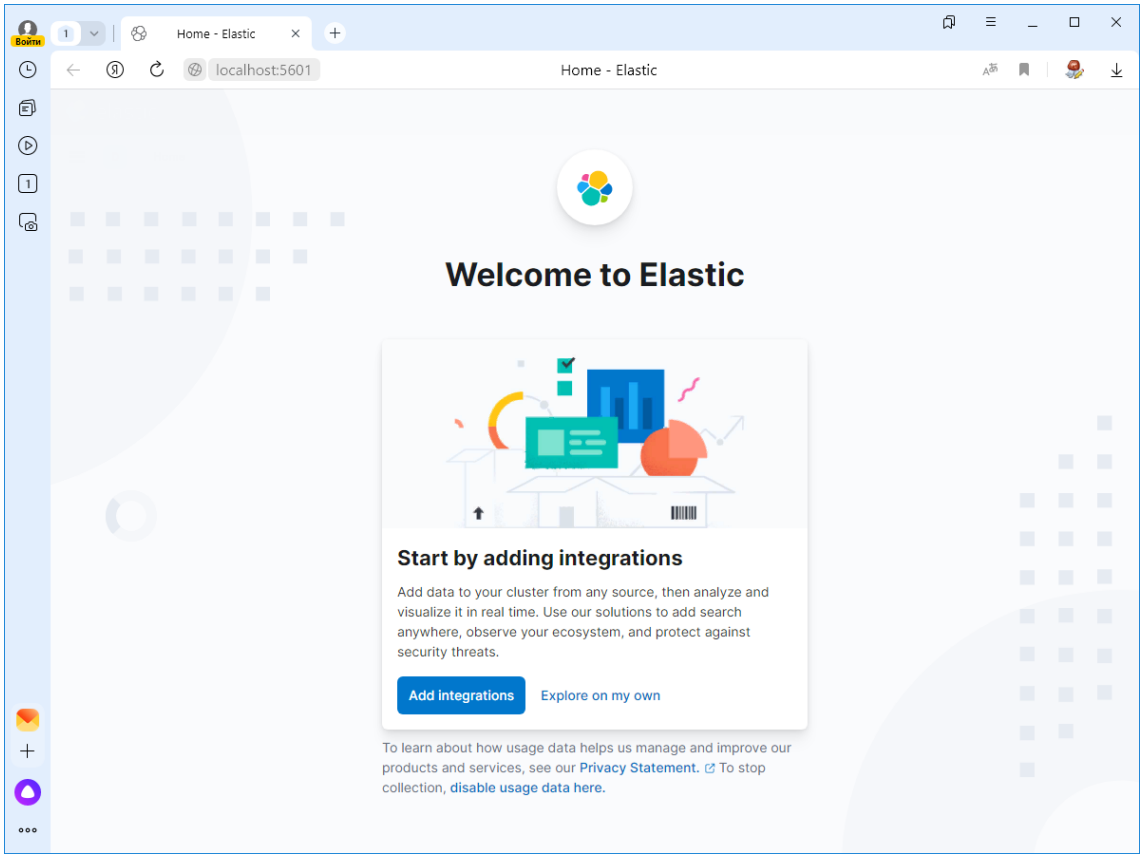
```
.\rabbitmq-service.bat remove
.\rabbitmq-service.bat install
.\rabbitmq-server.bat -detached
```

Снова проверьте вывод команды `.\rabbitmqctl.bat status`.

5.4 Проверка работоспособности Kibana

В данном разделе приведены инструкции по проверке работоспособности Kibana. Предполагается, что служба Kibana запущена на сервере.

