

КриптоПро

**"Центр Мониторинга"**

Руководство по установке и настройке

# Содержание

## Центр Мониторинга

Общее описание Центра Мониторинга

Лицензирование Центра Мониторинга

Типы лицензий

Ввод лицензии

Принцип работы Центра Мониторинга

Журнал событий Центра Мониторинга

Системные требования и права доступа

Установка развертывание обновление и удаление Центра Мониторинга

Установка

Развертывание

Настройка nginx

Удаление

Обновление

Порядок настройки Центра Мониторинга

Экземпляры тестирования

Тесты

Создание экземпляра теста из шаблона тестов

Добавление теста к экземпляру тестирования

Перечень тестов и их параметров

Общие настройки

Основные настройки

Настройка почтовой рассылки

Настройка мониторинга журналов

Веб-служба

# КриптоПро Центр Мониторинга (\*nix)

Настоящий документ содержит описание, а также руководство по установке и настройке программного комплекса «КриптоПро Центр Мониторинга».

Программный комплекс «КриптоПро Центр Мониторинга» — решение класса Network Performance Monitoring and Diagnostics (NPMD), предназначенное для мониторинга работоспособности ИТ-инфраструктуры системы электронной подписи и удостоверяющего центра, включающей [ПК «КриптоПро Ключ»](#), [СЭП «КриптоПро DSS»](#), [ПАК «КриптоПро УЦ»](#), [ПАК «Службы УЦ»](#) и [ПАКМ «КриптоПро HSM»](#) и оперативного уведомления администраторов о выявленных сбоях, ошибках функционирования и прочих нештатных ситуациях.

В этом документе:

- [Общее описание Центра Мониторинга](#)
- [Лицензирование Центра Мониторинга](#)
- [Принцип работы Центра Мониторинга](#)
- [Журнал событий Центра Мониторинга](#)
- [Системные требования и права доступа](#)
- [Установка, удаление, развертывание и обновление Центра Мониторинга](#)
- [Развертывание Центра Мониторинга](#)
- [Настройка Центра Мониторинга](#)

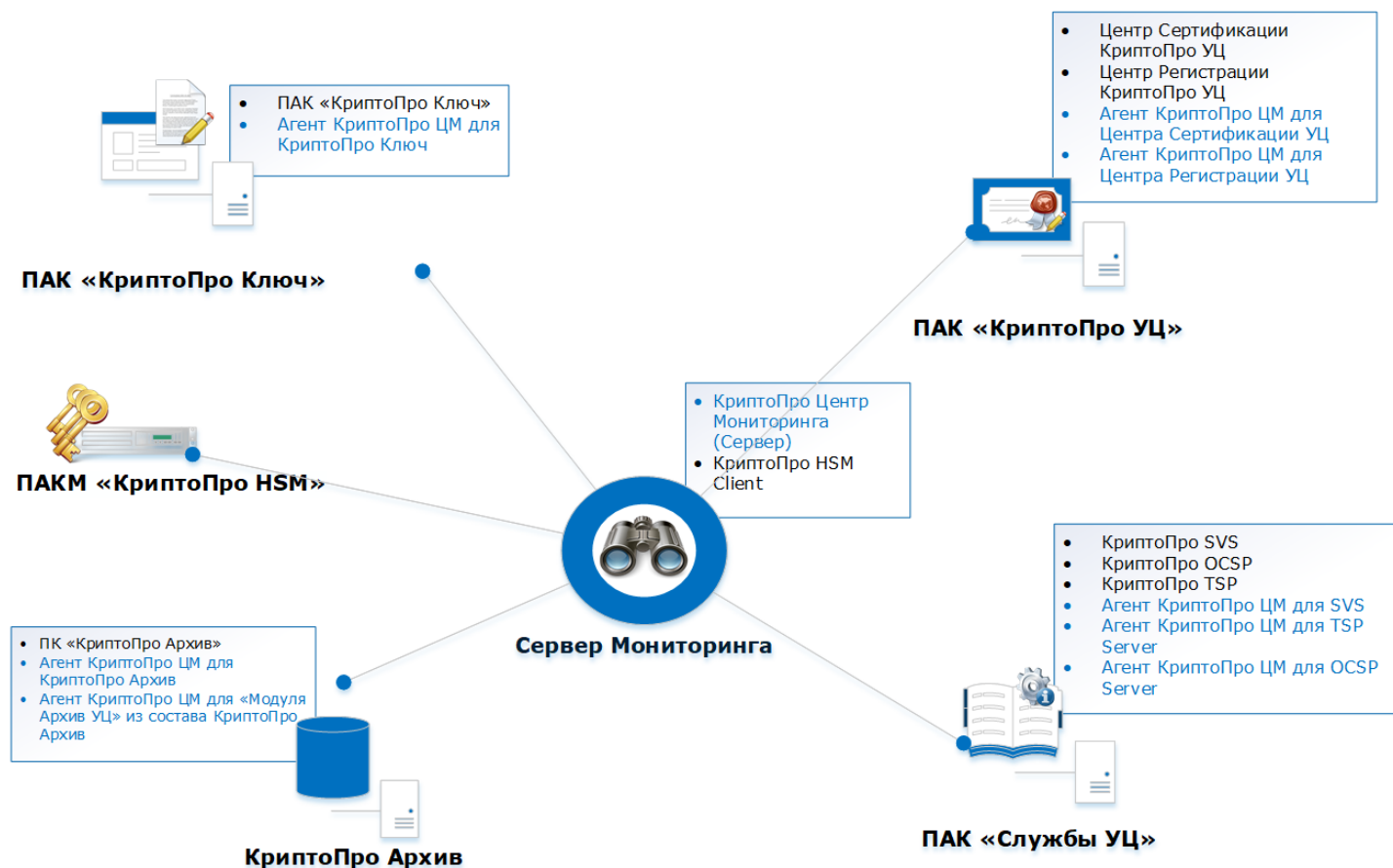
# Общее описание КристоПро Центр Мониторинга

Программный комплекс «КристоПро Центр Мониторинга» — решение класса Network Performance Monitoring and Diagnostics (NPM/D), предназначенное для мониторинга работоспособности ИТ-инфраструктуры системы электронной подписи и удостоверяющего центра, включающей ПК «КристоПро Ключ», ПАК «КристоПро УЦ» версии 2.0, ПАК «Службы УЦ» (OCSP, TSP, SVS), ПК «КристоПро Архив» и ПАКМ «КристоПро HSM» и оперативного уведомления администраторов о выявленных сбоях, ошибках функционирования и прочих нештатных ситуациях.

Каждый экземпляр программного комплекса «КристоПро Центр Мониторинга» может принадлежать к одному из двух типов:

- **Сервер Мониторинга** «КристоПро Центр Мониторинга» (далее – Сервер Мониторинга)
- **Агенты** «КристоПро Центр Мониторинга» (далее — Агенты). В настоящее время доступны следующие Агенты:
  - Агент КристоПро Центр Мониторинга для **КристоПро Ключ**;
  - Агент КристоПро Центр Мониторинга для **Центра Сертификации УЦ**;
  - Агент КристоПро Центр Мониторинга для **Центра Регистрации УЦ**;
  - Агент КристоПро Центр Мониторинга для **КристоПро TSP Server**;
  - Агент КристоПро Центр Мониторинга для **КристоПро OCSP Server**;
  - Агент КристоПро Центр Мониторинга для **КристоПро SVS**;
  - Агент КристоПро Центр Мониторинга для **КристоПро Архив**.

На рисунке ниже представлена схема взаимодействия компонентов ПК «КристоПро Центр Мониторинга». Для удобства представления на схеме для Сервера Мониторинга выделена отдельная рабочая станция, а Агенты распределены по серверам в соответствии с размещением программно-аппаратных комплексов, мониторинг которых необходимо осуществлять. Отдельно на схеме выделен ПАКМ КристоПро HSM, Агент для которого не требуется, так как мониторинг КристоПро HSM производится в рамках мониторинга КристоПро Ключ. Данная конфигурация не является единственным вариантом размещения компонентов ПК «КристоПро Центр Мониторинга» и может быть изменена в соответствии с требованиями к inspected программно-аппаратным комплексам.



Каждый экземпляр КристоПро Центр Мониторинга, вне зависимости от того, является ли он Сервером Мониторинга или одним из Агентов, имеет одинаковый принцип работы, системные требования и порядок настройки согласно настоящему документу.

## Примечание

Основным различием экземпляров (Сервера и Агентов) КристоПро Центр Мониторинга является лицензия, определяющая роль экземпляра в программном комплексе.

## Лицензирование КристоПро Центр Мониторинга

### Сервер Мониторинга

Сервер Мониторинга "КристоПро Центр Мониторинга" выполняет следующие задачи:

- Мониторинг серверов с помощью удаленных тестов;
- Централизованный сбор информации об удаленных тестах и проверках, выполняемых Агентами «КристоПро Центр Мониторинга»;
- Рассылка [почтовых уведомлений](#) об ошибках и предупреждениях;
- Передача интегрируемым системам результатов удаленных проверок и проверок, выполняемых Агентами;
- Интеграция с балансировщиками для определения доступности объектов мониторинга по результатам тестов.

Помимо перечисленного необходимо отметить, что Сервер Мониторинга обладает возможностью выполнять локальные тесты (в случае, если какие-либо объекты мониторинга расположены вместе с ним на одной рабочей станции).

Список доступных тестов для Сервера Мониторинга определяется [лицензией на КристоПро Центр Мониторинга](#).

### Агенты

Агенты, функционирующие в составе ПК «КристоПро Центр Мониторинга», выполняют следующие задачи:

- Мониторинг серверов с помощью локальных и удаленных тестов в рамках действующей [лицензии](#);
- Рассылка [почтовых уведомлений](#) и об ошибках и предупреждениях.

Список доступных тестов для Агента определяется [соответствующей лицензией](#).

## Лицензирование Центра Мониторинга

### Примечание

В данном разделе описаны типы лицензий для КриптоПро Центр Мониторинга в ОС \*nix, их особенности и влияние на работу программного комплекса. Процедура ввода лицензии описана в разделе [Ввод лицензии](#).

Тип лицензии КriptoПро Центр Мониторинга определяет доступность работы с экземплярами тестирования и экземплярами тестов. Если лицензия не введена или истекла, становится недоступным создание новых экземпляров тестирования, настройка тестов и тестирование. Существуют следующие типы лицензий на КriptoПро Центр Мониторинга:

**Лицензия по умолчанию.** Данная лицензия не имеет ограничения в работе с экземплярами тестирования и экземплярами тестов. Активируется автоматически при установке КриптоПро Центр Мониторинга и действует 3 месяца с момента установки. После ввода лицензии любого другого типа Лицензия по умолчанию отключается. После удаления всех лицензий любого типа Лицензия по умолчанию возвращается.

## Примечание

Срок действия Лицензии по умолчанию отсчитывается с момента создания экземпляра сервиса и не приостанавливается при вводе другой лицензии. Иными словами, если использовать другие лицензии 3 месяца, а потом вернуться к Лицензии по умолчанию, она окажется истекшей.

**Лицензия на право использования ПК «КриптоПро Центр Мониторинга» на одном сервере.** Данная лицензия не имеет ограничений на работу с экземплярами тестирования и экземплярами тестов. В лицензии явно прописан срок окончания действия. При вводе заменяет Лицензию по умолчанию.

**Лицензия на право использования «Агент КriptoПро Центр Мониторинга».** Данная лицензия имеет ограничения на работу с экземплярами тестирования и экземплярами тестов. При вводе заменяет Лицензию по умолчанию. Одновременно на одном сервере может быть введено несколько лицензий на право использования различных Агентов.

## Внимание!

Для работы некоторых тестов могут потребоваться дополнительные лицензии:

- КриптоПро TSP Client и КриптоПро OCSP Client из состава Служб УЦ 2.0;
- КриптоПро CSP 5.0.

В Таблице 1 указаны доступные для каждой лицензии экземпляры тестирования и тесты.

## Настройка экземпляров тестирования

## Настройка тестов

**Таблица 1 — Соответствие лицензий КriptoПро Центр Мониторинга и доступных экземпляров тестов**

Вид лицензии	Доступные экземпляры тестирования	Доступные экземпляры тестов
По умолчанию	Все	Все
КриптоПро Центр Мониторинга	Все	Все

ВИД ЛИЦЕНЗИИ	ДОСТУПНЫЕ ЭКЗЕМПЛЯРЫ ТЕСТИРОВАНИЯ	ДОСТУПНЫЕ ЭКЗЕМПЛЯРЫ ТЕСТОВ
Агент КристоПро Центр Мониторинга для КристоПро Ключ	Нетипизированный экземпляр, КристоПро Ключ, КристоПро HSM	<p>Тестовая подпись</p> <p>Тест криптопровайдеров Сервиса Подписи КристоПро Ключ</p> <p>Тест доступности обработчика УЦ</p> <p>Загрузка журналов HSM</p> <p>Тест указанного криптопровайдера</p> <p>Тест указанного сертификата</p> <p>Тест указанной базы данных</p> <p>Тест доступности указанной веб-службы</p> <p>Тест сроков действия CRL</p> <p>Получение журналов Агента Мониторинга</p> <p>Тест состояния удаленного Агента Мониторинга</p> <p>Тест лицензий HSM</p> <p>Тест состояния HSM</p> <p>Тест указанного скрипта</p> <p>Тест TSP-службы</p> <p>Тест OCSP-службы</p>
Агент КристоПро Центр Мониторинга для Центра Сертификации УЦ	Нетипизированный экземпляр, КристоПро HSM	<p>Тест сроков действия CRL</p> <p>Тест указанного криптопровайдера</p> <p>Тест указанного сертификата</p> <p>Тест указанной базы данных</p> <p>Тест доступности указанной веб-службы</p> <p>Получение журналов Агента Мониторинга</p> <p>Тест состояния удаленного Агента Мониторинга</p> <p>Тест лицензий HSM</p> <p>Тест состояния HSM</p> <p>Тест указанного скрипта</p> <p>Загрузка журналов HSM</p> <p>Тест состояния очереди nats-streaming-server</p>

ВИД ЛИЦЕНЗИИ	ДОСТУПНЫЕ ЭКЗЕМПЛЯРЫ ТЕСТИРОВАНИЯ	ДОСТУПНЫЕ ЭКЗЕМПЛЯРЫ ТЕСТОВ
Агент КриптоПро Центр Мониторинга для Центра Регистрации УЦ	Нетипизированный экземпляр	<p>Тест сроков действия CRL</p> <p>Тест указанного криптопровайдера</p> <p>Тест указанного сертификата</p> <p>Тест указанной базы данных</p> <p>Тест доступности указанной веб-службы</p> <p>Получение журналов Агента Мониторинга</p> <p>Тест состояния удаленного Агента Мониторинга</p> <p>Тест указанного скрипта</p> <p>Тест состояния очереди nats-streaming-server</p>
Агент КриптоПро Центр Мониторинга для OCSP Server	Нетипизированный экземпляр	<p>Тест сроков действия CRL</p> <p>Тест указанного сертификата</p> <p>Тест указанного криптопровайдера</p> <p>Тест указанной базы данных</p> <p>Тест доступности указанной веб-службы</p> <p>Получение журналов Агента Мониторинга</p> <p>Тест состояния удаленного Агента Мониторинга</p> <p>Тест указанного скрипта</p> <p>Тест OCSP-службы</p> <p>Тест синхронизации времени служб TSP и OCSP</p>
Агент КриптоПро Центр Мониторинга для TSP Server	Нетипизированный экземпляр	<p>Тест указанного сертификата</p> <p>Тест указанного криптопровайдера</p> <p>Тест указанной базы данных</p> <p>Тест доступности указанной веб-службы</p> <p>Получение журналов Агента Мониторинга</p> <p>Тест состояния удаленного Агента Мониторинга</p> <p>Тест указанного скрипта</p> <p>Тест TSP-службы</p>

ВИД ЛИЦЕНЗИИ	ДОСТУПНЫЕ ЭКЗЕМПЛЯРЫ ТЕСТИРОВАНИЯ	ДОСТУПНЫЕ ЭКЗЕМПЛЯРЫ ТЕСТОВ
Агент КriptoПро Центр Мониторинга для SVS	Нетипизированный экземпляр	<p>Тест указанного сертификата</p> <p>Тест указанного криптопровайдера</p> <p>Тест указанной базы данных</p> <p>Тест доступности указанной веб-службы</p> <p>Получение журналов Агента Мониторинга</p> <p>Тест состояния удаленного Агента Мониторинга</p> <p>Тест указанного скрипта</p> <p>Тест состояния очереди nats-streaming-server</p> <p>Тест OCSP-службы</p>
Агент КriptoПро Центр Мониторинга для КriptoПро Архив	Нетипизированный экземпляр	<p>Тест повторного усовершенствования подписи КriptoПро Архив</p> <p>Тест статуса контейнера КriptoПро Архив</p> <p>Тест состояния Elasticsearch</p> <p>Тест состояния ManticoreSearch</p> <p>Тест состояния RabbitMQ</p>