По умолчанию Kibana работает по адресу `http://localhost:5601`. Перейдите по этому адресу в браузере. Должна открыться приветственная страница:

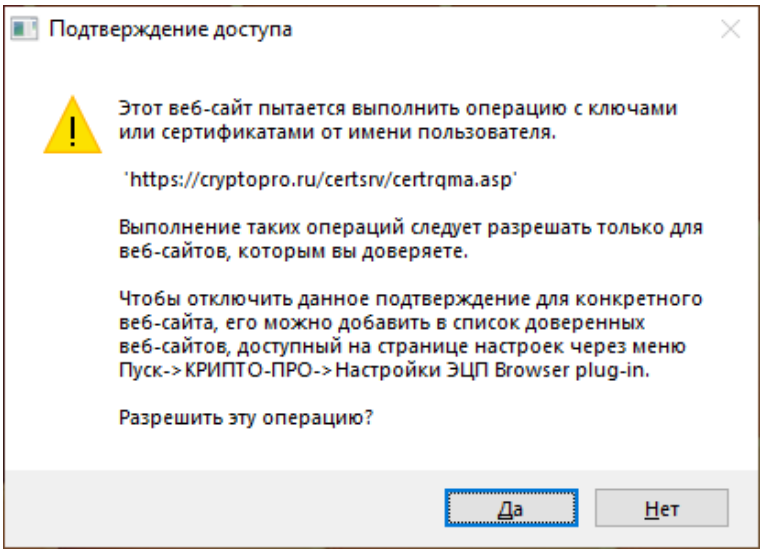


5.5 Выпуск тестового сертификата сервера с использованием тестового УЦ компании КриптоПро

ВАЖНО: созданный таким образом сертификат **не допускается** использовать в промышленных средах.