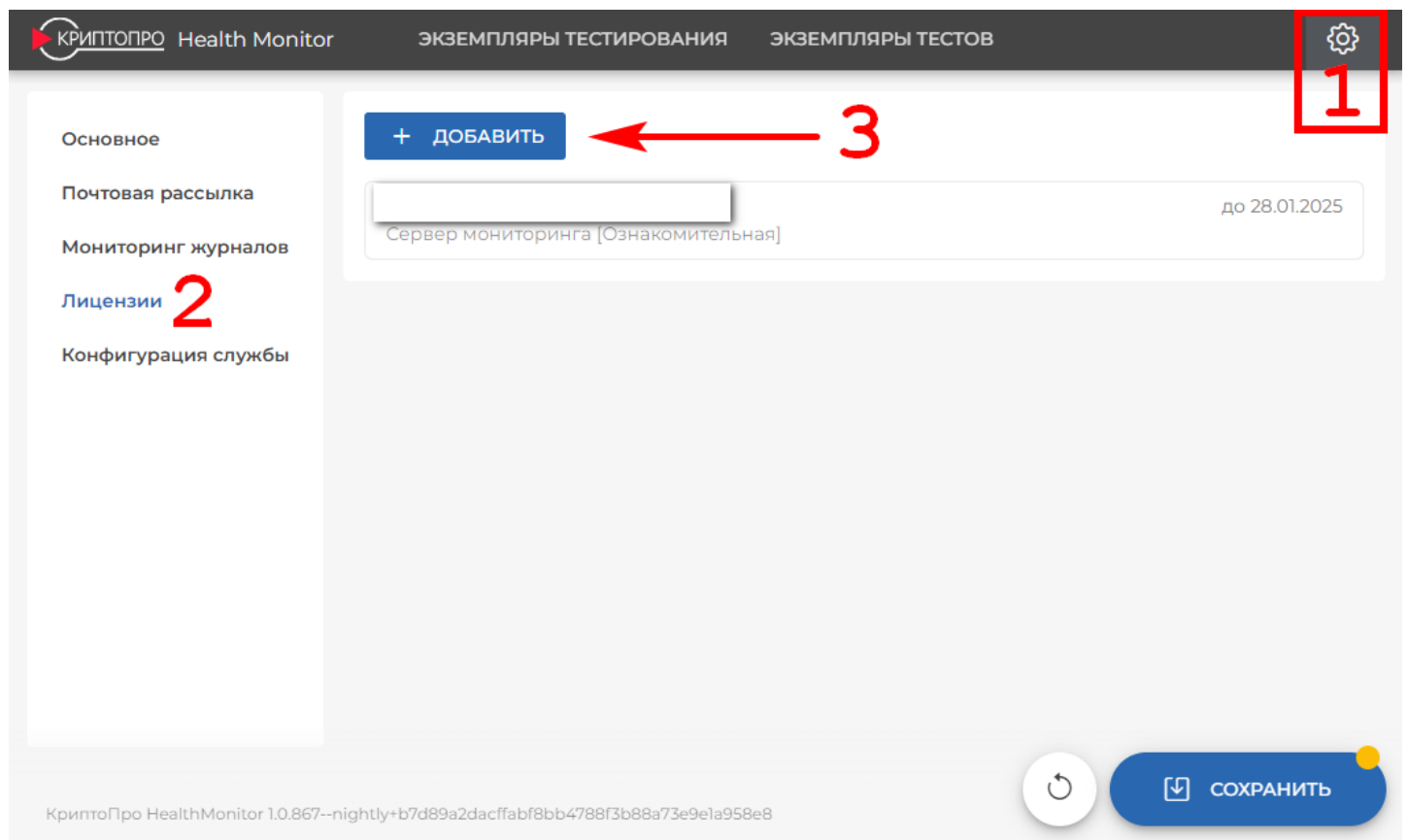
# Настройка лицензии

## Внимание!

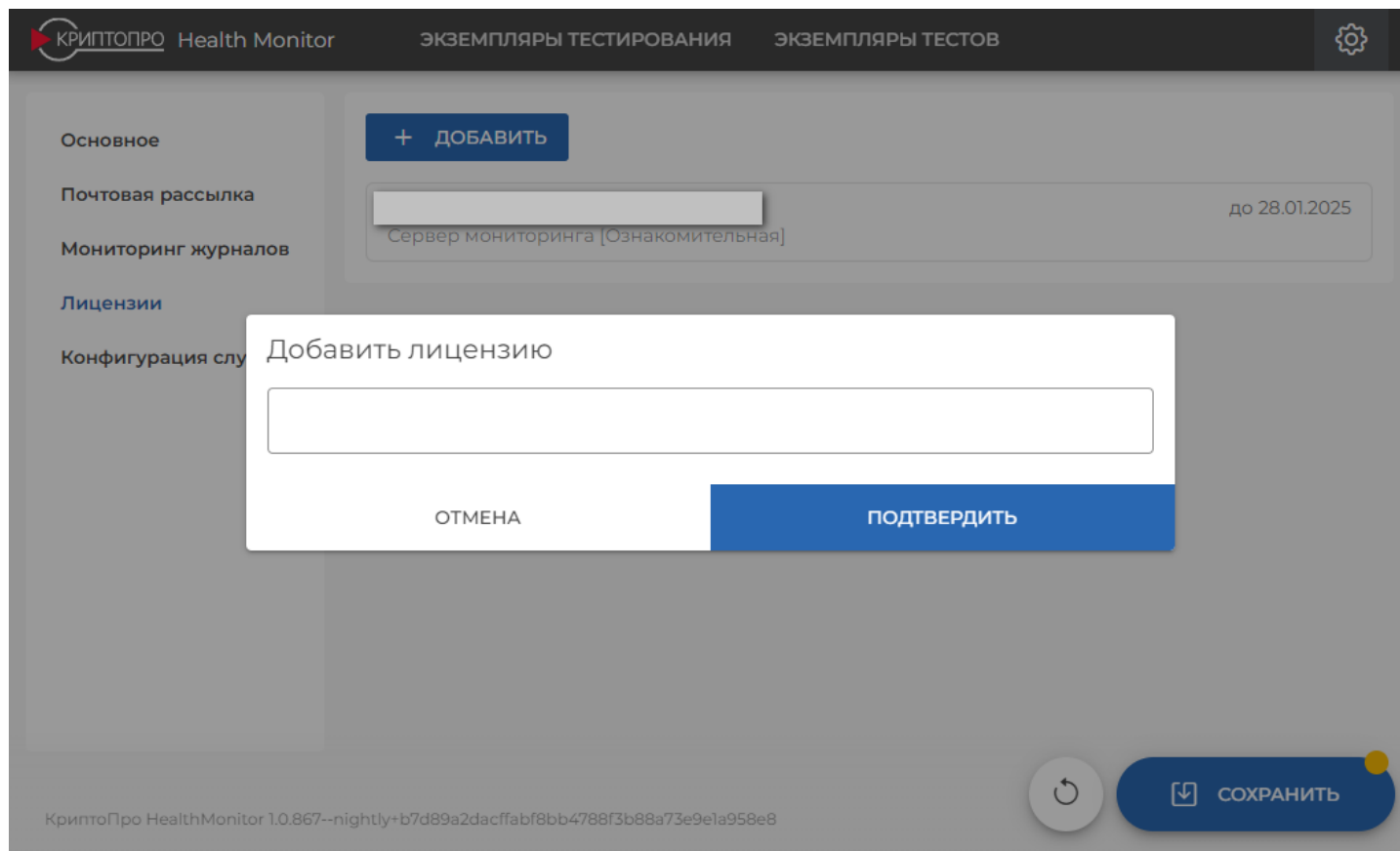
КриптоПро Центр Мониторинга не поддерживает лицензии, приобретенные для другой операционной системы. В случае если лицензия не подходит или прекратила свое действие по причине несовпадения операционной системы, необходимо приобрести лицензию на обновление соответствующих Агентов и Сервера Мониторинга.

По умолчанию после установки КриптоПро Центр Мониторинга активируется демонстрационная лицензия на 3 месяца. Она подразумевает возможность использования всех тестов, которые входят в определенный комплект поставки. По истечении срока действия демонстрационной лицензии на Сервере Мониторинга и на Агентах требуется ввести соответствующие лицензионные ключи.

Ввод лицензии одинаков как для Сервера Мониторинга, так и для любого из Агентов Мониторинга. Для ввода лицензии перейдите в веб-интерфейс КриптоПро Центр Мониторинга. Нажмите на кнопку с пиктограммой шестеренки для перехода к разделу общих настроек. Выберите вкладку «Лицензии». Для добавления новой лицензии нажмите кнопку «Добавить».



Введите лицензионный ключ в появившемся окне и нажмите кнопку "Подтвердить".



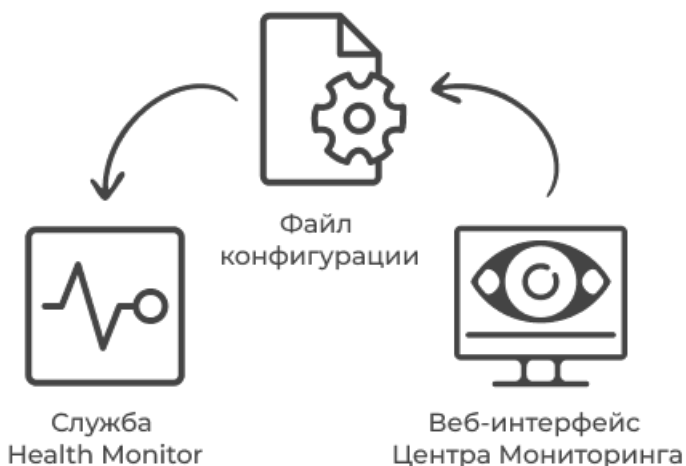
**Обязательно** сохраните конфигурацию путем нажатия кнопки «Сохранить» в правом нижнем углу экрана.

# Принцип работы Центра Мониторинга

Каждый экземпляр КriptoПро Центр Мониторинга вне зависимости от того, сервер это или агент, состоит из трех компонентов:

- Веб-интерфейс КriptoПро HealthMonitor;
- Файл Конфигурации;
- Служба КriptoПро HealthMonitor.

Эти компоненты связаны между собой следующим образом:



Из представленной схемы следует, что Веб-интерфейс явно не взаимодействует со Службой. Веб-интерфейс может только записывать изменения конфигурации в Файл Конфигурации. После того, как Файл Конфигурации был перезаписан, требуется перезапуск Службы, чтобы она использовала в последующем тестировании новую версию Файла Конфигурации.

## Примечание

После внесения изменений внутри Веб-интерфейса необходимо **перезапустить Службу**, чтобы внесенные изменения отразились на последующем тестировании.

## Веб-интерфейс

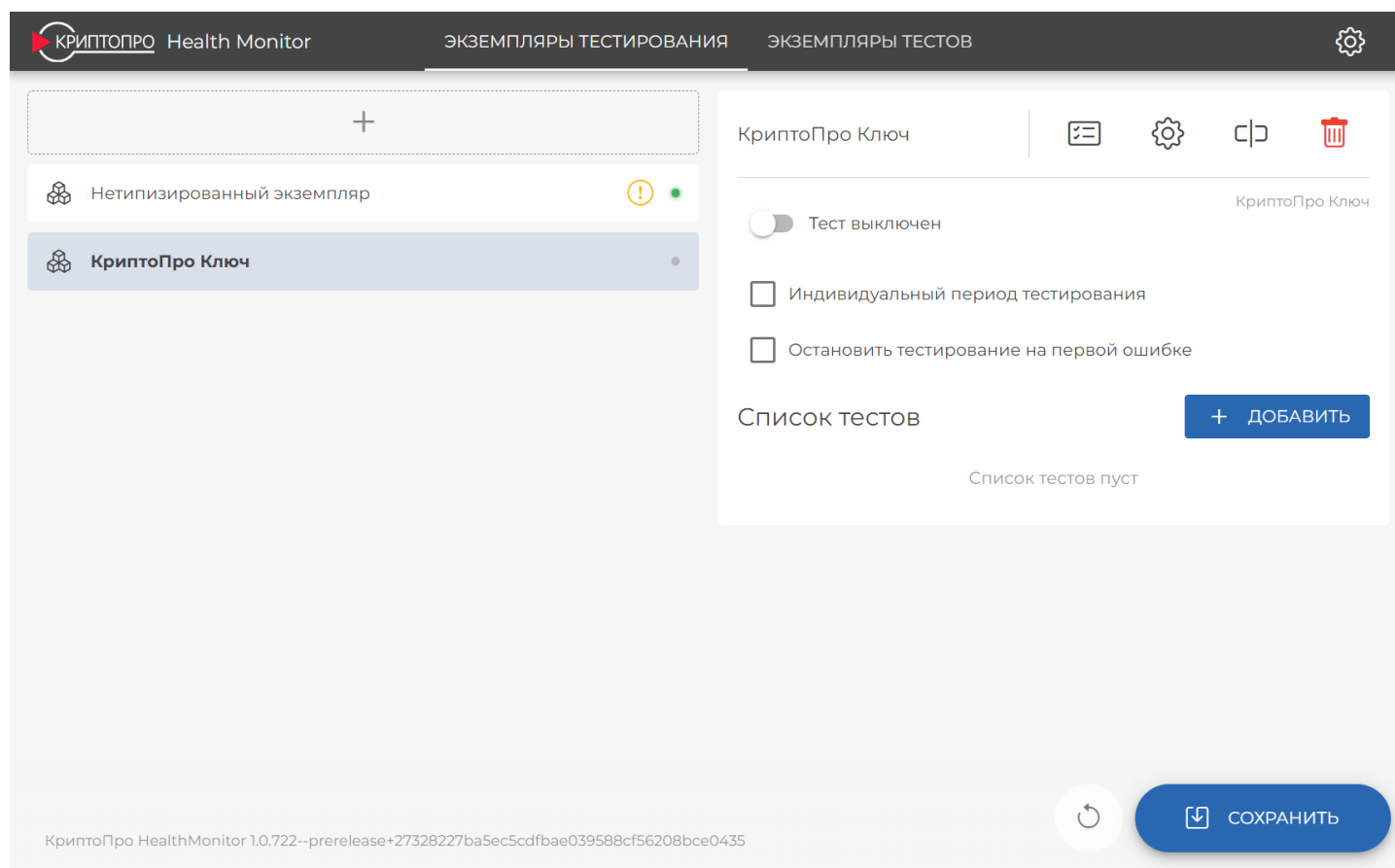
Веб-интерфейс КriptoПро Центр Мониторинга позволяет управлять при помощи графического интерфейса службой `сprohm-hmfe`, в свою очередь управляющую настройками тестов и экземпляров тестирования, а также общими настройками Сервера/Агента Мониторинга.

## Примечание

По умолчанию после установки Веб-интерфейс будет доступен по адресу `http://localhost:53001/#/app`.

После [установки](#) и [развертывания](#) Центра Мониторинга веб-интерфейс доступен по следующему адресу: `http://localhost:53001/#/app`. Основное окно Веб-интерфейса состоит из следующих элементов:

- [Экземпляры тестирования](#) — здесь настраиваются экземпляры систем, тестирование которых производится при помощи КriptoПро Центр Мониторинга.
- [Экземпляры тестов](#) — здесь находятся тесты, созданные из [шаблонов тестов](#) и настроенные под экземпляры тестирования.
- [Общие настройки](#) (пиктограмма шестеренки) — здесь располагаются общие настройки КriptoПро Центр Мониторинга.



При работе с Веб-интерфейсом необходимо обращать внимание, что при внесении ЛЮБЫХ изменений на Веб-интерфейсе требуется выполнять следующие действия:

- сохранять внесенные изменения путем нажатия кнопки «Сохранить». Без этого в некоторых случаях невозможно будет продолжить настройку. Кнопка «Сохранить» присутствует в каждом окне с настройками тестов и экземпляров тестирования.
- перезапускать службу Мониторинга `cprohm-hmsrv`. Без этого в некоторых случаях невозможно будет продолжить настройку.

### Файл конфигурации

Файлы конфигурации КриптоПро Центр Мониторинга содержат настройки Службы и Веб-интерфейса и размещены в следующих директориях:

- `/etc/opt/cprohm/hmsrv` - конфигурация Службы Мониторинга;
- `/etc/opt/cprohm/hmfe` - конфигурация веб-службы Веб-интерфейса.

Здесь и далее Файлом конфигурации будет называться именно файл, содержащий сведения об экземплярах тестов, экземплярах тестирования и лицензии Центра Мониторинга, — `MonitoringConfig.json`.

### Примечание

Файлы Конфигурации создаются и изменяются в автоматическом режиме (при внесении изменений через Веб-интерфейс) и не подлежат редактированию вручную.

Изменения, внесенные администратором КриптоПро Центр Мониторинга в Веб-интерфейсе, записываются в Файл Конфигурации. Файлы Конфигурации используются при работе [Службой КриптоПро HealthMonitor](#).

### Примечание

Файл Конфигурации перезаписывается при сохранении изменений, внесенных в настройки при работе с Веб-интерфейсом. При этом Служба мониторинга продолжает работать с версией файла, актуальной на момент ее запуска.

Для работы с новой версией файла необходимо пересчитать конфигурацию или **перезапустить Службу**.

В случае внесения изменений в настройки Веб-интерфейса (выполнение командлетов настройки) необходимо также перезапустить службу Веб-интерфейса.

## Служба

Служба мониторинга «КриптоПро HealthMonitor» раз в заданный период выполняет запуск тестов согласно своему Файлу Конфигурации. Служба работает с версией Файла Конфигурации, актуальной на момент запуска.

## Примечание

После того, как Файл Конфигурации был перезаписан, требуется **перезапуск Службы** или пересчитать конфигурацию, чтобы она использовала в дальнейшем тестировании новую версию Файла Конфигурации.

Сообщения о работе Службы «КриптоПро Health Monitor» записываются в автоматически создаваемый при установке ПК журнал событий.

## Управление Службой

После того, как Файл Конфигурации был перезаписан, требуется перезапуск Службы. Для перезапуска службы КриптоПро Health Monitor используется следующая команда:

```
sudo systemctl restart cprohm-hmsrv.service
```

Запуск службы или ее остановка производятся следующими командами.

```
# Запуск службы
sudo systemctl start --now cprohm-hmsrv.service
sudo systemctl start --now cprohm-hmfe.service

# Остановка службы
systemctl stop cprohm-hmsrv.service
systemctl stop cprohm-hmfe.service
```

# Журнал событий КристоПро Центр Мониторинга

Сообщения о работе Служб КристоПро Центр Мониторинга записываются в автоматически создаваемые при установке журналы событий:

- `/var/log/cprohm/hmsrv/cprohm-hmsrv*.log` (`/var/log/cprohm/hmsrv/cprohm-hmsrv*.clef`) - Служба Мониторинга;
- `/var/log/cprohm/hmfe/cprohm-hmfe*.log` (`/var/log/cprohm/hmfe/cprohm-hmfe*.clef`) - Служба Веб-интерфейса.

Новые файлы журнала создаются в каждый выбранный [интервал тестирования](#) и за каждые сутки.

Подробнее о настройке мониторинга журналов — в разделе [Мониторинг журналов](#).

## Поддерживаемые типы и форматы журналов событий

В КристоПро Центр Мониторинга реализована запись событий в файл при помощи библиотеки [Serilog](#). Для файла журнала Службы Мониторинга поддерживается [ротация](#), а также автоматическое удаление старых файлов.

## Настройка журналирования и ротации журналов мониторинга

Настройка журналов мониторинга производится при помощи командлета PowerShell `Set-HmLoggingProperties`. Настройка влияет и на журнал Службы Мониторинга, и на журнал Веб-интерфейса одновременно.

НАЗВАНИЕ СВОЙСТВА	ОПИСАНИЕ
<code>LogLevel</code>	Уровень логирования <a href="#">по умолчанию</a> .
<code>OutputTemplate</code>	Шаблон сообщения. Параметры и вид шаблона по умолчанию описаны ниже.
<code>RollingInterval</code>	Задаёт частоты создания нового файла журнала. Доступны значения: <code>Minute</code> , <code>Hour</code> , <code>Day</code> , <code>Month</code> , <code>Year</code> , <code>Infinite</code> . По умолчанию имеет значение <code>Day</code> .
<code>FileSizeLimitBytes</code>	Максимальный размер файла журнала в байтах, при достижении заданного размера будет создан новый файл. Для неограниченного роста необходимо указать 0. По умолчанию имеет значение 1MB.
<code>RetainedFileCountLimit</code>	Максимальное количество файлов журналов, при достижении этого значения старые файлы будут удаляться. Для отключения удаления необходимо указать 0.
<code>IsAsync</code>	Используется ли асинхронная запись в файл. Данный режим ускоряет производительность, но снижает надёжность. По умолчанию <code>false</code> .
<code>AsyncBufferSize</code>	Размер очереди для асинхронной записи. Определяется опытным путём, по умолчанию имеет значение 10000. Слишком большие значения увеличат объём занятой памяти и снизят надёжность из-за риска потерять все содержимое очереди в результате сбоя, слишком маленькие значения нивелируют преимущество асинхронной записи.
<code>AsyncBlockWhenFull</code>	Определяет режим работы асинхронной записи при превышении размера очереди, блокирование записи новых событий или игнорирование (отбрасывание не помещающихся сообщений с их потерей. По умолчанию <code>false</code> .
<code>FlushToDiskIntervalSeconds</code>	Интервал записи в файл на диск. По умолчанию 2 секунды.
<code>UseRenderedClef</code>	Построение текстовок записей журнала в удобно читаемом формате с учетом подстановочных параметров. По умолчанию <code>false</code> . Рекомендуется использовать при включении структурированного журналирования (параметр <code>UseStructuredLogging</code> ).

НАЗВАНИЕ СВОЙСТВА	ОПИСАНИЕ
UseStructuredLogging	Включение структурированного журналирования. По умолчанию false.
EnableDebugLogging	Параметр зарезервирован для дальнейшего использования.

Поддерживаются следующие виды журналирования:

- текстовое (используется по умолчанию);
- структурированное журналирование (JSON).

Текстовое журналирование

Режим журналирования используется по умолчанию. Журналы событий имеют расширение \*.log. Шаблон форматирования по умолчанию имеет следующий вид.

Примечание

В случае использования данного способа журналирования (по умолчанию) необходимо при настройке мониторинга журналов выбирать тип журнала CryptoPro.MonitoringTool.SerilogParser.LogReader.

```
{[Level:u3]} {EventId}: {Timestamp:o } | {RequestId,22} | {Message:l} | {Properties:j} |{NewLine}{Exception}<|
```

Компоненты шаблона (в случае если компонент отсутствует, он будет представлять собой пустое значение | |):

- {Level:u3} - уровень логирования в виде трехбуквенного сокращения в верхнем регистре: DBG, INF, WRN, ERR, CRT.
- {EventId} - идентификатор события мониторинга.
- {Timestamp:o} - метка времени в формате YYYY-MM-DDThh:mm:ss.ffffffzzz (ISO 8601).
- {RequestId,22} - уникальный идентификатор запроса. Представляет из себя 22 символа в формате ConnectionId:RequestNumber, где ConnectionId - это идентификатор HTTP соединения, а RequestNumber - номер HTTP запроса, полученного по данному соединению.
- {Message:l} - текст сообщения.
- {Propertie:j} - дополнительные свойства сообщения, не вошедшие в текстовку {Message}, в виде сериализованного в строку объекта JSON.
- {NewLine} - специальное свойство, отображающее новую строку.
- {Exception} - сообщение об ошибке вместе со стектрейсом (при наличии).

Символы {, }, :u3, :o, :lj, :j являются специальными элементами самого шаблона, они не попадают в результирующий вывод. Специальные символы | и <| облегчают его автоматизированный разбор, поэтому настоятельно не рекомендуется менять шаблон, так как на его формат ориентируется КриптоПро Центр Мониторинга во время анализа журналов.

Пример записи:

```
<|[INF] { Id: 2 } : 2024-10-23T13:16:38.3581225+03:00 | 0HN7HSNB5Q8GS:00000002 | Request finished HTTP/1.1 GET http://hostname:53001/api/Configuration - 200 null application/json; charset=utf-8 0.5856ms | {"SourceContext":"Microsoft.AspNetCore.Hosting.Diagnostics","RequestPath":"/api/Confi$
```

Структурированное журналирование

Структурированное журналирование представляет собой запись журналов событий в формате JSON. Переход на использование структурированного журналирования с использованием serilog осуществляется при помощи следующей команды:

```
Set-HmLoggingProperties -UseStructuredLogging $true -UseRenderedClef $true
```

Журналы событий имеют расширение \*.clef. Шаблон форматирования по умолчанию имеет следующий вид.

КОМПОНЕНТ	ИМЯ	ОПИСАНИЕ	ОБЯЗАТЕЛЬНОСТЬ
@t	Timestamp	Метка времени в формате YYYY-MM-DDThh:mm:ss.ffffffzzz (ISO 8601).	Обязательный
@m	Message	Текст сообщения	
@mt	Message Template	Шаблон сообщения. Будет отображен вместо поля Message, если при настройке структурированного журналирования не был взведен флаг -UseRenderedClef \$true	
@l	Level	Уровень логирования	Отсутствие означает, чтобы событие являлся информационным
@x	Exception	Сообщение об ошибке вместе со стектрейсом (при наличии).	
@i	Event id	Идентификатор события мониторинга	

Примечание

В случае использования данного способа журналирования необходимо при **настройке мониторинга журналов** выбирать тип журнала `CryptoPro.MonitoringTool.SerilogParser.LogLineReader`.