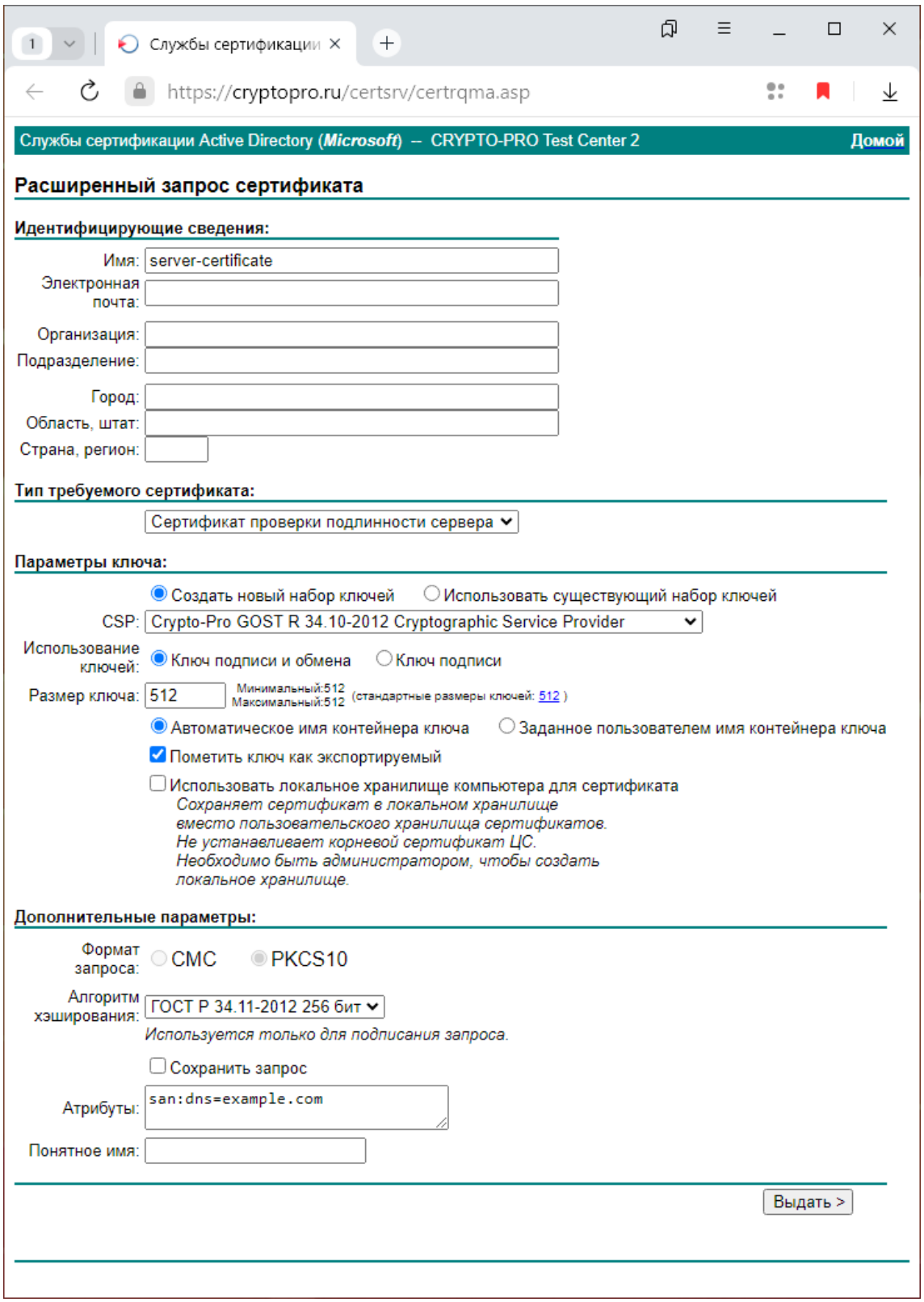
Установите КриптоПро CSP и КриптоПро ЭЦП Browser plug-in. Перейдите на сайт службы сертификации CRYPTO-PRO Test Center 2 с использованием браузера, поддерживающего алгоритмы ГОСТ: Яндекс.Браузер или Chromium-Gost. В примере ниже используется Яндекс.Браузер.