Пример записи:

```
{ "@t": "2024-10-23T13:14:32.2100090Z", "@m": "Content root path: \\opt/cprohm/hmfe\\", "@i": "cc26f24e", "ContentRoot": "/opt/cprohm/hmfe", "SourceContext": "Microsoft.Hosting.Lifetime", "ProcessId": 21753, "ThreadId": 1 }
```

Коды событий

Каждое из событий, создаваемых Службой для журнала событий мониторинга, абстрактно можно сгруппировать по следующим характеристикам:

- группа;
- тип;
- код.

Каждое из событий может иметь один из трех типов, представленных в Таблице 2.

Для событий типов `i` и `w` может быть настроено оповещение администратора программного комплекса [по почте](#).

Таблица 2 — Описание типов событий

ТИП СОБЫТИЯ	ОБОЗНАЧЕНИЕ	ОПИСАНИЕ
Сведения (Information)	i	Информационное сообщение, иллюстрирующее важные моменты в работе Службы.
Предупреждение (Warning)	w	Сообщение с важной информацией, предупреждающей о необходимых действиях с системой во избежание появления ошибок.

ТИП СОБЫТИЯ	ОБОЗНАЧЕНИЕ	ОПИСАНИЕ
Ошибка (Error)	e	Сообщение об ошибке.

Группы событий, их типы и коды представлены в Таблице 3. Остальные характеристики событий (дата, время и проч.) являются типовыми и отображаются в журнале событий.

Таблица 3 — События журнала Центра Мониторинга

код события	тип события	название
Информационные события Службы (100-199)		
100	i	Нетипизированное информационное сообщение
101	i	Запуск сервиса: начало
102	i	Запуск сервиса: конец
103	i	Тесты успешно сконфигурированы
104	i	Остановка сервиса: начало
105	i	Остановка сервиса: конец
106	i	Ожидается завершение тестов
107	i	Запуск тестов
108	i	Тесты завершены
109	i	Результат выполнения тестов (тесты без ошибок)
110	i	Результат выполнения тестов (одна или несколько ошибок в тестах)
111	i	Отправка отчетов успешно сконфигурирована
112	i	Веб-служба успешно сконфигурирована
113	i	Отправка отчетов по SMS успешно сконфигурирована
114	i	Обновление конфигурации тестирования
115	i	Отслеживаемый тест [{0}] для [{1}] вновь успешно завершён (после завершения с ошибкой)
Ошибки работы Службы (200-299)		
200	e	Нетипизированная ошибка
201	e	Ошибка при чтении конфигурации тестов

КОД СОБЫТИЯ	ТИП СОБЫТИЯ	НАЗВАНИЕ
202	e	Ошибка при инициализации тестов
203	e	Не удалось настроить рассылку по Email
204	e	Не удалось запустить таймер для запуска тестов
205	e	Произошла ошибка при отправке Email
206	e	Не удалось настроить веб-службу
207	e	Ошибка при отправке SMS
208	e	Ошибка при настройке SMS-оповещения
<b>Разрешение сборок КriptoПро Ключ (400-499)</b>		
400	i	Общее сообщение с трассировкой
401	i	Разрешение сборки
402	e	Ошибка разрешения сборки
403	i	Успех разрешения сборки
<b>Ошибки тестов (500-599)</b>		
500	e	Нетипизированная ошибка теста КriptoПро Ключ с (id события по умолчанию)
501	e	Ошибка теста AuthenticationTest (Тестовая аутентификация)
502	e	Ошибка теста ComplexSignatureTest (Тестовая подпись)
503	e	Ошибка теста CryptoProviderTest (Тест криптопровайдеров Сервиса Подписи КriptoПро Ключ)
504	e	Ошибка теста EndpointTest (Тест конечных точек КriptoПро Ключ)
505	e	Ошибка теста EnrollsTest (Тест доступности обработчика УЦ)
506	e	Ошибка теста FeCertificateValidationTest (Проверка сертификатов Веб-интерфейса КriptoПро Ключ)
507	e	Ошибка теста OcspTest (Тест доступности службы OCSP)
508	e	Ошибка теста SsCertificateValidationTest (Проверка сертификатов Сервиса Подписи КriptoПро Ключ)
509	e	Ошибка теста SsDataBaseConnectionTest (Тест подключения к БД Сервиса Подписи КriptoПро Ключ)
510	e	Ошибка теста StsCertificateValidationTest (Проверка сертификатов Центра Идентификации КriptoПро Ключ)

КОД СОБЫТИЯ	ТИП СОБЫТИЯ	НАЗВАНИЕ
511	е	Ошибка теста StsDataBaseConnectionTest (Тест подключения к БД сервиса Центра Идентификации КриптоПро Ключ)
512	е	Ошибка теста SvsTest (Тест Сервиса Проверки Подписи)
513	е	Ошибка теста TspTest (Тест TSP-службы)
514	е	Ошибка теста CrItest (Тест CRL)
515	е	Ошибка теста HsmLogTest (Загрузка журналов HSM)
516	е	Ошибка теста SimpleCryptoProviderTest (Тест указанного криптопровайдера)
517	е	Ошибка теста SimpleCertificateTest (Тест указанного сертификата)
518	е	Ошибка теста SimpleDataBaseConnectionTest (Тест указанной базы данных)
519	е	Ошибка теста SimpleServiceTest (Тест указанной службы)
520	е	Ошибка теста SimpleHttpAvailabilityTest (Тест указанной веб службы)
521	е	Ошибка теста CrIVerificationTest (Тест срока действия CRL)
522	е	Ошибка теста PingCaTest (Тестирование связи с Центром Сертификации УЦ)
523	е	Ошибка теста RaServiceBrokerTest (Тест компонента Service Broker Центра Регистрации УЦ)
524	е	Ошибка теста RaQueuesOverflowTest (Проверка количества сообщений в системных очередях ЦР УЦ)
525	е	Ошибка теста RaQueuesStateTest (Тест состояния очередей Центра Регистрации УЦ)
526	е	Ошибка теста RaDataBaseConnectionTest (Тест подключения к БД Центра Регистрации УЦ)
527	е	Ошибка теста StsLicenseTest (Тест лицензий Центра Идентификации КриптоПро Ключ)
528	е	Ошибка теста SsLicenseTest (Тест лицензий Сервиса Подписи КриптоПро Ключ)
529	е	Ошибка теста UsedMemoryTest (Проверка используемой оперативной памяти)
530	е	Ошибка теста UsedDiskSpaceTest (Проверка используемого места на диске)
531	е	Ошибка теста GetLogsTest (Получение журналов Агента Мониторинга)
532	е	Ошибка теста HsmStatusTest (Тест состояния HSM)
533	е	Ошибка теста GetLastTestStatusTest (Тест состояния удаленного Агента Мониторинга)
534	е	Ошибка теста SimplePowershellTest (Выполнение указанного скрипта)
535	е	Ошибка теста NGateTest (Тест NGate)

КОД СОБЫТИЯ	ТИП СОБЫТИЯ	НАЗВАНИЕ
536	e	Ошибка теста CaDataBaseConnection (Тест подключения к БД Центра Сертификации УЦ)
537	e	Ошибка теста PerfomanceCounterTest (Мониторинг счетчика производительности)
538	e	Ошибка теста StsCryptoProviderTest (Тест криптопровайдера Центра Идентификации КриптоПро Ключ)
539	e	Ошибка теста AuditCryptoProviderTest (Тест криптопровайдера Сервиса Аудита)
540	e	Ошибка теста ClientSecretTest (Тест проверки срока действия ClientSecret)
541	e	Ошибка теста TspOcspTimeTest (Тест синхронизации времени служб TSP и OCSP)
542	e	Ошибка теста DssOperationStatisticTestError (Тест сбойных операций)
543	e	Ошибка теста SimpleCryptoContainerTest (Тест указанного криптоконтейнера ключа)
544	e	Ошибка теста SimpleShellTest (Выполнение указанного Bash скрипта)
545	e	Ошибка теста MyDssCryptoProviderTest (Тест криптопровайдеров для мобильного приложения)
546	e	Ошибка теста GammaCryptoProviderTest (Тест оставшихся ключей указанного криптопровайдера)
553	e	Ошибка теста HsmLicenseTest (Тест лицензий HSM)
<b>Предупреждения тестов (600-699)</b>		
600	w	Нетипизированное предупреждение теста КриптоПро Ключ (id события по умолчанию)
603	w	Предупреждение теста CryptoProviderTest (Тест криптопровайдеров Сервиса Подписи КриптоПро Ключ)
606	w	Предупреждение теста FeCertificateValidationTest (проверка сертификатов Веб интерфейса КриптоПро Ключ)
608	w	Предупреждение теста SsCertificateValidationTest (проверка сертификатов Сервиса Подписи КриптоПро Ключ)
610	w	Предупреждение теста StsCertificateValidationTest (проверка сертификатов Центра Идентификации КриптоПро Ключ)
617	w	Предупреждение теста SimpleCertificateTest (тест указанного сертификата)
622	w	Предупреждение теста PingCaTest (Тестирование связи с Центром Сертификации УЦ)
627	w	Предупреждение теста StsLicenseTest (Тест лицензий Центра Идентификации КриптоПро Ключ)
628	w	Предупреждение теста SsLicenseTest (Тест лицензий Сервиса Подписи КриптоПро Ключ)
631	w	Предупреждение теста GetLogsTest (Получение журналов Агента Мониторинга)

КОД СОБЫТИЯ	ТИП СОБЫТИЯ	НАЗВАНИЕ
632	w	Предупреждение теста HsmStatusTest (Тест состояния HSM)
640	w	Предупреждение теста ClientSecretTest (Тест проверки срока действия ClientSecret)
643	w	Предупреждение теста SimpleCryptoContainerTest (Тест указанного криптоконтейнера ключа)
645	w	Предупреждение теста MyDssCryptoProviderTest (Текст криптопровайдеров для мобильного приложения)
646	w	Ошибка теста GammaCryptoProviderTest (Тест оставшихся ключей указанного криптопровайдера)
653	w	Предупреждение теста HsmLicenseTest (Тест лицензий HSM)

## Системные требования

В случае, если Центр Мониторинга устанавливается на отдельной машине, предъявляются следующие основные требования к общесистемному и прикладному программному обеспечению.

Для функционирования в \*nix-системах:

- ОС CH Astra Linux SE Смоленск;
- веб-сервер nginx 1.18.0 и выше;
- [КриптоПро CSP](#) (необходим, если тестируемый КриптоПро Ключ использует межсервисные сертификаты ГОСТ);
- КриптоПро TSP Client из состава [Служб УЦ 2.0](#);
- КриптоПро OCSP Client из состава [Служб УЦ 2.0](#);
- КриптоПро HSM Client (для подключения к КриптоПро HSM).

### Примечание

КриптоПро Центр Мониторинга не имеет собственной базы данных, хотя и может использовать [тесты](#), которым требуется подключение к БД КриптоПро Ключ или другой системы. В связи с этим, требования к СУБД в настоящем документе не предъявляются.

## Установка, удаление и обновление Центра Мониторинга

Процедура установки, развертывания, удаления или обновления Центра Мониторинга одинакова для любого из экземпляров — как центрального сервера, так и агентов.

- [Установка](#)
- [Развертывание компонентов](#)
- [Обновление](#)
- [Удаление](#)

# Установка Центра Мониторинга

## Примечание

Для установки требуются права Администратора ОС.

### 1. Установка пакетов из состава дистрибутива "КриптоПро Центр Мониторинга" на сервер ЦМ и инспектируемые сервера

```
tar -xvf cprohm_<XXX>_amd64.tar.gz
sudo dpkg -i cprohm-base_<XXX>_amd64.deb
sudo dpkg -i cprohm-cprokeytests_<XXX>_amd64.deb
```

## Примечание

Для обеспечения работы некоторых тестов может потребоваться установка дополнительного ПО:

- КриптоПро CSP 5.0;
- КриптоПро TSP Client и КриптоПро OCSP Client из состава [Служб УЦ 2.0](#) (требуется установка пакетов `cprocsp-pki-cades*.deb` и `cprocsp-legacy*.deb` из состава КриптоПро CSP).

### 2. Установка PowerShell из состава дистрибутива "КриптоПро Центр Мониторинга".

```
sudo dpkg -i powershell_7.4.1-1.deb_amd64_signed.deb
```

### 3. Импорт модулей PowerShell

Для автоматической загрузки модулей PowerShell КриптоПро Центр Мониторинга требуется создать PowerShell-профиль или добавить в существующий следующие данные:

```
:/opt/cprohm/powershell/Modules
```

Каталог с PowerShell-профилем расположен по следующему адресу: `/opt/microsoft/powershell/7/profile.ps1`. В случае отсутствия файла профиля его необходимо создать самостоятельно. В этом случае содержимое файла должно выглядеть следующим образом:

```
$env:PSModulePath+=':/opt/cprohm/powershell/Modules'
```

```
# Запуск PowerShell:
pwsh
```

```
# Отображение списка доступных модулей:
Get-Module -ListAvailable
```

```
# В списке должны присутствовать модули с названием CryptoPro.MonitoringTool.Powershell для КриптоПро ЦМ.
```

```
# Выход из PowerShell
exit
```

### 4. Подготовка сервисной УЗ КриптоПро Центр Мониторинга

Для работы КриптоПро ЦМ используется сервисная учетная запись. Выбор учетной записи зависит от типа установки КриптоПро ЦМ (Сервер или Агент).

#### Для КриптоПро ЦМ (Сервер)

В случае установки КриптоПро ЦМ (Сервер) рекомендуется создать отдельную сервисную учетную запись:

```
SERVICE_ACC="<имя учетной записи>"
sudo useradd -M -G hmsrv,hmfe $SERVICE_ACC
```

#### Для КриптоПро ЦМ (Агент) с установленным веб-приложением

В случае установки КриптоПро ЦМ (Агент) на сервере приложений необходимо использовать сервисную учетную запись, созданную в процессе разворачивания соответствующего приложения.

```
# Добавление имеющейся сервисной УЗ
SERVICE_ACC="<имя учетной записи>"
sudo usermod -aG hmsrv,hmfe $SERVICE_ACC
```

## 5. (Опционально) Настройка прав доступа к конфигурированию Центра Мониторинга

### Примечание

Права на каталоги Службы мониторинга (`/etc/opt/cprohm/hmsrv`) и Веб-интерфейса Мониторинга (`/etc/opt/cprohm/hmfe`) принадлежат по умолчанию группе `hmsrvadmin`. В случае если роли Администратора Мониторинга и Администратора ОС выполняют различные пользователи, в указанную группу `hmsrvadmin` необходимо добавить пользователя, осуществляющего конфигурирование Центра Мониторинга.

# Развертывание КристоПро Центр Мониторинга

## Примечание

Развертывание Центра Мониторинга выполняется аналогично для любого из экземпляров — как Сервера Мониторинга, так и каждого из Агентов. Для развертывания требуются права Администратора ОС либо пользователя, добавленного в группу `hmsrvadmin`.

## Создание экземпляра сервиса

Для развертывания экземпляра сервиса КристоПро Центр Мониторинга необходимо выполнить следующие действия.

```
# Запуск PowerShell
pwsh

# Развертывание экземпляра сервиса КристоПро ЦМ
Install-HmInstance -ServiceAccountName <Имя учетной записи>
```

Дополнительно могут быть указаны следующие параметры:

- `-ListenPort` - порт Службы Мониторинга (по умолчанию равен 53000);
- `-ListenConfigPort` - порт Веб-интерфейса Мониторинга (по умолчанию равен 53001);
- `-SkipServiceRegistration` - флаг, указывающий, что регистрация Службы Мониторинга в `systemd` будет пропущена.

## Настройка получения последнего запуска тестов на Веб-интерфейсе

### Внимание!

В КристоПро Центр Мониторинга отсутствует собственная аутентификация при доступе к Веб-интерфейсу/Службе. При публикации сервисов может потребоваться **настройка защищенного соединения** с использованием ГОСТ-TLS. В этом случае требуется другая **настройка получения последнего запуска тестов**.

Для возможности отображения статуса последнего запуска тестов необходимо выполнить настройку Веб-интерфейса. Для настройки получения статуса последнего запуска тестов необходимо выполнить команду ниже, передав в качестве значения адрес Службы Мониторинга. По умолчанию используется значение `http://localhost:53000`.

```
# Добавление отображения статуса последнего запуска тестов
Set-HmFeProperties -MonitoringServiceUrl http://localhost:53000

# Выход из PowerShell:
exit
```

## Примечание

По умолчанию после установки Веб-интерфейс Мониторинга будет доступен по адресу `http://localhost:53001/#/app`.

## Активация и запуск сервисов

```
# Запуск сервисов
sudo systemctl daemon-reload
sudo systemctl enable --now cprohm-hmsrv.service
sudo systemctl enable --now cprohm-hmfe.service

# Проверка активации сервисов
systemctl status cprohm-hmsrv.service
systemctl status cprohm-hmfe.service
```

# Настройка защищенного соединения с использованием ГОСТ-TLS

## Установка и настройка nginx

```
sudo dpkg -i cprocsp-nginx-64_5.0.XXXXX-X_amd64.deb #nginx
```

### Настройка доступа к веб-интерфейсу Центра Мониторинга по протоколу ГОСТ-TLS с односторонней аутентификацией

Для настройки необходимо выполнить следующие действия.

1. Открыть конфигурационный файл `cpnginx.conf` (`/etc/opt/cprocsp/cpnginx/cpnginx.conf`).
2. Добавить подключение к Веб-интерфейсу Центра Мониторинга через 443 порт.

```
server {
    listen 443 ssl;
    ...
    location /hm {
        rewrite /hm(.+) $1 break;
        rewrite /hm /hm/ permanent;
        proxy_pass http://localhost:<ПОРТ ВЕБ-ИНТЕРФЕЙСА МОНИТОРИНГА>;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
    location /hmsrv {
        rewrite /hmsrv(.+) $1 break;
        rewrite /hmsrv /hmsrv/ permanent;
        proxy_pass http://localhost:<ПОРТ СЛУЖБЫ МОНИТОРИНГА>;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
    ...
}
```

3. Отредактировать файл сервиса `cpnrohm-hmfe` (`/etc/systemd/system/cpnrohm-hmfe.service`), добавив в него следующий параметр:

```
Environment=DSS_APPLICATION_NAME=hm
```

4. Перезапустить сервис `cpnginx`.

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

### Настройка доступа к веб-интерфейсу Центра Мониторинга по протоколу ГОСТ-TLS с двусторонней аутентификацией

Для настройки необходимо выполнить следующие действия.

1. Открыть конфигурационный файл `cpnginx.conf` (`/etc/opt/cprocsp/cpnginx/cpnginx.conf`).
2. Добавить подключение к Веб-интерфейсу Центра Мониторинга через 443 порт.

```
server {
    listen 4430 ssl;
    ...
    location /hm {
        set $auth 0;
        if ( $sspi_client_fingerprint = 'ОТПЕЧАТОК СЕРТИФИКАТА ПОЛЬЗОВАТЕЛЯ' ) {
            set $auth 1;
        }
        if ( $auth = 0 ) {
            return 403;
        }
        rewrite /hm(.+) $1 break;
        rewrite /hm /hm/ permanent;
        proxy_pass http://localhost:<ПОРТ ВЕБ-ИНТЕРФЕЙСА МОНИТОРИНГА>;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
    ...
}
```

3. Отредактировать файл сервиса `cprohm-hmfe` (`/etc/systemd/system/cprohm-hmfe.service`), добавив в него следующий параметр:

```
Environment=DSS_APPLICATION_NAME=hm
```

4. Перезапустить сервис `cpnginx`.

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

## Настройка получения последнего запуска тестов на Веб-интерфейсе

### Примечание

Для выполнения данного пункта требуется **созданный экземпляр** Центра Мониторинга.

После настройки `nginx`, описанной в данном разделе, необходимо указать новый адрес Службы Мониторинга, даже если он был задан [ранее](#).

### Примечание

Адрес Службы Мониторинга имеет определенный формат (необходимо указывать `/hmsrv` после адреса узла).

```
Set-HmFeProperties -MonitoringServiceUrl <HOST>/hmsrv
```

```
# Выход из PowerShell:
```

```
exit
```

## Удаление Центра Мониторинга

Для удаления ПО «КриптоПро Центр Мониторинга» необходимо выполнить следующие действия.

```
sudo pwsh

Import-Module /opt/cprohm/powershell/Modules/CryptoPro.MonitoringTool.PowerShell
Uninstall-HmInstance
exit

sudo apt remove cprohm-base
```

### Внимание!

В случае если производится удаление экземпляра Агента Мониторинга, необходимо также удалить соответствующие пакеты при помощи команды `sudo apt remove <имя пакета>`.

# Обновление Центра Мониторинга

Для обновления ПО «КриптоПро Центр Мониторинга» необходимо выполнить следующие действия.

## Примечание

В зависимости от версии, до которой производится обновление, необходимо уточнить полные названия установочных пакетов ЦМ.

## Остановка служб КриптоПро Центр Мониторинга

```
sudo systemctl stop cprohm-hmfe.service
sudo systemctl stop cprohm-hmsrv.service
```

## Распаковка и установка дистрибутива

```
tar -xzf cprohm_XXX_amd64.tar.gz
sudo dpkg -i cprohm-base_XXX_amd64.deb
```

## Импорт модуля PowerShell и обновление

```
sudo pwsh
Import-Module /opt/cprohm/powershell/Modules/CryptoPro.MonitoringTool.PowerShell
Update-HmInstance
exit
```

## Запуск служб

```
sudo systemctl start cprohm-hmsrv
sudo systemctl start cprohm-hmfe
```

## Проверка статуса служб

```
sudo systemctl status cprohm-hmsrv
sudo systemctl status cprohm-hmfe
```

# Настройка КriptoПро Центр Мониторинга

Настройка КriptoПро Центр Мониторинга состоит из трех основных разделов:

- [Экземпляры тестирования](#) — здесь настраиваются экземпляры систем, тестирование которых производится при помощи КriptoПро Центр Мониторинга.
- [Экземпляры тестов](#) — здесь находятся тесты, полученные из шаблонов и специально настроенные под экземпляры тестирования.
- [Общие настройки](#) — здесь располагаются общие настройки КriptoПро Центр Мониторинга.