В появившемся окне выберите **Да**:

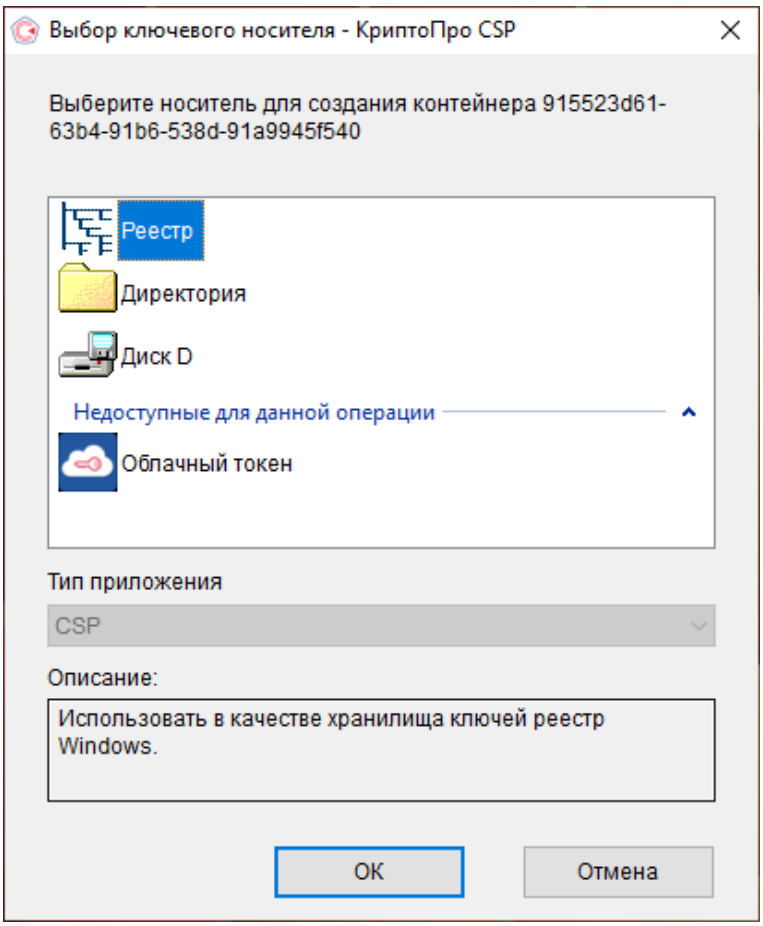


Введите имя сертификата в поле **Имя**, выберите **Тип требуемого сертификата**: «Сертификат проверки подлинности сервера», отметьте пункт **Пометить ключ как экспортируемый** и в поле **Атрибуты** опционально укажите дополнительное имя субъекта следующим образом: `san:dns=<domain.name>`, где `<domain.name>` замените на доменное имя сервера. При необходимости использования нескольких дополнительных имён субъекта используйте синтаксис `san:dns=<domain.name1>&dns=<domain.name2>...`.

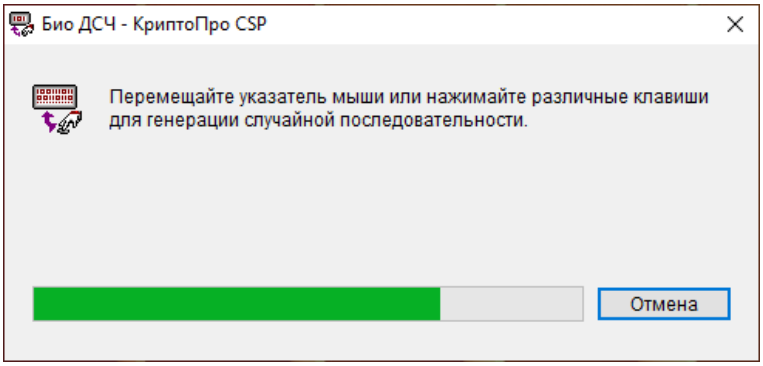
Пример заполненной страницы:



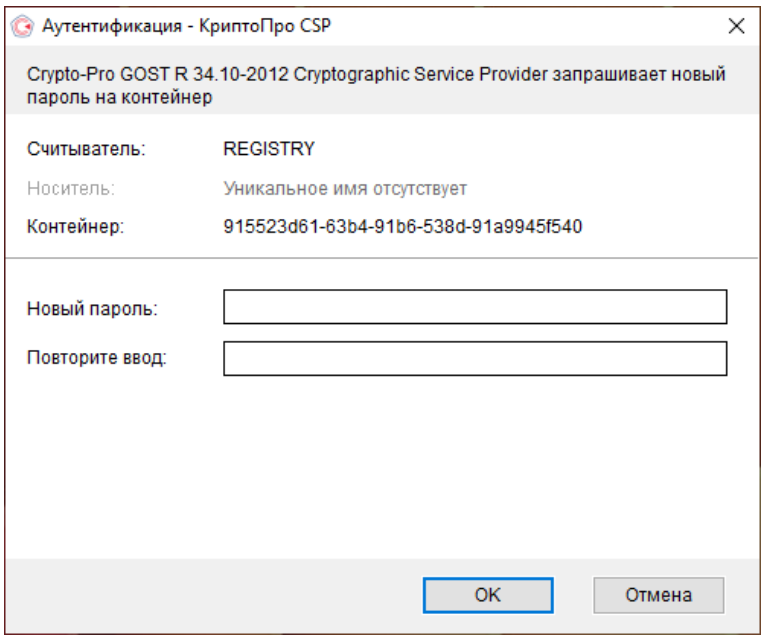
Нажмите **Выдать**. В качестве ключевого носителя выберите **Реестр** и нажмите **ОК**:



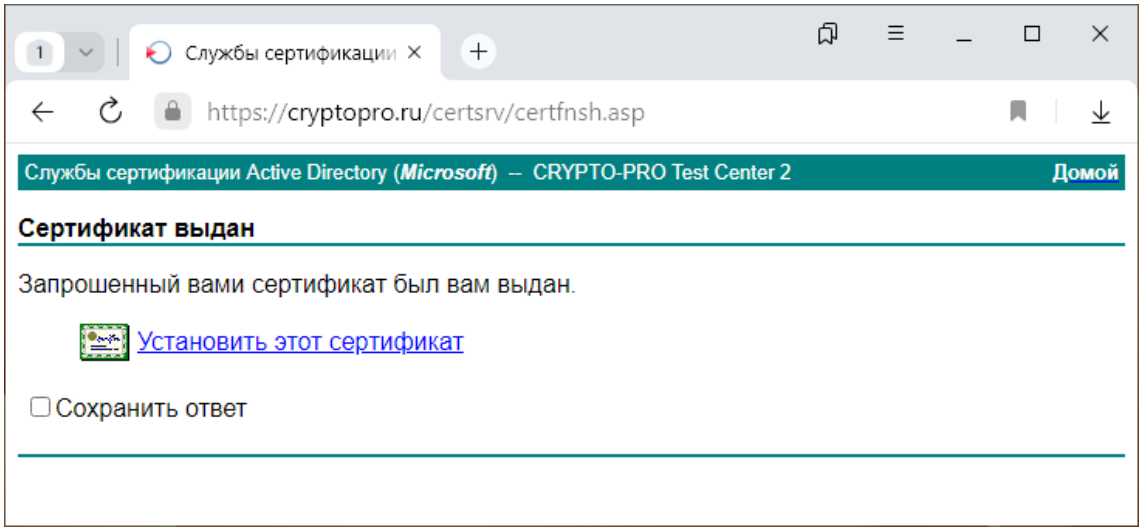
Следуйте инструкциям для генерации случайной последовательности:



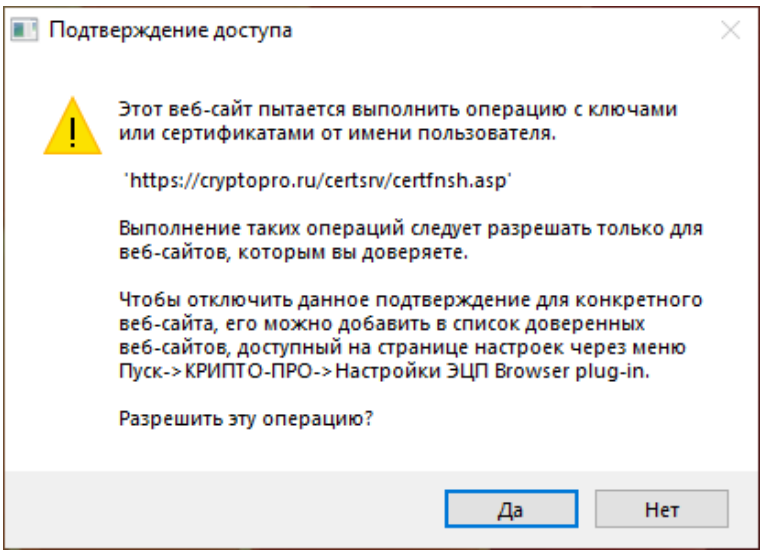
Не устанавливая пароль, нажмите **ОК**:



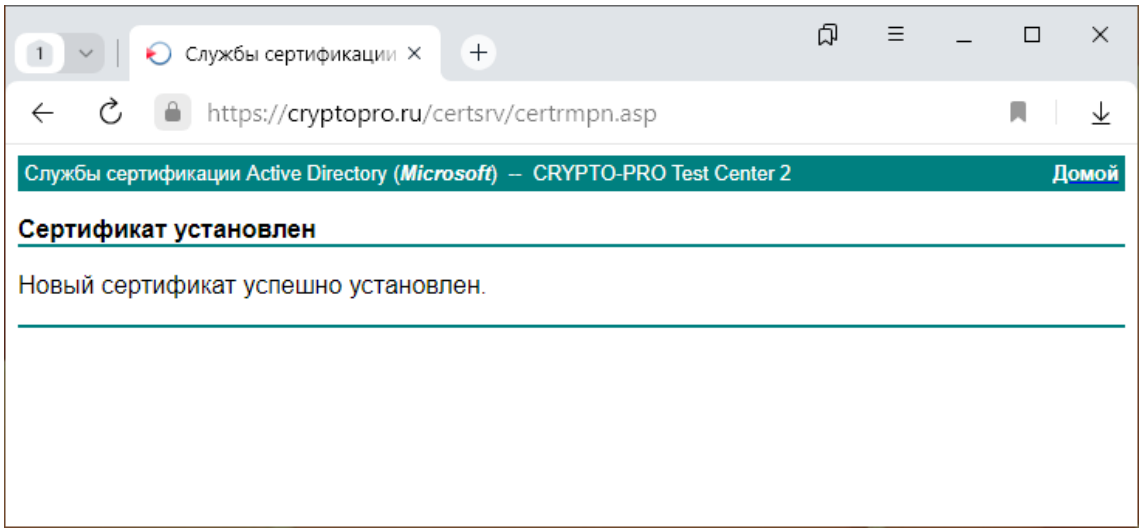
В окне браузера нажмите **Установить этот сертификат**:



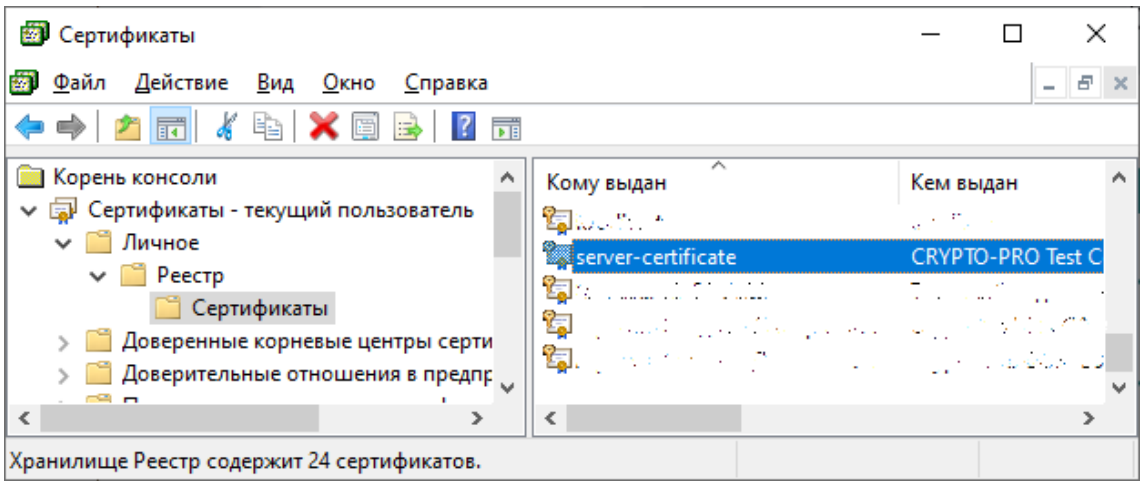
Подтвердите выполнение операции, нажав **Да**:



В окне браузера появится уведомление о том, что сертификат успешно установлен:

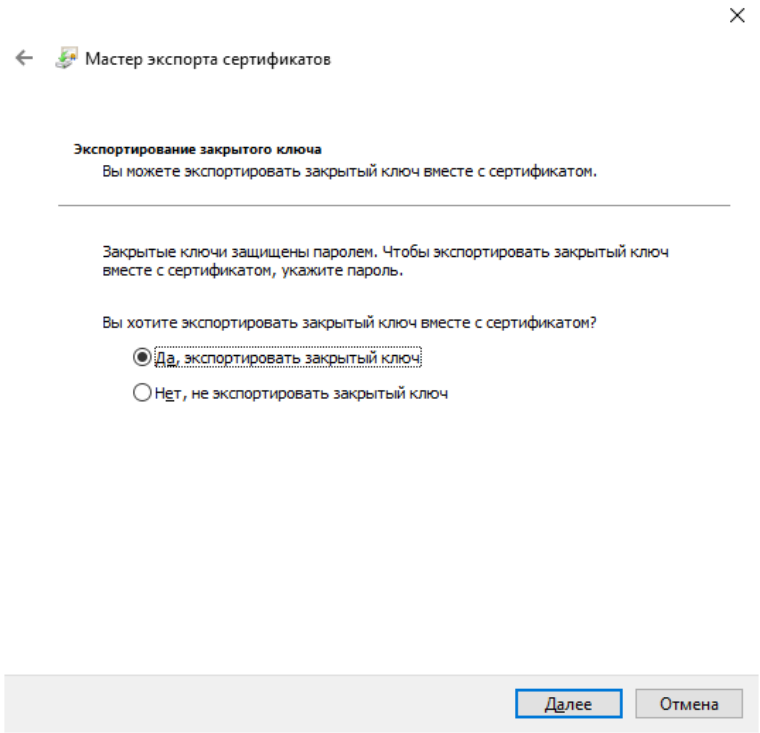


Сертификат можно экспортировать из хранилища **Текущего пользователя** в оснастке **Сертификаты**:

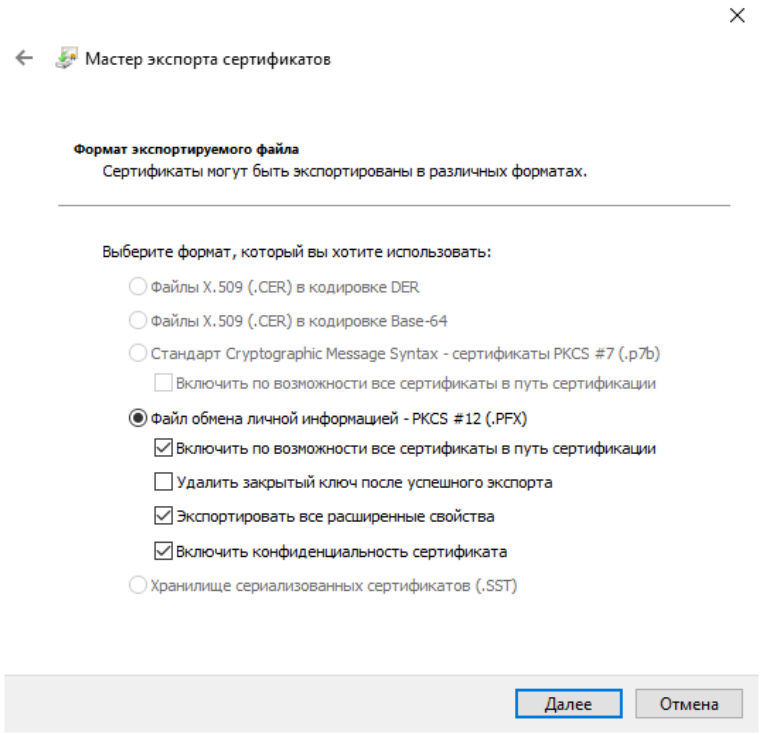


Для экспорта нажмите на сертификат в оснастке правой кнопкой мыши и выберите **Все задачи** > **Экспорт…** > **Далее**.