## Примечание

Управление тестами и экземплярами тестирования осуществляется при помощи Веб-интерфейса, доступному по следующему адресу по умолчанию (в зависимости от настроек при развертывании адрес и порт могли быть изменены): `http://localhost:53001/#/app/`.

Настройку любого экземпляра КriptoПро Центр Мониторинга, вне зависимости от типа лицензии, **ВАЖНО** осуществлять в следующем порядке:

1. [Настройка лицензии](#).
2. [Основные настройки](#).
3. [Настройка экземпляров тестирования](#).
4. [Настройка экземпляров тестов](#).
5. [Добавление тестов к экземпляру тестирования](#).
6. Другие настройки:
  - [Период тестирования](#);
  - [Настройка мониторинга журналов](#);
  - [Веб-служба](#).

## Примечание

Все указанные настройки могут изменяться/дополняться вместе с новыми версиями КriptoПро Центр Мониторинга.

# Настройка экземпляров тестирования

В настоящее время в КристоПро Центр Мониторинга доступны для тестирования следующие типы экземпляров:

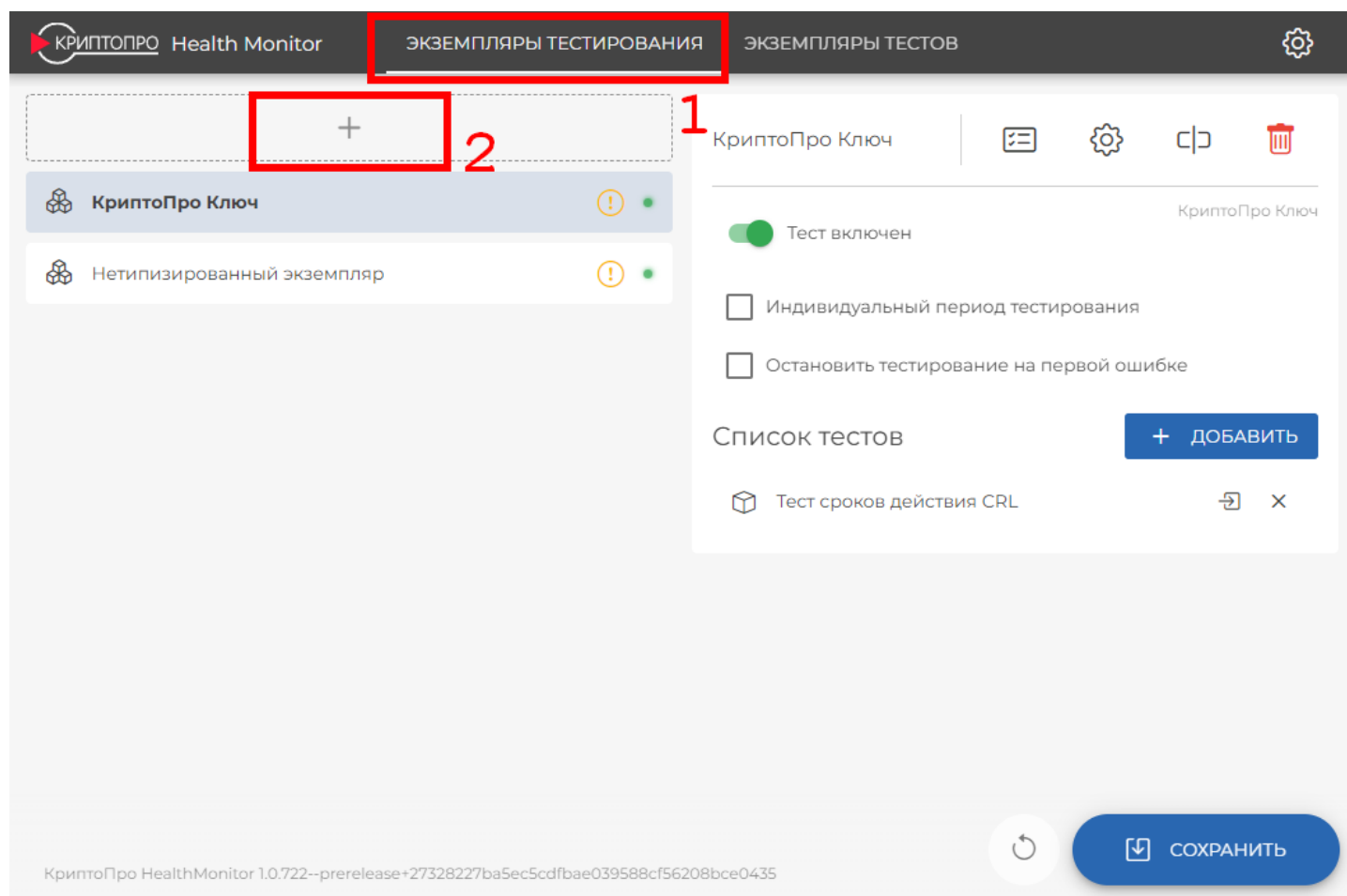
- КристоПро Ключ;
- Нетипизированный экземпляр;
- КристоПро HSM.

Для экземпляров [КристоПро Ключ](#) и [КристоПро HSM](#) в КристоПро Центр Мониторинга доступны дополнительные настройки (пиктограмма шестеренки в карточке экземпляра), в то время как для нетипизированного экземпляра какие-либо дополнительные настройки отсутствуют.

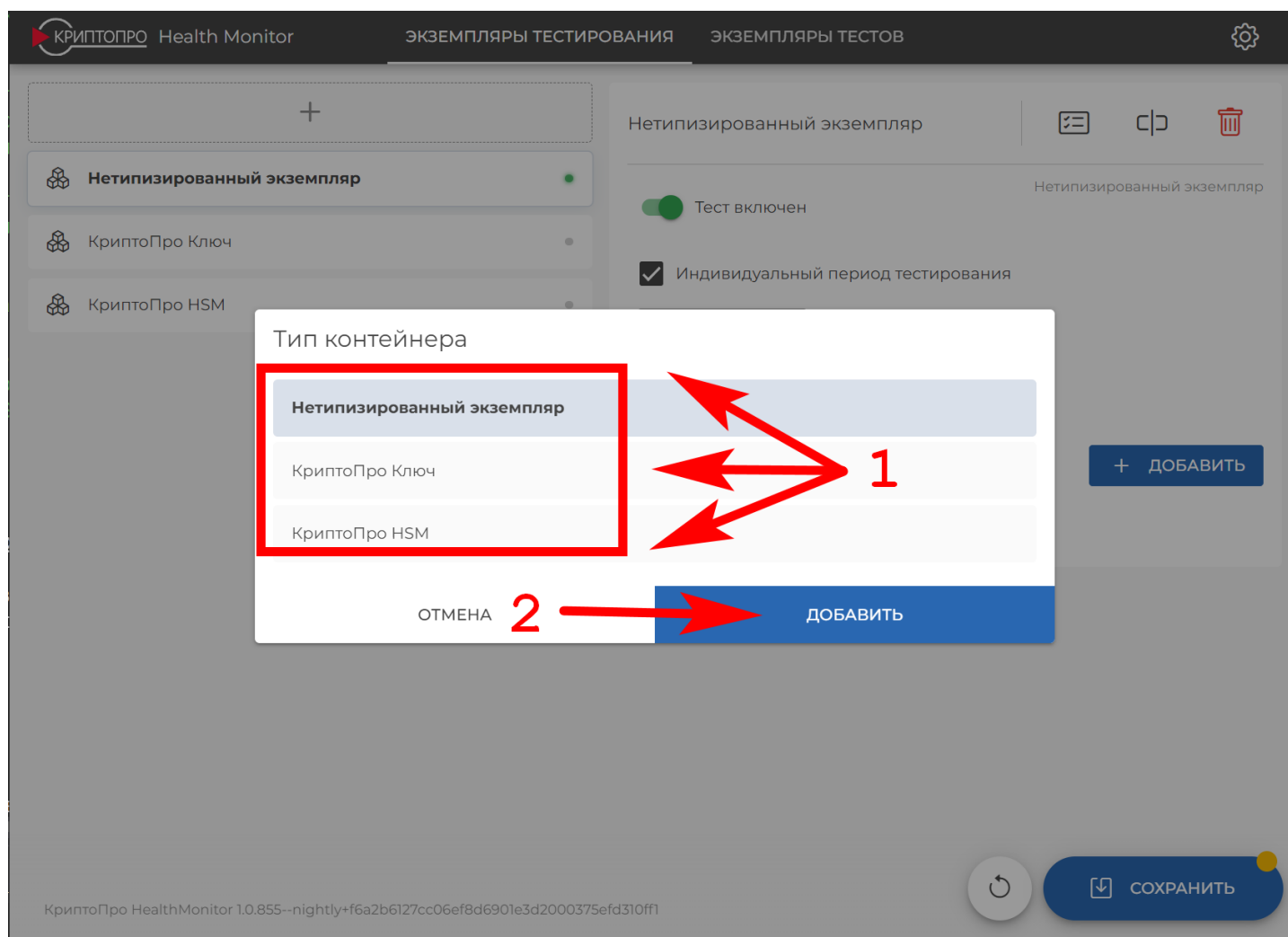
## Примечание

Экземпляр тестирования необязательно соответствует однозначно инспектируемой системе. Экземпляр тестирования означает определенный набор тестов и (в случае с экземпляром типа КристоПро Ключ) набор настроек.

Чтобы добавить экземпляр тестирования, перейдите в раздел «Экземпляры тестирования» (1) и добавьте новый экземпляр нажатием пиктограммы "+" (2).

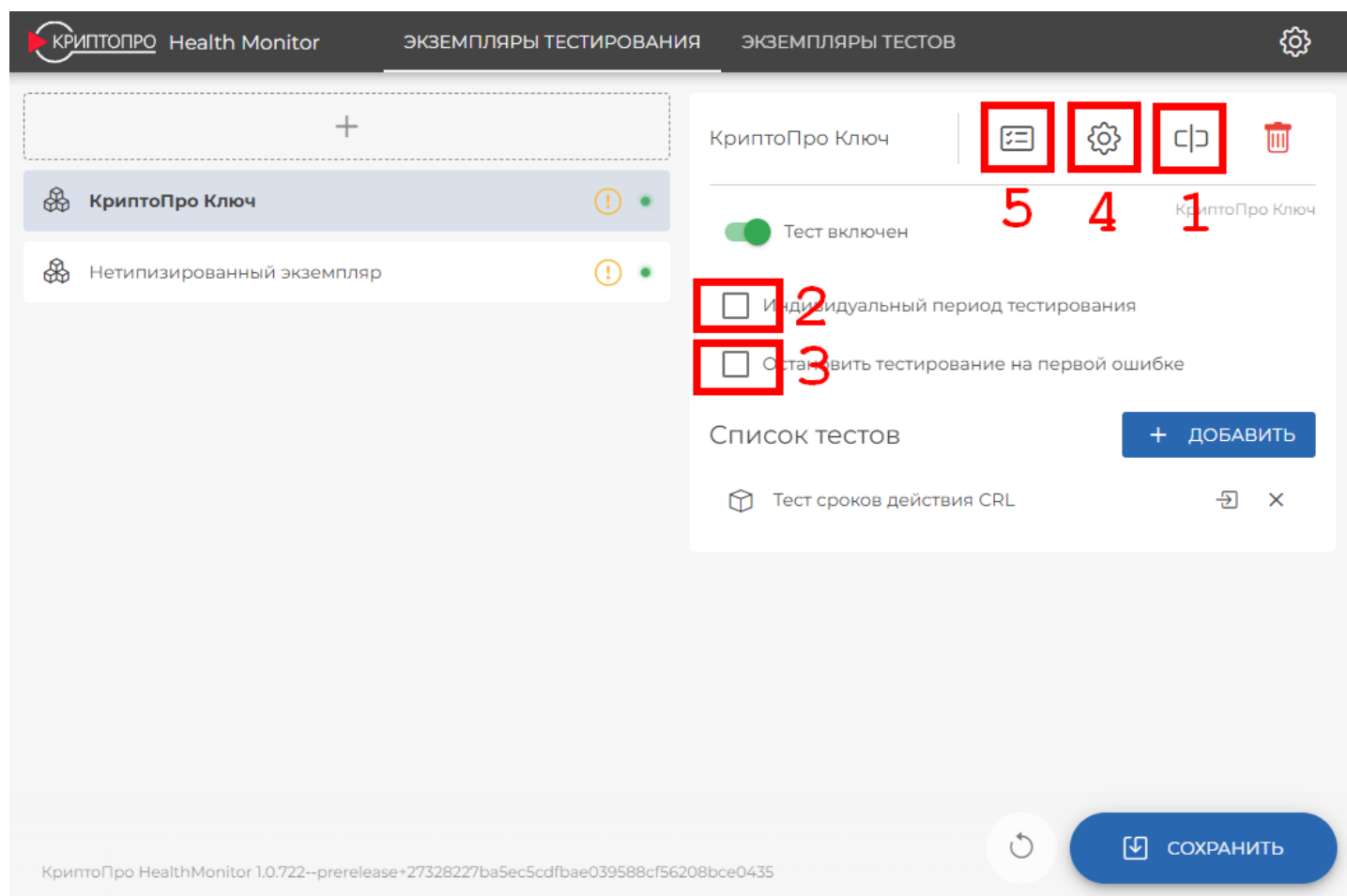


В окне добавления экземпляра тестирования откройте выпадающий список и выберите тип экземпляра, который необходимо добавить в работу (1). Нажмите «Добавить» (2).



Новый экземпляр будет отображаться в разделе «Экземпляры тестирования».

- Имя созданного экземпляра тестирования можно изменить, нажав на него и выбрав пиктограмму (1) в карточке экземпляра справа.
- При помощи чекбокса (2) можно настроить для данного экземпляра индивидуальный период тестирования в минутах
- При помощи чекбокса (3) можно включить настройку остановки тестирования экземпляра при первой ошибке.
- Дополнительные настройки экземпляра доступны по нажатию пиктограммы с шестеренкой (4). Дополнительные настройки доступны только для экземпляров типа [КриптоПро Ключ](#) и [КриптоПро HSM](#).
- Результат выполнения тестов можно посмотреть, нажав на пиктограмму "Результаты тестов" (5).
- Настройки тестов, для которых выполняется отслеживание запуска, можно посмотреть, нажав на пиктограмму "[Отслеживание запуска тестов](#)". Данная настройка становится доступной только после того как [созданы](#) экземпляры тестов и [добавлены](#) к текущему экземпляру тестирования.



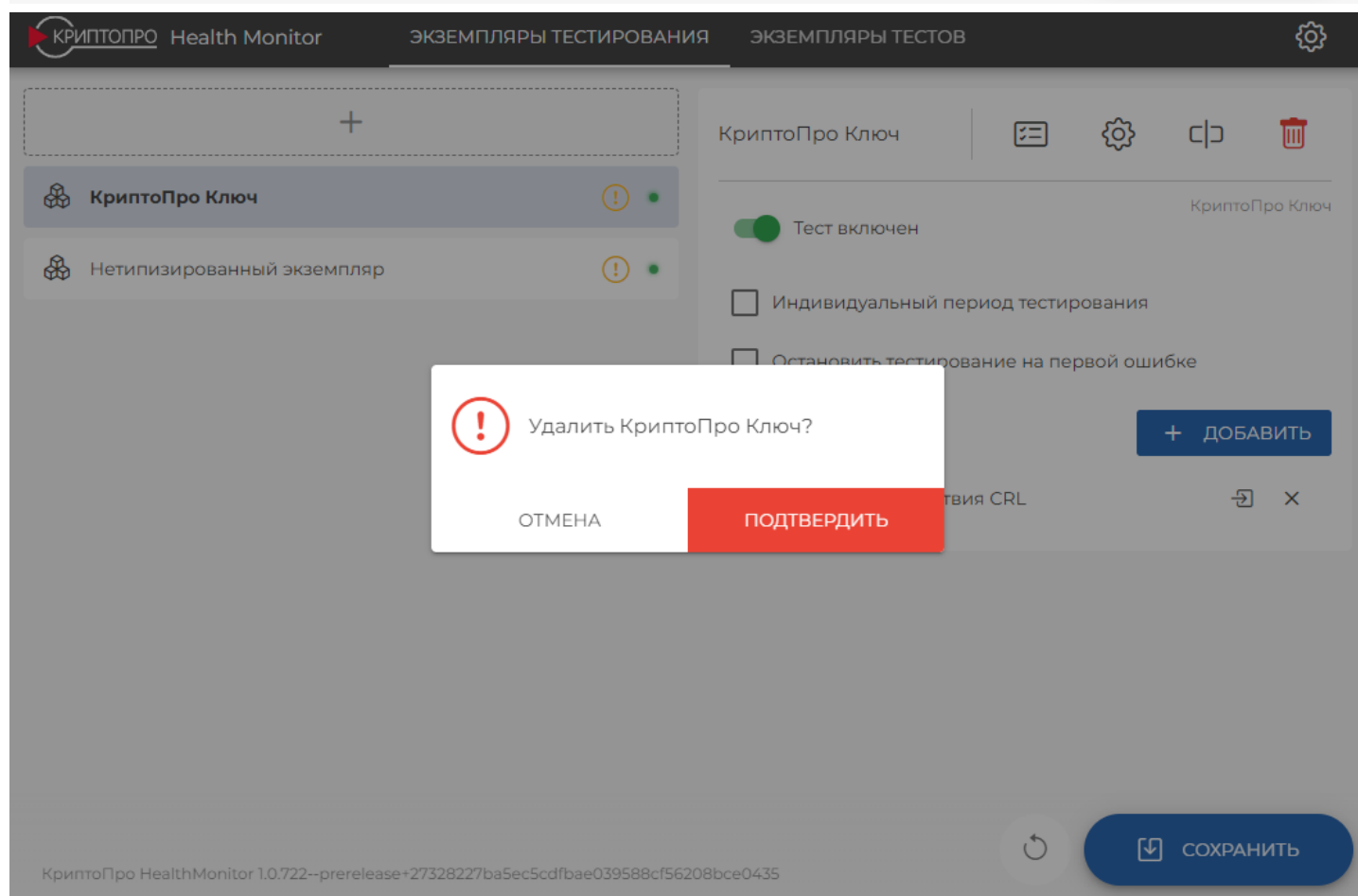
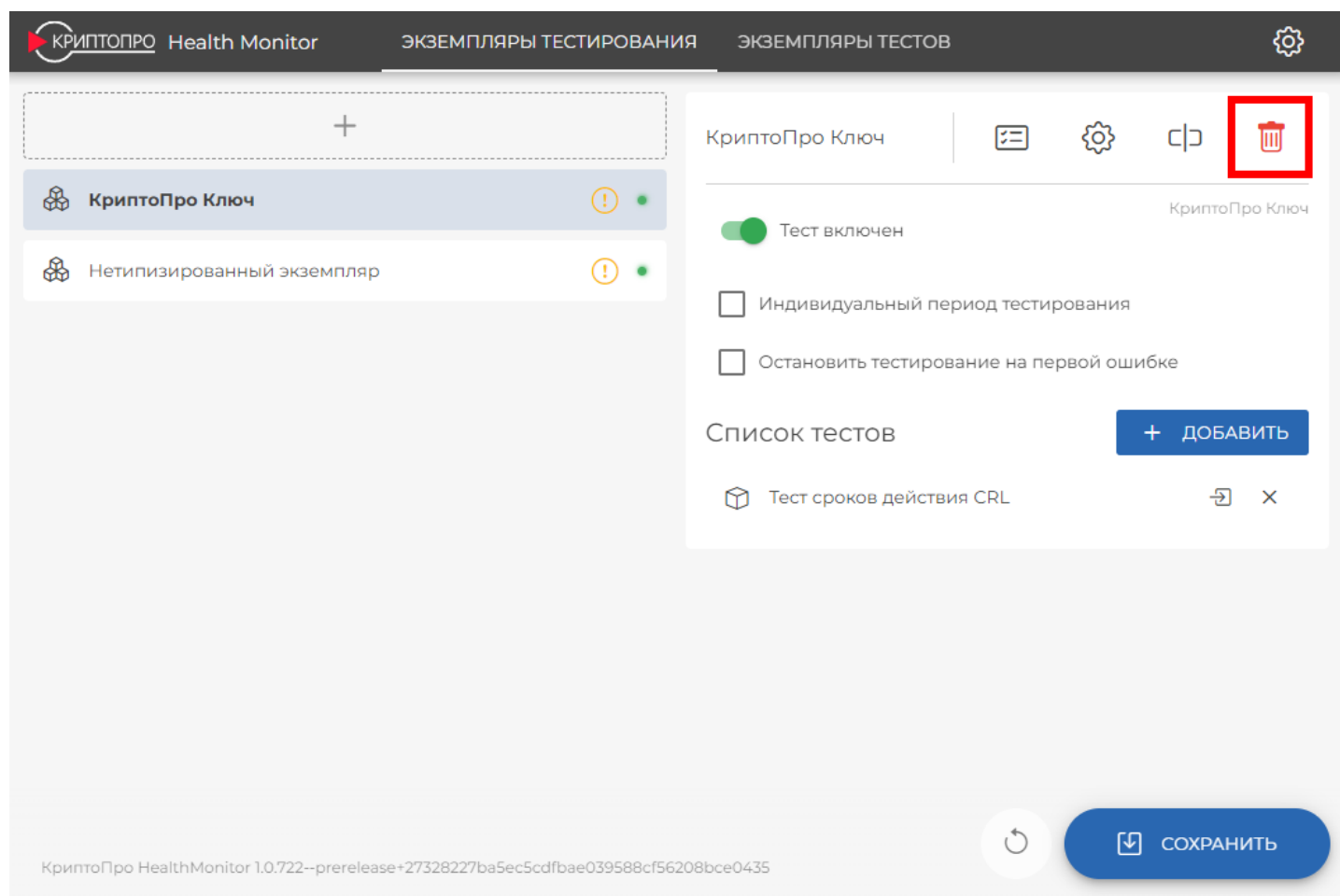
По умолчанию все новые создаваемые экземпляры имеют имена **КриптоПро Ключ**, **КриптоПро HSM** или **Нетипизированный экземпляр**. Дублирование имен экземпляров невозможно, поэтому при добавлении экземпляра с именем, которое уже есть в списке, к имени нового экземпляра добавится его номер по порядку (например: КриптоПро Ключ, КриптоПро Ключ (1), КриптоПро Ключ (2)...).

После добавления экземпляра необходимо добавить **тесты**, которые для него будут выполняться. Для экземпляра тестирования типа КриптоПро Ключ необходимо дополнительно выполнить ряд **настроек** (пиктограмма с шестеренкой в карточке экземпляра).

### Примечание

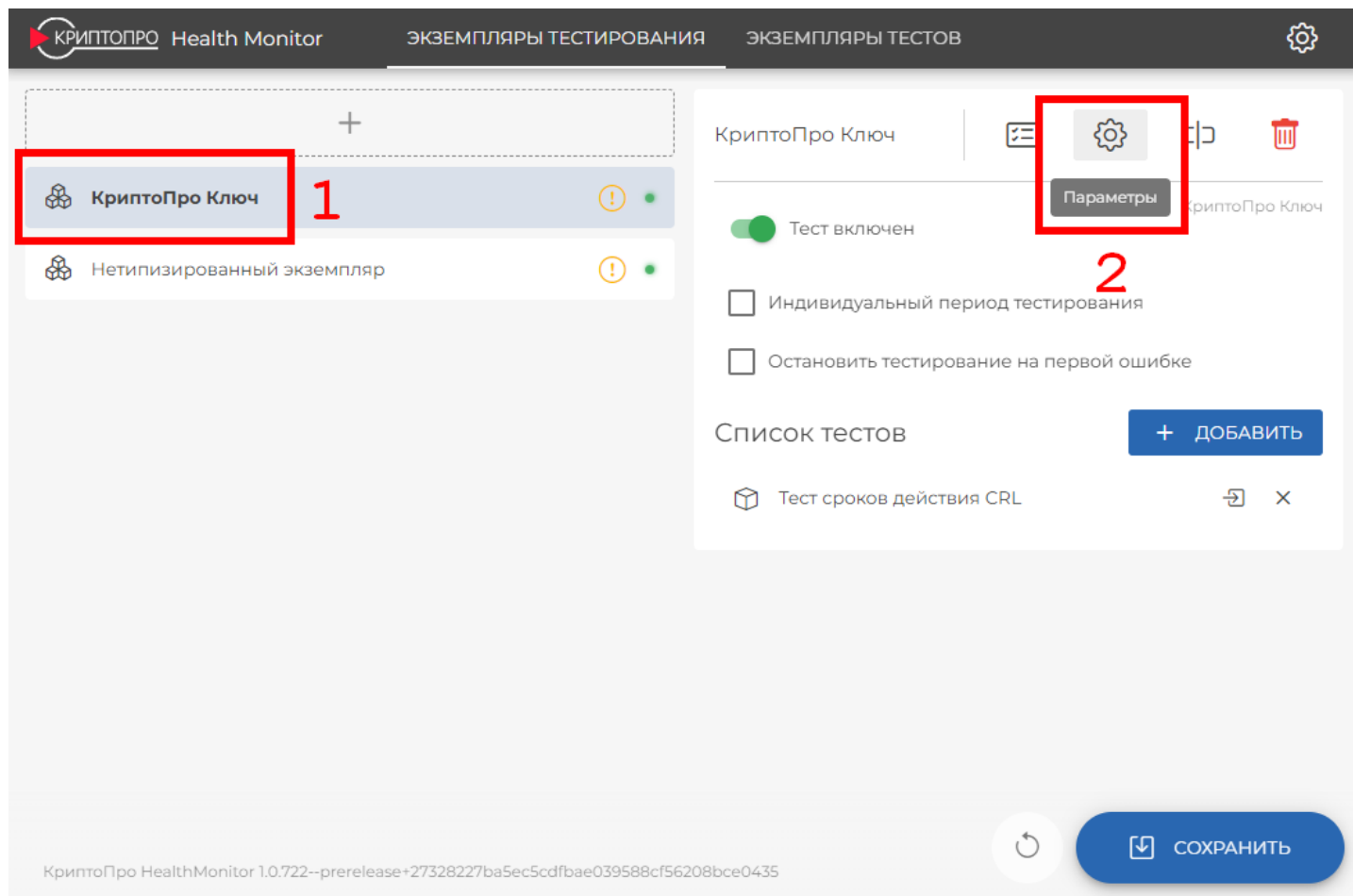
После завершения настройки экземпляра тестирования необходимо активировать переключатель "Тест включен", чтобы запустить тестирование.

Для удаления экземпляра тестирования выберите его в меню слева и в карточке данного теста (справа) выберите пиктограмму корзины. Подтвердите свой выбор.



### Параметры экземпляра тестирования КриптоПро Ключ

Для задания параметров экземпляра тестирования КриптоПро Ключ в разделе «Экземпляры тестирования» выберите созданный ранее экземпляр типа КриптоПро Ключ (1) и перейдите в Параметры (пиктограмма шестеренки, 2).



Заполните предложенные поля на вкладке «Параметры контейнера». Описание всех настраиваемых параметров экземпляра представлено в Таблице 4. После выполнения всех настроек нажмите кнопку «Применить».

КРИПТОПРО

Health Monitor

ЭКЗЕМПЛЯРЫ ТЕСТИРОВАНИЯ

ЭКЗЕМПЛЯРЫ ТЕСТОВ

КриптоПро Ключ

Нетипизирован

Параметры контейнера

Имя тестового пользователя

admin

Пароль тестового пользователя

.....

Адрес КриптоПро Ключ

http://localhost

Имя приложения сервиса подписи

SignServer

Имя приложения центра идентификации

STS

Имя приложения веб-сервиса

Frontend

Имя приложения Сервиса Аудита

AnalyticsService

Идентификатор проверяющей стороны

urn:cryptopro:dss:signserver:SignServer

Параметры подключения

ClientId

ayharuyarey

ClientSecret

.....

ОТМЕНА

ПРИМЕНИТЬ

КриптоПро Ключ

я

шибке

+ ДОБАВИТЬ

✕

КриптоПро HealthMonitor 1.0.722--prerelease+27328227ba5ec5cdfbae039588cf56208bce0435

СОХРАНИТЬ

## Примечание

После того как в параметры экземпляра тестирования вносятся изменения, на кнопке "Сохранить" появляется желтый значок, означающий, что конфигурацию необходимо сохранить.

## Примечание

После изменения параметров экземпляра необходимо сохранить изменения путем нажатия кнопки «Сохранить» и перезапустить Службу мониторинга.

**Таблица 4 — Параметры экземпляра тестирования КриптоПро Ключ**

ПАРАМЕТР	ОПИСАНИЕ
Имя тестового пользователя	Логин Пользователя на Центре Идентификации КриптоПро Ключ. <b>Внимание:</b> для данного Пользователя должна быть настроена аутентификация по логину и паролю или только идентификация.
Пароль тестового пользователя	Пароль Пользователя на Центре Идентификации КриптоПро Ключ. Если для Пользователя назначен метод входа «Только идентификация», данное поле можно оставить пустым.

ПАРАМЕТР	ОПИСАНИЕ
Адрес КристоПро Ключ	Адрес сервера, на котором расположен «КристоПро Ключ». Значение по умолчанию — <code>http://localhost</code> . <b>Внимание:</b> для тестирования все компоненты DSS должны быть развернуты на одном сервере.
Имя приложения Сервиса Подписи	Соответствует имени веб-приложения тестируемого Сервиса Подписи. Получить значение можно при помощи командлета <code>Get-SignInstance</code> (параметр <code>-ApplicationName</code> ).
Имя приложения Центра Идентификации	Соответствует имени веб-приложения тестируемого Центра Идентификации. Получить значение можно при помощи командлета <code>Get-IdsInstance</code> (параметр <code>-ApplicationName</code> ).
Имя приложения Веб-интерфейса	Соответствует имени веб-приложения тестируемого Веб-интерфейса. Получить значение можно при помощи командлета <code>Get-FeInstance</code> (параметр <code>-ApplicationName</code> ).
Имя приложения Сервиса Аудита	Соответствует имени веб-приложения тестируемого Сервиса Аудита. Получить значение можно при помощи командлета <code>Get-AuditInstance</code> (параметр <code>-ApplicationName</code> ).
Идентификатор проверяющей стороны	Идентификатор Сервиса Подписи как проверяющей стороны. Если не заполнено, будет подставлено следующее значение по умолчанию: <code>urn:cryptopro:dss:signserver:&lt;Имя приложения Сервиса Подписи (как в параметре выше)&gt;</code> . Получить значение можно при помощи командлета <code>Get-IdsRelyingPartyTrust</code> .

## Параметры подключения

В данном разделе доступны для заполнения следующие параметры:

- `ClientId`,
- `ClientSecret`.

Для заполнения параметров требуется сгенерировать в КристоПро Ключ данные для доступа по протоколу [OpenID Connect 1.0](#).

```
# Генерация секрета
Add-IdsClient -Identifier HealthMonitor -Name HealthMonitor -AllowedFlow ResourceOwner -GenerateSecret -
SecretLifetime 0

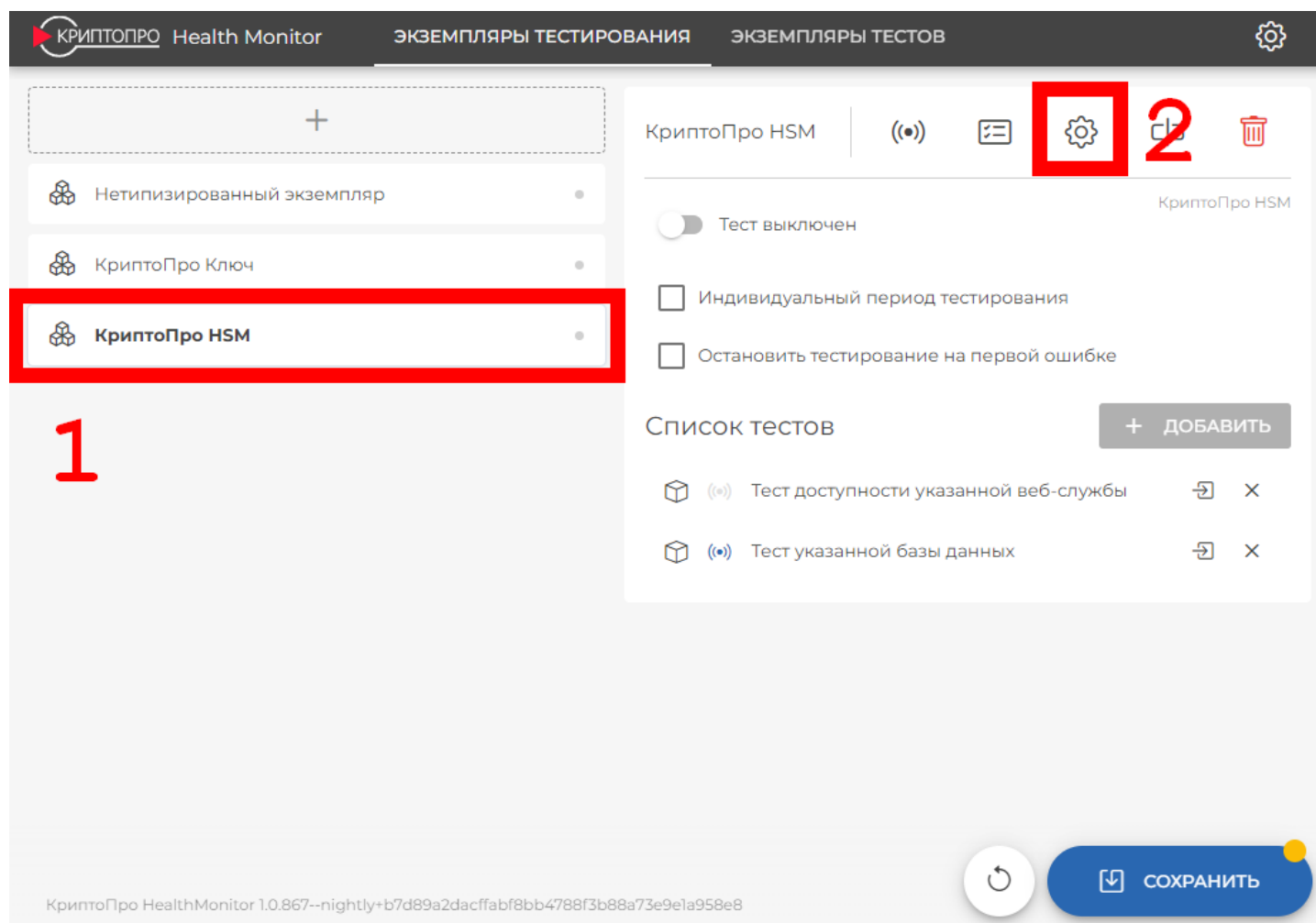
# Получение сгенерированного секрета
(Get-IdsClient -ClientId HealthMonitor).ClientSecrets
```

## Примечание

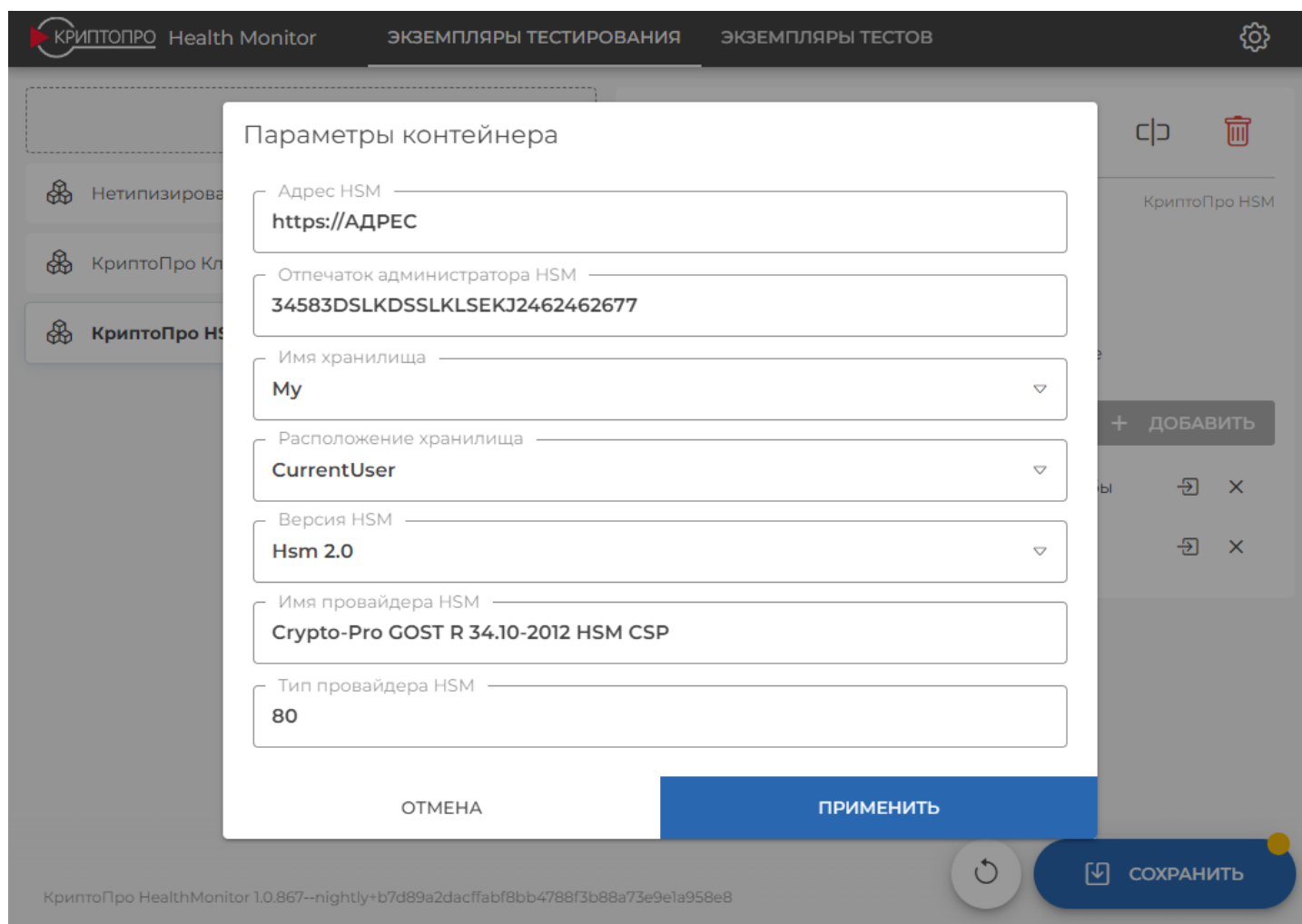
При создании секрета был использован параметр `-SecretLifetime 0`. В данном случае будет создан клиент с бессрочным секретом. Параметр позволяет указать время действия секрета. Если параметр отсутствует, срок действия секрета по умолчанию составит 1 год.

## Параметры экземпляра тестирования КристоПро HSM

Для задания параметров экземпляра тестирования КристоПро HSM в разделе «Экземпляры тестирования» выберите созданный ранее экземпляр типа КристоПро HSM (1) и перейдите в Параметры (пиктограмма шестеренки, 2).



Заполните предложенные поля на вкладке «Параметры контейнера». Описание всех настраиваемых параметров экземпляра представлено в Таблице 5. После выполнения всех настроек нажмите кнопку «Применить».



### Примечание

После того как в параметры экземпляра тестирования вносятся изменения, на кнопке "Сохранить" появляется желтый значок, означающий, что конфигурацию необходимо сохранить.

### Примечание

После изменения параметров экземпляра необходимо сохранить изменения путем нажатия кнопки «Сохранить» и перезапустить Службу мониторинга.

### Таблица 5 — Параметры экземпляра тестирования КриптоПро HSM

ПАРАМЕТР	ОПИСАНИЕ
Адрес HSM	Адрес для подключения к КриптоПро HSM
Отпечаток сертификата аудитора HSM	Отпечаток сертификата аудитора HSM
Имя хранилища	Хранилище сертификатов, куда установлен сертификат аудитора HSM на машине с Агентом Мониторинга
Расположение хранилища	Тип хранилища (текущий пользователь или локальный компьютер)
Версия HSM	1.0 или 2.0 в зависимости от используемой версии HSM

ПАРАМЕТР	ОПИСАНИЕ
Имя криптопровайдера HSM	Crypto-Pro GOST R 34.10-2012 HSM CSP - имя криптопровайдера используется по умолчанию для тестирования. Актуальная информация о доступных криптопровайдерах содержится в документе ЖТЯИ.00096-01 90 01. КриптоПро HSM. Инструкция по использованию
Тип криптопровайдера HSM	80 - тип криптопровайдера используется по умолчанию для тестирования. Актуальная информация о доступных криптопровайдерах содержится в документе ЖТЯИ.00096-01 90 01. КриптоПро HSM. Инструкция по использованию

# Настройка экземпляров тестов

Экземпляром теста в КriptoПро Центр Мониторинга называется тест, созданный из шаблона теста, и настроенный (при наличии настроек).