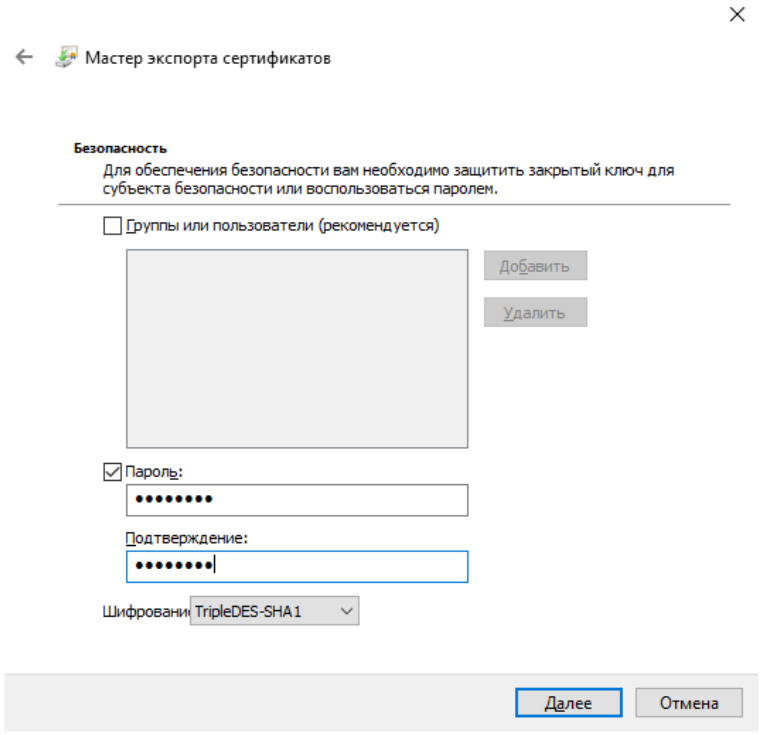
Отметьте пункт **Да, экспортировать закрытый ключ** и нажмите **Далее**:



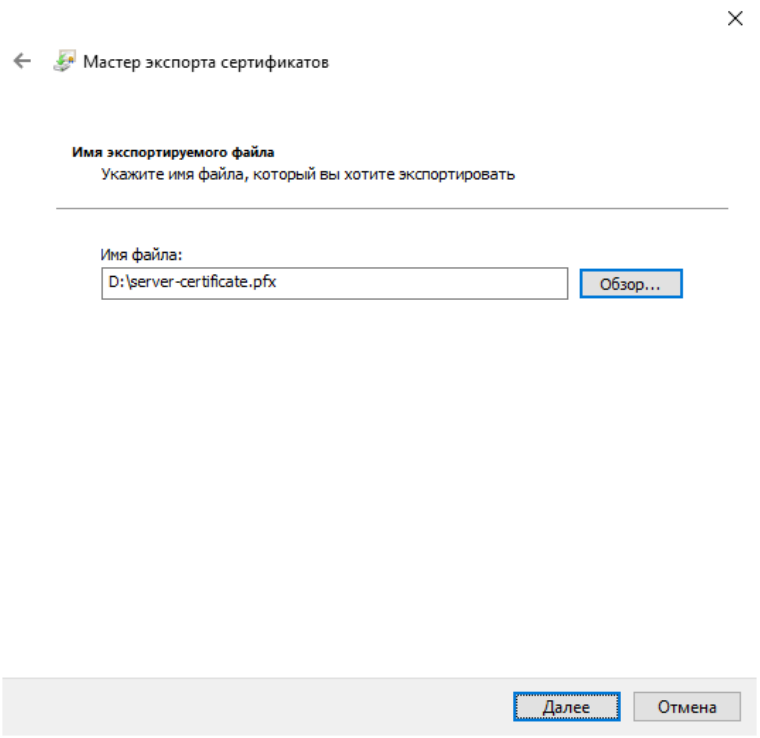
Выберите **Экспортировать все расширенные свойства** и нажмите **Далее**:



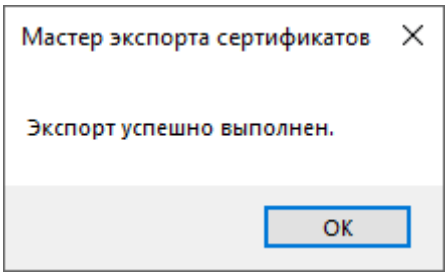
Выберите **Пароль**, задайте пароль для создаваемого PFX и нажмите **Далее**:



Укажите путь для экспорта, нажмите **Далее** и **Готово:**



Появится уведомление об успешном экспорте сертификата с закрытым ключом, а сертификат будет экспортирован по указанному пути:



Полученный сертификат готов для установки на сервер с КриптоПро Архив.

ВАЖНО: созданный таким образом сертификат **не допускается** использовать в промышленных средах.