В этом разделе:

- [Создание тестов из шаблона](#)
- [Описание всех тестов и их параметров](#)
- [Добавление тестов к экземпляру тестирования](#)

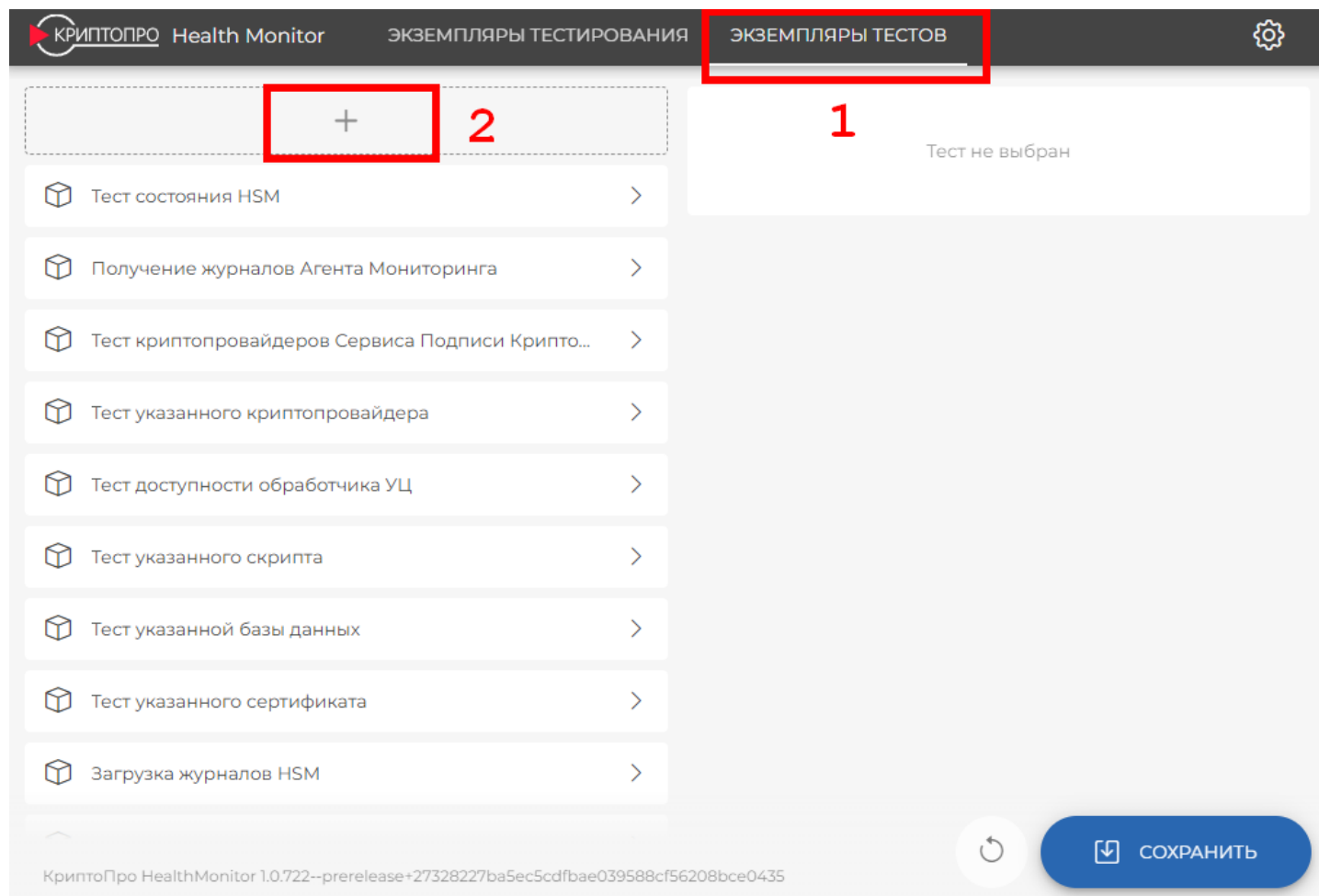
## Примечание

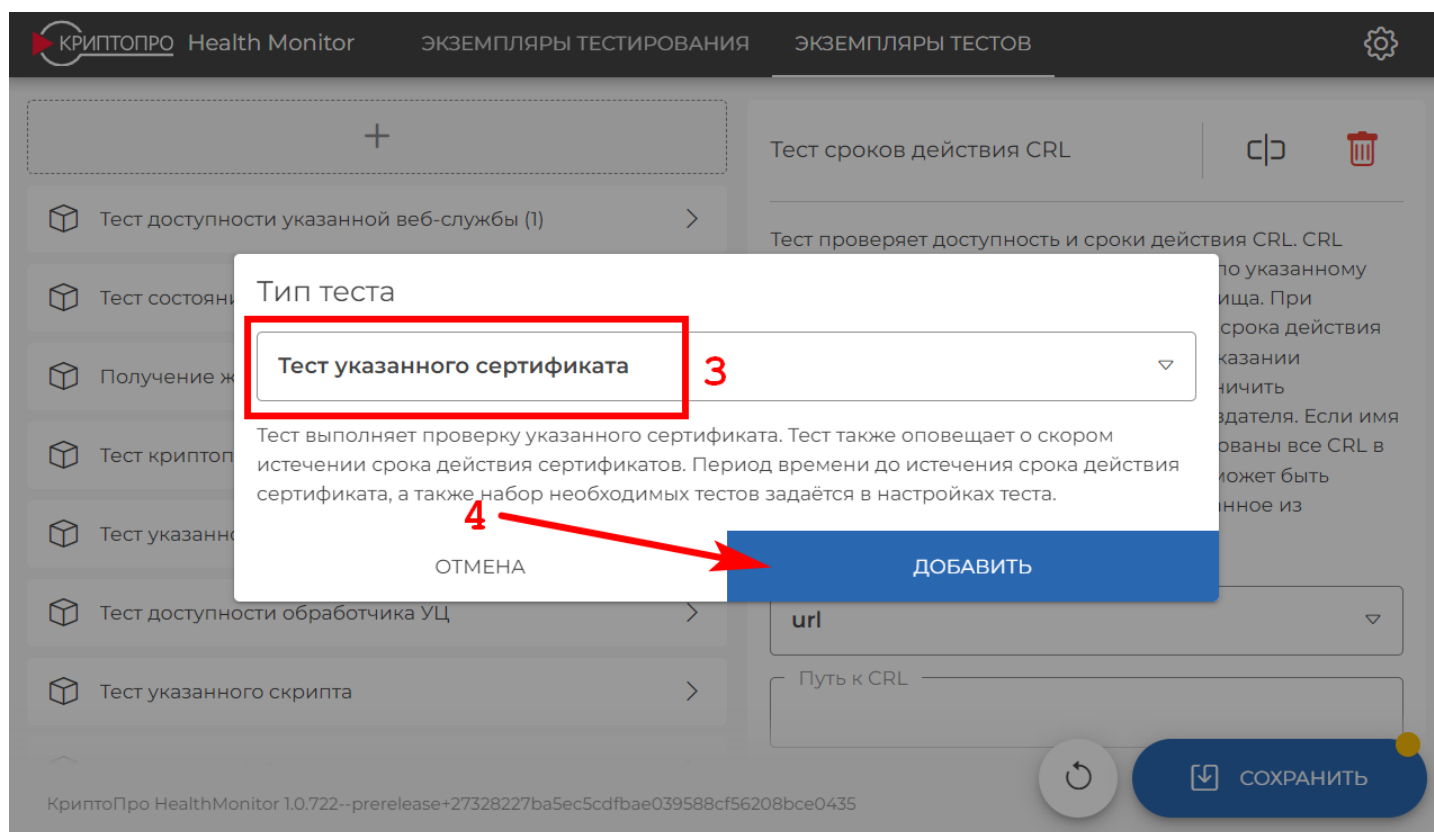
Некоторые тесты могут потребовать установки дополнительных пакетов и/или ввода дополнительной лицензии. Перед созданием теста необходимо проверить требования к нему в разделах [лицензии](#), [установки компонентов](#) и [системных требований](#) Центра Мониторинга.

## Создание экземпляра теста из шаблона тестов

Перед созданием экземпляра теста убедитесь, что [введена](#) правильная лицензия на определенный экземпляр Центра Мониторинга (Агент, Сервер).

Чтобы добавить экземпляр теста из шаблона, перейдите в раздел «Экземпляры тестов» (1) и добавьте новый тест нажатием пиктограммы "+" (2). После этого выберите из выпадающего списка (3) шаблон теста, который нужно добавить, и нажмите «Добавить» (4).





Новый тест будет отображаться в разделе «Экземпляры тестов». Имя созданного теста можно изменить, выделив его и нажав левой кнопкой на его имя, либо при помощи контекстного меню (нажатие правой кнопкой мыши – Переименовать). По умолчанию все новые создаваемые экземпляры имеют имена как в шаблоне теста. Дублирование имен тестов невозможно, поэтому при добавлении теста с именем, которое уже есть в списке, к имени нового экземпляра добавится его номер по порядку (например: Тест сроков действия CRL, Тест сроков действия CRL (1), Тест сроков действия CRL (2)...).

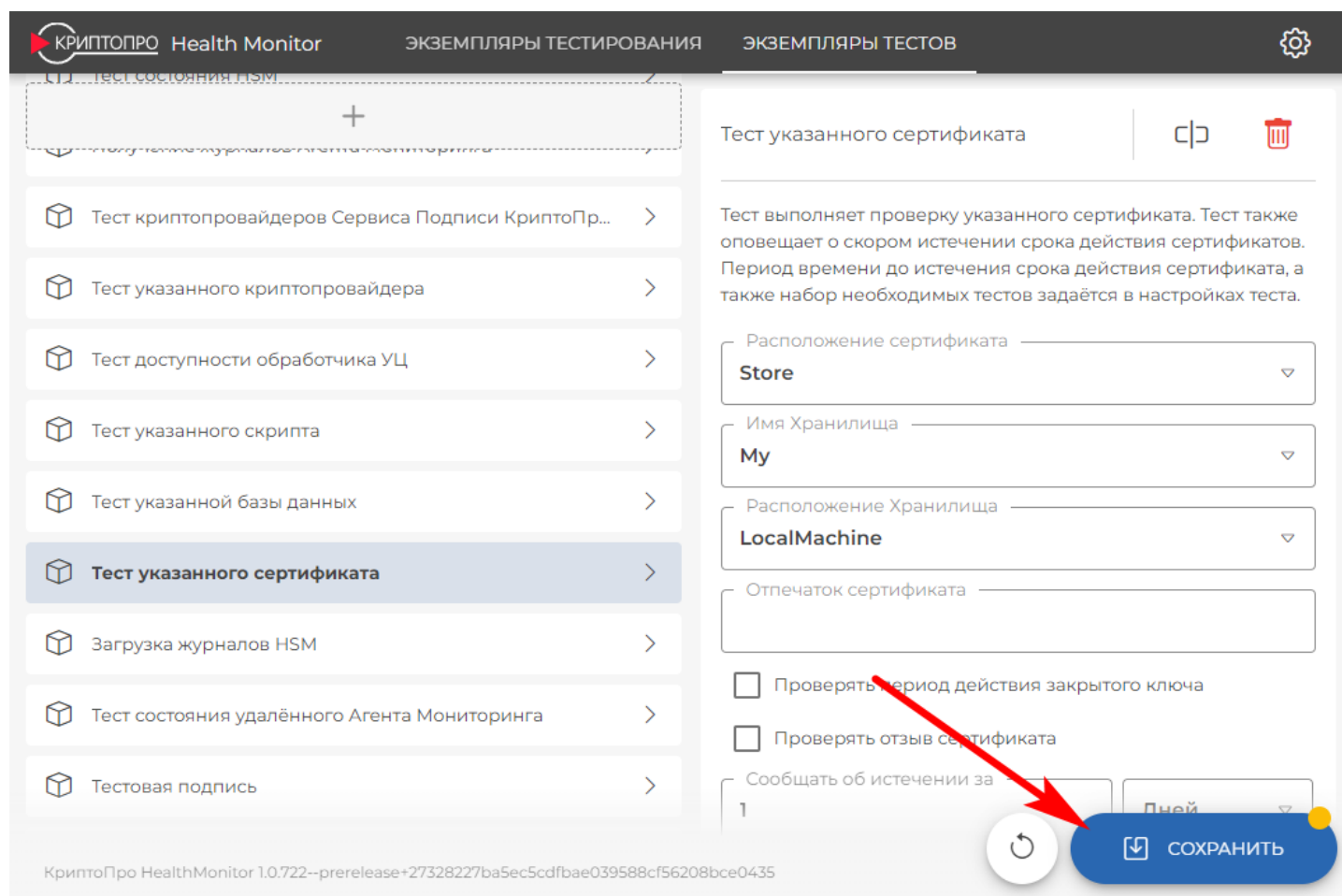
Выполните [настройку добавленных тестов](#).

### Примечание

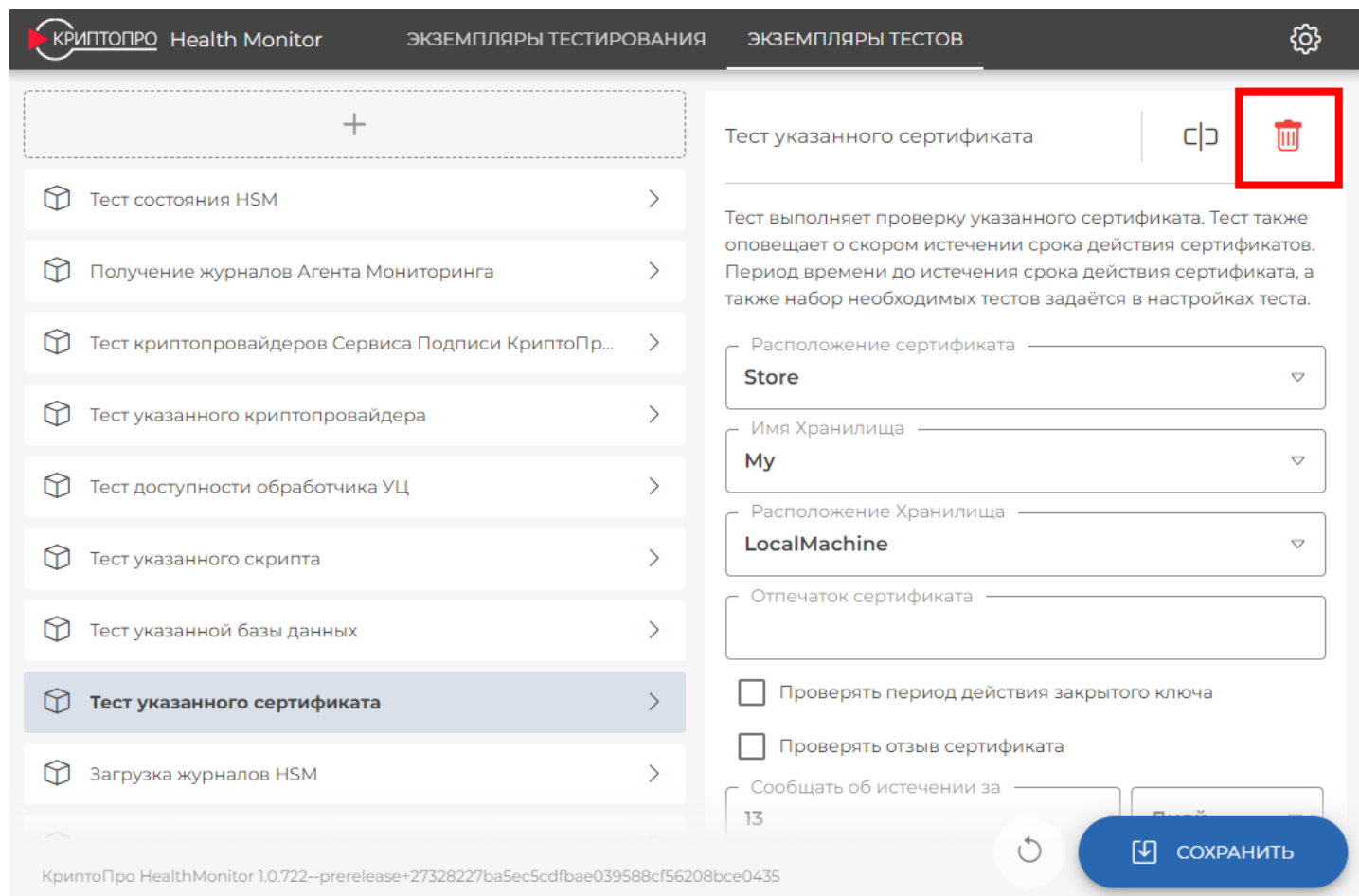
После изменения параметров необходимо сохранить изменения путем нажатия кнопки «Сохранить» и [перезапустить](#) Службу мониторинга.

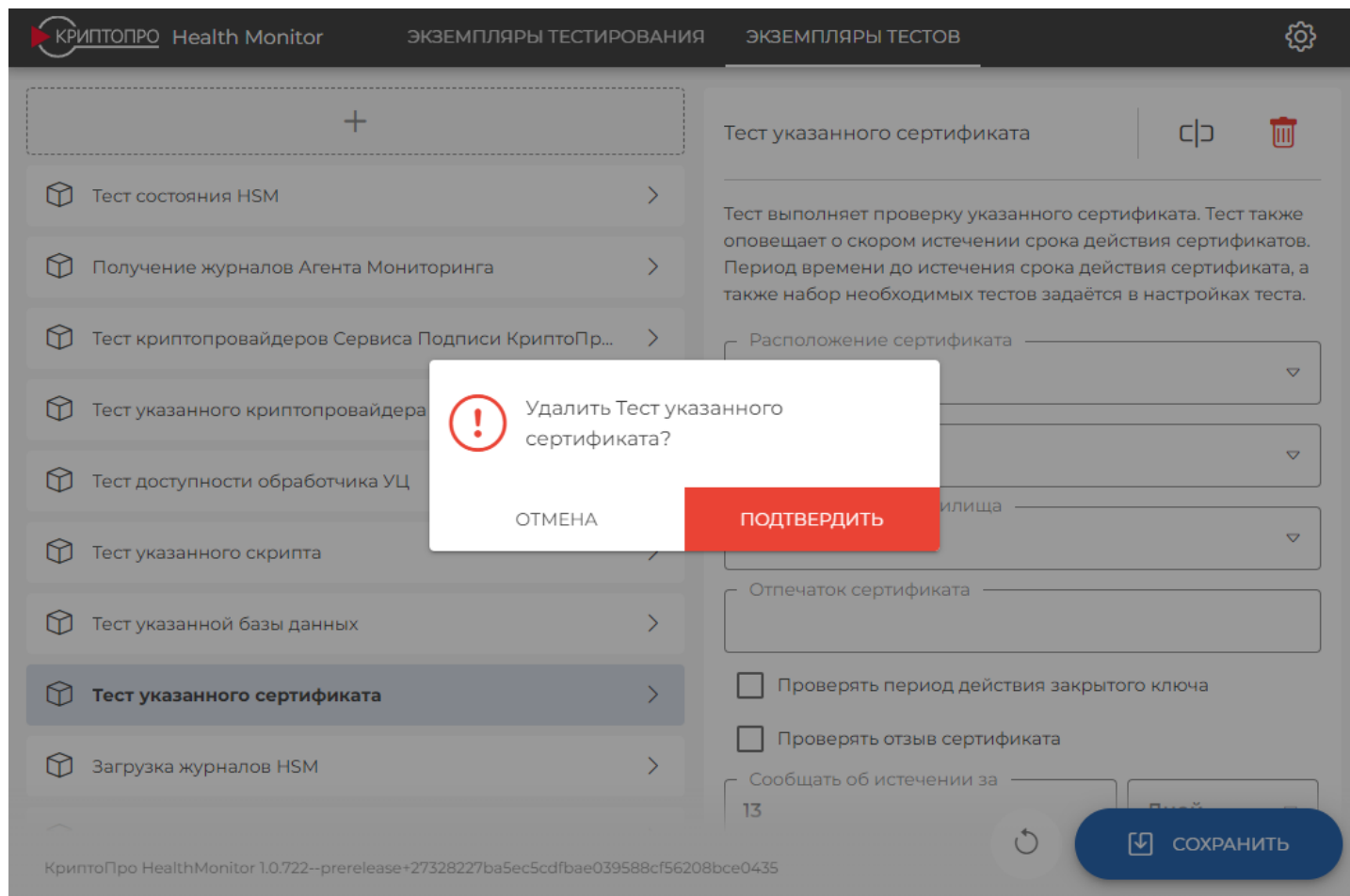
### Примечание

После того как в параметры теста вносятся изменения, на кнопке "Сохранить" появляется желтый значок, означающий, что конфигурацию необходимо сохранить.



Для удаления экземпляра теста выберите его в меню слева и в карточке данного теста (справа) выберите пиктограмму корзины. Подтвердите свой выбор.

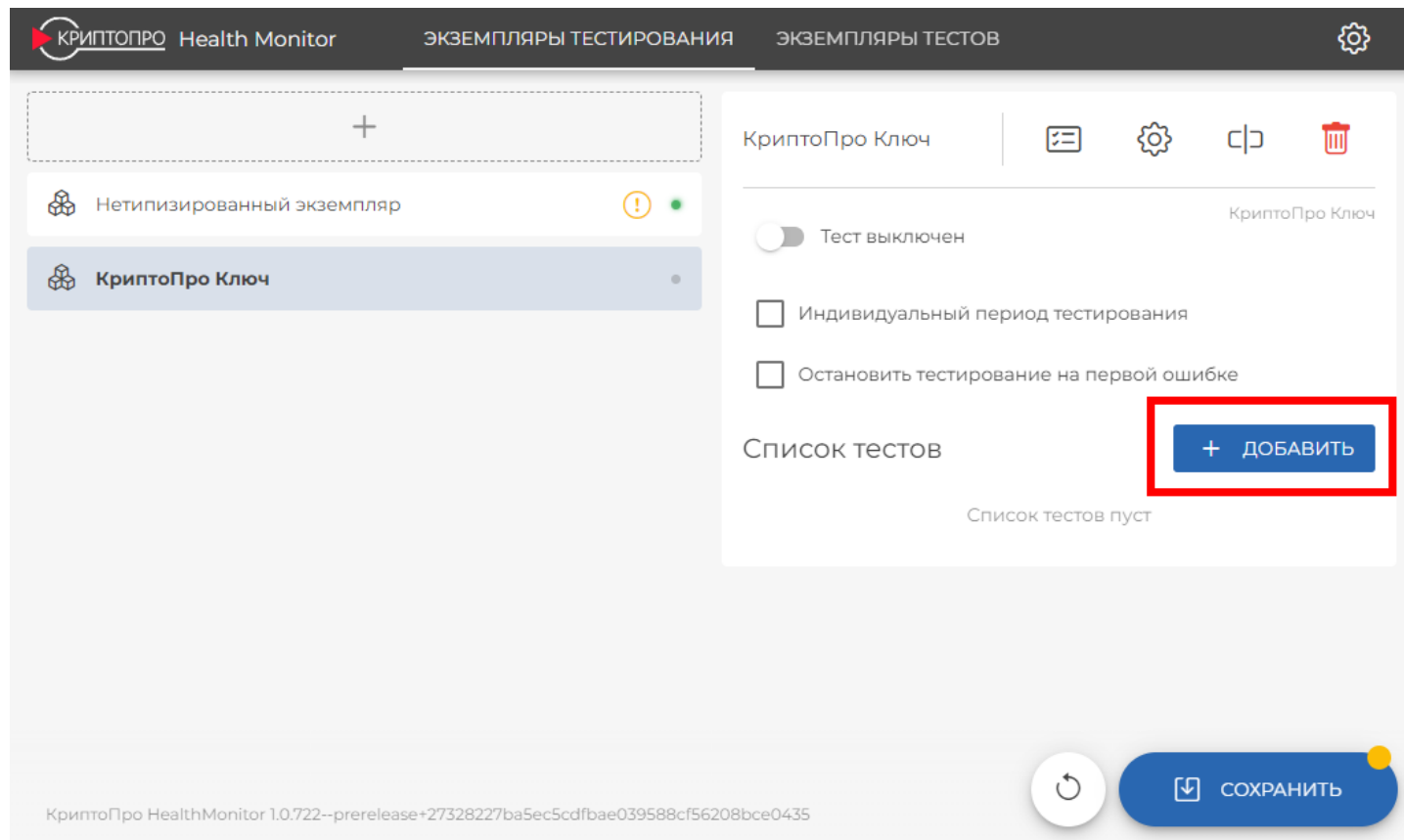




## Добавление теста к экземпляру тестирования

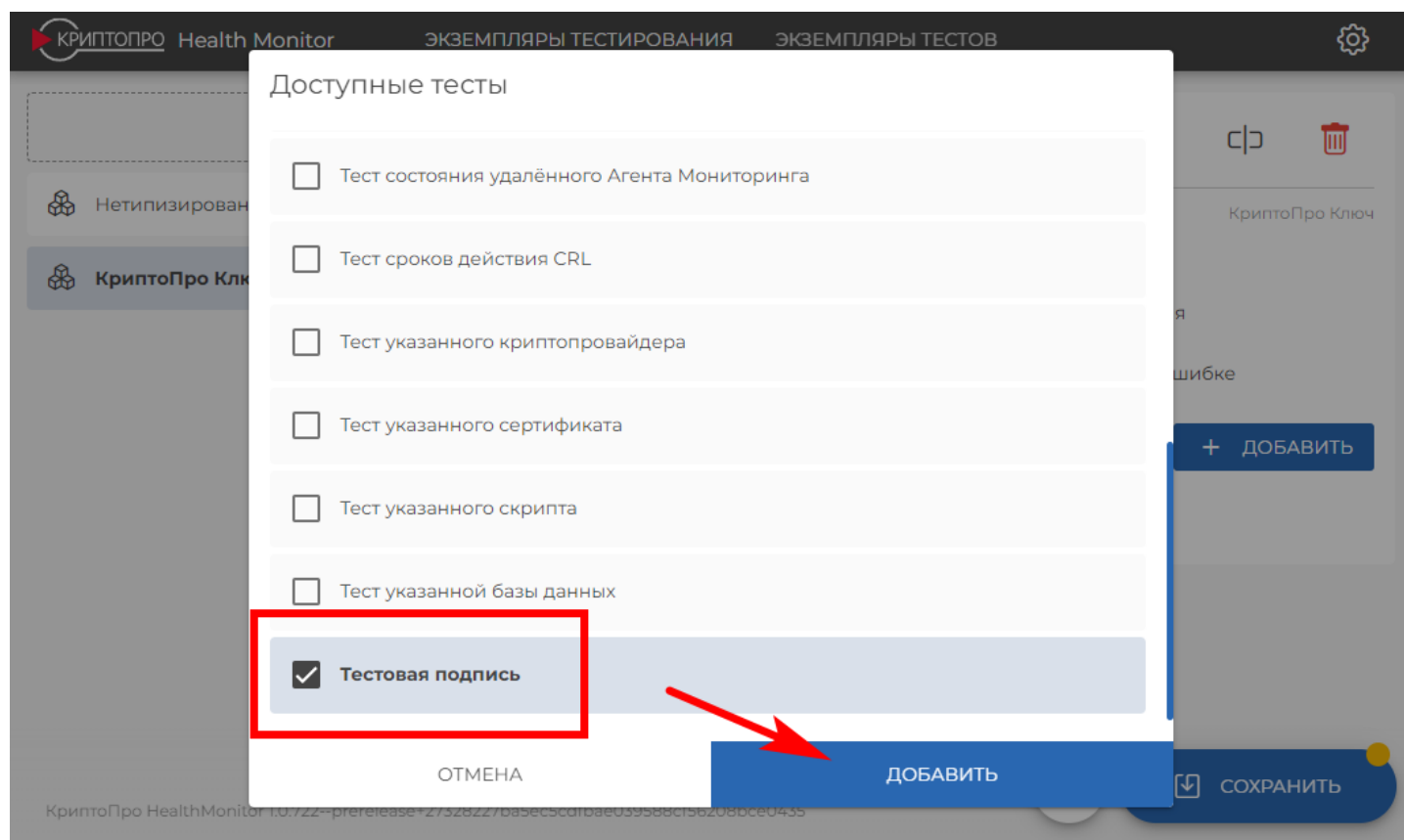
Перед созданием экземпляра теста убедитесь, что [введена](#) правильная лицензия на определенный экземпляр Центра Мониторинга (Агент, Сервер) , а также добавлены и настроены все необходимые [экземпляры тестирования](#) и [экземпляры тестов](#).

Перейдите к разделу «Экземпляры тестирования» и нажмите на экземпляр, к которому нужно добавить тесты (например, КriptoПро Ключ). В карточке экземпляра справа в разделе "Список тестов" нажмите кнопку "Добавить".



В области «Доступные тесты» отображаются добавленные и настроенные тесты, подходящие для выполнения с выбранным экземпляром тестирования. Если некоторые тесты были добавлены после обновления настроек экземпляра, они могут быть не видны. Для получения актуального списка доступных тестов нажмите на иконку обновления рядом с кнопкой "Сохранить" внизу страницы.

Для **добавления** тестов к экземпляру тестирования необходимо выделить один или несколько тестов в области «Доступные тесты» и нажать на кнопку "Добавить". Выбранные тесты переместятся в область «Список тестов».

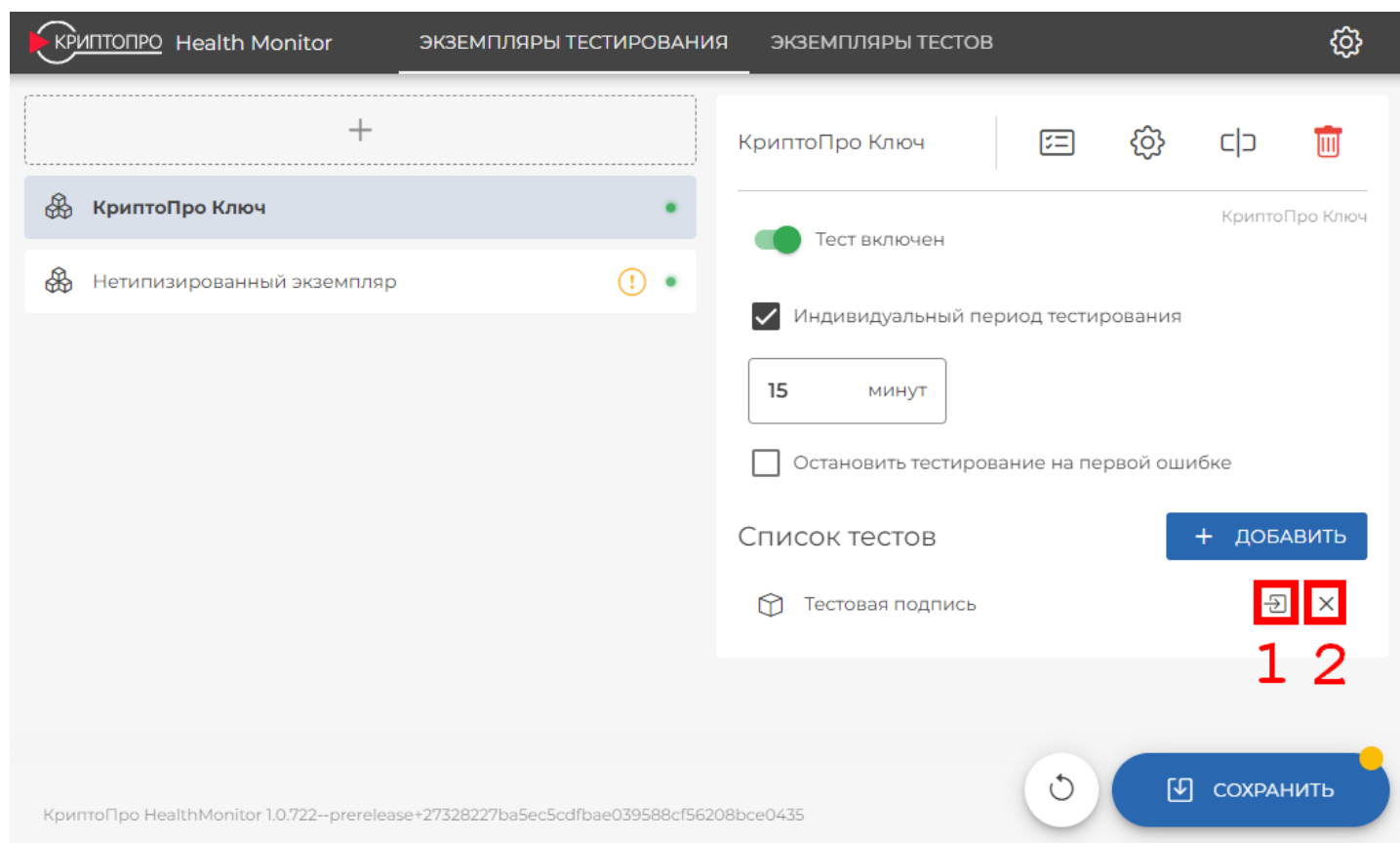


Для **перехода** к экземпляру теста с целью изменения его настроек необходимо нажать на пиктограмму (1) напротив присоединенного к экземпляру теста.

Для **удаления** экземпляра теста из связки с экземпляром тестирования необходимо нажать на пиктограмму удаления (2) напротив присоединенного к экземпляру теста.

### Примечание

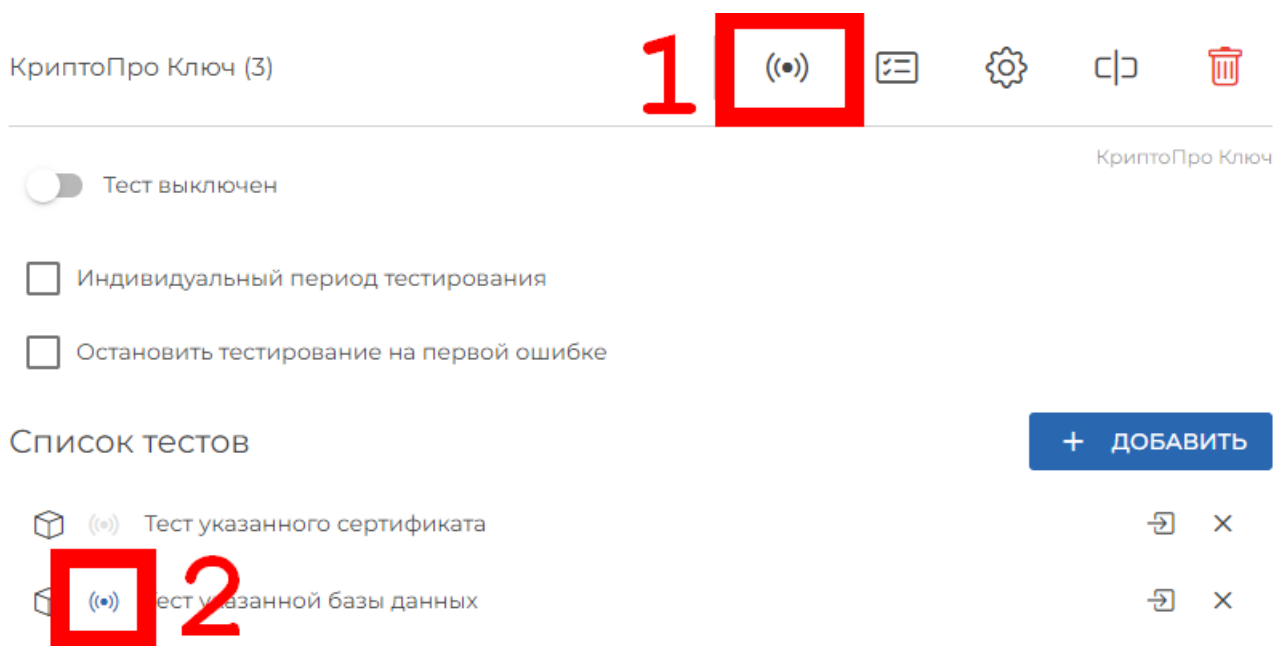
После того как в параметры экземпляра тестирования вносятся изменения, на кнопке "Сохранить" появляется желтый значок, означающий, что конфигурацию необходимо сохранить.



### Отслеживание статуса запуска тестов

После добавления теста к экземпляру тестирования в свойствах данного экземпляра появится пиктограмма отслеживания запуска тестов (1). Для каждого из тестов, для которых включено отслеживание, будет произведено дополнительное оповещение администратора в случае если данный тест был завершен с ошибкой, а позднее выполнен успешно.

Для добавленных к экземпляру тестирования тестов, запуск которых отслеживается, активирован соответствующий индикатор (2).



# Перечень тестов и их параметров

В Таблице 6 приводится описание всех доступных в КриптоПро Центр Мониторинга тестов, а также их параметров.

Таблица 6 — перечень тестов и их параметров

ТЕСТ	ОПИСАНИЕ	ПАРАМЕТРЫ
Тест указанного скрипта	Тест выполняет указанный powershell-скрипт. При указании пути необходимо указать полный путь к скрипту. Тест завершается успешно, если указанный скрипт завершился без исключения.	* Путь к файлу скрипта
Загрузка журналов HSM	При исполнении теста выполняется <a href="#">загрузка журнала аудита и журнала событий HSM</a> . Путь для сохранения журналов должен существовать. Период запуска теста, путь для сохранения журналов и параметры подключения к HSM задаются в настройках теста. Тест не проверяет журналы HSM на наличие ошибок.	* Адрес HSM * Версия HSM (HSM 1.0/ HSM 2.0) * Отпечаток сертификата аудитора HSM * Период тестирования - <div>&lt;количество&gt;</div> часов/дней/месяцев/лет
Получение журналов Агента Мониторинга	Тест проверяет наличие ошибок и предупреждений в журналах на удаленной машине с установленным агентом мониторинга. Для конфигурации теста необходимо задать адрес службы удаленного агента и журналы, события с которых необходимо получать. В случае обнаружения ошибок в удаленном журнале текст ошибки будет записан в результат теста.	* Адрес веб-службы мониторинга * Список журналов для проверки (журналы и коды исключаемых событий добавляются аналогично <a href="#">настройке мониторинга журналов</a> )
Тест доступности указанной веб-службы	Тест проверяет доступность указанной веб-службы. Проверяется только сетевая доступность службы. Тест завершается успешно, если получен ответ HTTP 200. Если требуется проверять доступность нескольких служб, то необходимо создать несколько экземпляров теста. Тест также может быть использован для получения результатов <a href="#">удаленных проверок Агентов Мониторинга</a> .	* Адрес службы
Тест криптопровайдеров Сервиса Подписи КриптоПро Ключ	Тест проверяет доступность зарегистрированных на Сервисе Подписи DSS криптопровайдеров (в том числе и HSM). Во время теста проверяется доступность только криптопровайдеров в состоянии «Включен». При тестировании группы криптопровайдеров тест завершается успешно, если хотя бы один криптопровайдер из группы доступен.	* Тестировать группы криптопровайдеров (чекбокс) * Тестировать период действия Мастер-ключа * Сообщать об истечении за <div>&lt;количество&gt;</div> часов/дней/месяцев/лет
Тест лицензий HSM	Тест проверяет сроки действия лицензий HSM. В случае истечения лицензии тест завершается с ошибкой. Для отслеживания скорого истечения лицензии можно настроить предупреждение через параметры теста.	* Сообщать об истечении срока действия за <div>&lt;количество&gt;</div> часов/дней/месяцев/лет
Тест состояния HSM	Тест получает текущее состояние HSM и проверяет наличие свободного места на жёстком диске HSM и количество оставшегося ключевого материала (гаммы). Если количество гаммы или оставшееся свободное место на диске меньше заданного значения - тест завершается с ошибкой.	* Адрес HSM * Отпечаток сертификата аудитора HSM * Предупреждать об истечении гаммы за (ключей) * Предупреждать о заканчивающемся месте за (Мбайт)

ТЕСТ	ОПИСАНИЕ	ПАРАМЕТРЫ
Тест состояния удаленного Агента Мониторинга	Тест запрашивает у указанного агента мониторинга результат последнего запуска тестов. Тест завершается успешно, если последний запуск всех тестов агента завершился успешно. Если необходимо тестировать несколько экземпляров тестирования или агентов - необходимо создать несколько экземпляров теста.	<ul style="list-style-type: none"> <li>* Адрес веб-службы агента мониторинга</li> <li>* Имя экземпляра тестирования (на агенте мониторинга)</li> </ul>
Тест сроков действия CRL	Тест проверяет доступность и сроки действия CRL. CRL могут быть загружены из указанной папки по указанному сетевому адресу или из указанного хранилища. При выполнении теста производится проверка срока действия полученных CRL на текущий момент. При указании хранилища как источника CRL можно ограничить тестирование только для CRL указанного издателя. Если имя издателя не было указано, будут протестированы все CRL в хранилище.	<ul style="list-style-type: none"> <li>* Тип источника CRL (URL / Папка / Хранилище сертификатов)</li> <li>* Путь к CRL</li> <li>* Имя издателя</li> <li>* Проверять дату следующей публикации (чекбокс)</li> </ul>
Тест указанного криптопровайдера	Тест проверяет доступность указанного криптопровайдера (в том числе HSM). При отсутствии имени криптопровайдера будет использован криптопровайдер указанного типа по умолчанию. Во время теста доступность проверяется путём создания контекста криптопровайдера и получения его параметров.	<ul style="list-style-type: none"> <li>* Имя криптопровайдера (текстовое)</li> <li>* Тип криптопровайдера (число)</li> </ul>
Тест указанного сертификата	Тест выполняет проверку указанного сертификата. Тест также оповещает о скором истечении срока действия сертификатов. Период времени до истечения срока действия сертификата, а также набор необходимых тестов задаётся в настройках теста.	<ul style="list-style-type: none"> <li>* Имя хранилища сертификатов (Подгружается автоматически)</li> <li>* Расположение хранилища сертификатов (Current User / Local Machine)</li> <li>* Отпечаток сертификата (подгружается автоматически в зависимости от выбранного хранилища)</li> <li>* Проверять период действия закрытого ключа (чекбокс)</li> <li>* Проверять аннулирование сертификата (чекбокс)</li> <li>* Сообщать об истечении за &lt;количество&gt; часов/дней/месяцев/лет</li> </ul>
Тест указанной базы данных	Тест проверяет доступность базы данных. Строка подключения к SQL-серверу указывается в параметрах теста. Если используется Windows-аутентификация, то подключение к SQL-серверу будет осуществляться с учётными данными службы HealthMonitor. Если используется SQL-аутентификация, то подключение к SQL-серверу будет осуществляться с учётными данными, указанными в строке подключения.	<ul style="list-style-type: none"> <li>* Строка подключения к БД</li> </ul>

ТЕСТ	ОПИСАНИЕ	ПАРАМЕТРЫ
Тестовая подпись	<p>Тест создания подписи. Тест проверяет корректность выполнения операций в DSS по созданию электронных подписей следующих форматов:</p> <ol style="list-style-type: none"> <li>1. Усовершенствованная подпись (CMS Advanced Electronic Signatures, CAdES);</li> <li>2. XML Digital Signature (XMLDSig);</li> <li>3. Электронная подпись ГОСТ 34.10–2001, ГОСТ 34.10–2012;</li> <li>4. Подпись документов формата PDF;</li> <li>5. Подпись документов Microsoft Office;</li> </ol> <p>Для выполнения теста необходимо настроить подключение к Сервису Подписи и Центру Идентификации; задать учётные данные (логин/пароль) пользователя от имени, которого будет создана тестовая подпись (в параметрах экземпляра тестирования DSS). Тест использует учётные данные пользователя ЦИ, для которого настроена аутентификация по логин/паролю или только идентификация. Если идентификатор сертификата не указан, будет использоваться сертификат по умолчанию. Если требуется проверить несколько форматов подписи, то необходимо создать соответствующее количество экземпляров данного теста.</p>	<p>* Тип подписи (XMLDSig/ ГОСТ3410/ CAdES/ PDF/ MSOffice/ CMS)</p> <p>* Параметры подписи</p> <p><b>Для XMLDSig:</b></p> <ul style="list-style-type: none"> <li>- Enveloped</li> <li>- Enveloping</li> </ul> <p>-</p> <p>подпись по шаблону ГОСТ 34.10 2001 и ГОСТ 34.11–94</p> <p>-</p> <p>подпись по шаблону ГОСТ 34.10 2012 с длиной хэш-кода 256 бит</p> <p>-</p> <p>подпись по шаблону ГОСТ 34.10 2012 с длиной хэш-кода 512 бит</p> <p>-</p> <p><b>Для CAdES:</b></p> <ul style="list-style-type: none"> <li>- CAdES-BES</li> <li>- CAdES-T</li> <li>- CAdES-X Long Type 1</li> </ul> <p><b>Для PDF:</b></p> <ul style="list-style-type: none"> <li>- CMS</li> <li>- CAdES-T</li> <li>- CAdES-X Long Type 1</li> </ul> <p>* Адрес TSP-службы (только для CAdES-T и CAdES XLT1)</p> <p>* Идентификатор сертификата</p>
Тест доступности обработчика УЦ	<p>Тест проверяет доступность обработчика Удостоверяющего Центра. Идентификатор обработчика УЦ можно получить при помощи командлета Get-DssEnrollment. Если требуется проверить доступность нескольких Удостоверяющих Центров, необходимо добавить соответствующее количество экземпляров данного теста. Тест осуществляет подключение к Сервису Подписи DSS с учётными данными Пользователя DSS, чтобы проверить наличие обработчика УЦ в настройках экземпляра Сервиса Подписи DSS.</p> <p><b>Внимание:</b> У Пользователя DSS должен быть хотя бы один действительный сертификат и настроена аутентификация в DSS по логину/паролю или только идентификация.</p>	<p>* ID обработчика УЦ (в БД Сервиса Подписи DSS)</p>
Тест повторного усовершенствования подписи КриптоПро Архив	<p>Тест повторно усовершенствует подписи в контейнере. Идентификатор контейнера необходимо задать через параметры теста. Тест завершается успешно, если все подписи в контейнере усовершенствованы менее чем за 30 секунд.</p>	<p>* Адрес службы admin-api</p> <p>* Путь к сертификату в формате PFX</p> <p>* Пароль от сертификата</p> <p>* Идентификатор контейнера КриптоПро Архив</p>
Тест статуса контейнера КриптоПро Архив	<p>Тест проверяет статус контейнера. Идентификатор контейнера необходимо задать через параметры теста. Тест завершается успешно, если контейнер имеет статус "Архивное хранение".</p>	<p>* Адрес службы admin-api</p> <p>* Путь к сертификату в формате PFX</p> <p>* Пароль от сертификата</p> <p>* Идентификатор контейнера КриптоПро Архив</p>

ТЕСТ	ОПИСАНИЕ	ПАРАМЕТРЫ
Тест состояния Elasticsearch	Тест проверяет состояние кластера Elasticsearch. Тест завершается успешно, если кластер находится в состоянии <code>Green</code> .	<ul style="list-style-type: none"> <li>* Адрес службы Elasticsearch. Значение по умолчанию: <code>"http://localhost:9200"</code></li> <li>.</li> </ul>
Тест состояния ManticoreSearch	Тест проверяет состояние службы ManticoreSearch.	<ul style="list-style-type: none"> <li>* Адрес службы ManticoreSearch. Значение по умолчанию: <code>"http://127.0.0.1:9308"</code></li> <li>.</li> </ul>
Тест состояния RabbitMQ	Тест проверяет доступность службы RabbitMQ. В параметре <code>HostName</code> должно быть указано только доменное имя или IP-адрес службы RabbitMQ без указания протокола и порта.	<ul style="list-style-type: none"> <li>* Адрес службы RabbitMQ. Значение по умолчанию: <code>"localhost"</code></li> <li>* Имя пользователя RabbitMQ. Значение по умолчанию: <code>"cryptopro_app"</code></li> <li>* Пароль пользователя RabbitMQ. Значение по умолчанию: <code>"cryptopro"</code></li> <li>* Виртуальный хост RabbitMQ. Значение по умолчанию: <code>"archive"</code></li> <li>* Порт службы RabbitMQ. Значение по умолчанию: <code>"5672"</code></li> </ul>
Тест состояния очереди nats-streaming-server	Тест проверяет состояние очереди nats-streaming-service. В случае если размер указанной очереди для указанного клиента превышает пороговое значение - тест завершается с ошибкой.	<ul style="list-style-type: none"> <li>* Адрес службы. Значение по умолчанию: <code>"http://localhost:8222"</code></li> <li>* Имя очереди (канала)</li> <li>* Имя клиента (обработчика очереди)</li> <li>* Пороговое значение размера очереди. Значение по умолчанию: <code>"10"</code></li> <li>* Число итераций для усреднения. Значение по умолчанию: <code>"2"</code></li> <li>* Период опроса счётчика, секунд. Значение по умолчанию: <code>"30"</code></li> </ul>
Тест OCSP-службы	Тест проверяет доступность OCSP-службы. При тестировании происходит создание запроса на получение статуса сертификата и проверка соответствующего ответа. Если адрес OCSP-службы не указан, то используется следующий алгоритм: производятся попытки получить статус сертификата у OCSP-служб, адреса которых указаны в расширении AIA-сертификата (если есть). Если по какой-либо причине это сделать не удалось, используется адрес по умолчанию из групповой политики (если она существует). Если одна из служб вернула ответ, который прошёл проверки, то дальнейшие послышки запросов прекращаются. Если требуется проверять доступность нескольких OCSP-служб, то необходимо создать несколько экземпляров данного теста.	<ul style="list-style-type: none"> <li>* Имя хранилища сертификатов (Подгружается автоматически)</li> <li>* Расположение хранилища сертификатов (<code>Current User / Local Machine</code>)</li> <li>* Отпечаток сертификата (подгружается автоматически в зависимости от выбранного хранилища)</li> <li>* Адрес OCSP-службы</li> </ul>

ТЕСТ	ОПИСАНИЕ	ПАРАМЕТРЫ
Тест TSP-службы	Тест проверяет доступность службы штампов времени (TSP-службы). При тестировании происходит создание запроса на получение штампа времени и проверка полученного штампа. Если требуется проверять доступность нескольких TSP-служб, то необходимо создать несколько экземпляров данного теста.	<ul style="list-style-type: none"> <li>* Адрес TSP-службы</li> <li>* Алгоритм хэширования (ГОСТ 34.11-2001, ГОСТ 34.11-2012 256 бит, ГОСТ 34.11-2012 512 бит, SHA-1, SHA-2, SHA-3 256 бит, SHA-3 512 бит)</li> </ul>
Тест синхронизации времени служб TSP и OCSP	Тест проверяет синхронизацию времени служб TSP и OCSP путём сравнения времени в ответах служб. При тестировании происходит создание запроса на получение статуса сертификата и проверка соответствующего ответа. Если адрес OCSP-службы не указан, то используется следующий алгоритм: производятся попытки получить статус сертификата у OCSP-служб, адреса которых указаны в расширении AIA-сертификата (если есть). Если по какой-либо причине это сделать не удалось, используется адрес по умолчанию из групповой политики (если она существует). Если одна из служб вернула ответ, который прошёл проверки, то дальнейшие послышки запросов прекращаются. Далее происходит создание запроса на получение штампа времени и проверка полученного штампа. Затем происходит сравнение полей времени в ответах обеих служб. Если разница между временами больше указанной допустимой точности - тест завершается с ошибкой.	<ul style="list-style-type: none"> <li>* Имя Хранилища</li> <li>* Расположение Хранилища</li> <li>* Отпечаток сертификата</li> <li>* Адрес OCSP-службы</li> <li>* Адрес TSP-службы</li> <li>* Алгоритм хэширования</li> <li>* Допустимая точность (в секундах)</li> </ul>

## Общие настройки

Раздел позволяет настроить общие параметры тестирования, оповещение и лицензии Центра Мониторинга. Данные настройки представлены следующими вкладками:

- [Основные настройки](#);
- [Настройка почтовой рассылки](#);
- [Настройка мониторинга журналов](#);
- [Лицензия](#);
- [Веб-служба](#).

# Основные настройки

Для ввода основных настроек КриптоПро Центр Мониторинга в разделе «Общие настройки» (пиктограмма шестеренки) перейдите на вкладку «Основное» .

Для настройки доступны следующие параметры:

- **Период тестирования по умолчанию** — интервал времени в минутах, через который будут запускаться настроенные тесты и рассылаться почтовые сообщения.

КРИПТОПРО

Health Monitor

ЭКЗЕМПЛЯРЫ ТЕСТИРОВАНИЯ

ЭКЗЕМПЛЯРЫ ТЕСТОВ

Основное

Почтовая рассылка

Мониторинг журналов

Лицензии

Конфигурация службы

Период тестирования по умолчанию

5

минут

Режим мониторинга

Default

КриптоПро HealthMonitor 1.0.867--nightly+b7d89a2dacffabf8bb4788f3b88a73e9e1a958e8

СОХРАНИТЬ

# Настройка почтовой рассылки

Для настройки почтовой рассылки в разделе «Общие настройки» перейдите на вкладку «Почтовая рассылка» (1).

Чтобы настройка почтовой рассылки стала доступной, активируйте переключатель **«Отправка отчётов включена»** (2).

Описание параметров почтовой рассылки представлено в Таблице 7.

Таблица 7 — Параметры почтовой рассылки

ПАРАМЕТР	ОПИСАНИЕ
Использовать SSL (чекбокс)	Установка данного чекбокса означает использование протокола SSL при отправке сообщений.
Период рассылки предупреждений	Период, раз в который происходит рассылка почтовых сообщений о событиях типа <code>w</code> ( <a href="#">Предупреждение</a> ). <b>Внимание:</b> раз в заданный период рассылаются только предупреждения, полученные Службой в течение последнего перед отсылкой периода тестирования.
Заголовок письма	Текст, указанный в данном поле, будет отображаться в теме письма с оповещением.
Адрес отправителя	В данном поле необходимо указать адрес отправителя писем с оповещением.
Адрес SMTP-сервера	Адрес почтового сервера, с которого отправляются письма.
Порт SMTP-сервера	Порт почтового сервера, с которого отправляются письма.
Тип аутентификации	Тип аутентификации на указанном почтовом сервере ( <code>Windows-аутентификация</code> / <code>Имя пользователя и пароль</code> / <code>Без аутентификации</code> ).
Имя пользователя (отправителя)	Логин пользователя (отправителя) для подключения к почтовому серверу.
Пароль (отправителя)	Пароль пользователя (отправителя) для подключения к почтовому серверу.
Период рассылки уведомлений об активности	Период рассылки уведомлений о работоспособности ("HeartBeat") Службы мониторинга. Если Служба активна и рассылка включена, уведомления будут рассылаться с указанным интервалом (в минутах).

**Примечание**

После внесения изменений необходимо сохранить изменения (3), и перезапустить Службу мониторинга.



Основное

**Почтовая рассылка** 1

Мониторинг журналов

Лицензии

Конфигурация службы

☒ Отправка отчётов включена 2☐ Использовать SSL

Период рассылки предупреждений

1

Дней

Заголовок письма

Адрес отправителя

Адрес smtp сервера

Порт smtp сервера

25

Имя пользователя отправителя

Пароль отправителя

Период рассылки уведомлений об активности

600

минут

3

КриптоПро HealthMonitor 1.0.871.4609+099ef84c97ae8ab4cle20704f11b9ac1697d9aea



СОХРАНИТЬ

# Настройка мониторинга журналов

Настройка мониторинга журналов является поднастройкой почтовой рассылки и требует включения [почтовой рассылки](#) на вкладке «Почтовая рассылка» (активируйте переключатель «**Отправка отчётов включена**»).

На данной вкладке указываются журналы, из которых КриптоПро Центр Мониторинга считывает события после прохождения тестов и оповещает администратора о [событиях](#) типов ☐ **e** и ☐ **w** посредством email-сообщений, настроенных на вкладке «Почтовая рассылка».

## Внимание!

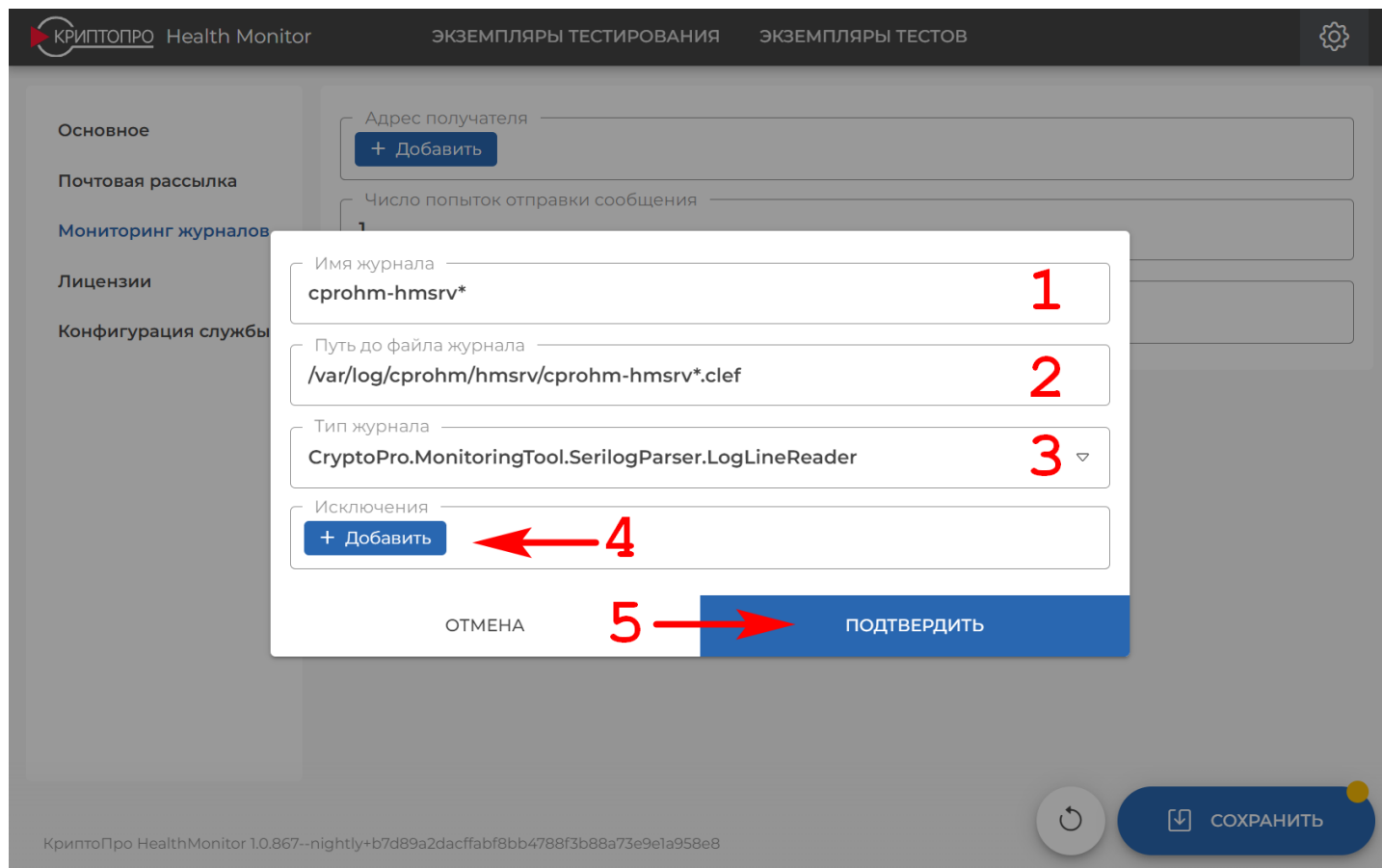
В Центре Мониторинга поддерживаются журналы со строго определенным [форматом](#).

Для того чтобы добавить новый журнал, добавьте получателей в разделе "Адрес получателя" (1), нажав кнопку «Добавить» в данном разделе, заполните поле «Число попыток отправки сообщения» (2) и нажмите кнопку «Добавить» в разделе «Журналы для мониторинга» (3).

При добавлении журнала мониторинга укажите Имя журнала (1), полный Путь к файлу журнала (2), Тип журнала (`CryptoPro.MonitoringTool.SerilogParser.LogReader` если было выбрано журналирование по умолчанию, `CryptoPro.MonitoringTool.SerilogParser.LogLineReader` если было включено структурированное журналирование) (3), исключения (коды событий, о которых **НЕ НУЖНО** оповещать, разделенные ";") (4) и нажмите кнопку «Подтвердить» (5).

Собственные журналы Центра Мониторинга по умолчанию расположены в следующих директориях:

- `/var/log/cprohm/hmsrv/cprohm-hmsrv*.log` (`/var/log/cprohm/hmsrv/cprohm-hmsrv*.clef`) - Служба Мониторинга;
- `/var/log/cprohm/hmfe/cprohm-hmfe*.log` (`/var/log/cprohm/hmfe/cprohm-hmfe*.clef`) - Служба Веб-интерфейса.



Чтобы удалить адрес получателя или журнал мониторинга из списка, нажмите на пиктограмму крестика рядом с ним.

### Примечание

После изменения настроек мониторинга журналов необходимо сохранить изменения путем нажатия кнопки «Сохранить» и перезапустить Службу мониторинга.

# Веб-служба

Веб-служба мониторинга предназначена для обмена данными о тестировании между Сервером Мониторинга и Агентами Мониторинга. Настроить Веб-службу возможно на любом экземпляре КриптоПро Центр Мониторинга, однако основной вариант использования подразумевает ее работу на Агентах, которые с ее помощью смогут отправлять информацию о тестах на Сервер Мониторинга. Сервер Мониторинга получает сведения от Веб-службы при помощи [Теста состояния удаленного Агента Мониторинга](#).

Взаимодействие с Веб-службой осуществляется путем отправки к ней GET-запроса вида:

**GET <Адрес службы>/<Имя экземпляра тестирования>/GetLastTestStatus**

**Пример запроса:**

<http://win-srv:8080/monitor/cprokey/GetLastTestStatus>

Возможны два варианта ответа веб-службы:

- HTTP 200 (успех);
- HTTP 500 (ошибка).

Веб-служба вернет HTTP 200, если в предыдущем запуске тестов на Агенте, к которому делается запрос, для указанного экземпляра тестирования не произошло ошибок.

Веб-служба вернет HTTP 500, если в предыдущем запуске тестов на Агенте, к которому делается запрос, были ошибки. В данный ответ помещаются сведения о результатах последнего запуска тестирования в формате JSON (см. Таблица 8).

**Таблица 8 — Ответ Веб-службы**

ПОЛЕ	ТИП	ОПИСАНИЕ
DetailedInformation	List<string>	Список результатов последнего запуска тестов
ErrorMessage	String	Краткое описание ошибки. Допустимые значения: * Тестирование экземпляра [Имя экземпляра] еще не проводилось; * Один или несколько тестов завершились с ошибкой.
Time	String	Время форматирования данного сообщения в UTC.

**Пример ответа:**

```
{ "DetailedInformation":  
  [ "cprokey -> Тестовая аутентификация -> успешно завершён",  
    "cprokey -> Тестовая подпись -> успешно завершён",  
    "cprokey -> Тест криптопровайдеров Сервиса Подписи КриптоПро Ключ -> успешно завершён",  
    "cprokey -> Проверка сертификатов веб интерфейса КриптоПро Ключ -> успешно завершён",  
    "cprokey -> Проверка сертификатов сервиса ЦИ КриптоПро Ключ -> завершён с ошибкой",  
    "cprokey -> Проверка сертификатов сервиса подписи КриптоПро Ключ -> успешно завершён"],  
  "ErrorMessage": "КриптоПро Ключ: Один или несколько тестов завершились с ошибкой.",  
  "Time": "2019-01-29T10:18:04Z" }
```

Сервер Мониторинга также может получать результаты тестирования от Агента Мониторинга при помощи Веб-службы. Для этого используется [Тест состояния удаленного Агента Мониторинга](#). Укажите следующие настройки данного теста:

- **Адрес веб-службы Агента Мониторинга** — Адрес службы из настроек Веб-службы на Агенте (Например, `http://win-srv:8080/monitor`)
- **Имя экземпляра тестирования** — Имя тестируемого экземпляра на Агенте (Например, `cprokey`).
- Сохраните настройки теста при помощи кнопки «Сохранить».

Тест запрашивает у указанного агента мониторинга результат последнего запуска тестов. Тест завершается успешно, если последний запуск всех тестов агента завершился успешно. Если необходимо тестировать несколько экземпляров тестирования или агентов - необходимо создать несколько экземпляров теста.

Адрес веб-службы агента мониторинга

**http://monitoring.agent:53000/monitor**

Имя экземпляра тестирования